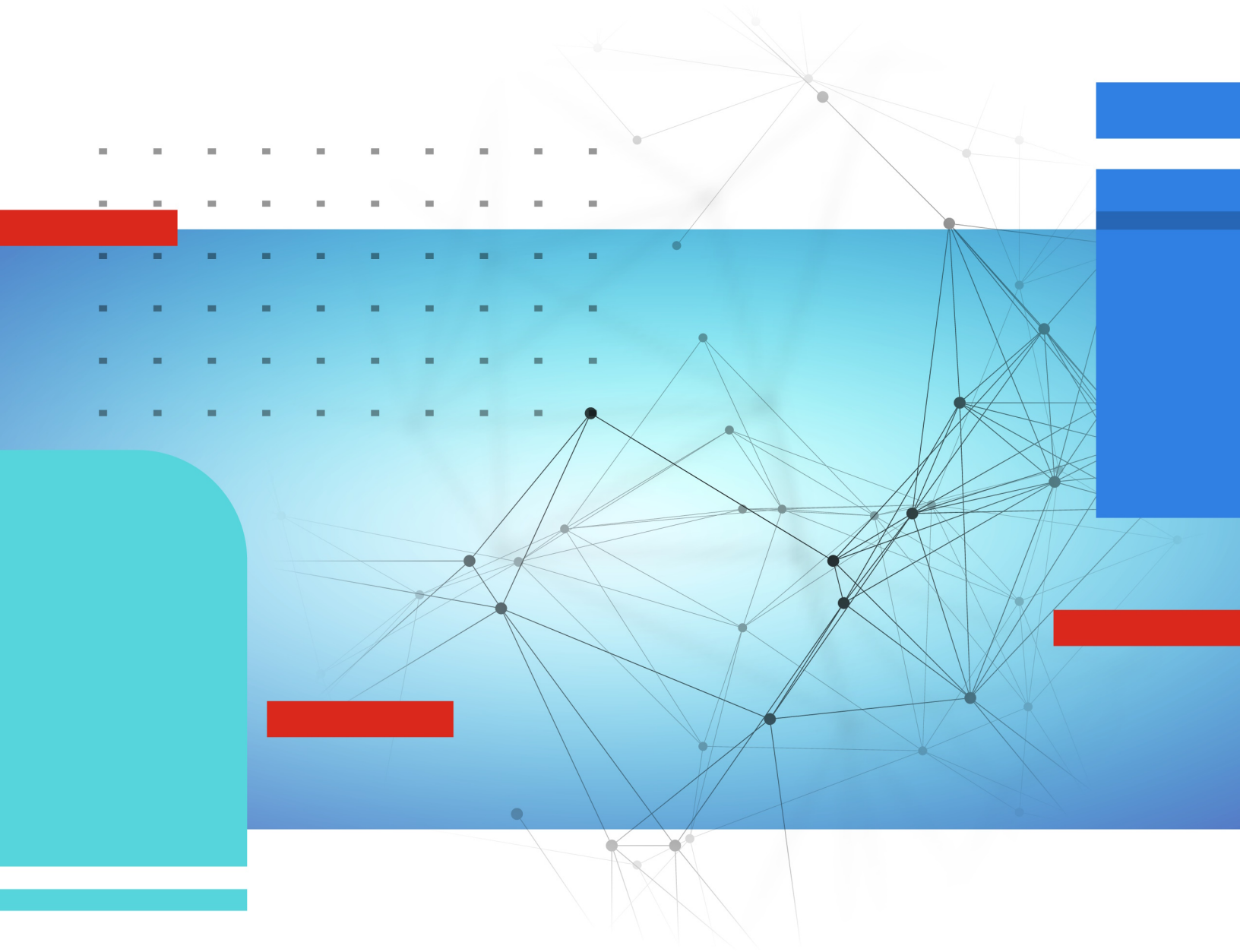
Administration Guide

FortiProxy 7.6.3



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com



August 26, 2025
FortiProxy 7.6.3 Administration Guide
45-763-1080757-20250826

TABLE OF CONTENTS

Change log **15**
Getting started **16**
Summary of steps 17
Setting up FortiProxy for management access 18
Configuring basic settings 19
Registering FortiProxy 22
Configuring a policy 23
Backing up the configuration 24
Troubleshooting your installation 24
Using the GUI 25
Connecting using a web browser 25
Menus 26
Tables 27
Entering values 32
GUI-based global search 33
Loading artifacts from a CDN 35
Accessing online documentation 35
Recovering missing graphical components 36
Using the CLI 37
Connecting to the CLI 38
CLI basics 41
Command syntax 48
Subcommands 50
Permissions 53
CLI error codes 53
Configuration and management 54
Accessing Fortinet Developer Network 54
Product registration with FortiCare 57
FortiCare and FortiGate Cloud login 57
FortiCare Register button 61
Transfer a device to another FortiCloud account 62
Deregistering a FortiProxy 65
FortiProxy models 66
Supported protocols 66
Deployments **67**
Transparent and NAT/route modes 67
Web proxy 68
Web proxy concepts 69
Explicit web proxy concepts 71
Transparent web proxy concepts 72
Explicit web proxy topologies 73
WAN optimization 73
WAN optimization transparent mode 74
WAN optimization topologies 75

Web caching ... 78
Collaboration web caching ... 79
Web-caching topologies ... 80
WCCP ... 81
WCCP topology ... 82
Dashboard ... 83
Managing widgets ... 85
System Information widget ... 86
Licenses widget ... 87
Virtual Machine widget ... 88
FortiProxy Cloud widget ... 88
Security Fabric widget ... 89
Administrators widget ... 90
CPU widget ... 90
Memory widget ... 91
Sessions widget ... 91
IPSec widget ... 92
Forward Server Monitor widget ... 93
License Sharing Information widget ... 94
License Usage History widget ... 95
Sensor Information widget ... 96
User dropdown menu ... 97
GUI-based global search ... 97
FortiView ... 98
FortiView dependencies ... 98
FortiView interface ... 101
FortiView consoles ... 101
Using the process monitor ... 108
Proxy Settings ... 109
Explicit Proxy ... 109
Create or edit an explicit proxy ... 110
Secure explicit proxy ... 114
Proxy chaining ... 116
Proxy chaining over IPsec tunnel ... 119
Forward HTTPS requests to a web server without the need for an HTTP CONNECT message ... 125
HTTP connection coalescing and concurrent multiplexing for explicit proxy ... 127
Secure explicit proxy with client certificates ... 129
Display CORS content in explicit proxy ... 132
Explicit proxy logging ... 135
Configuring fast fallback for explicit proxy ... 139
Web Proxy Setting ... 143
Logging client IP for forward traffic and HTTP transaction ... 144
Web Proxy Profile ... 145
Create or edit a web proxy profile ... 146

Create or edit an HTTP header 149
Restricted SaaS access 151
Forwarding Server 159
Create or edit a forwarding server 160
Grouping forwarding servers and load balancing traffic to the servers 165
Server URL 166
Create or edit a URL match entry 167
FTP Proxy 169
FTPS handling 171
Proxy Options 171
Video streaming splitting 173
Configuring TCP windows 173
Handling SSL offloaded traffic from an external decryption device 174
HTTP domain fronting blocking 175
Create or edit a proxy option profile 175
Create a CIFS proxy option 178
SSL Keyring 179
Network 181
Interfaces 181
Create or edit an interface 188
Create or edit a zone 194
GRE Tunnel 196
Create or edit a GRE tunnel 197
DNS Settings 199
Important DNS CLI commands 201
Using the FortiProxy unit as an IPv6 DDNS client for generic DDNS 205
Use DNS over TLS for default FortiGuard DNS servers 205
Alternate DNS servers 206
DNS Service 207
Create or edit a DNS service 208
Create or edit a DNS zone 209
Create or edit a DNS entry 211
Transparent conditional DNS forwarder 212
Interfaces in non-management VDOMs as the source IP address of the DNS conditional forwarding server 216
Diagnostics 218
Multiple packet captures 223
Static routes 224
Create or edit a static route 225
Policy routes 227
Configuring a policy route 228
VXLAN 230
Zero Trust Network Access 232
Zero Trust Network Access introduction 232
ZTNA telemetry, tags, and policy enforcement 233
Application gateway 234
Basic ZTNA configuration components 234

Establish device identity and trust context with FortiClient EMS 235
SSL certificate based authentication 244
Basic ZTNA configuration 246
Configure a FortiClient EMS connector 247
Configure a ZTNA server 250
Configure a ZTNA rule 254
Configure a firewall policy for full ZTNA 256
Optional authentication 258
ZTNA advanced configurations 260
ZTNA policy access control of unmanageable and unknown devices 260
HTTP2 connection coalescing and concurrent multiplexing for ZTNA 264
ZTNA traffic forwarding proxy 267
ZTNA agentless web-based application access 279
ZTNA configuration examples 291
ZTNA HTTPS access proxy example 292
ZTNA HTTPS access proxy with basic authentication example 302
ZTNA TCP forwarding access proxy example 311
ZTNA SSH access proxy example 318
ZTNA application gateway with SAML authentication example 326
Secure LDAP connection from FortiAuthenticator with zero trust tunnel example 331
Access control between on-net devices and internal web server using security posture tags 332
UTM scanning on TCP forwarding access proxy traffic 339
ZTNA Zero Trust application gateway example 342
ZTNA inline CASB for SaaS application access control 343
ZTNA application gateway with KDC to access shared drives 348
Custom replacement message for ZTNA virtual hosts 353
ZTNA for UDP traffic 357
ZTNA troubleshooting and debugging commands 367
Troubleshooting usage and output 368
ZTNA troubleshooting scenarios 374
ZTNA access control 374
IP/MAC based access control 376
Other useful CLI commands 381
Policy & Objects 382
Policy 382
Create or edit a policy 387
Policy views 402
New layout for policies 402
Policy matching 407
Web cache policy address formats 416
HTTP2 connection coalescing and concurrent multiplexing for virtual server load balancing 417
Authentication Rules 419
Create or edit an authentication rule 422
Create or edit an authentication scheme 424
Agentless NTLM support 426

Domain name source when doing NTLM authentication 427
Proxy Auth Setting 427
Traffic shaping 431
Configuration methods 431
Traffic shaping policies 432
Response shaping policies NEW 439
Traffic shaping profile 441
Traffic shapers 444
DSCP marking in firewall shaping policies 453
Examples 454
Isolator Setting 468
Servers 468
Profiles 469
Setting 470
DNS Lookup 471
Central SNAT 472
Create or edit a central SNAT policy 473
PAC Policy 476
Create or edit a PAC policy 477
Edit a PAC file 479
Policy Test 480
URL Lookup 481
Decrypted Traffic Mirror 481
Addresses 483
Create or edit an address 485
Create or edit an address group 501
Create or edit an IPv6 address template 502
Edit a subnet segment 504
Internet Service Database 506
Services 507
Create or edit an application service 508
Create or edit a service 509
Create or edit a service group 511
Create a service category 515
Schedules 516
Create or edit a schedule 517
Create or edit a schedule group 519
Virtual IPs 521
Sample configuration 521
Create or edit a virtual IP 522
Create or edit a virtual IP group 526
Virtual IPs with port forwarding 527
Virtual server load balance 529
IP Pools 535
Create or edit an IP pool 536
Security Profiles 538
Antivirus 541

Create or edit an antivirus profile ... 542
Advanced configurations ... 550
Configuration examples ... 561
Web Filter ... 565
Create or edit a web filter profile ... 566
Create or edit a URL filter ... 573
Create or edit a content filter ... 574
FortiGuard filter ... 575
Video Filter ... 580
Create or edit a video filter profile ... 580
Create or edit a channel override entry ... 583
Filtering based on title ... 583
Filtering based on description ... 585
Configuring a video filter keyword list ... 586
DNS Filter ... 588
Create or edit a DNS filter profile ... 589
Create or edit a domain filter ... 593
Create or edit a DNS translation entry ... 594
HTTP3 deep inspection, QUIC certificate inspection, DNS over QUIC and DNS over HTTP3 for transparent and local-in DNS modes ... 594
Application Control ... 598
Create or edit an application sensor ... 599
Create or edit a default network service ... 602
Add or edit an application override ... 603
Add or edit a filter override ... 603
Basic category filters and overrides ... 604
Inline CASB ... 608
Example 1: privilege control ... 609
Example 2: safe search ... 611
Example 3: tenant control ... 612
Example 4: UTM bypass ... 614
Example 5: customized SaaS application and user activity ... 615
Intrusion Prevention ... 618
Create or edit an IPS sensor ... 619
Add or edit an IPS signature or filter ... 621
File Filter ... 622
Create or edit a file filter profile ... 623
Create or edit a file filter rule ... 624
SSL/SSH Inspection ... 625
SSL/SSH inspection profile ... 625
Create or edit an SSL/SSH inspection profile ... 626
Control TLS connections that utilize Encrypted Client Hello ... 635
Application Signatures ... 644
Create or edit an application signature ... 645
Create or edit an application group ... 646
IPS Signatures ... 647
Highlight of on-hold IPS signatures ... 648
Create or edit an IPS signature ... 649

Web Rating Overrides 650
Create or edit a web rating override 651
Create or edit a custom category 653
Web Risk Overrides 653
Web Profile Overrides 654
Create or edit a web profile override 655
Profile Groups 657
Web Filter Risk Level 659
Data Loss Prevention 660
Protocol support for DLP inspection 661
Archiving 661
Logging and blocking files by file name 661
DLP techniques 662
Basic DLP settings 663
Advanced DLP configurations 669
DLP fingerprinting 672
Sensitivity labels 676
Exact data matching 680
DLP examples 689
DLP File Pattern 717
Create or edit a DLP file pattern 718
Content Analyses 719
Image Analysis 719
Create or edit an Image Analysis profile 721
ICAP Profile 724
Create or edit an ICAP profile 725
ICAP Remote Server 729
Create or edit an ICAP remote server 729
ICAP Load Balancing 731
ICAP Local Server 732
Create or edit an ICAP local server 733
Create or edit an ICAP service 735
ICAP scanning with FTP 736
WAN Optimization 738
Profiles 738
Create or edit a WAN optimization profile 739
Peers 742
Create or edit a WAN optimization peer 743
Authentication Groups 744
Create or edit an authentication group 745
Web Cache 747
Settings 747
HTTP traffic caching reports 751
Prefetch URLs 751
Reverse Cache Server 753
Create or edit a reverse cache server 754

Prefetch File 755
Create or edit a prefetch file 756
WCCP Settings 758
WCCP service groups, numbers, IDs, and well-known services 758
WCCP configuration overview 759
Example: Caching HTTP sessions 760
WCCP packet flow 763
Configure forward and return methods and adding authentication 763
WCCP messages 764
Troubleshooting WCCP 765
User Agent 766
Create or edit a user agent 767
VPN 768
IPsec Tunnels 768
Edit an IPsec tunnel 769
IPsec Wizard 773
Create a custom VPN tunnel 775
IPsec Tunnel Template 780
FortiProxy-to-FortiProxy 780
Basic site-to-site VPN with pre-shared key 780
Site-to-site VPN with digital certificate 785
GRE over IPsec 791
User & Authentication 797
User Definition 797
Creating or editing a user 798
Customizing complexity options for the local user password policy NEW 803
User Groups 807
Create or edit a user group 809
Guest Management 811
Create or edit a guest user account 812
Create multiple guest user accounts 813
Basic authentication with cached client certificates 813
LDAP Servers 818
Create or edit an LDAP server 819
Creating an administrator that can be authenticated by an LDAP server 820
RADIUS Servers 821
Create or edit a RADIUS server 822
Configuring a RADSEC client 824
TACACS+ Servers 828
Create or edit a TACACS server 829
Kerberos 830
Create or edit a Kerberos authentication service 831
Using Kerberos authentication with Windows AD cross-forest 832
SAML 835
Create or edit a SAML server 837
OIDC 839

FortiProxy configuration 839
Callback URL configuration in IdP 842
Configuring multiple Identity Providers (IDP) NEW 843
FortiTokens 844
Registering and activating a hard token 846
Assigning a FortiToken to a user account 848
Activating a mobile token 851
Managing FortiTokens 855
FortiToken Cloud 857
Synchronizing LDAP Active Directory users to FortiToken Cloud using the two-factor filter 857
Troubleshooting and diagnosis 861
System 864
Administrators 864
Create or edit an administrator 866
Create or edit a REST API administrator 870
Separating the SSHD host key from the administration server certificate 871
Admin Profiles 872
Create or edit an administrator profile 874
Fabric Management 875
Upgrading individual device firmware 877
Authorizing devices 878
Downloading a firmware image 878
Settings 879
Using the default certificate for HTTPS administrative access 882
TLS configuration 886
Trusted platform module support 886
VDOM 889
Configuration 889
Configure global security profiles 897
Transparent mode management 898
Backing up and restoring configurations in multi VDOM mode 900
HA 904
HA virtual cluster setup 909
HA cluster out-of-band management 916
Upgrading FortiProxies in an HA cluster 922
SNMP 923
Basic configuration 926
Fortinet MIBs 929
SNMP agent 931
Create or edit an SNMP community 931
Create or edit an SNMP user 934
Important SNMP traps 936
SNMP examples 939
Replacement Messages 944
Replacement Message Groups 960
Custom ZTNA virtual host replacement message 961
FortiGuard 962

Setting automatic updates for FortiGuard packages 965
FortiGuard Outbreak Prevention 965
Antiphish pattern database 966
Licensing in air-gap environments 966
Reputable Websites 967
Feature Visibility 970
Certificates 973
Certificate list 974
Certificate Signing Requests 975
Import a local certificate 978
Import a CA certificate 982
Upload a remote certificate 982
Import a CRL 982
View certificate details 983
Default certificate authority 983
Enrollment over Secure Transport for automatic certificate management 984
FortiProxy encryption algorithm cipher suites 996
HTTPS access 996
SSH access 997
Additional features 999
Other Products 1001
Integrating FortiProxy with SafeNet Luna Network HSM 1004
Configuration backups and reset 1006
Backing up and restoring configurations from the GUI 1007
Backing up and restoring configurations from the CLI 1009
Configuration revision 1013
Restore factory defaults 1014
Secure file copy 1015
Security Fabric 1016
Automation stitches 1016
Creating automation stitches 1017
Triggers 1028
Actions 1034
Fabric Connectors 1077
Creating a Security Fabric Group 1077
Simplify EMS pairing with Security Fabric so one approval is needed for all devices 1081
Configuring logging and analytics 1082
Configuring FortiClient EMS 1090
External Connectors 1106
Threat feeds 1107
Asset Identity Center 1132
Diagnostics for the unified user device store 1133
Log & Report 1135
Debug logs 1136
Logs for the execution of CLI commands 1136

Filter WAD log messages by process types or IDs 1137
Types of logs 1138
System Events 1140
Security Events 1143
Reports 1145
FortiAnalyzer reports 1146
Local reports 1146
Log settings 1147
Global Settings 1148
Local Logs 1148
Threat Weight 1149
Configuring logs in the CLI 1150
Email alerts 1151
Email Alert Settings 1152
Port Exhaustion Alert 1155
Logging to FortiAnalyzer 1156
FortiAnalyzer log caching 1156
Configuring multiple FortiAnalyzers (or syslog servers) per VDOM 1158
Configuring multiple FortiAnalyzers on a FortiProxy in multi-VDOM mode 1160
Log fields for long-live sessions 1163
Example 1164
Appendices 1165
Perl regular expressions 1166
Block common spam phrases 1167
Block purposely misspelled words 1167
Block any word in a phrase 1167
Preload cache content and web crawler 1168
execute preload list 1168
execute preload show-log 1168
execute preload url 1168
execute preload url-delete 1169
Examples 1169
Automatic backup to an FTP or TFTP server 1170
Manual backups to a remote FTP or TFTP using IPv4 1170
Manual backups to a remote FTP or TFTP using IPv6 1170
Scheduled automatic backups with an auto script 1171
Manual backups with SCP 1172
Scheduled automatic backups with SCP 1173
Custom signature keywords 1175
Information keywords 1175
Session keywords 1176
Content keywords 1180
IP header keywords 1191
TCP header keywords 1193
UDP header keywords 1195
ICMP keywords 1196

Other keywords 1196
FortiProxy bypass mode 1199
Formatting and loading FortiProxy firmware image using TFTP 1199
Prerequisites 1200

Change log

Date	Change Description
2025-04-09	Initial release.
2025-04-10	Added Traffic shaping based on HTTP response NEW on page 463 and updated OIDC on page 839.
2025-04-22	Updated Policy matching on page 407.
2025-04-24	Updated Policy matching on page 407.
2025-05-05	Updated Block access to LLM applications using keywords and FQDN on page 701
2025-05-06	Added Proxy chaining over IPsec tunnel on page 119.
2025-05-21	Updated Create or edit an SSL/SSH inspection profile on page 626.
2025-07-10	Updated Threat feeds on page 1107.
2025-07-15	Updated OIDC on page 839.
2025-08-08	Updated the following topics: • Create or edit an antivirus profile on page 542 • Import a local certificate on page 978

Getting started

FortiProxy provides a secure web gateway that protects against web attacks using URL filtering, visibility and control of encrypted web traffic through SSL and SSH inspection, and the application of granular web application policies. Flexible deployment modes cover inline, explicit, and transparent deployments.

- Application Control allows you to identify and control applications on networks and endpoints regardless of the port, protocol, and IP address used. It gives you unmatched visibility and control over application traffic, even traffic from unknown applications and sources.
- SSL and SSH inspection allows you to determine which inspection method will be applied to SSH and SSL traffic; identify how to treat invalid, unsupported or untrusted SSL certificates; and configure which web sites or web site categories are exempt from SSL inspection.
- Web filtering provides web URL filtering to block access to harmful, inappropriate, and dangerous web sites that can contain phishing/pharming attacks, malware such as spyware, or objectionable content that can expose your organization to legal liability. Based on automatic research tools and targeted research analysis, real-time updates enable you to apply highly-granular policies that filter web access based on 78 web content categories, over 45 million rated web sites, and more than two billion web pages—all continuously updated.
- The FortiProxy data loss prevention (DLP) system allows you to prevent sensitive data from leaving your network. When you define sensitive data patterns, data matching these patterns will be blocked or logged and allowed when passing through the FortiProxy unit. You configure the DLP system by creating individual filters based on file type, file size, a regular expression, an advanced rule, or a compound rule, in a DLP sensor and assign the sensor to a security policy. Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network and to archive some or all of the content passing through the FortiProxy unit.

The FortiProxy unit also provides WAN optimization, web caching, and WCCP. FortiProxy WAN optimization and web caching improve performance and security of traffic passing between locations on your wide area network (WAN) or from the Internet to your web servers. You can use the FortiProxy unit as an explicit FTP and web proxy server. In addition, you can add web caching to any HTTP sessions including WAN optimization, explicit web proxy, and other HTTP sessions.

Use the following resources to get started with FortiProxy:

Task	Documentation links
Follow the steps to set up a new FortiProxy	See Summary of steps on page 17. If you are migrating a configuration from another vendor to FortiProxy, see the Migration section of the Best Practices guide.
Learn about best practices for FortiProxy	Review Basic configuration in the Best Practices guide.
Learn about new FortiProxy features	See FortiProxy Release Notes > What's new section.

Task	Documentation links
Review information about FortiProxy releases, including resolved and known issues	See FortiProxy Release Notes.



For the latest information about FortiProxy 7.6, see the latest patch version of the Administration Guide.

Summary of steps

These steps summarize how to get your FortiProxy up and running by using the GUI. For information about the Command Line Interface (CLI), see Using the CLI on page 37.

1. Set up your FortiProxy for initial management access with the GUI. See Setting up FortiProxy for management access on page 18.

For more information	Go to
Physical appliances	Go to FortiProxy Hardware Guides to view QuickStart Guides for all supported FortiProxy models.
Hypervisors, such as FortiProxy-VM on ESXi, KVM, Hyper-V, and so on.	Go to FortiProxy Public Cloud or FortiProxy Private Cloud and follow the deployment guide for your hypervisor, for example, Microsoft Hyper-V Deployment Guide.

   Depending on the topology and FortiProxy model, internet access may not yet be configured for the FortiProxy. If no internet access, you cannot yet register the FortiProxy with Fortinet until later in the setup.
2. In the GUI, complete the basic configuration steps for FortiProxy. After this step, all FortiProxy models should have internet access. See Configuring basic settings on page 19.
3. Register FortiProxy with Fortinet by using your FortiCare/FortiCloud account with Fortinet Technical Support (https://support.fortinet.com). See Registering FortiProxy on page 22.
4. Configure a policy for the FortiProxy to give clients behind FortiProxy access to the internet. See Create or edit a policy on page 387.
5. Back up the configuration. See Backing up the configuration on page 24.
6. If necessary, troubleshoot the installation. See Troubleshooting your installation on page 24.

After completing the Getting started section, next steps can include:

- Getting familiar with the FortiProxy GUI and CLI:
  - See Using the GUI on page 25.
  - See Using the CLI on page 37.
- Configuring FortiProxy features. The following table lists a few of the features available with FortiProxy. Many additional features are available:

For	Go to
Security profiles	See Antivirus on page 541, Intrusion Prevention on page 618, Web Filter on page 565, and Application Control on page 598.
VPN	See VPN on page 768.
Fortinet Security Fabric	See Security Fabric on page 1016.
User & Authentication	See User & Authentication on page 797.
Zero Trust Network Access (ZTNA)	See Zero Trust Network Access introduction on page 232.

Setting up FortiProxy for management access

After you receive your FortiProxy, open the box, connect the cables for management and internet access, and use a management computer to access the FortiProxy GUI.

For information about setting up FortiProxy on hypervisors, such as FortiProxy-VM on ESXi, KVM, Hyper-V, and so on, go to FortiProxy Public Cloud or FortiProxy Private Cloud and follow the deployment guide for your hypervisor and cloud computing platform, for example, Microsoft Hyper-V Deployment Guide.

To set up FortiProxy for initial management access:

1. Unpack the FortiProxy box, and locate the following items:
   - FortiProxy device
   - Power cable
   - Ethernet cable

   You will also need to provide the following items:
   - Second Ethernet cable. Only one Ethernet cable is provided to connect the FortiProxy to a management computer. Locate a second Ethernet cable to connect the FortiProxy to a port for internet access.
   - Management computer to access the FortiProxy GUI
2. Use the power cable to connect the FortiProxy to a power source.
3. Configure a port for dedicated management access using the `set dedicated-to management` option under `config system interface`. This is called out-of-band management and is recommended.

   Alternatively, you can configure in-band management by using the Internal or LAN interface for FortiProxy management, in which case the management traffic is shared with internal traffic. This is not recommended.
4. Use an Ethernet cable to connect the management port to a management computer. For information about your FortiProxy hardware model, go to FortiProxy Hardware Guides.
5. Use a second Ethernet cable to connect the WAN on the FortiProxy to an upstream router, switch, or modem with access to the internet. You can select an interface of your choice for the WAN connection as the FortiProxy has no dedicated WAN interfaces.

   Internet access is available when the FortiProxy model has addressing mode set to DHCP by default on the WAN interface, and the WAN interface is connected to a network with a DHCP

server assigning the correct IP and gateway for internet access. If these conditions are not met, then internet access is not available after connecting your WAN interface. See Configuring basic settings on page 19.

6. On the management computer, assign an address in the 192.168.1.0/24 network.
7. In a web browser, go to https://192.168.1.99 and enter the default user name, `admin`, and leave the password field blank.

   By default, the management interface or the internal interface is configured to allow HTTPS access with the IP address 192.168.1.99.

   The GUI is displayed in your browser.
8. Complete the basic configurations. See Configuring basic settings on page 19.

Configuring basic settings

Complete the following basic settings on the FortiProxy to get the device up and running

1. Plan interface usage for MGMT, WAN, and LAN access, and configure the interfaces. See Planning and configuring the MGMT, WAN, and LAN interfaces on page 19.
2. Configure the default route. See Configuring the default route on page 21.
3. Configure the hostname. See Configuring the hostname on page 21.
4. Change the password by clicking the account icon at the top right corner and selecting *Change Password*.
5. Set up the dashboard according to your needs. See Dashboard on page 83.
6. Ensure internet and FortiGuard connectivity. See Ensuring internet and FortiGuard connectivity on page 22.
7. Use the default certificate for HTTPs administrative access. See Using the default certificate for HTTPS administrative access on page 22.

After configuring the basic settings, the FortiProxy can access the internet and communicate with FortiGuard. Next, you can register the FortiProxy with Fortinet. See Registering FortiProxy on page 22. Policies are also ready to be configured using the WAN and LAN interfaces.

Planning and configuring the MGMT, WAN, and LAN interfaces

On a typical deployment where the FortiProxy is configured as an edge firewall, the administrator typically sets up access control between the LAN and WAN interface, and permanent management access either through in-band management or out-of-band management. The following sections outline steps to plan and configure your management, WAN, and LAN interfaces

Management access

So far the new FortiProxy setup has been completed over a dedicated management interface. There is also a separate management network for accessing the FortiProxy and other devices on the network. This is called out-of-band management and is the recommended option.

WAN interface

FortiProxy models do not have dedicated WAN interfaces. You can configure an interface for WAN access and then connect the interface to your upstream router, L3 switch, or modem.

To configure a WAN interface in the GUI:

1. Go to *Network* > *Interfaces*. Select an interface and click *Edit*.
2. (Optional) Enter an *Alias*, such as WAN.
3. In the *Address* section, enter the *IP/Netmask*.
4. In *Administrative Access* section, select the access options as needed. For a WAN interface, it is recommended to only allow *PING*.
5. Click *OK*.

To configure a WAN interface in the CLI:

```
config system interface
    edit "port2"
        set ip 203.0.113.99 255.255.255.0
        set allowaccess ping
        set alias "WAN"
    next
end
```

LAN interface

FortiProxy does not have a default LAN interface. You must select an interface for LAN access and connect this interface to an internal switch that connects to your LAN network.

To configure a LAN interface in the GUI:

1. Go to *Network* > *Interfaces*. Select an interface and click *Edit*.
2. (Optional) Enter an *Alias*, such as LAN.
3. In the *Address* section, enter the *IP/Netmask*.
4. In *Administrative Access* section, select the access options as needed, such as *PING*. For in-band management, you may also want to allow administrative access for HTTPS and SSH.
5. Optionally, enable *DHCP Server* and configure as needed.
6. Click *OK*.

To configure a LAN interface in the CLI:

```
config system interface
  edit "port1"
    set ip 192.168.10.99 255.255.255.0
    set allowaccess ping https ssh
    set alias "LAN"
  next
end
```

```
config system dhcp server
    edit 1
        set dns-service default
        set default-gateway 192.168.10.99
        set netmask 255.255.255.0
        set interface "port1"
        config ip-range
            edit 1
                set start-ip 192.168.10.2
                set end-ip 192.168.10.254
            next
        end
    next
end
```

Configuring the default route

Setting the default route enables the FortiProxy to route traffic through this interface and default gateway when no specific routes are found for a particular destination. The gateway address should be your upstream router or L3 switch that the FortiProxy is connected to. Set the interface to be the WAN interface that the gateway is connected to.

If the WAN interface uses DHCP for address assignment, the default route may already be learned from the DHCP server, and this step is not needed.

To configure the default route in the GUI:

1. Go to *Network* > *Static Routes* and click *Create New*.
2. Leave the destination subnet as *0.0.0.0/0.0.0.0*. This is known as a default route, since it would match any IPv4 address.
3. Enter the *Gateway Address*.
4. Select an *Interface*.
5. Click *OK*.

To configure the default route in the CLI:

```
config router static
    edit 1
        set gateway 203.0.113.1
        set device port2
    next
end
```

Configuring the hostname

Setting the FortiProxy's hostname assists with identifying the device, and it is especially useful when managing multiple FortiProxies. Choose a meaningful hostname as it is used in the CLI console, SNMP system name, device name for FortiProxy Cloud, and to identify a member of an HA cluster.

To configure the hostname in the GUI:

1. Go to *System* > *Settings*.
2. Enter a name in the *Host name* field.
3. Click *Apply*.

To configure the hostname in the CLI:

```
config system global
    set hostname 2000E
end
```

Ensuring internet and FortiGuard connectivity

This step is not necessary for the configuration; however, it is necessary in order to keep your FortiProxy up to date against the latest threats. Updates are provided to FortiProxies that are registered and make a request to the FortiGuard network to verify if there are any more recent definitions.

Use `execute ping <domain.tld>` to ensure the DNS resolution is able to resolve the following FortiGuard servers:

- fds1.fortinet.com
- service.fortiguard.net
- update.fortiguard.net

You also need to ensure the necessary ports are permitted outbound in the event your FortiProxy is behind a filtering device. Refer to the Ports and Protocols document for more information.

Using the default certificate for HTTPS administrative access

By default, the FortiProxy uses the Fortinet_GUI_Server certificate for HTTPS administrative access. Administrators should download the CA certificate and install it on their PC to avoid warnings in their browser. See Using the default certificate for HTTPS administrative access on page 882 for more information.

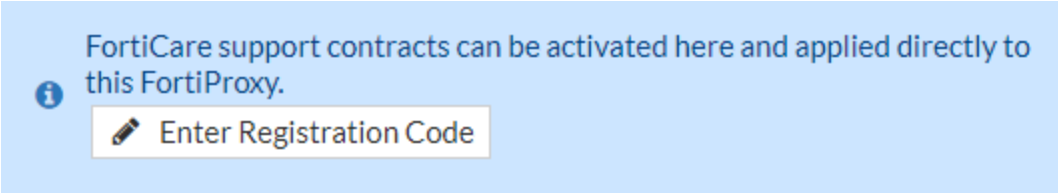
Registering FortiProxy



The service contract number is needed to complete registrations on the FortiCloud support portal. You can find this 12-digit number in the email that contains your service registration document (sent from do-not-reply-contract@fortinet.com) in the service entitlement summary.

To register your FortiProxy in the GUI:

1. Connect to the FortiProxy GUI. The *Dashboard* > *Status* page opens. Note that the licenses are grayed out because the device or virtual machine is not registered.
2. Go to *System* > *FortiGuard* and click *Enter Registration Code*.



3. Enter the contract registration code from your service registration document.
4. Click *OK*.

To register the FortiProxy on the FortiCloud support portal:

FortiProxies can be registered with the *Register More* button in the Products views. For details, see Registering assets in the FortiCloud Account Services Asset Management guide.

Configuring a policy

When devices are behind FortiProxy, you must configure a policy on FortiProxy to grant the devices access to the internet. In other words, a policy must be in place for any traffic that passes through a FortiProxy.

To create a policy in the GUI:

1. Go to *Policy & Objects* > *Policy*.
2. Click *Create New*. The *New Proxy Policy* pane is displayed.
3. Enter a Name and configure the following necessary settings:

Incoming Interface	LAN (port1)
Outgoing Interface	WAN (port2)
Source	Source IPv4 address name and address group names
Destination	Destination IPv4 address name and address group names
Schedule	Always
Service	All
Action	Accept

4. Click *Save*.

Backing up the configuration

You can back up the configuration in FortiProxy or YAML format. You have the option to save the configuration file in FortiProxy format to various locations including the local PC and USB key.

Troubleshooting your installation

If your FortiProxy does not function as desired after installation, try the following troubleshooting tips:

1. **Check for equipment issues**
   Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiProxy to the network.
2. **Check the physical network connections**
   Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged, and make sure that each cable connects to the correct device and the correct Ethernet port on that device.
3. **Verify that you can connect to the internal IP address of the FortiProxy**
   Connect to the GUI from the FortiProxy's internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`. If you cannot connect to the internal interface, verify the IP configuration of the PC. If you can ping the interface but cannot connect to the GUI, check the settings for administrative access on that interface. Alternatively, use SSH to connect to the CLI, and then confirm that HTTPS has been enabled for Administrative Access on the interface.
4. **Check the FortiProxy interface configurations**
   Check the configuration of the FortiProxy interface connected to the internal network (under *Network* > *Interfaces*) and check that *Addressing mode* is set to the correct mode.
5. **Verify the static routing configuration**
   Go to *Network* > *Static Routes* and verify that the default route is correct. Go to *Monitor* > *Routing Monitor* and verify that the default route appears in the list as a static route. Along with the default route, you should see two routes shown as *Connected*, one for each connected FortiProxy interface.
6. **Verify that you can connect to the Internet-facing interface's IP address**
   Ping the IP address of the Internet-facing interface of your FortiProxy. If you cannot connect to the interface, the FortiProxy is not allowing sessions from the internal interface to Internet-facing interface. Verify that PING has been enabled for *Administrative Access* on the interface.
7. **Verify that you can connect to the gateway provided by your ISP**
   Ping the default gateway IP address from a PC on the internal network. If you cannot reach the gateway, contact your ISP to verify that you are using the correct gateway.
8. **Verify that you can communicate from the FortiProxy to the Internet**
   Access the FortiProxy CLI and use the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.
9. **Verify the DNS configurations of the FortiProxy and the PCs**
   Check for DNS errors by pinging or using traceroute to connect to a domain name; for example: `ping www.fortinet.com`.
   If the name cannot be resolved, the FortiProxy or PC cannot connect to a DNS server and you should confirm that the DNS server IP addresses are present and correct.

10. **Confirm that the FortiProxy can connect to the FortiGuard network**
    Once the FortiProxy is on your network, you should confirm that it can reach the FortiGuard network. First, check the *Licenses* widget to make sure that the status of all FortiGuard services matches the services that you have purchased. Go to *System* > *FortiGuard*, and, in the Filtering section, click *Test Connectivity*. After a few minutes, the GUI should indicate a successful connection. Verify that your FortiProxy can resolve and reach FortiGuard at `service.fortiguard.net` by pinging the domain name. If you can reach this service, you can then verify the connection to FortiGuard servers by running the command `diagnose debug rating`. This displays a list of FortiGuard IP gateways you can connect to, as well as the following information:
    - `Weight`: Based on the difference in time zone between the FortiProxy and this server
    - `RTT`: Return trip time
    - `Flags`: D (IP returned from DNS), I (Contract server contacted), T (being timed), F (failed)
    - `TZ`: Server time zone
    - `Curr Lost`: Current number of consecutive lost packets
    - `Total Lost`: Total number of lost packets
11. **Contact Fortinet Support for assistance**

If you require further assistance, visit the Fortinet Support website.

Using the GUI

This section presents an introduction to the graphical user interface (GUI) on your FortiProxy.

The following topics are included in this section:

- Connecting using a web browser
- Menus
- Tables
- Entering values
- GUI-based global search
- Loading artifacts from a CDN on page 35
- Accessing online documentation on page 35
- Recovering missing graphical components on page 36

For information about using the dashboards, see Dashboard on page 83.

Connecting using a web browser

In order to connect to the GUI using a web browser, an interface must be configured to allow administrative access over HTTPS or over both HTTPS and HTTP. By default, an interface has already been set up that allows HTTPS access with the IP address 192.168.1.99.

Browse to https://192.168.1.99 and enter your username and password. If you have not changed the admin account's password, use the default user name, `admin`, and leave the password field blank.

The GUI will now display in your browser, and you will be required to provide a password for the administrator account.

To use a different interface to access the GUI:

1. Go to *Network* > *Interfaces* and edit the interface you wish to use for access. Take note of its assigned IP address.
2. In *Administrative Access*, select *HTTPS*, and any other protocol you require. You can also select *HTTP*, although this is not recommended as the connection is insecure.
3. Click *OK*.
4. Browse to the IP address using your chosen protocol.
   The GUI will now be displayed in your browser.

Menus



If you believe your FortiProxy model supports a menu that does not appear in the GUI, go to *System* > *Feature Visibility* and ensure the feature is enabled. For more information, see Feature Visibility on page 970.

The GUI contains the following main menus, which provide access to configuration options for most FortiProxy features:

Dashboard	The dashboard displays various widgets and monitors that display important system information and allow you to configure some system options. For more information, see Dashboard on page 83.
Network	Options for networking, including configuring system interfaces and routing options. For more information, see Network on page 181.
Policy & Objects	Configure policies, protocol options, and supporting content for policies, including schedules, addresses, and traffic shapers. For more information, see Policy & Objects on page 382.
Security Profiles	Configure your FortiProxy's security features, including Antivirus, Web Filter, and Application Control. For more information, see Security Profiles on page 538.
VPN	Configure options for IPsec and SSL virtual private networks (VPNs). For more information, see IPsec Tunnels on page 768 and .
User & Authentication	Configure user accounts, groups, and authentication methods, including external authentication and single sign-on (SSO). For more information, see User & Authentication on page 797.
System	Configure system settings, such as administrators, HA, FortiGuard, and certificates.

	For more information, see System on page 864.
Security Fabric	Access the physical topology, logical topology, automation, and settings of the Fortinet Security Fabric. For more information, see Security Fabric on page 1016.
Log & Report	Configure logging and alert email as well as reports. For more information, see Log & Report on page 1135.

Tables

Many GUI pages contain tables of information that can be filtered and customized to display specific information in a specific way. Some tables allow content to be edited directly on that table, or rows to be copied and pasted.

Filters

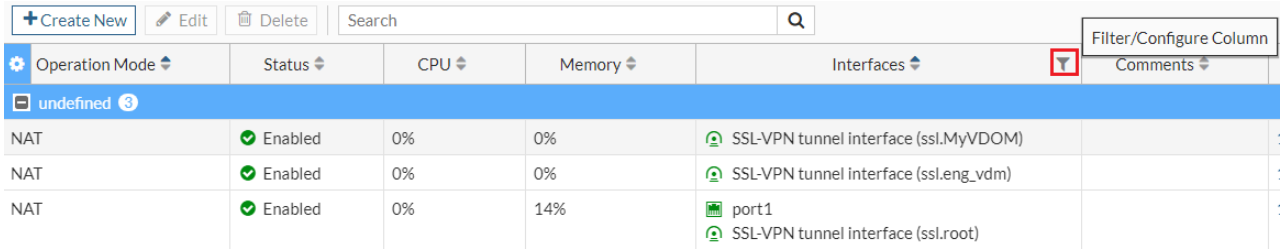
Filters are used to locate a specific set of information or content in a table. They can be particularly useful for locating specific log entries. The filtering options vary, depending on the type of information in the log.

Depending on the table content, filters can be applied using the filter bar, using a column filter, or based on a cell's content. Some tables allow filtering based on regular expressions.

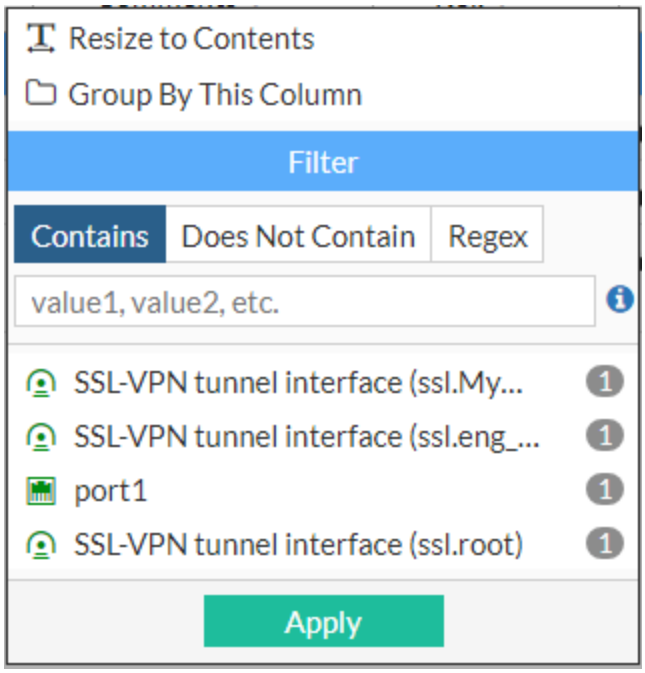
Administrators with read and write access can define filters. Multiple filters can be applied at one time.

To create a column filter:

1. Click the filter icon on the right side of the column header.



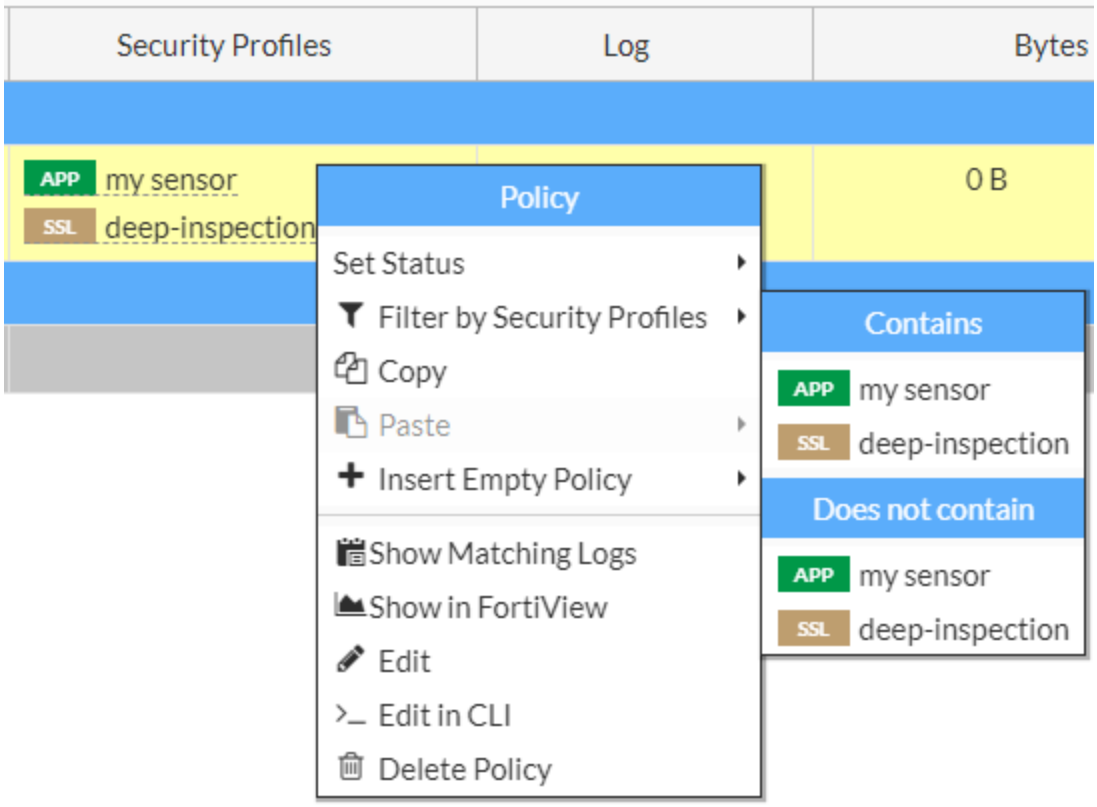
2. Choose a filter type from the available options.



3. Enter the filter text, or select from the available values.
4. Click *Apply*.

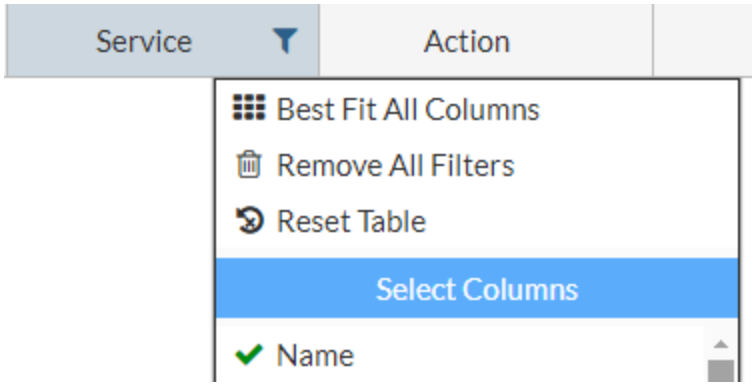
To create a filter based on a cell's content:

1. Right-click on a cell in the table.
2. Select *Filter by [column name]* and configure a filtering option from the menu.



To remove all filters:

1. Right-click a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.
2. Select *Remove All Filters*.

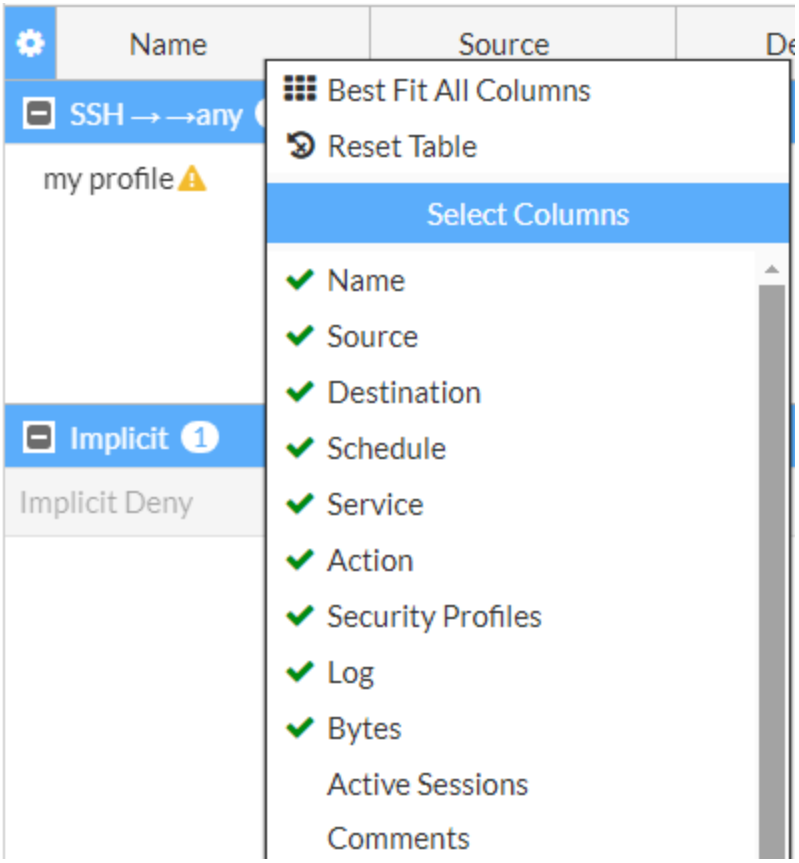


Column settings

Columns can be rearranged, resized, and added or removed from tables.

To add or remove columns:

1. Right-click a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.



2. Select columns to add or remove.
3. Click *Apply*.

To rearrange the columns in a table:

1. Click and drag the column header.

To resize a column:

1. Click and drag the right border of the column header.

To resize a column to fit its contents:

1. Click the dots or filter icon on the right side of the column header and select *Resize to Contents*.



To resize all of the columns in a table to fit their content:

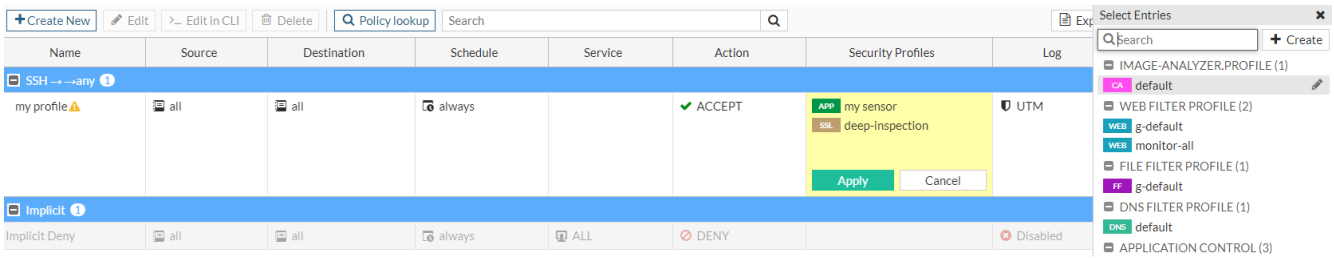
1. Right a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.
2. Click *Best Fit All Columns*.

To reset a table to its default view:

1. Right a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.
2. Click *Reset Table*.

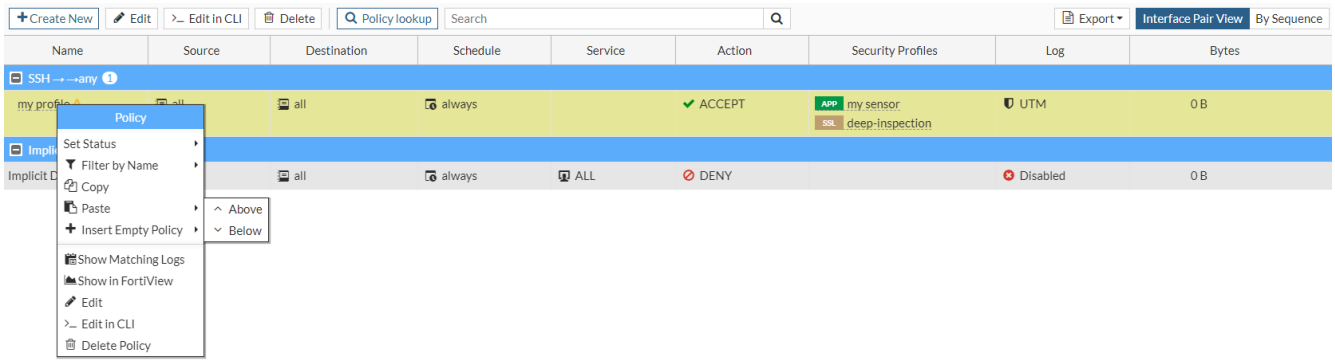
Editing objects

In some tables, parts of a configuration can be edited directly in the table. For example, security profiles can be added to an existing policy by clicking the edit icon in a cell in the *Security Profiles* column.



Copying rows

In some tables, rows can be copied and pasted using the right-click menu. For example, a policy can be duplicated by copying and pasting it.



Entering values

Numerous fields in the GUI and CLI require text strings or numbers to be entered when configuring the FortiProxy. When entering values in the GUI, you will be prevented from entering invalid characters, and a warning message will be shown explaining what values are not allowed. If invalid values are entered in a CLI command, the setting will be rejected when you apply it.

- Text strings on page 32
- Numbers on page 33

Text strings

Text strings are used to name entities in the FortiProxy configuration. For example, the name of a firewall address, administrator, or interface are all text strings.

The following characters cannot be used in text strings, as they present cross-site scripting (XSS) vulnerabilities:

- “ - double quotes
- ' - single quote
- > - greater than
- < - less than

Most GUI text fields prevent XSS vulnerable characters from being added.



VDOM names and hostnames can only use numbers (0-9), letters (a-z and A-Z), dashes, and underscores.

The `tree` CLI command can be used to view the number of characters allowed in a name field. For example, entering the following commands show that a firewall address name can contain up to 79 characters, while its FQDN can contain 255 characters:

```
# tree firewall address
-- [address] --*name    (79)
             |- uuid
             |- subnet
             |- type
             |- route-tag       (0,4294967295)
             |- sub-type
             |- clearpass-spt
             |- [macaddr] --*macaddr    (127)
             |- start-ip
             |- end-ip
             |- fqdn    (255)
             |- country         (2)
             |- wildcard-fqdn   (255)
             |- cache-ttl       (0,86400)
             |- wildcard
```

```
            |- sdn     (35)
            |- [fsso-group] --*name    (511)
            |- interface       (35)
            |- tenant  (35)
            |- organization    (35)
            |- epg-name        (255)
            |- subnet-name     (255)
            |- sdn-tag         (15)
            |- policy-group    (15)
            |- obj-tag         (255)
            |- obj-type
            |- tag-detection-level     (15)
            |- tag-type        (63)
            |- dirty
            |- hw-vendor       (35)
            |- hw-model        (35)
            |- os      (35)
            |- sw-version      (35)
            |- comment
            |- associated-interface    (35)
            |- color   (0,32)
            |- filter
            |- sdn-addr-type
            |- node-ip-only
            |- obj-id
            |- [list] --*ip    (35)
                      |- obj-id        (127)
                      +- net-id        (127)
            |- [tagging] --*name       (63)
                         |- category   (63)
                         +- [tags] --*name     (79)
            |- allow-routing
            +- fabric-object
```

Numbers

Numbers are used to set sizes, rates, addresses, port numbers, priorities, and other such numeric values. They can be entered as a series of digits (without commas or spaces), in a dotted decimal format (such as IP addresses), or separated by colons (such as MAC addresses). Most numeric values use base 10 numbers, while some use hexadecimal values.

Most GUI and CLI fields prevent invalid numbers from being entered. The CLI help text includes information about the range of values allowed for applicable settings.

GUI-based global search

The global search option in the GUI allows users to search for keywords appearing in objects and navigation menus to quickly access the object and configuration page. Click the magnifying glass icon in the top-left corner of the banner to access the global search.

The global search includes the following features:

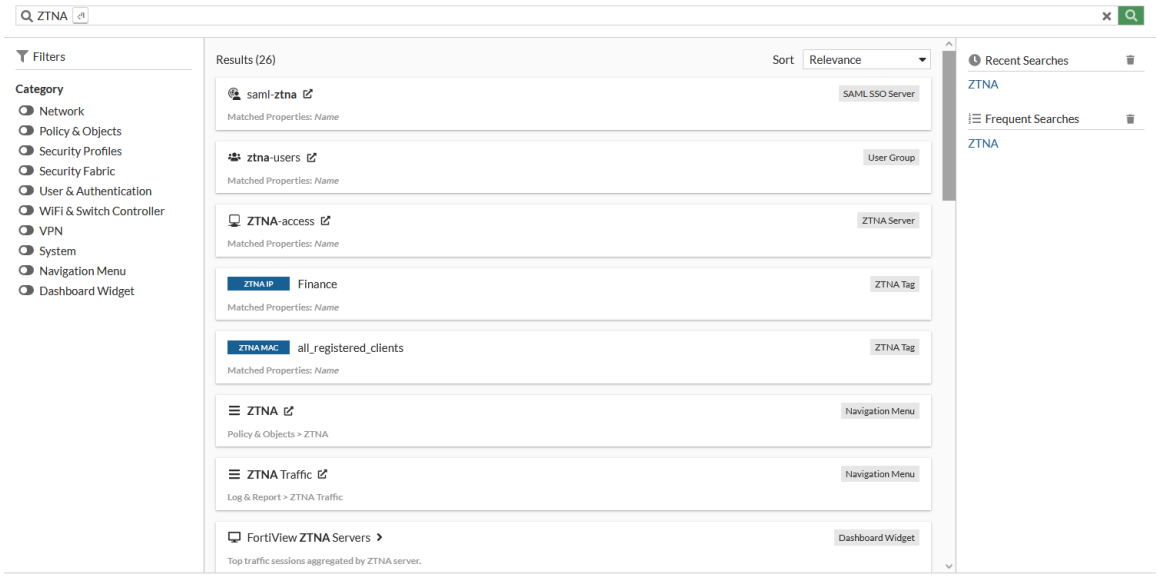
- Keep a history of frequent and recent searches
- Sort results by relevance (by search weight), or alphabetically in increasing or decreasing order
- Search by category
- Search in Security Fabric members (accessed by the Security Fabric members dropdown menu in the banner)
- Search for dashboard widgets and monitors, and preview the widget or go directly to the monitor dashboard if it exists.

Examples

In this example, searching for the word *ZTNA* yields the following results:

- A ZTNA server, user group, and SAML SSO server that have the *ZTNA* in the *Name* field.
- Various ZTNA tag.
- ZTNA navigation tree items: *Policy & Objects > ZTNA* and *Log & Report > ZTNA Traffic*.
- The FortiView ZTNA Servers dashboard widget.

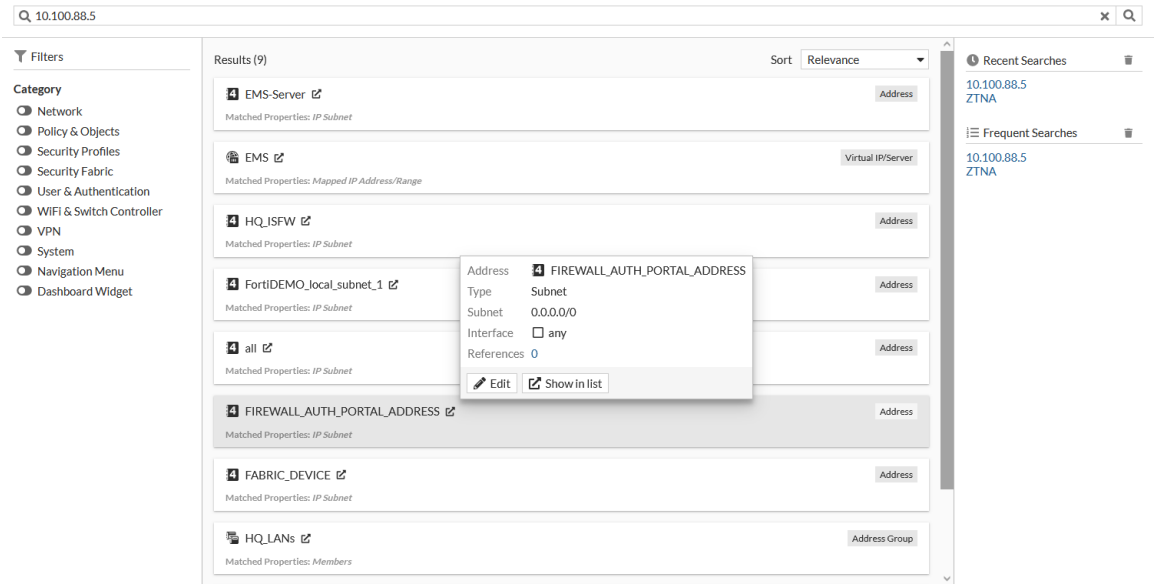
CMDB objects have a higher search weight (50) than navigation objects (20), so the navigation menus and widgets appears at the bottom of the results when sorting by relevance.



In this example, searching for the address *10.100.88.5* yields the following results:

- Various address objects that have a subnet of 10.100.88.5.
- A Virtual IP/Server object, *EMS*, that has a mapped IP address/range with 10.100.88.5.
- Address objects that have IP subnets of 0.0.0.0/0, which the search term falls into.
- Address group objects that contains members addresses that have IP subnets of 0.0.0.0/0.

Sorting by *Relevance* displays address objects that are more closely matched at the top (10.100.88.5), and more loosely matched at the bottom (0.0.0.0).



Loading artifacts from a CDN

To improve GUI performance, loading static GUI artifacts cached in CDN (content delivery network) servers closer to the user instead of the FortiProxy can be enabled. This allows the GUI to load more quickly with less latency for administrators who are accessing the FortiProxy remotely. Upon failure, the files fall back to loading from the FortiProxy. The CDN is only used after successful administrator logins.

To configure loading static GUI files from a CDN:

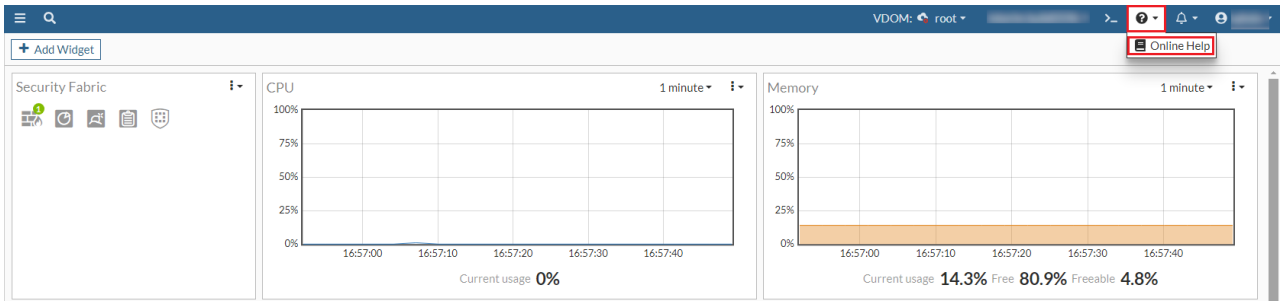
```
config system global
    set gui-cdn-usage {enable | disable}
end
```

Accessing online documentation

Documentation resources can be accessed from the GUI to troubleshoot issues and get the most out of FortiProxy.

To access support resources:

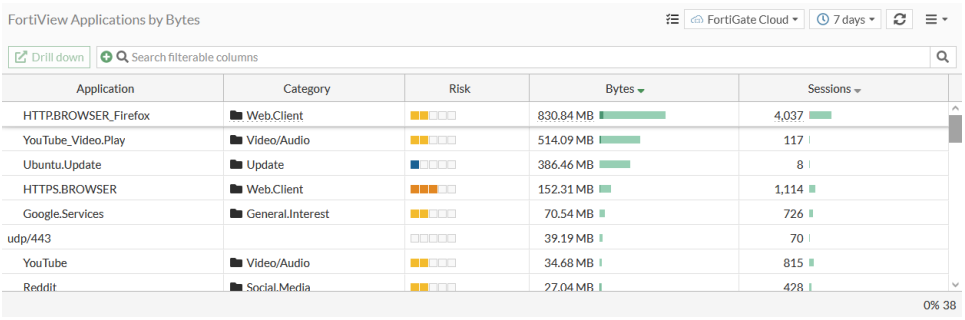
1. Click *Help* in the top menu and select *Online Help* from the dropdown menu to access relevant help documentation.



Recovering missing graphical components

Errors can sometimes cause the application icons, or other minor graphical components, to no longer show up in the GUI.

For example, in the *FortiView Applications* monitor, the icons could be missing from the *Application* column.



The `diagnose fortiguard-resources update` command can be used to delete cached files and force downloads of the FortiGuard resource, including icons.

Command	Downloaded resource
`diagnose fortiguard-resources update sprite-map`	Application icon sprite map (CSS & PNG).
`diagnose fortiguard-resources update sprite-isdb`	Application icon sprite ISDB (CSS & PNG).
`diagnose fortiguard-resources update app-info <id>`	Application info for a given ID.
`diagnose fortiguard-resources update ips-information <id>`	IPS information for a given ID.
`diagnose fortiguard-resources update wf-categories`	Web filter categories.
`diagnose fortiguard-resources update app-categories`	Application categories.
`diagnose fortiguard-resources update prefix-links`	Prefix links.
`diagnose fortiguard-resources update static-links`	Static links.
`diagnose fortiguard-resources update fortiproxy-end-of-support`	FortiProxy product life cycle information.

To recover missing application icons:

1. Run the update command:

```
# diagnose fortiguard-resources update sprite-isdb
Deleted cached resource file: sprite-isdb.css
Deleted cached resource file: sprite-isdb.png
Deleted cached resource file: sprite_map_front.css
Request URL: "https://globalproductapi.fortinet.net/v1/ref?key=spritemap&f=fos&v=2"
Host "globalproductapi.fortinet.net" resolved to "209.52.38.140"

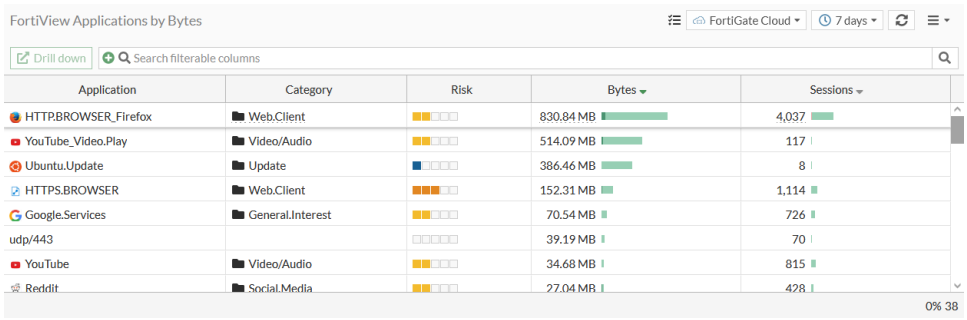
Performing HTTP request...

Response identified resource location as "https://filestore.fortinet.com/fortiguard/isdb_
logos96/sprite.tar.gz"
Host "filestore.fortinet.com" resolved to "209.52.38.129"

Performing HTTP request...

Successfully downloaded sprite-isdb.css:
  Size: 18142 bytes
  ETag: "5d9814eb50b0a9f8c7b0271e8c5baf39"
  MD5:  a0474459f96edabbc61bfae9b40a9aec
Successfully downloaded sprite-isdb.png:
  Size: 294937 bytes
  ETag: "5d9814eb50b0a9f8c7b0271e8c5baf39"
  MD5:  c98ce9dc8d3c2ae174233798f7124937
```

2. Refresh the browser window. You might also need to clear your browser cache.



Using the CLI

The Command Line Interface (CLI) can be used in lieu of the GUI to configure the FortiProxy. Some settings are not available in the GUI, and can only be accessed using the CLI.

This section briefly explains basic CLI usage. For information about the CLI config commands, see the FortiProxy CLI Reference.

- Connecting to the CLI on page 38
- CLI basics on page 41

- Command syntax on page 48
- Subcommands on page 50
- Permissions on page 53
- CLI error codes on page 53

Connecting to the CLI

You can connect to the CLI using a direct console connection, SSH, or the CLI console in the GUI.

You can access the CLI outside of the GUI in three ways:

- Console connection: Connect your computer directly to the console port of your FortiProxy.
- SSH access: Connect your computer through any network interface attached to one of the network ports on your FortiProxy.

To open a CLI console, click the _> icon in the top right corner of the GUI. The console opens on top of the GUI. It can be minimized and multiple consoles can be opened. On many GUI pages, the CLI console can be opened with that pages specific commands already shown by clicking *Edit in CLI* in the right-side gutter.

To edit policies and objects directly in the CLI, right-click on the element and select *Edit in CLI*.

Console connection

A direct console connection to the CLI is created by directly connecting your management computer or console to the FortiProxy using its DB-9 or RJ-45 console port.

Direct console access to the FortiProxy may be required if:

- You are installing the FortiProxy for the first time and it is not configured to connect to your network.
- You are restoring the firmware using a boot interrupt. Network access to the CLI will not be available until after the boot process has completed, making direct console access the only option.

To connect to the FortiProxy console, you need:

- A console cable to connect the console port on the FortiProxy to a communications port on the computer. Depending on your device, this is one of:
  - null modem cable (DB-9 to DB-9)
  - DB-9 to RJ-45 cable (a DB-9-to-USB adapter can be used)
  - USB to RJ-45 cable
- A computer with an available communications port
- Terminal emulation software

To connect to the CLI using a direct console connection:

1. Using the console cable, connect the FortiProxy unit's console port to the serial communications (COM) port on your management computer.

2. Start a terminal emulation program on the management computer, select the COM port, and use the following settings:

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

3. Press *Enter* on the keyboard to connect to the CLI.
4. Log in to the CLI using your username and password (default: *admin* and no password). You can now enter CLI commands, including configuring access to the CLI through SSH.

SSH access

SSH access to the CLI is accomplished by connecting your computer to the FortiProxy using one of its network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.



If you do not want to use an SSH client and you have access to the GUI, you can access the CLI through the network using the CLI console in the GUI.

SSH must be enabled on the network interface that is associated with the physical network port that is used.

If your computer is not connected either directly or through a switch to the FortiProxy, you must also configure the FortiProxy with a static route to a router that can forward packets from the FortiProxy to the computer. This can be done using a local console connection, or in the GUI.

To connect to the FortiProxy CLI using SSH, you need:

- A computer with an available serial communications (COM) port and RJ-45 port
- An appropriate console cable
- Terminal emulation software
- A network cable
- Prior configuration of the operating mode, network interface, and static route.

To enable SSH access to the CLI using a local console connection:

1. Using the network cable, connect the FortiProxy unit's port either directly to your computer's network port, or to a network through which your computer can reach the FortiProxy.
2. Note the number of the physical network port.
3. Using direct console connection, connect and log into the CLI.

4. Enter the following command:

```
config system interface
    edit <interface_str>
        append allowaccess ssh
    next
end
```

Where <interface_str> is the name of the network interface associated with the physical network port, such as port1.

5. Confirm the configuration using the following command to show the interface's settings:

```
show system interface <interface_str>
```

For example:

```
show system interface port1
    config system interface
        edit "port1"
            set vdom "root"
            set ip 192.168.1.99 255.255.255.0
            set allowaccess ping https ssh
            set type hard-switch
            set stp enable
            set role lan
            set snmp-index 6
        next
    end
```

Connecting using SSH

Once the FortiProxy is configured to accept SSH connections, use an SSH client on your management computer to connect to the CLI.

The following instructions use PuTTy. The steps may vary in other terminal emulators.

To connect to the CLI using SSH:

1. On your management computer, start PuTTy.
2. In the *Host Name (or IP address)* field, enter the IP address of the network interface that you are connected to and that has SSH access enabled.
3. Set the port number to 22, if it is not set automatically.
4. Select *SSH* for the *Connection type*.
5. Click *Open*. The SSH client connect to the FortiProxy.
   The SSH client may display a warning if this is the first time that you are connecting to the FortiProxy and its SSH key is not yet recognized by the SSH client, or if you previously connected to the FortiProxy using a different IP address or SSH key. This is normal if the management computer is connected directly to the FortiProxy with no network hosts in between.
6. Click *Yes* to accept the FortiProxy's SSH key.
   The CLI displays the log in prompt.
7. Enter a valid administrator account name, such as admin, then press *Enter*.

8. Enter the administrator account password, then press *Enter*.
   The CLI console shows the command prompt (FortiProxy hostname followed by a #). You can now enter CLI commands.



If three incorrect log in or password attempts occur in a row, you will be disconnected. If this occurs, wait for one minute, then reconnect and attempt to log in again.

CLI basics

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

Help

Press the question mark (?) key to display command help and complete commands.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Enter a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.
- Enter a command followed by an option and press the question mark (?) key to display a list of additional options available for that command option combination and a description of each option.
- Enter a question mark after entering a portion of a command to see a list of valid complete commands and their descriptions. If there is only one valid command, it will be automatically filled in.

Shortcuts and key commands

Shortcut key	Action
?	List valid complete or subsequent commands. If multiple commands can complete the command, they are listed with their descriptions.
Tab	Complete the word with the next available match. Press multiple times to cycle through available matches.
Up arrow or Ctrl + P	Recall the previous command. Command memory is limited to the current session.
Down arrow, or Ctrl + N	Recall the next command.
Left or Right arrow	Move the cursor left or right within the command line.

Shortcut key	Action
Ctrl + A	Move the cursor to the beginning of the command line.
Ctrl + E	Move the cursor to the end of the command line.
Ctrl + B	Move the cursor backwards one word.
Ctrl + F	Move the cursor forwards one word.
Ctrl + D	Delete the current character.
Ctrl + C	Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as `config` or `edit`, this closes the CLI connection.
\ then Enter	Continue typing a command on the next line for a multiline command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command, enter a space instead of a backslash, and then press *Enter*.

Command tree

Enter `tree` to display the CLI command tree. To capture the full output, connect to your device using a terminal emulation program and capture the output to a log file. For some commands, use the `tree` command to view all available variables and subcommands.

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` could be abbreviated to `g sy stat`.

Adding and removing options from lists

When configuring a list, the `set` command will remove the previous configuration.

For example, if a user group currently includes members A, B, and C, the command `set member D` will remove members A, B, and C. To avoid removing the existing members from the group, the command `set members A B C D` must be used.

To avoid this issue, the following commands are available:

append	Add an option to an existing list. For example, `append member D` adds user D to the user group without removing any of the existing members.
select	Clear all of the options except for those specified.

	For example, `select member B` removes all member from the group except for member B.
unselect	Remove an option from an existing list. For example, `unselect member C` removes only member C from the group, without affecting the other members.

Environment variables

The following environment variables are support by the CLI. Variable names are case-sensitive.

$USERFROM	The management access type (`ssh`, `jsconsole`, and so on) and the IPv4 address of the administrator that configured the item.
$USERNAME	The account name of the administrator that configured the item.
$SerialNum	The serial number of the FortiProxy.

For example, to set a FortiProxy device's host name to its serial number, use the following CLI command:

```
config system global
    set hostname $SerialNum
end
```

Special characters

The following characters cannot be used in most CLI commands: <, >, (,), #, ', and "

If one of those characters, or a space, needs to be entered as part of a string, it can be entered by using a special command, enclosing the entire string in quotes, or preceding it with an escape character (backslash, \).

To enter a question mark (?) or a tab, *Ctrl + V* or *Ctrl + Shift +* - (depending on the method being used to access the CLI) must be entered first.



Question marks and tabs cannot be copied into the CLI Console or some SSH clients. They must be typed in.

Character	Keys
?	Ctrl + V or Ctrl + Shift + - then ?
Tab	Ctrl + V then Tab
Space (as part of a string value, not to end the string)	Enclose the string in single or double quotation marks: `"Security Administrator"` or `'Security Administrator'`.

Character	Keys
	Precede the space with a backslash: `Security\ Administrator`.
' (as part of a string value, not to begin or end the string)	\'
" (as part of a string value, not to begin or end the string)	\"
\	\\

Using grep to filter command output

The `get`, `show`, and `diagnose` commands can produce large amounts of output. The `grep` command can be used to filter the output so that it only shows the required information.

The grep command is based on the standard UNIX grep, used for searching text output based on regular expressions.

For example, the following command displays the MAC address of the internal interface:

```
get hardware nic internal | grep Current_HWaddr
    Current_HWaddr        00:09:0f:cb:c2:75
```

The following command will display all TCP sessions that are in the session list, including the session list line number in the output:

```
get system session list | grep -n tcp
```

The following command will display all of the lines in the HTTP replacement message that contain `URL` or `url`:

```
show system replacemsg http | grep -i url
```

The following options can also be used:

```
-A <num> After
```

```
-B <num> Before
```

```
-C <num> Context
```

The `-f` option is available to support contextual output, in order to show the complete configuration. The following example shows the difference in the output when `-f` is used versus when it is not used:

Without `-f`:

```
show | grep ldap-group1
```

With `-f`:

```
    edit "ldap-group1"
        set groups "ldap-group1"
```

```
show | grep -f ldap-group1
    config user group
        edit "ldap-group1"
            set member "pc40-LDAP"
        next
    end
    config firewall policy
        edit 2
            set srcintf "port31"
            set dstintf "port32"
            set srcaddr "all"
            set action accept
            set identity-based enable
            set nat enable
            config identity-based-policy
                edit 1
                    set schedule "always"
                    set groups "ldap-group1"
                    set dstaddr "all"
                    set service "ALL"
                next
            end
        next
    end
```

Language support and regular expressions

Characters such as ñ and é, symbols, and ideographs are sometimes acceptable input. Support varies depending on the type of item that is being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values can be input using your language of choice. To use other languages in those cases, the correct encoding must be used.

Input is stored using Unicode UTF-8 encoding, but is not normalized from other encodings into UTF-8 before it is stored. If your input method encodes some characters differently than in UTF-8, configured items may not display or operate as expected.

Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using a different encoding, or if an HTTP client sends a request in a different encoding, matches may not be what is expected.

For example, with Shift-JIS, backslashes could be inadvertently interpreted as the symbol for the Japanese yen (¥), and vice versa. A regular expression intended to match HTTP requests containing monetary values with a yen symbol may not work it if the symbol is entered using the wrong encoding.

For best results:

- use UTF-8 encoding, or
- use only characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS, and other encoding methods, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients.



HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary based on the client's operating system or input language. If the client's encoding method cannot be predicted, you might only be able to match the parts of the request that are in English, as the values for English characters tend to be encoded identically, regardless of the encoding method.

If the FortiProxy is configured to use an encoding method other than UTF-8, the management computer's language may need to be changed, including the web browse and terminal emulator. If the FortiProxy is configured using non-ASCII characters, all the systems that interact with the FortiProxy must also support the same encoding method. If possible, the same encoding method should be used throughout the configuration to avoid needing to change the language settings on the management computer.

The GUI and CLI client normally interpret output as encoded using UTF-8. If they do not, configured items may not display correctly. Exceptions include items such as regular expression that may be configured using other encodings to match the encoding of HTTP requests that the FortiProxy receives.

To enter non-ASCII characters in a terminal emulator:

1. On the management computer, start the terminal client.
2. Configure the client to send and receive characters using UTF-8 encoding.
   Support for sending and receiving international characters varies by terminal client.
3. Log in to the FortiProxy.
4. At the command prompt, type your command and press *Enter*.
   Words that use encoded characters may need to be enclosed in single quotes (').
   Depending on your terminal client's language support, you may need to interpret the characters into character codes before pressing *Enter*. For example, you might need to enter: `edit '\743\601\613\743\601\652'`
5. The CLI displays the command and its output.

Screen paging

By default, the CLI will pause after displaying each page worth of text when a command has multiple pages of output. this can be useful when viewing lengthy outputs that might exceed the buffer of terminal emulator.

When the display pauses and shows `--More--`, you can:

- Press *Enter* to show the next line,
- Press *Q* to stop showing results and return to the command prompt,

- Press an arrow key, *Insert*, *Home*, *Delete*, *End*, *Page Up*, or *Page Down* to show the next few pages,
- Press any other key to show the next page, or
- Wait for about 30 seconds for the console to truncate the output and return to the command prompt.

When pausing the screen is disabled, press *Ctrl + C* to stop the output and log out of the FortiProxy.

To disable pausing the CLI output:

```
config system console
    set output standard
end
```

To enable pausing the CLI output:

```
config system console
    set output more
end
```

Changing the baud rate

The baud rate of the local console connection can be changed from its default value of 9600.

To change the baud rate:

```
config system console
    set baudrate {9600 | 19200 | 38400 | 57600 | 115200}
end
```

Editing the configuration file

The FortiProxy configuration file can be edited on an external host by backing up the configuration, editing the configuration file, and then restoring the configuration to the FortiProxy.

Editing the configuration file can save time is many changes need to be made, particularly if the plain text editor that you are using provides features such as batch changes.

To edit the configuration file:

1. Backup the configuration. See Configuration backups and reset on page 1006 for details.
2. Open the configuration file in a plain text editor that supports UNIX-style line endings.

3. Edit the file as needed.



Do not edit the first line of the configuration file.

This line contains information about the firmware version and FortiProxy model. If you change the model number, the FortiProxy will reject the configuration when you attempt to restore it.

4. Restore the modified configuration to the FortiProxy. See Configuration backups and reset on page 1006 for details.
The FortiProxy downloads the configuration file and checks that the model information is correct. If it is correct, the configuration file is loaded and each line is checked for errors. If a command is invalid, that command is ignored. If the configuration file is valid, the FortiProxy restarts and loads the downloaded configuration.

Command syntax

When entering a command, the CLI console requires that you use valid syntax and conform to expected input constraints. It rejects invalid commands. Indentation is used to indicate the levels of nested commands.

Each command line consists of a command word, usually followed by configuration data or a specific item that the command uses or affects.

Notation

Brackets, vertical bars, and spaces are used to denote valid syntax. Constraint notations, such as <address_ipv4>, indicate which data types or string patterns are acceptable value input.

All syntax uses the following conventions:

Angle brackets < >	Indicate a variable of the specified data type.
Curly brackets { }	Indicate that a variable or variables are mandatory.
Square brackets [ ]	Indicate that the variable or variables are optional. For example: `show system interface [<name_str>]` To show the settings for all interfaces, you can enter `show system interface` To show the settings for the Port1 interface, you can enter `show system interface port1`.
Vertical bar |	A vertical bar separates alternative, mutually exclusive options. For example: `set protocol {ftp | sftp}` You can enter either `set protocol ftp` or `set protocol sftp`.
Space	A space separates non-mutually exclusive options. For example:

```
   set allowaccess {ping https ssh snmp http fgfm radius-acct probe-response
        capwap ftm}
```

You can enter any of the following:

```
   set allowaccess ping
    set allowaccess https ping ssh
   set allowaccess http https snmp ssh ping
```

In most cases, to make changes to lists that contain options separated by spaces, you need to retype the entire list, including all the options that you want to apply and excluding all the options that you want to remove.

Optional values and ranges

Any field that is optional will use square-brackets. The overall config command will still be valid whether or not the option is configured.

Square-brackets can be used is to show that multiple options can be set, even intermixed with ranges. The following example shows a field that can be set to either a specific value or range, or multiple instances:

```
config firewall service custom
    set iprange <range1> [<range2> <range3> ...]
end
```

next

The next command is used to maintain a hierarchy and flow to CLI commands. It is at the same indentation level as the preceding edit command, to mark where a table entry finishes.

The following example shows the next command used in the subcommand entries:

```
config dlp filepattern
    edit <1>
        set name <name>
        set comment [comment]
        config entries
            edit <2>
                set filter-type {pattern | type}
            next
```

After configuring table entry <2> then entering next, the <2> table entry is saved and the console returns to the entries prompt:

```
FGT60E1Q23456789 (entries) #
```

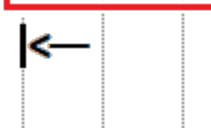
You can now create more table entries as needed, or enter end to save the table and return to the filepattern table element prompt.

end

The end command is used to maintain a hierarchy and flow to CLI commands.

The following example shows the same command and subcommand as the next command example, except end has been entered instead of next after the subcommand:

```
config dlp filepattern
    edit <1>
        set name <name>
        set comment [comment]
        config entries
            edit <2>
                set filter-type {pattern | type}
    end
```



Entering end will save the <2> table entry and the table, and exit the entries subcommand entirely. The console returns to the filepattern table element prompt:

```
[redacted]6789 (1) #
```

Subcommands

Subcommands are available from within the scope of some commands. When you enter a subcommand level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

Applicable subcommands are available until you exit the command, or descend an additional level into another subcommand. Subcommand scope is indicated by indentation.

For example, the edit subcommand is only available in commands that affects tables, and the next subcommand is available only in the edit subcommand:

```
config system interface
    edit port1
        set status up
    next
end
```

The available subcommands vary by command. From a command prompt under the config command, subcommands that affect tables and fields could be available.

Table subcommands

edit <table_row>	Create or edit a table value.
	In objects such as security policies, `<table_row>` is a sequence number. To create a new table entry without accidentally editing an existing entry, enter `edit 0`. The CLI will confirm that creation of entry 0, but will assign the next unused number when the entry is saved after entering `end` or `next`.
	For example, to create a new firewall policy, enter the following commands:
	`config firewall policy`
	`  edit 0`
	`  ...`
	`  next`
	`end`
	To edit an existing policy, enter the following commands:
	`config firewall policy`
	`  edit 27`
	`  ...`
	`  next`
	`end`
	The `edit` subcommand changes the command prompt to the name of the table value that is being edited, such as `(27) #`.

delete <table_row>	Delete a table value.
	For example, to delete firewall policy 27, enter the following commands:
	`config firewall policy`
	`  delete 27`
	`end`

purge	Clear all table values. The `purge` command cannot be undone. To restore purged table values, the configuration must be restored from a backup.

move	Move an ordered table value.
	In the firewall policy table, this is equivalent to dragging a policy into a new position. It does not change the policy's ID number.
	For example, to move policy 27 to policy 30, enter the following commands:
	`config firewall policy`
	`  move 27 to 30`
	`end`

	The `move` subcommand is only available in tables where the order of the table entries matters.

clone <table_row> to <table_row>	Make a clone of a table entry.
	For example, to create firewall policy 30 as a clone of policy 27, enter the following commands:
	`config firewall policy`
	`  clone 27 to 30`
	`end`
	The `clone` subcommand may not be available for all tables.

rename <table_row> to <table_row>	Rename a table entry.
	For example to rename an administrator from Fry to Leela, enter the following commands:
	`config system admin`
	`  rename Fry to Leela`
	`end`
	The `rename` subcommand is only available in tables where the entries can be renamed.

get	List the current table entries.
	For example, to view the existing firewall policy table entries, enter the following commands:
	`config firewall policy`
	`  get`

show	Show the configuration. Only table entries that are not set to default values are shown.
end	Save the configuration and exit the current `config` command.



Purging the `system interface` or `system admin` tables does not reset default table values. This can result in being unable to connect to or log in to the FortiProxy, requiring the FortiProxy to be formatted and restored.

Field subcommands

set <field> <value>	Modify the value of a field. For example, the command `set fsso enable` sets the `fsso` field to the value `enable`.
unset	Set the field to its default value.
select	Clear all of the options except for those specified.

	For example, if a group contains members A, B, C, and D, to remove all members except for B, use the command `select member B`.
unselect	Remove an option from an existing list. For example, if a group contains members A, B, C, and D, to remove only member B, use the command `unselect member B`.
append	Add an option to an existing multi-option table value.
clear	Clear all the options from a multi-option table value.
get	List the configuration of the current table entry, including default and customized values.
show	Show the configuration. Only values that are not set to default values are shown.
next	Save changes to the table entry and exit the `edit` command so that you can configure the next table entry.
abort	Exit the command without saving.
end	Save the configuration and exit the current `config` command.

Permissions

Administrator (or access) profiles control what CLI commands an administrator can access by assigning read, write, or no access to each area of FortiProxy. For information, see Admin Profiles on page 872.

Read access is required to view configurations. Write access is required to make configuration changes. Depending on your account's profile, you may not have access to all CLI commands. To have access to all CLI commands, an administrator account with the *super_admin* profile must be used, such as the *admin* account.

Accounts assigned the *super_admin* profile are similar to the root administrator account. They have full permission to view and change all FortiProxy configuration options, including viewing and changing other administrator accounts.

To increase account security, set strong passwords for all administrator accounts and change the passwords regularly. See Settings on page 879 for more information.

CLI error codes

CLI error codes are shown in the command line if the command execution fails. The message includes a summary, followed by `Command fail. Return code -X`, where `-X` is the error code. For example:

```
# set test
Command parse error before ‘test’
Command fail. Return code -61
```

The following table lists common error codes and their descriptions.

Return Code	Description
1	Generic CLI syntax error
-1	Invalid length of value.
-4	Maximum number of entries has been reached.
-5	A duplicate entry already exists.
-8	Invalid IP Address.
-37	Permission denied.
-56	Empty values are not allowed.
-61	Input not as expected.
-160	CFG_ER_GENERIC (common generic configuration error)
-553	Name conflicts with an interface, VDOM, switch-interface, zone, or interface name used for hardware switch interfaces.
-651	Input value is invalid.

Configuration and management

FortiProxy can be managed through the graphical user interface (GUI) or the Command Line Interface (CLI) as well as other tools.

For	Use
Direct or individual configuration	FortiProxy GUI and CLI. See Using the GUI on page 25 and Using the CLI on page 37.
Mass provisioning, management, and orchestration	FortiManager and FortiGate Cloud. See the FortiManager page and the FortiGate Cloud page on the Fortinet Document Library.
Automation	REST API accessible through Fortinet Developer Network (FNDN). See Accessing Fortinet Developer Network on page 54 and Create or edit a REST API administrator on page 870.

Accessing Fortinet Developer Network

The Fortinet Developer Network (FNDN) is a subscription-based community that helps administrators enhance and increase the effectiveness of Fortinet products. Administrators can access the FortiAPI forum in FNDN to help create applications that interact with Fortinet products, such as custom web portals, automated deployment and provisioning systems, and scripted tasks. FNDN makes it easy for

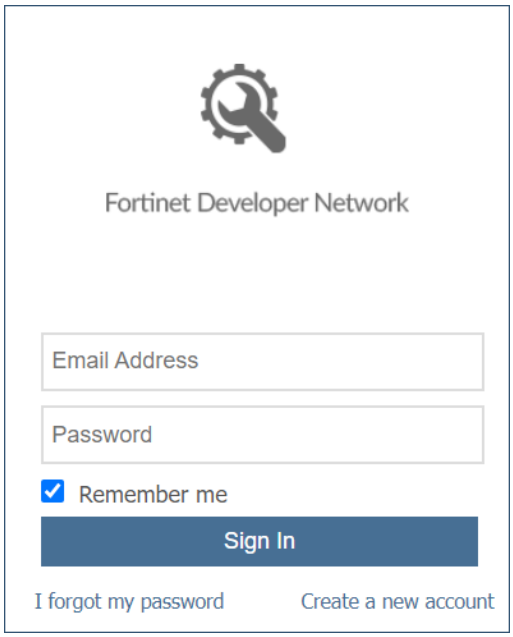
administrators and Fortinet professionals to interact, share sample code, and upload their own tools. The FortiProxy REST API documentation is available within the FortiAPI forum.

All FNDN users must be sponsored by two Fortinet employees. The sponsors must be able to confirm the user's identity and need for access. Approvals from both sponsors are required before access is granted to new users. The sponsors' email addresses are required to create a new FNDN account.

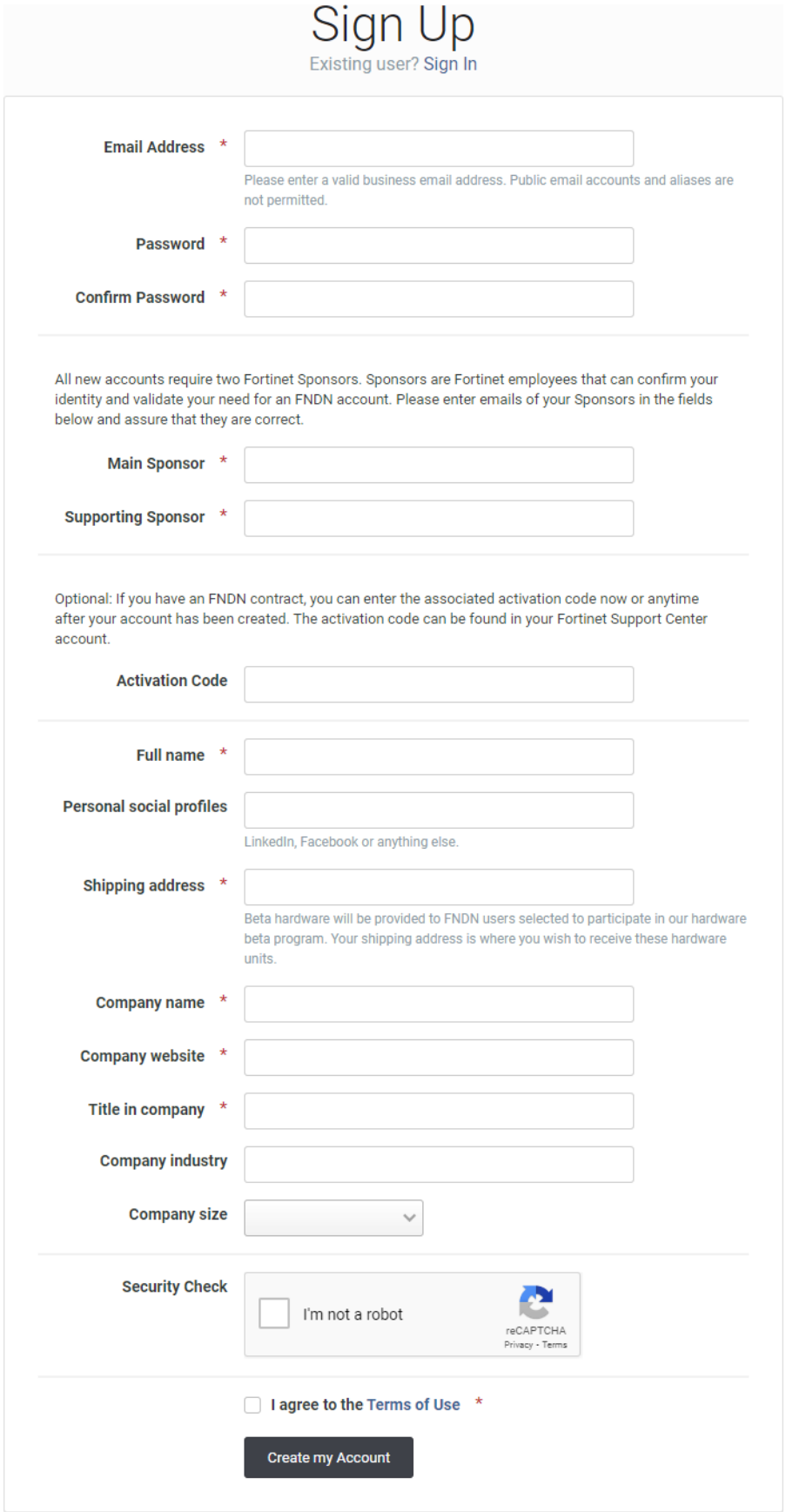
Basic and licensed access options are available. Refer to the Fortinet Developer Network data sheet for more information.

To create an FNDN account:

1. Obtain sponsorship from two Fortinet employees.
2. Go to the FNDN website, https://fndn.fortinet.net/. The log in page appears.



3. Click *Create a new account*. The *Sign Up* page appears.
4. Enter the information in the form fields and agree to the *Terms of Use*.


Sign Up
Existing user? Sign In
Email Address *
Please enter a valid business email address. Public email accounts and aliases are not permitted.
Password *
Confirm Password *
All new accounts require two Fortinet Sponsors. Sponsors are Fortinet employees that can confirm your identity and validate your need for an FNDN account. Please enter emails of your Sponsors in the fields below and assure that they are correct.
Main Sponsor *
Supporting Sponsor *
Optional: If you have an FNDN contract, you can enter the associated activation code now or anytime after your account has been created. The activation code can be found in your Fortinet Support Center account.
Activation Code
Full name *
Personal social profiles
LinkedIn, Facebook or anything else.
Shipping address *
Beta hardware will be provided to FNDN users selected to participate in our hardware beta program. Your shipping address is where you wish to receive these hardware units.
Company name *
Company website *
Title in company *
Company industry
Company size
Security Check
I'm not a robot
reCAPTCHA
Privacy - Terms
I agree to the Terms of Use *
Create my Account

5. Click *Create my Account*.
   New accounts are reviewed and approved by an FNDN administrator. After both sponsors approve the request, an FNDN administrator reviews the request and approves account access in around one business day if all requirements are met.

Product registration with FortiCare

It is recommended to register your product with Fortinet. A FortiCare/FortiCloud account with Fortinet Technical Support (https://support.fortinet.com) is required to register products. This section describes how to register the product and includes information about other tasks performed with a FortiCare/FortiCloud account.

- FortiCare and FortiGate Cloud login on page 57
- FortiCare Register button on page 61
- Transfer a device to another FortiCloud account on page 62
- Deregistering a FortiProxy on page 65

FortiCare and FortiGate Cloud login

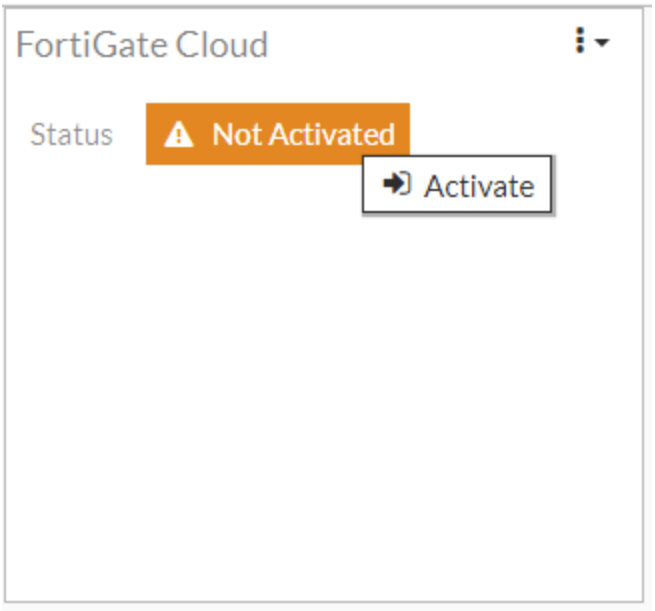
With FortiCloud, FortiProxy supports a unified login to FortiCare and FortiGate Cloud. The FortiGate Cloud setup is a subset of the FortiCare setup.

- If the FortiProxy is not registered, activating FortiGate Cloud will force you to register with FortiCare.
- If a FortiProxy is registered in FortiCare using a FortiCloud account, then only that FortiCloud account can be used to activate FortiGate Cloud.
- If a different FortiCloud account was already used to activate FortiGate Cloud, then a notification asking you to migrate to FortiCloud is shown in the GUI after upgrading FortiProxy.

The CLI can be used to activate FortiGate Cloud without registration, or with a different FortiCloud account.

To activate FortiGate Cloud and register with FortiCare at the same time:

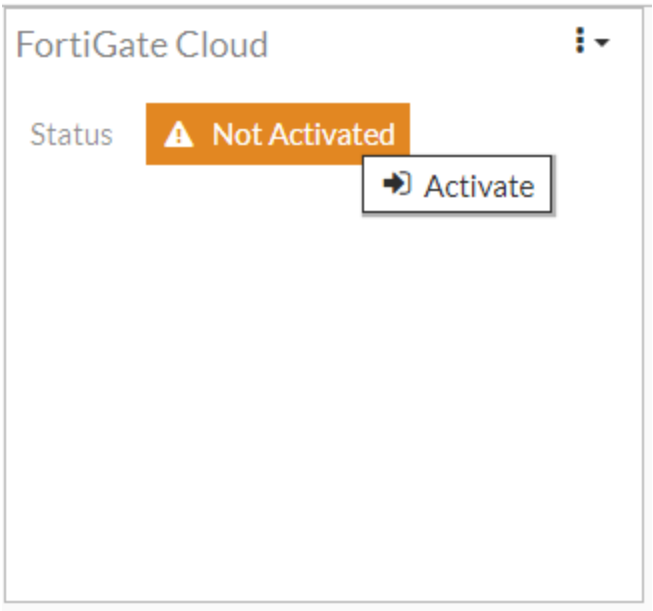
1. Go to *Dashboard* > *Status*.
2. In the FortiGate Cloud widget, click *Not Activated* > *Activate*.



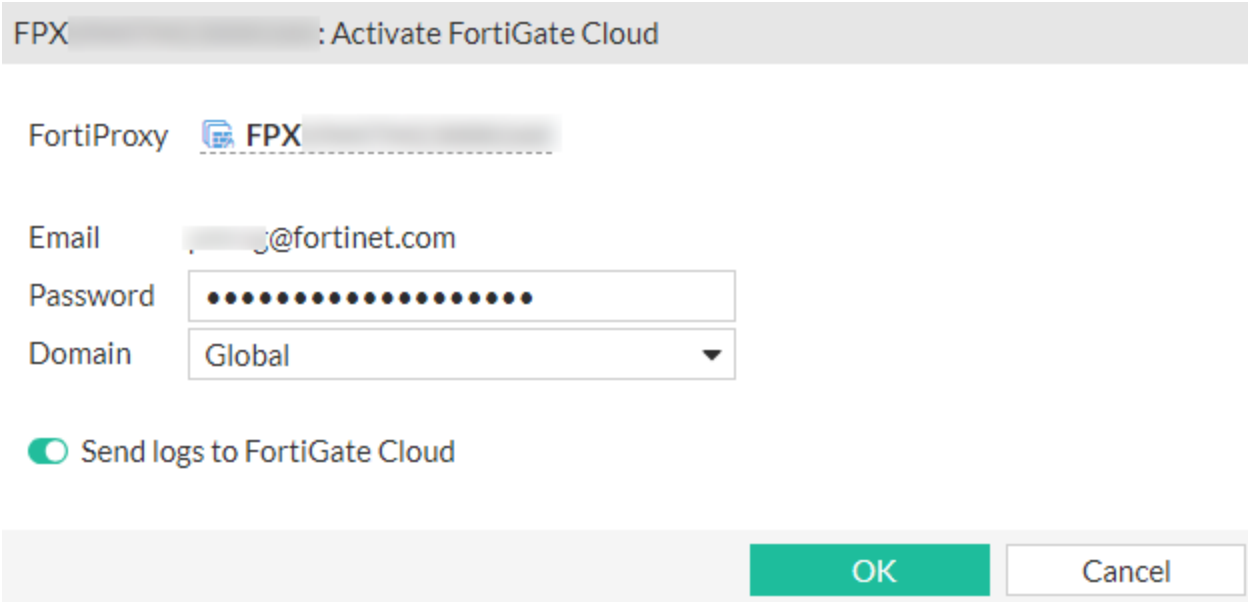
   You must register with FortiCare before activating FortiGate Cloud.
3. Enter your FortiCare *Email* address and *Password*.
4. Select your *Country/Region*, *Reseller*, and *End-user type*.
5. Enable *Sign in to FortiGate Cloud using the same account*.
6. Click *OK*.

To activate FortiGate Cloud on an already registered FortiProxy:

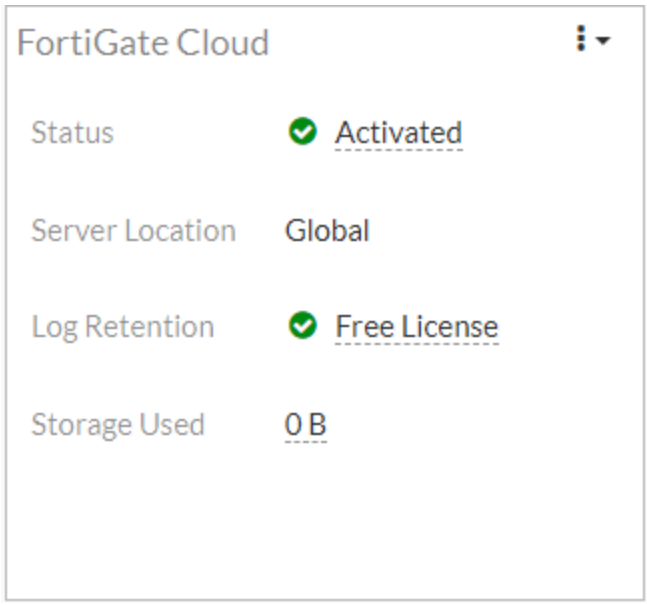
1. Go to *Dashboard* > *Status*.
2. In the *FortiGate Cloud* widget, click *Not Activated* > *Activate*.



3. Enter the password for the account that was used to register the FortiProxy.

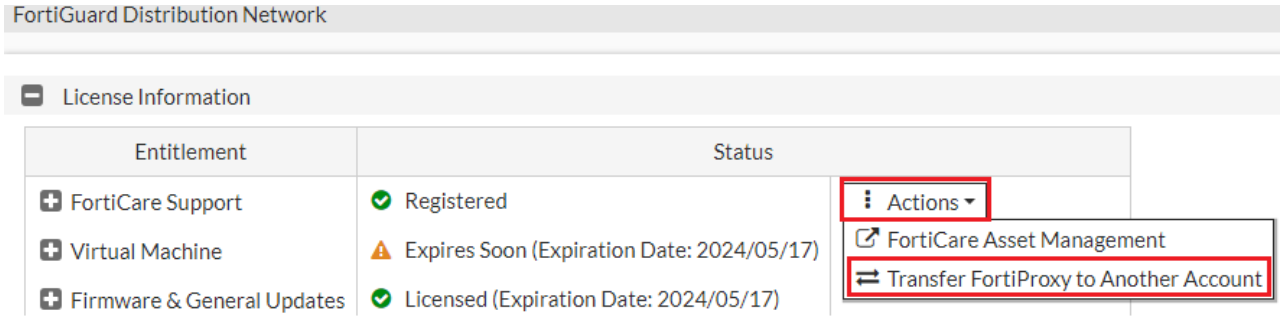


4. Click *OK*.
   The *FortiGate Cloud* widget now shows the activated FortiCloud account.

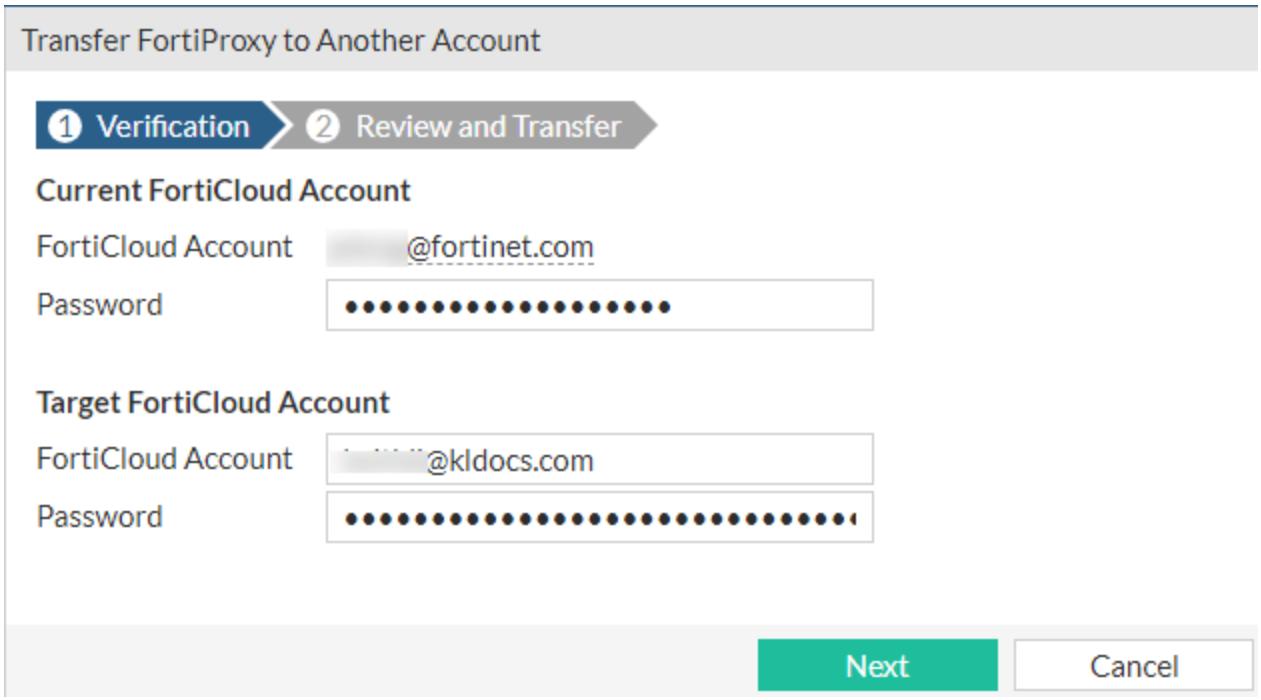


To migrate from the activated FortiGate Cloud account to the registered FortiCloud account:

1. Go to *System* > *FortiGuard*.
2. In the *FortiCare Support* row, click *Actions* > *Transfer FortiProxy to Another Account*.



3. Enter the *Password* of the current FortiCloud account.



4. Enter the target *FortiCloud Account* name and *Password*, then click *Next*.
5. Review the information in the *From* and *To* fields, then click *Transfer*.

To activate FortiGate Cloud using an account that is not used for registration:

1. Enter the following with the credentials for the account being used to activate FortiGate Cloud:

```
# execute fortiguard-log login <account_id> <password>
```

2. Check the account type:

```
# diagnose fdsm contract-controller-update
Protocol=2.0|Response=202|Firmware=FAZ-4K-FW-2.50-
100|SerialNumber=FAMS000000000000|Persistent=false|ResponseItem=HomeServer:172.16.95.151:443*A
lterServer:172.16.95.151:443*Contract:20200408*NextRequest:86400*UploadConfig:False*Management
Mode:Local*ManagementID:737941253*AccountType:multitenancy

Result=Success
```

A FortiCloud account that is not used for the support portal account cannot be used to register FortiProxy. Attempting to activate FortiGate Cloud with this type of account will fail.

FortiCare Register button

The FortiCare *Register* button is displayed in the GUI on various Fabric and device related pages and widgets.

- To access the *Register* button on a topology page, click on or hover over the FortiProxy device:
- To access the button from the *System > Fabric Management* or *System > HA* page, right-click on the device name.

Clicking *Register* opens the *Device Registration* pane. If a device is already registered, the pane still opens and displays the device information.

Primary and secondary HA members can be registered to FortiCare at the same time from the primary unit by using the *Register* button. The secondary unit will register through the HA proxy.

In this example, a HA member is registered from the *Physical Topology* page.

To register a HA member to FortiCare:

1. On the primary unit, go to *Security Fabric > Physical Topology*, or expand the *Security Fabric* widget on the *Status* dashboard.
2. Hover over the HA member and click *Register*. The *Device Registration* pane opens.
3. Select the device and click *Register*.
4. Enter the required FortiCloud account information (password, country or region, reseller) and click *Submit*.
5. Once the registration is complete, click *Close*.

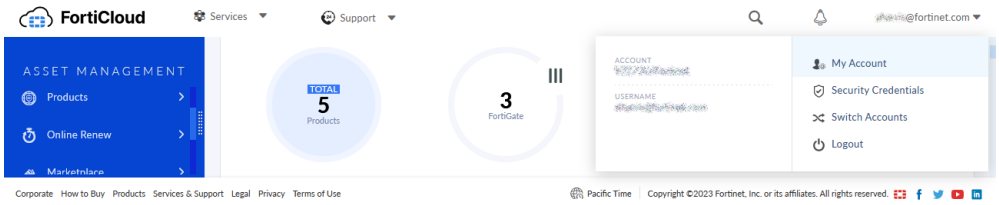
Transfer a device to another FortiCloud account

Master account users can transfer a device from one FortiCloud/FortiCare account to another. Users can transfer a device up to three times within a twelve-month time period. If more transfers are required within the twelve-month time period, contact Technical Support to request the transfer.

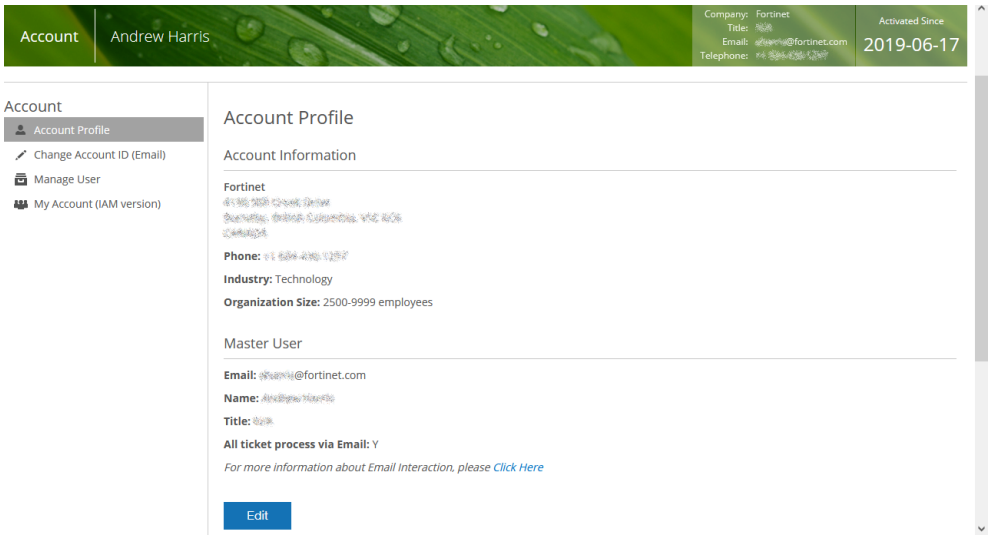
Requirements:

To transfer an account, you must:

- Have access to the FortiProxy, as well as both the FortiCloud and FortiCare accounts.
- Be a master account user.
  To verify if you are the master account user, log in to support.fortinet.com. Click the username, then select *My Account*.



The *Account Profile* page opens.

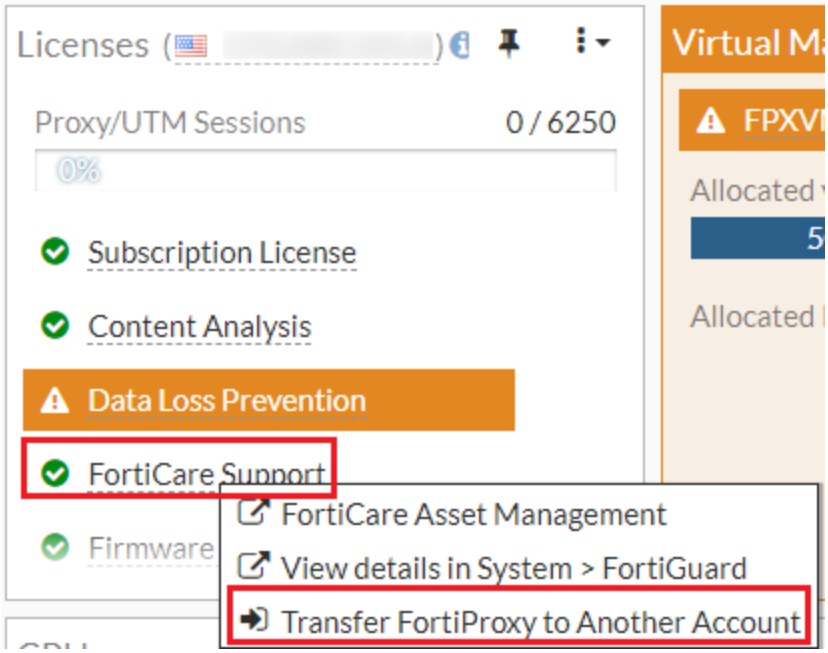


To transfer an account in the GUI:

1. Go to *Dashboard* > *Status*.
2. In the *Licenses* widget, click the *FortiCare Support* link, then click *Transfer FortiProxy to Another Account*.

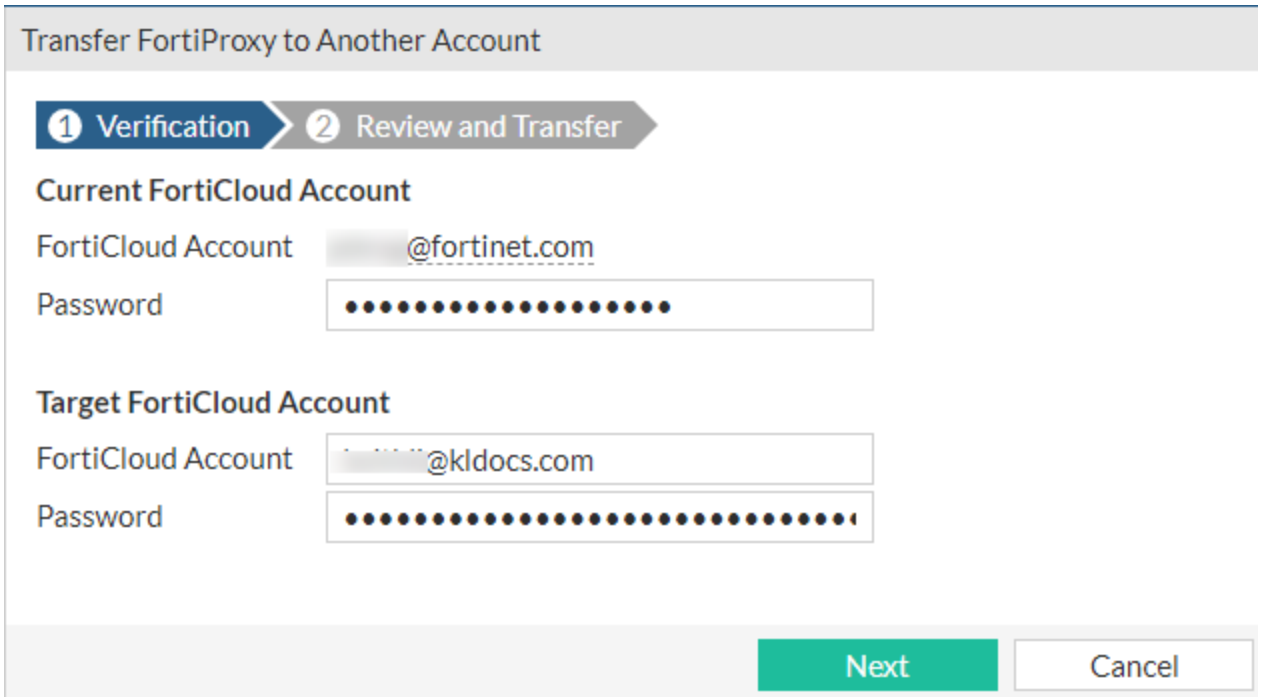


You can also transfer an account from *System* > *FortiGuard*.

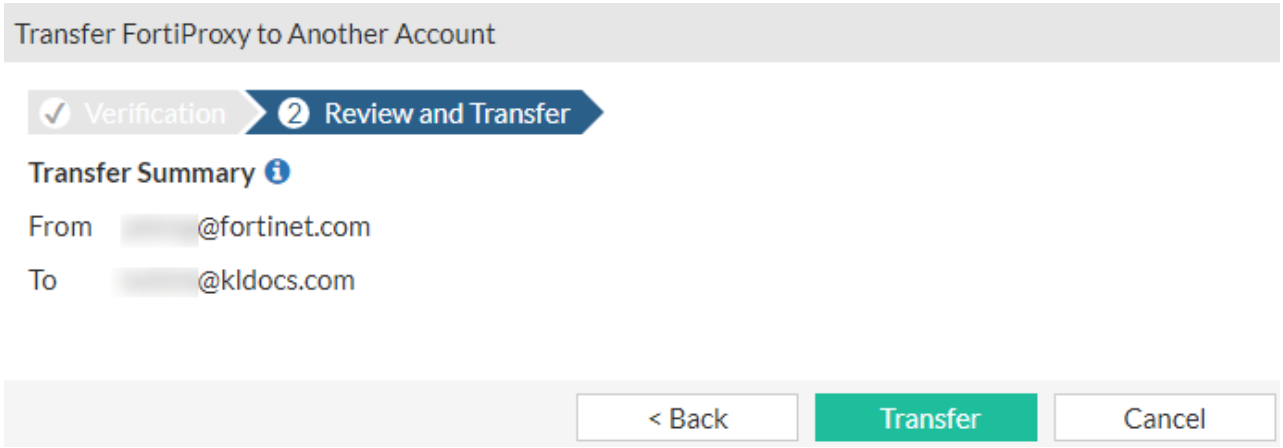


3. In the *Current FortiCloud Account* fields, enter the username and password for the current account. In the *Target FortiCloud Account* fields, enter the new username and password.

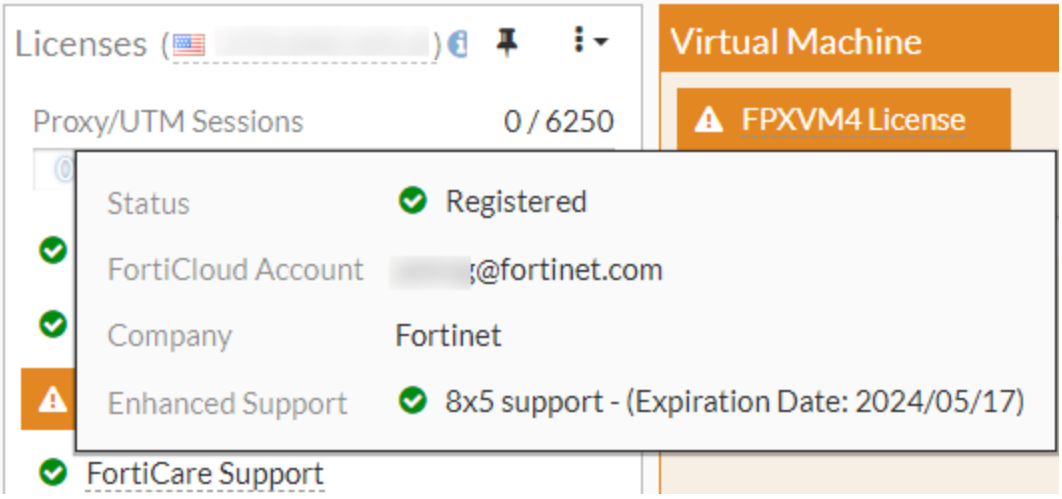
4. Click *Next*.



5. Review the information, then click *Transfer*.



After the transfer is complete, the new the FortiCloud account is displayed in the *Licenses* widget.



Deregistering a FortiProxy

An administrator can deregister a FortiProxy if the device has been registered for three or more years, using the GUI or CLI, without having to contact FortiCare administration. After the device is deregistered, all associated contracts are also deregistered, and all of the administrator's information is wiped.

To deregister the FortiProxy in the GUI:

1. Go to *System* > *FortiGuard* and in the *FortiCare Support* row select *Actions* > *Deregister FortiProxy*.
   The FortiCare Deregistration pane opens.
2. Enter your password then click *Next*.
3. Confirm the FortiProxy deregistration then click *Submit*.
   If the FortiProxy has been registered for less then three years, the deregistration will fail.

To deregister the FortiProxy in the CLI:

```
# diagnose forticare direct-registration product-deregister <accountID> <password>
```

If the FortiProxy has been registered for less then three years, the deregistration will fail:

```
forticare_product_deregister:1335: Failed to get response (rc = 0, http_code = 403)
Unit deregistration unsuccessful.
```

FortiProxy models

Not all FortiProxy models have the same features. Additionally, a particular feature may be available only through the CLI on some models, while that same feature may be viewed in the GUI on other models. If you believe your FortiProxy model supports a feature that does not appear in the GUI, go to *System > Feature Visibility* and confirm that the feature is enabled. For more information, see Feature Visibility on page 970.

For further information about features that vary by model, refer to your model's QuickStart Guide.

Supported protocols

FortiProxy supports the following protocols:

Application layer security	VPN
• SSH • FTP/FTPS/FTPoHTTP/FTPoHTTPConnect • SMTP/SMTPS • IMAP/IMAPS • POP3/POP3S • CIFS/SMB • MAPI/MAPIoRPC/MAPIoHTTPS • DNS • ICAP/WCCP • SCP/SFTP	• IPsec • SSL

Deployments

This section describes the following:

- Transparent and NAT/route modes on page 67
- Web proxy on page 68
- WAN optimization on page 73
- Web caching on page 78
- WCCP on page 81

Transparent and NAT/route modes

A FortiProxy unit can operate in either NAT/route mode or transparent mode.

In NAT/route mode, a FortiProxy unit is installed as a gateway or router between multiple networks, such as a private network and the internet. One function of NAT/route mode is to allow the FortiProxy to hide the IP addresses on the private network using NAT.

The FortiProxy operates in layer 2 to forward traffic between network devices such as routers, firewalls, and switches. For example. it can be installed inline between a router and a switch to perform security scanning without changing the network topology or modifying the IP addresses.

Transparent mode is used primarily when there is a need to increase network protection but changing the configuration of the network itself is impractical. When you add a FortiProxy that is in transparent mode to a network, it only needs to be provided with a management IP address in order to access the device. It is recommended to configure a dedicated management interface when out-of-band management is required in transparent mode. See Transparent mode management on page 898.



Changing the operation mode removes most configurations, including any policies and address objects. To keep your configuration, back it up before changing the mode.

To back up your configuration in the GUI:

1. Click on the user name and select *Configuration* > *Backup*.
2. Select where to store the backup file, *Local PC* or *USB Disk* (if available).
3. Optionally, enable *Encryption* and enter a password.
4. Click *OK*.

To back up your configuration in the CLI:

```
# execute backup {config | full-config} {flash | ftp | management-station |
      sftp | tftp | usb | usb-mode} ...
```

To change from NAT/route mode to transparent mode:

```
config system settings
    set opmode transparent
    set manageip <IP_address>
    set gateway <gateway_address>
end
```

The gateway setting is optional, but after the operation mode has been changed, the gateway configuration is in the static router settings:

```
config router static
    edit <seq-num>
        set gateway <IP_address>
    next
end
```

To change from transparent mode to NAT/route mode:

```
config system settings
    set opmode nat
    set ip <IP_address>
    set device <interface>
    set gateway <gateway_address>
end
```

The IP and device settings are mandatory, and the gateway setting is optional. After the operation mode is changed, the IP address configuration is in the interface settings and the gateway and device configurations are in the static router settings:

```
config system interface
    edit <interface>
        set ip <IP_address>
    next
end
```

```
config router static
    edit <seq-num>
        set gateway <IP_address>
        device <interface>
    next
end
```

Web proxy

Web proxy covers both transparent proxy and explicit proxy.

This section covers the following topics:

- Web proxy concepts
- Explicit web proxy concepts
- Transparent web proxy concepts
- Explicit web proxy topologies

Web proxy concepts

This section covers the following concepts that apply to both transparent proxy and explicit proxy:

- Proxy policy
- Proxy authentication
- Proxy addresses
- Web proxy firewall services and service groups
- Learn client IP

Proxy policy

Any time a security profile that uses a proxy is enabled, you need to configure the proxy options. Certain inspections defined in security profiles require that the traffic be held in proxy while the inspection is carried out, and the proxy options define how the traffic will be processed and to what level the traffic will be processed. In the same way that there can be multiple security profiles of a single type, there can also be a number of unique proxy option profiles so that, as the requirements for a policy differ from one policy to the next, you can also configure a different proxy option profile for each individual policy or you can use one profile repeatedly.

The proxy options support the following protocols:

- HTTP
- FTP
- CIFS
- SSH

The configuration for each of these protocols is handled separately.

Proxy authentication

Authentication is separated from authorization for user-based policies. You can add authentication to proxy policies to control access to the policy and to identify users and apply different UTM features to different users. The described authentication methodology works with explicit web proxy and transparent proxy.

Authentication of web proxy sessions uses HTTP basic and digest authentication as described in RFC 2617 (HTTP Authentication: Basic and Digest Access Authentication) and prompts the user for credentials from the browser allowing individual users to be identified by their web browser instead of IP address. HTTP authentication allows the FortiProxy unit to distinguish between multiple users accessing services from a shared IP address.

The authentication rule table defines how to identify user-ID. It uses the match factors:

- Protocol
- Source address

For one address and protocol, there is only one authentication rule. It is possible to configure multiple authentication methods for one address. The client browser will chose one authentication method from the authentication methods list, but you cannot control which authentication method will be chosen by the browser.

Proxy addresses

Proxy addresses are used for both transparent web proxy and explicit web proxy.

In some respects, they can be like FQDN addresses in that they refer to an alphanumeric string that is assigned to an IP address, but then they go an additional level of granularity by using additional information and criteria to further specify locations or types of traffic within the web site itself.

Proxy address group

In the same way that IPv4 and IPv6 addresses can only be grouped together, proxy addresses can only be grouped with other proxy addresses. Unlike other address groups, the proxy address groups are further divided into source address groups and destination address groups.

Web proxy firewall services and service groups

Web proxy services are similar to standard firewall services. You can configure web proxy services to define one or more protocols and port numbers that are associated with each web proxy service. Web proxy services can also be grouped into web proxy service groups.

One way in which web proxy services differ from firewall services is the protocol type you can select. The following protocol types are available:

- ALL
- CONNECT
- FTP
- HTTP
- SOCKS-TCP
- SOCKS-UDP

Learn client IP

If there is another NATing device between the FortiProxy unit and the client (browser), this feature can be used to identify the real client in spite of the address translation. Knowing the actual client is imperative in cases where authorization is taking place.

Explicit web proxy concepts

The following is information that is specific to explicit proxy. Any information that is common to web proxy in general is covered in Web proxy concepts on page 69.

You can use the FortiProxy explicit web proxy to enable explicit proxying of IPv4 and IPv6 HTTP and HTTPS traffic on one or more FortiProxy interfaces. The explicit web proxy also supports proxying FTP sessions from a web browser and proxy auto-config (PAC) to provide automatic proxy configurations for explicit web proxy users. From the CLI you can also configure the explicit web proxy to support SOCKS sessions from a web browser. The explicit web and FTP proxies can be operating at the same time on the same or on different FortiProxy interfaces.

In most cases, you would configure the explicit web proxy for users on a network by enabling the explicit web proxy on the FortiProxy interface connected to that network. Users on the network would configure their web browsers to use a proxy server for HTTP and HTTPS, FTP, or SOCKS and set the proxy server IP address to the IP address of the FortiProxy interface connected to their network. Users could also enter the PAC URL into their web browser PAC configuration to automate their web proxy configuration using a PAC file stored on the FortiProxy unit.



Enabling the explicit web proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

If the FortiProxy unit is operating in transparent mode, users would configure their browsers to use a proxy server with the FortiProxy management IP address.

The web proxy receives web browser sessions to be proxied at FortiProxy interfaces with the explicit web proxy enabled. The web proxy uses FortiProxy routing to route sessions through the FortiProxy unit to a destination interface. Before a session leaves the exiting interface, the explicit web proxy changes the source addresses of the session packets to the IP address of the exiting interface. When the FortiProxy unit is operating in transparent mode, the explicit web proxy changes the source addresses to the management IP address. You can configure the explicit web proxy to keep the original client IP address.

Example explicit web proxy topology



To allow all explicit web proxy traffic to pass through the FortiProxy unit you can set the explicit web proxy default firewall policy action to *ACCEPT*. However, in most cases you would want to use security policies to control explicit web proxy traffic and apply security features such as access control/authentication, virus scanning, web filtering, application control, and traffic logging. You can

do this by keeping the default explicit web proxy security policy action to *DENY* and then adding web-proxy security policies.

You can also change the explicit web proxy default security policy action to accept and add explicit web proxy security policies. If you do this, sessions that match web-proxy security policies are processed according to the security policy settings. Connections to the explicit web proxy that do not match a web-proxy security policy are allowed with no restrictions or additional security processing. **NOTE:** This configuration is not recommended and is not a best practice.

The explicit web-proxy can accept VIP addresses for destination addresses. If an external IP matches a VIP policy, the IP is changed to the mapped-IP of the VIP.

Web-proxy policies can selectively accept or deny traffic, apply authentication, enable traffic logging, and use security profiles to apply virus scanning, web filtering, IPS, application control, DLP, and SSL/SSH inspection to explicit web proxy traffic.

You cannot configure IPsec or traffic shaping for explicit web proxy traffic. Web proxy policies can only include firewall addresses not assigned to a FortiProxy unit interface or with interface set to *any*. (On the web-based manager, you must set the interface to *any*. In the CLI you must unset the associated interface.)

Authentication of explicit web proxy sessions uses HTTP authentication and can be based on the user's source IP address or on cookies from the user's web browser.

To use the explicit web proxy, you must add the IP address of a FortiProxy interface on which the explicit web proxy is enabled and the explicit web proxy port number (default 8080) to the proxy configuration settings of their web browsers.

You can also enable web caching for explicit web proxy sessions.

Transparent web proxy concepts

In addition to the explicit web proxy, the FortiProxy unit supports a transparent web proxy. While it does not have as many features as explicit web proxy, the transparent proxy has the advantage that nothing needs to be done on the user's system to forward supported web traffic over to the proxy. There is no need to reconfigure the browser or publish a PAC file. Everything is transparent to the end user, hence the name. This makes it easier to incorporate new users into a proxy deployment.

You can use the transparent proxy to apply web authentication to HTTP traffic accepted by a firewall policy.

Normal FortiProxy authentication is IP-address based. Users are authenticated according to their IP address and access is allowed or denied based on this IP address. On networks where authentication based on IP address will not work, you can use the transparent web proxy to apply web authentication that is based on the user's browser and not on their IP address. This authentication method allows you to identify individual users even if multiple users on your network are connecting to the FortiProxy unit from the same IP address.

Explicit web proxy topologies

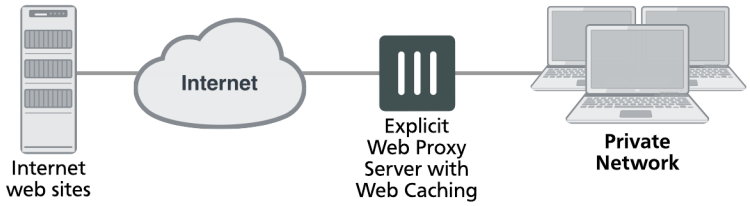
You can configure a FortiProxy unit to be an explicit web proxy server for Internet web browsing of IPv4 and IPv6 web traffic. To use the explicit web proxy, users must add the IP address of the FortiProxy interface configured for the explicit web proxy to their web browser proxy configuration.

Explicit web proxy topology



If the FortiProxy unit supports web caching, you can also add web caching to the security policy that accepts explicit web proxy sessions. The FortiProxy unit then caches Internet web pages on a hard disk to improve web browsing performance.

Explicit web proxy with web caching topology



WAN optimization

FortiProxy WAN optimization consists of a number of techniques that you can apply to improve the efficiency of communication across your WAN. These techniques include protocol optimization, byte caching, web caching, SSL offloading, and secure tunneling. Protocol optimization can improve the efficiency of traffic that uses the CIFS, FTP, HTTP, or MAPI protocol, as well as general TCP traffic. Byte caching caches files and other data on FortiProxy units to reduce the amount of data transmitted across the WAN. Web caching stores web pages o FortiProxy units to reduce latency and delays between the WAN and web servers. SSL offloading offloads SSL decryption and encryption from web servers onto FortiProxy SSL acceleration hardware. Secure tunneling secures traffic as it crosses the WAN.

You can apply different combinations of these WAN optimization techniques to a single traffic stream depending on the traffic type. For example, you can apply byte caching and secure tunneling to any TCP traffic. For HTTP and HTTPS traffic, you can also apply protocol optimization and web caching.

You can configure a FortiProxy unit to be an explicit web proxy server for both IPv4 and IPv6 traffic and an explicit FTP proxy server. Users on your internal network can browse the Internet through the explicit web proxy server or connect to FTP servers through the explicit FTP proxy server. You can also configure these proxies to protect access to web or FTP servers behind the FortiProxy unit using a reverse proxy configuration.

Web caching can be applied to any HTTP or HTTPS traffic, this includes normal traffic accepted by a security policy, explicit web proxy traffic, and WAN optimization traffic.

You can also configure a FortiProxy unit to operate as a Web Cache Communication Protocol (WCCP) client or server. WCCP provides the ability to offload web caching to one or more redundant web caching servers.

FortiProxy units can also apply security profiles to traffic as part of a WAN optimization, explicit web proxy, explicit FTP proxy, web cache and WCCP configuration. Security policies that include any of these options can also include settings to apply all forms of security profiles supported by your FortiProxy unit.

To check how much memory has been allocated for the WAN-optimization daemon (WAD), use the `diagnose wad memory track [<mem-id>]` command.

WAN optimization supports TLS 1.3.

WAN optimization transparent mode

WAN optimization is transparent to users. This means that with WAN optimization in place, clients connect to servers in the same way as they would without WAN optimization. However, servers receiving packets after WAN optimization “see” different source addresses depending on whether or not transparent mode is selected for WAN optimization. If transparent mode is selected, WAN optimization keeps the original source address of the packets, so servers appear to receive traffic directly from clients. Routing on the server network should be configured to route traffic with client source IP addresses from the server-side FortiProxy unit to the server and back to the server-side FortiProxy unit.



Some protocols, for example CIFS, may not function as expected if transparent mode is not selected. In most cases, for CIFS WAN optimization you should select transparent mode and make sure the server network can route traffic as described to support transparent mode.

If transparent mode is not selected, the source address of the packets received by servers is changed to the address of the server-side FortiProxy unit interface that sends the packets to the servers. So servers appear to receive packets from the server-side FortiProxy unit. Routing on the server network is simpler in this case because client addresses are not involved. All traffic appears to come from the server-side FortiProxy unit and not from individual clients.

Do not confuse WAN optimization transparent mode with FortiProxy transparent mode. WAN optimization transparent mode is similar to source NAT. FortiProxy transparent mode is a system setting that controls how the FortiProxy unit processes traffic. See Transparent and NAT/route modes on page 67.

WAN optimization topologies

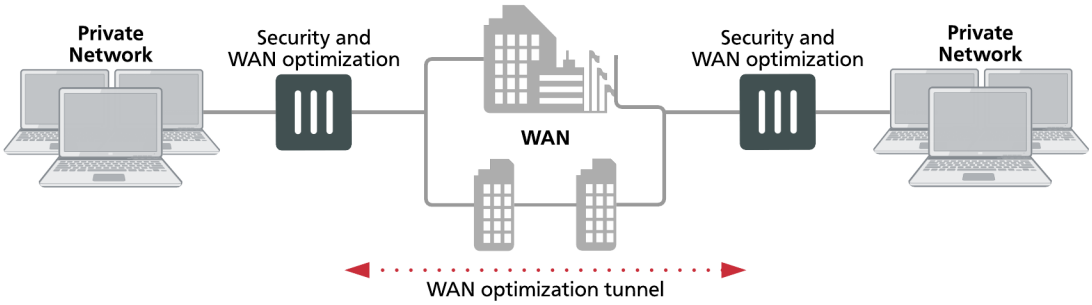
The WAN optimization topologies are described in the following sections:

- Basic WAN optimization topology
- Out-of-path WAN optimization topology
- Topology for multiple networks
- WAN optimization with web caching

Basic WAN optimization topology

The basic FortiProxy WAN optimization topology consists of two FortiProxy units operating as WAN optimization peers intercepting and optimizing traffic crossing the WAN between the private networks.

Security device and WAN optimization topology



FortiProxy units can be deployed as security devices that protect private networks connected to the WAN and also perform WAN optimization. In this configuration, the FortiProxy units are configured as typical security devices for the private networks and are also configured for WAN optimization. The WAN optimization configuration intercepts traffic to be optimized as it passes through the FortiProxy unit and uses a WAN optimization tunnel with another FortiProxy unit to optimize the traffic that crosses the WAN.

You can also deploy WAN optimization on single-purpose FortiProxy units that only perform WAN optimization. In the out of path WAN optimization topology shown below, FortiProxy units are located on the WAN outside of the private networks. You can also install the WAN optimization FortiProxy units behind the security devices on the private networks.

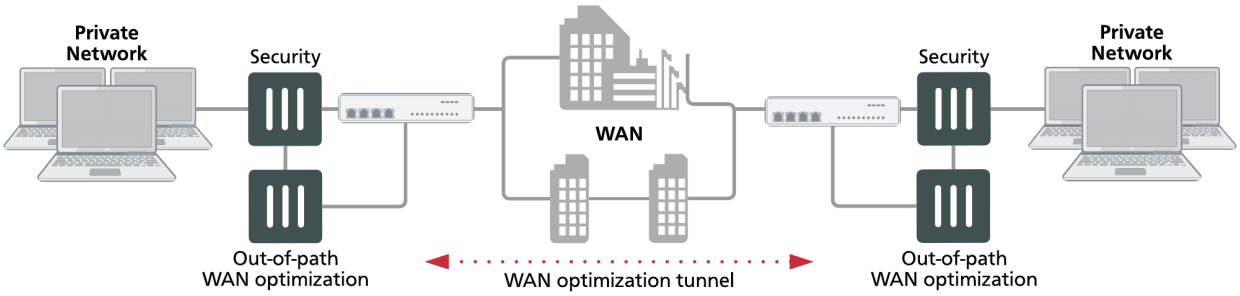
The WAN optimization configuration is the same for FortiProxy units deployed as security devices and for single-purpose WAN optimization FortiProxy units. The only differences would result from the different network topologies.

Out-of-path WAN optimization topology

In an out-of-path topology, one or both of the FortiProxy units configured for WAN optimization are not directly in the main data path. Instead, the out-of-path FortiProxy unit is connected to a device on the data path, and the device is configured to redirect sessions to be optimized to the out-of-path FortiProxy unit.

The following out-of-path FortiProxy units are configured for WAN optimization and connected directly to FortiProxy units in the data path. The FortiProxy units in the data path use a method such as policy routing to redirect traffic to be optimized to the out-of-path FortiProxy units. The out-of-path FortiProxy units establish a WAN optimization tunnel between each other and optimize the redirected traffic.

Out-of-path WAN optimization



One of the benefits of out-of-path WAN optimization is that out-of-path FortiProxy units only perform WAN optimization and do not have to process other traffic. An in-path FortiProxy unit configured for WAN optimization also has to process other non-optimized traffic on the data path.

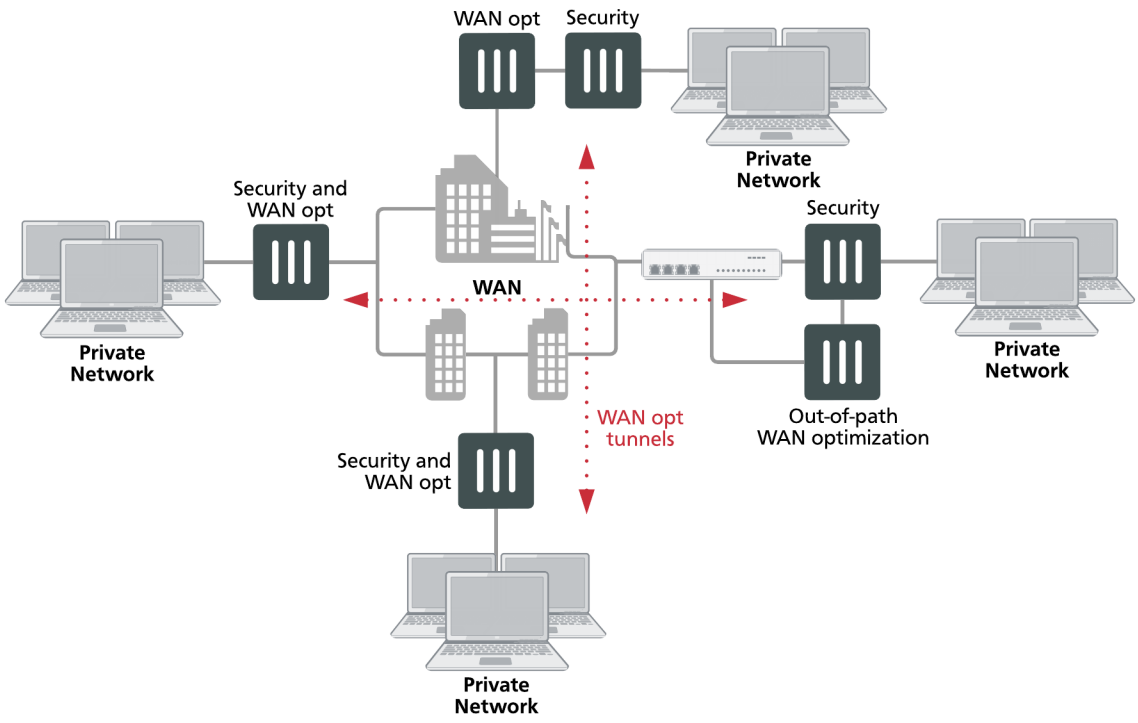
The out-of-path FortiProxy units can operate in NAT/Route or transparent mode.

Other out-of-path topologies are also possible. For example, you can install the out-of-path FortiProxy units on the private networks instead of on the WAN. Also, the out-of-path FortiProxy units can have one connection to the network instead of two. In a one-arm configuration such as this, security policies and routing have to be configured to send the WAN optimization tunnel out the same interface as the one that received the traffic.

Topology for multiple networks

As shown in the following figure, you can create multiple WAN optimization configurations between many private networks. Whenever WAN optimization occurs, it is always between two FortiProxy units, but you can configure any FortiProxy unit to perform WAN optimization with any of the other FortiProxy units that are part of your WAN.

WAN optimization among multiple networks

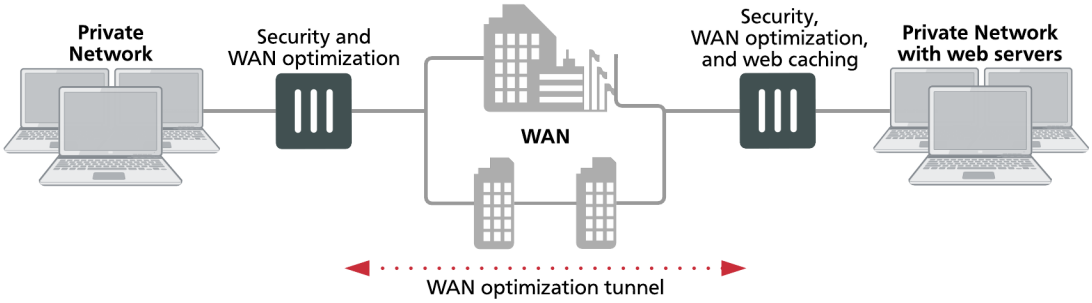


You can also configure WAN optimization between FortiProxy units with different roles on the WAN. FortiProxy units configured as security devices and for WAN optimization can perform WAN optimization as if they are single-purpose FortiProxy units just configured for WAN optimization.

WAN optimization with web caching

You can add web caching to a WAN optimization topology when users on a private network communicate with web servers located across the WAN on another private network.

WAN optimization with web-caching topology



The topology above is the same as that shown in Basic WAN optimization topology on page 75 with the addition of web caching to the FortiProxy unit in front of the private network that includes the web servers. You can also add web caching to the FortiProxy unit that is protecting the private network. In a similar way, you can add web caching to any WAN optimization topology.

Web caching

Web caching is a form of object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency.

Web caching involves storing HTML pages, images, videos, servlet responses, and other web-based objects for later retrieval. These objects are stored in the web cache storage location defined by the `config system storage` command. You can also go to *System > Advanced* to view the storage locations on the FortiProxy unit hard disks in the *System Storage Setting* section.

There are three significant advantages to using web caching to improve HTTP performance:

- Reduced bandwidth consumption because fewer requests and responses go over the WAN or Internet
- Reduced web server load because there are fewer requests for web servers to handle
- Reduced latency because responses for cached requests are available from a local FortiProxy unit instead of from across the WAN or Internet

When enabled in a web-caching policy, the FortiProxy unit caches HTTP traffic processed by that policy. A web-caching policy specifies the source and destination addresses and destination ports of the traffic to be cached.

Web caching caches compressed and uncompressed versions of the same file separately. If the HTTP considers the compressed and uncompressed versions of a file as the same object, only the compressed or uncompressed file will be cached.

You can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform. FortiProxy high-performance web-caching virtual

appliances address bandwidth saturation, high latency, and poor performance caused by caching popular internet content locally for carriers, service providers, enterprises and educational networks.

The FortiProxy unit supports the following:

- KVM hypervisor
- VMware hypervisor
- Xen hypervisor
- Hyper-V hypervisor

Collaboration web caching

Collaboration web caching allows multiple FortiProxy units within one organization to share all cached objects.

Cache-sharing requests are broadcasted from one FortiProxy unit to one or more destination FortiProxy units to prevent loops. The first FortiProxy unit to respond to a cache-sharing request is accepted, and the rest of the responses are ignored. Cache data from a remote (destination) FortiProxy unit participating in collaboration web caching is not saved to the local (source) FortiProxy disk; instead the data is saved to the local memory cache.

NOTE: Sending and receiving cache-sharing requests can impact the performance of FortiProxy units that participate in collaboration web caching. The performance impact depends on how many cache-sharing requests are being handled.

Use the following commands to connect a source FortiProxy unit to a destination FortiProxy unit for collaboration web caching:

```
config wanopt cache-service
   set collaboration enable
   set device-id “fch-1”
   config dst-peer
      edit “peer-id”
         set ip xxx.xxx.xxx.xxx
      next
   end
end
```

Use the following commands to identify all FortiProxy units participating in collaboration web caching:

```
config wanopt cache-service
   set collaboration enable
   set device-id “peer-id”
   set acceptable-peers any
end
```

Use the following commands to allow a FortiProxy unit to accept cache-sharing requests:

```
config wanopt cache-service
   set collaboration enable
   set acceptable-peers any
end
```

For example, use the following commands to allow a destination FortiProxy unit to accept cache-sharing requests from a single source FortiProxy unit:

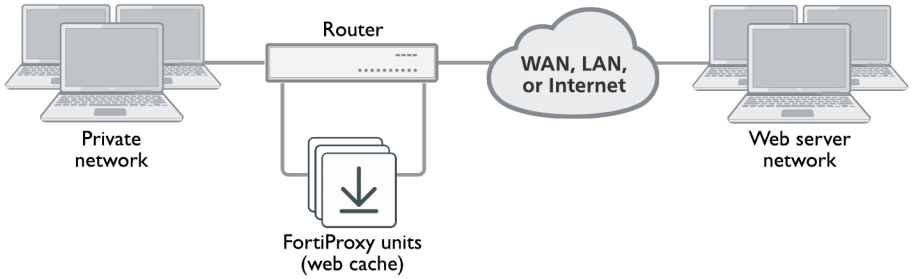
```
config wanopt cache-service
   set collaboration enable
   set acceptable-peers src-peer
   set device-id “peer-id”
   config src-peer
      edit “fch-1”
         set ip xxx.xxx.xxx.xxx
      next
   end
```

Web-caching topologies

FortiProxy web caching involves one or more FortiProxy units installed between users and web servers. The FortiProxy unit can operate in both Network Address Translator (NAT) and transparent modes. The FortiProxy unit intercepts HTTP requests for web objects accepted by web cache policies, requests the web objects from the web servers, caches the web objects, and returns the web objects to the users. When the FortiProxy unit intercepts subsequent requests for cached web pages, the FortiProxy unit contacts the destination web server just to check for changes.

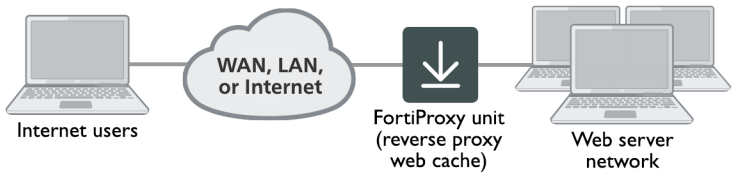
Most commonly the topology uses a router to route HTTP and HTTPS traffic to be cached to one or more FortiProxy units. Traffic that should not be cached bypasses the FortiProxy units. This is a scalable topology that allows you to add more FortiProxy units if usage increases.

Web-caching topology with web traffic routed to FortiProxy units



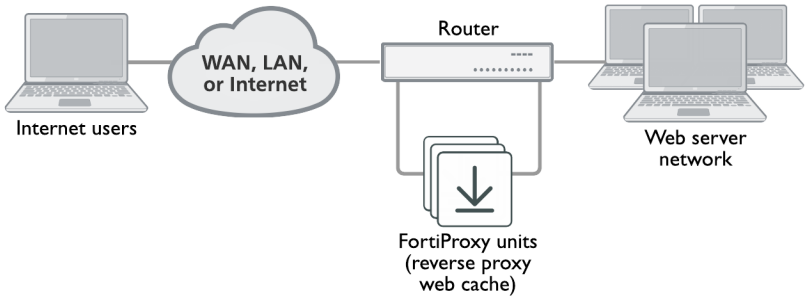
You can also configure reverse proxy web caching. In this configuration, users on the Internet browse to a web server installed behind a FortiProxy unit. The FortiProxy unit intercepts the web traffic (HTTP and HTTPS) and caches pages from the web server. Reverse proxy web caching on the FortiProxy unit reduces the number of requests that the web server must handle, leaving it free to process new requests that it has not serviced before. Because all traffic is to be cached, the FortiProxy unit can be installed in transparent mode directly between the web server and the Internet.

Reverse proxy web-caching topology



The reverse proxy configuration can also include a router to route web traffic to a group of FortiProxy units operating in transparent mode. This solution for reverse proxy web caching is also scalable.

Reverse proxy web-caching topology with web traffic routed to FortiProxy unit



When web objects and video are cached on the FortiProxy hard disk, the FortiProxy unit returns traffic back to client using the cached object from cache storage. The clients do not connect directly to the server.

When web objects and video are not available in the FortiProxy hard disk, the FortiProxy unit forwards the request to original server. If the HTTP response indicates it is a object that can be cached, the object is forwarded to cache storage, and the HTTP request is served from cache storage. Any other HTTP request for the same object will be served from cache storage as well.

The FortiProxy unit forwards HTTP responses that cannot be cached from the server back to the client that originated the HTTP request.

All non-HTTP traffic and HTTP traffic that is not cached by FortiProxy will pass through the unit. HTTP traffic is not cached by the FortiProxy unit if a web cache policy has not been added for it.

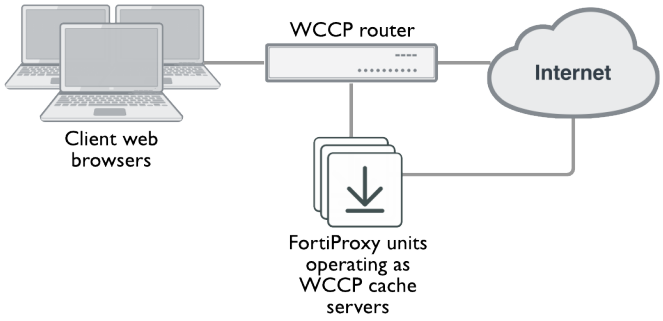
WCCP

You can also configure a FortiProxy unit to operate as a Web Cache Communication Protocol (WCCP) client. WCCP provides the ability to offload web caching to one or more redundant web-caching servers.

WCCP topology

You can operate a FortiProxy unit as a WCCP cache engine. As a cache engine, the FortiProxy unit returns the required cached content to the client web browser. If the cache server does not have the required content, it accesses the content, caches it, and returns the content to the client web browser.

WCCP topology



WCCP is transparent to client web browsers. The web browsers do not have to be configured to use a web proxy.

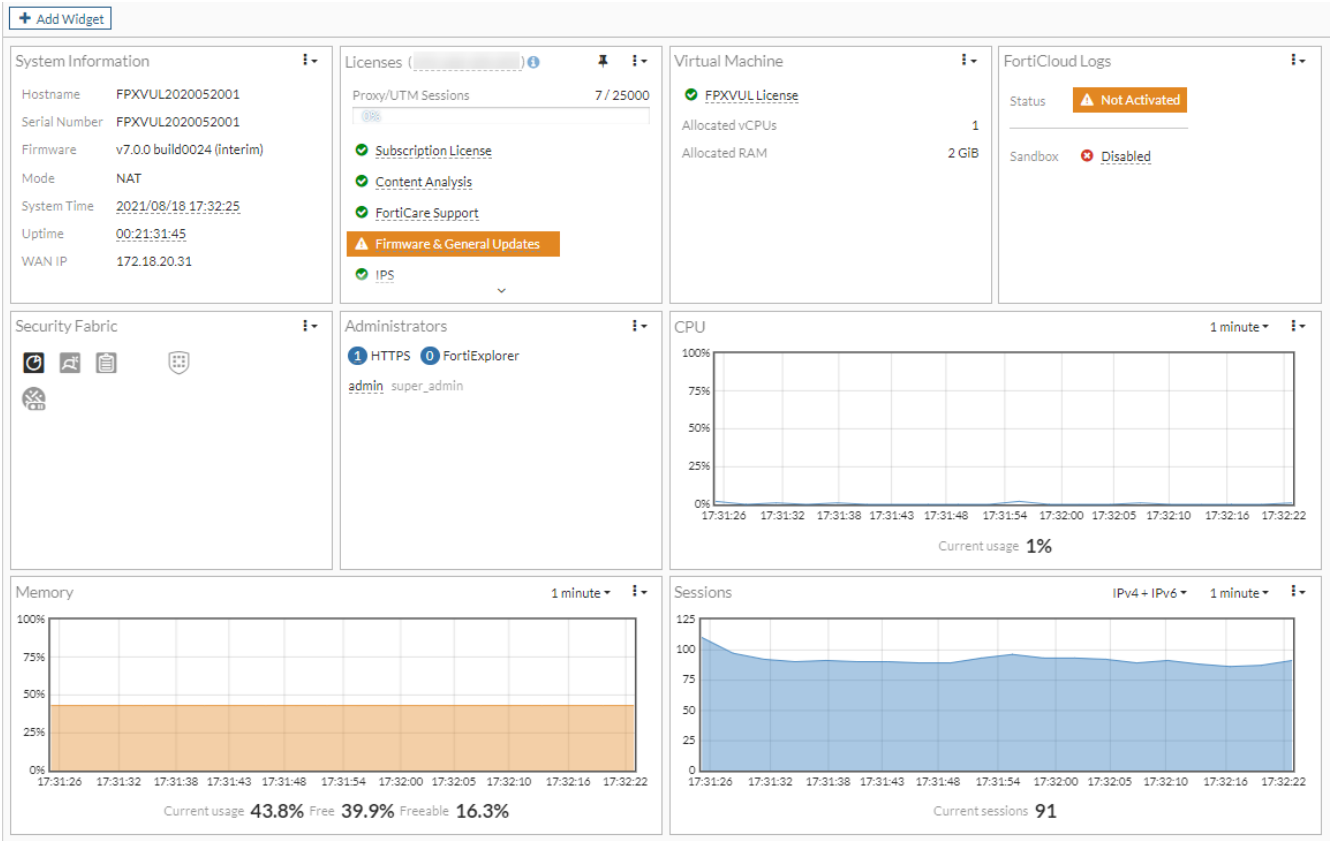
Dashboard

The dashboard provides a location to view real-time system information. By default, the dashboard displays the key statistics of the FortiProxy unit itself, providing the memory and CPU status, licenses, and current number of sessions.

The dashboard provides a Network Operations Center (NOC) view with a focus on alerts. Widgets are interactive; by clicking or hovering over most widgets, you can get additional information or follow links to other pages.

To access the main dashboard, go to *Dashboard* > *Status*.

Your browser must support JavaScript to view the dashboard.



The following widgets are displayed:

- System Information
- Licenses
- Virtual Machine
- FortiGate Cloud

- Security Fabric
- Administrators
- CPU
- Memory
- Proxy Sessions
- Advanced Threat Protection Statistics

You can add the following FortiView widgets to the dashboard:

- FortiView Applications
- FortiView Cloud Applications
- FortiView Countries/Regions
- FortiView Destination Firewall Objects
- FortiView Destination Interfaces
- FortiView Destination Owners
- FortiView Destinations
- FortiView Interface Pairs
- FortiView Policies
- FortiView Search Phrases
- FortiView Servers
- FortiView Sessions
- FortiView Source Firewall Objects
- FortiView Source Interfaces
- FortiView Sources
- FortiView Sources - WAN
- FortiView Traffic Shaping
- FortiView VPN
- FortiView Web Categories
- FortiView Web Sites

This section describes the following:

- Managing widgets
- System Information widget
- Licenses widget
- Virtual Machine widget
- FortiProxy Cloud widget
- Security Fabric widget
- Administrators widget
- CPU widget
- Memory widget
- Sessions widget
- IPSec widget
- Forward Server Monitor widget
- License Sharing Information widget
- License Usage History widget

- Sensor Information widget
- User dropdown menu
- GUI-based global search

Managing widgets

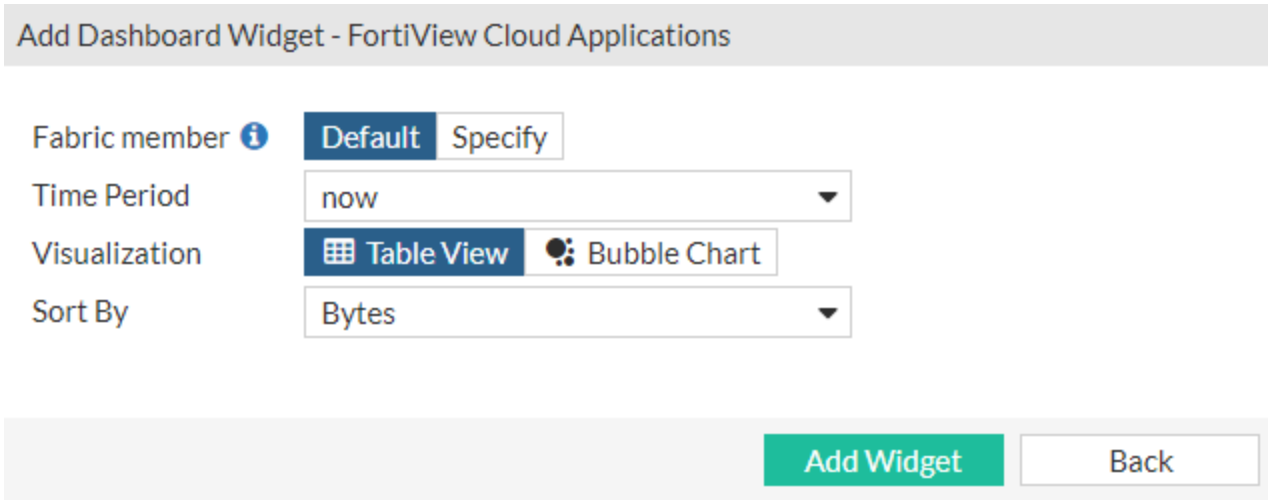
To rearrange widgets on the dashboard, drag the widgets by their title bars.

All widgets have the following two title bar options:

Resize	Select the size of the widget.
Remove	Remove the widget from the dashboard.

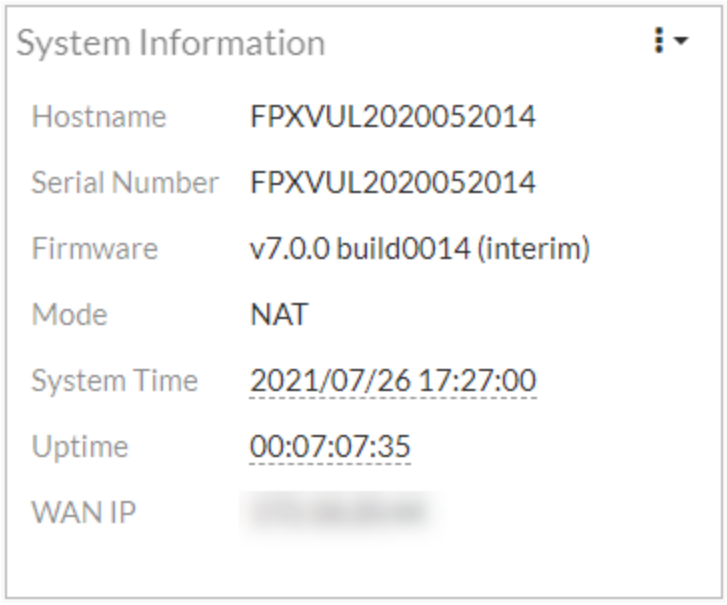
To add a FortiView widget to a dashboard:

1. Go to *Dashboard* > *Status*.
2. At the top the dashboard, click *Add Widget*.
3. Click *+* for the FortiView widget that you want to add.
   The *Add Dashboard Widget*window opens.



4. Click *Specify* if you want the widget to monitor all FortiProxy units instead of a single FortiProxy unit.
5. Select the time period to display.
6. Select *Table View* or *Bubble Chart*.
7. Select the *Sort By* value.
8. Click *Add Widget*.
   The new widget is displayed in the main dashboard.
9. Click *Close*.

System Information widget



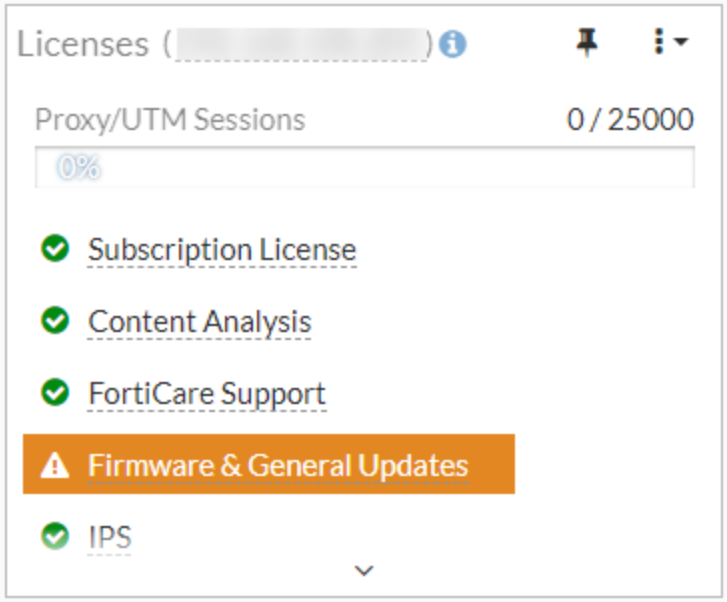
The *System Information* widget displays general system information, such as the FortiProxy unit serial number, firmware version, host name, and system time. Clicking on the widget provides you links to two other pages:

- To configure settings, go to *System* > *Settings*.
- To update the firmware version, go to *System* > *Firmware*.

Hostname	The host name of the current FortiProxy unit.
Serial Number	The serial number of the FortiProxy unit. The serial number is specific to that unit and does not change with firmware upgrades.
Firmware	The version of the firmware currently installed on the FortiProxy unit. To update the firmware version, go to *System* > *Firmware*. By installing an older firmware image, some system settings might be lost. You should always back up your configuration before changing the firmware image. To back up your configuration, go to *<user_name>* > *Configuration* > *Backup*. You must register your unit with Fortinet Customer Support to access firmware updates for your model. For more information, go to https://support.fortinet.com or contact Fortinet Customer Service & Support.
Mode	The current operating mode of the FortiProxy unit. A unit can operate in NAT mode or transparent mode.
System Time	The current date and time according to the FortiProxy unit's internal clock.

Uptime	The time in days, hours, and minutes since the FortiProxy unit was started.
WAN IP	The WAN IP address and location. Additionally, if the WAN IP is blocked in the FortiGuard server, there is a notification in the notification area, located in the upper right-hand corner of the Dashboard. Clicking on the notification opens a window with the relevant blocklist information.

Licenses widget

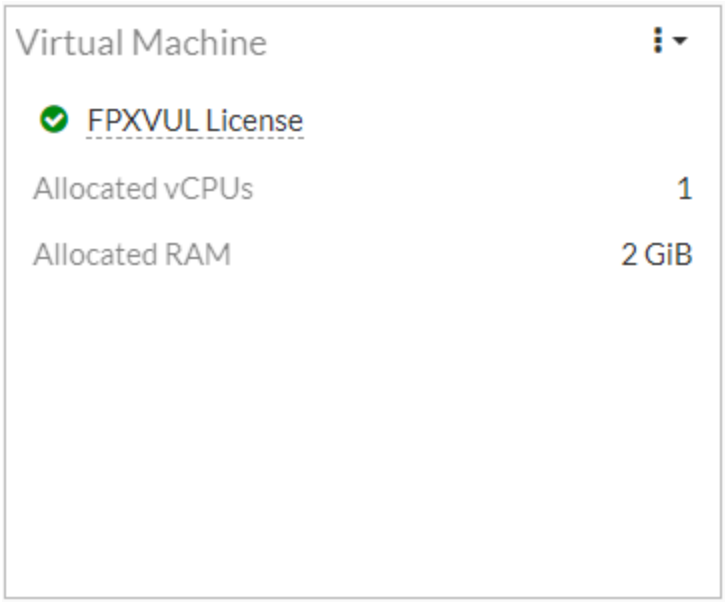


The *Licenses* widget displays the statuses of your licenses and FortiGuard subscriptions. It also allows you to update your device's registration status and FortiGuard definitions.

Hovering over the Licenses widget displays status information for Subscription License, Content Analysis, FortiCare Support, IPS, AntiVirus, and Web Filtering. Clicking on each license provides links to renew, register, subscribe, or add your FortiCare contract number.

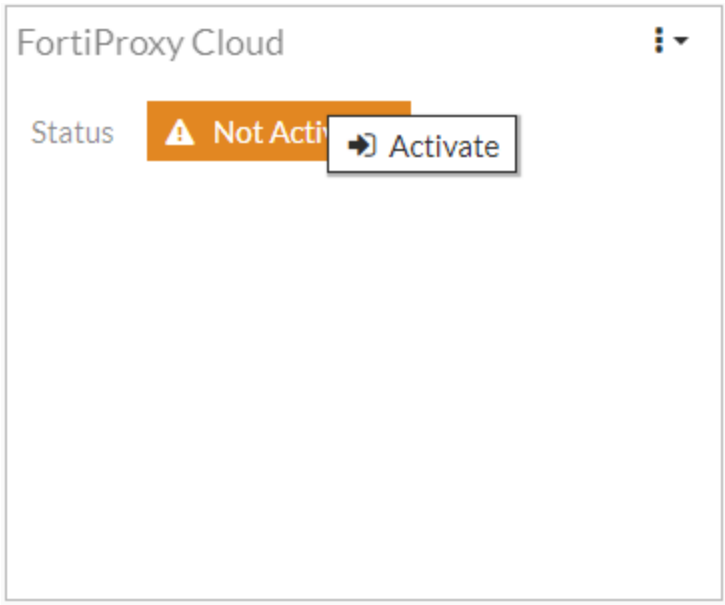
Go to *System* > *FortiGuard* to register for FortiCare Support, upgrade databases, and view details. See FortiGuard on page 962.

Virtual Machine widget



This widget displays license information, number of allocated vCPUs, and how much RAM has been allocated.

FortiProxy Cloud widget



This widget displays the FortiProxy Cloud status and provides a link to activate FortiProxy Cloud.

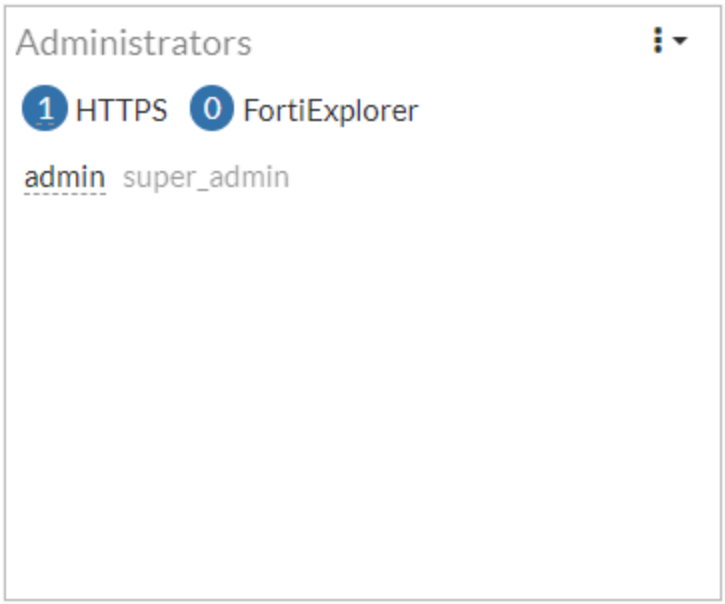
Security Fabric widget



You can hover over the icons along the top of the Security Fabric widget to get a quick view of the status of various components of in the Security Fabric. Hover over the host name to display system information.

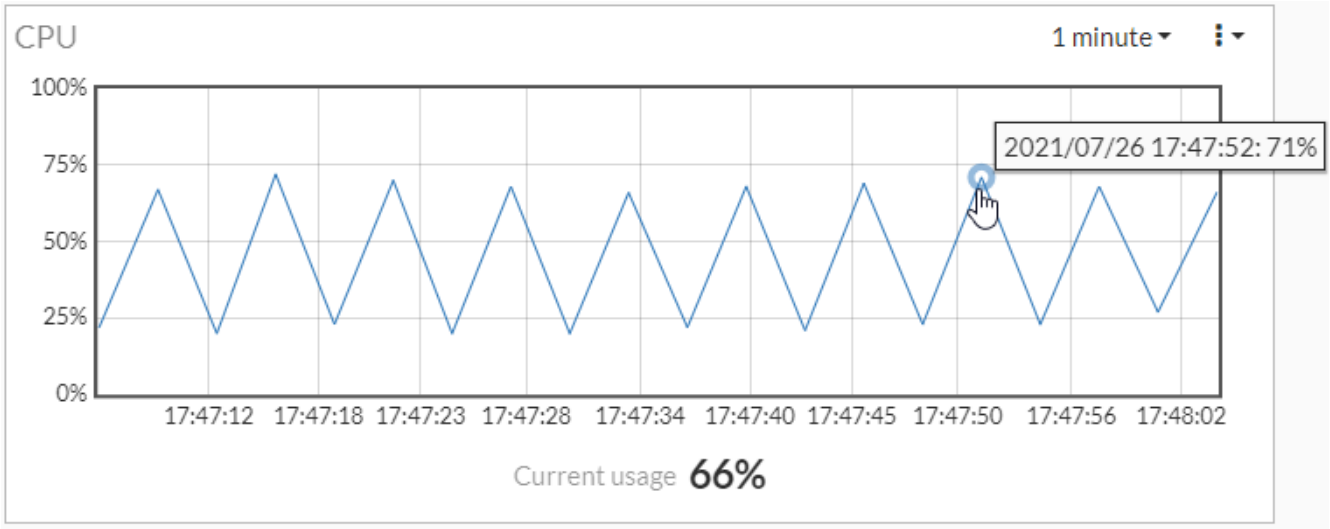
Click on an icon for a link to configure the settings for that component.

Administrators widget



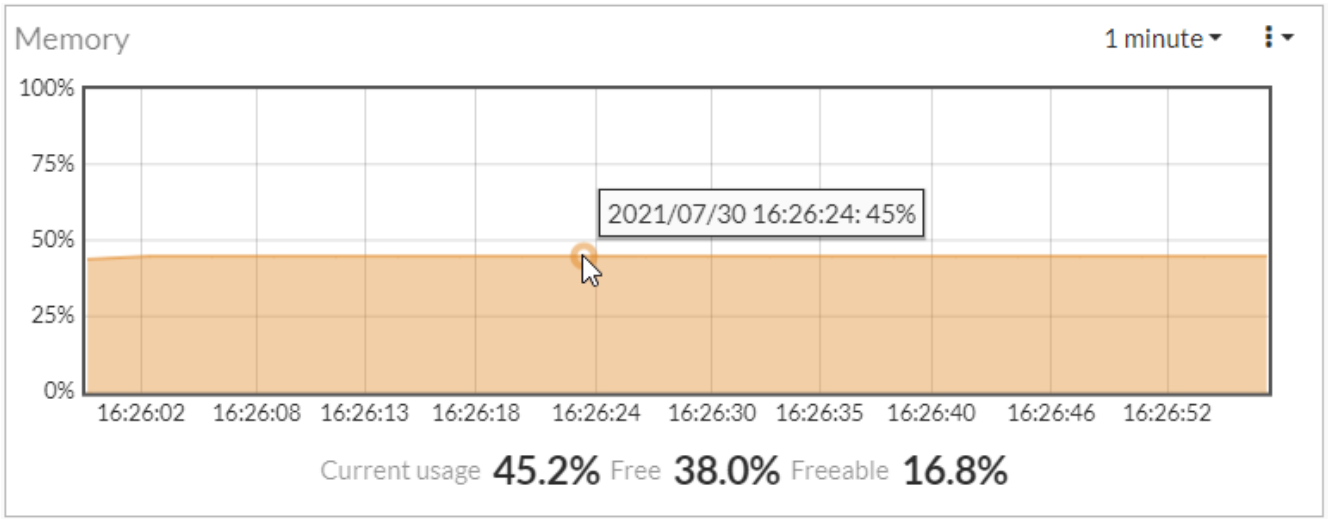
This widget allows you to view which administrators are logged in and how many sessions are active. Clicking on the widget provides you a link to a page displaying active administrator sessions.

CPU widget



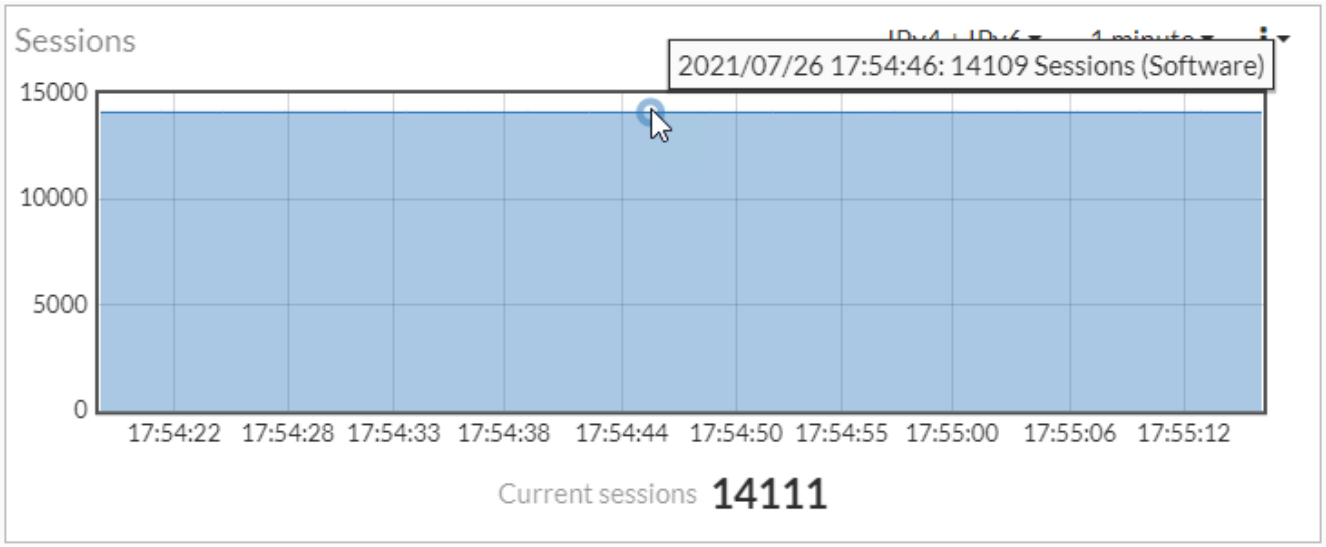
The real-time CPU usage is displayed for different time frames. Select the time frame from the drop-down list at the top of the widget. Hovering over any point on the graph displays the average CPU usage along with a time stamp.

Memory widget



Real-time memory usage is displayed for different time frames. Select the time frame from the drop-down list at the top of the widget. Hovering over any point on the graph displays the percentage of memory used along with a time stamp.

Sessions widget



This widget allows you to view how many proxy sessions are active. Select the time frame from the drop-down list at the top of the widget. Select whether to display *IPv4*, *IPv6*, or *IPv4 + IPv6* sessions. Hovering over any point on the graph displays the number of proxy sessions with a time stamp.

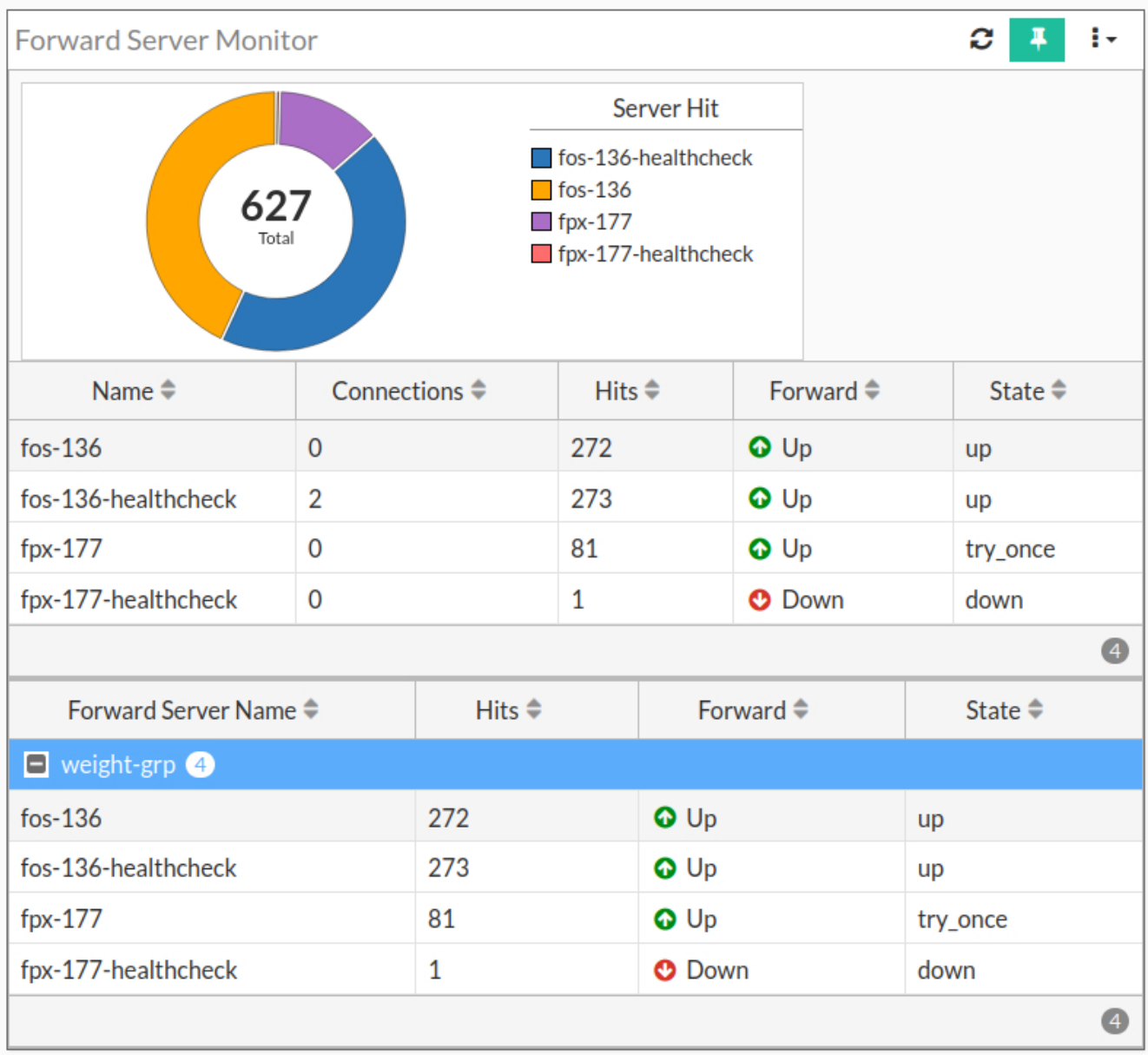
IPSec widget

The *IPsec* widget displays information about Phase 1 and Phase 2 tunnels. The widget also identifies users who have not enabled two-factor authentication.

To view the IPSec widget:

1. Go to *Dashboard* and click *Add Widget*.
2. Under *Network*, click *IPsec*.
3. Click *Default* or specify the FortiProxy unit.
4. Click *Add Widget*.
5. Click *Close*.
6. The *IPsec* overview widget is displayed.
7. Hover over the widget and click *Expand to full screen*. A warning appears when an unauthenticated user is detected.

Forward Server Monitor widget



This widget allows you to monitor the forward server status, connections, and hits. Hover over the graph or server name in the widget to get a quick view of the server status. Forward servers with *Health Check* disabled will always be *Up* in the *Forward* column. When such a forward server is part of a server group, it serves as a backup option when no other server is up and running. The *State* column provides more specific state information about the forward server. The following states are available:

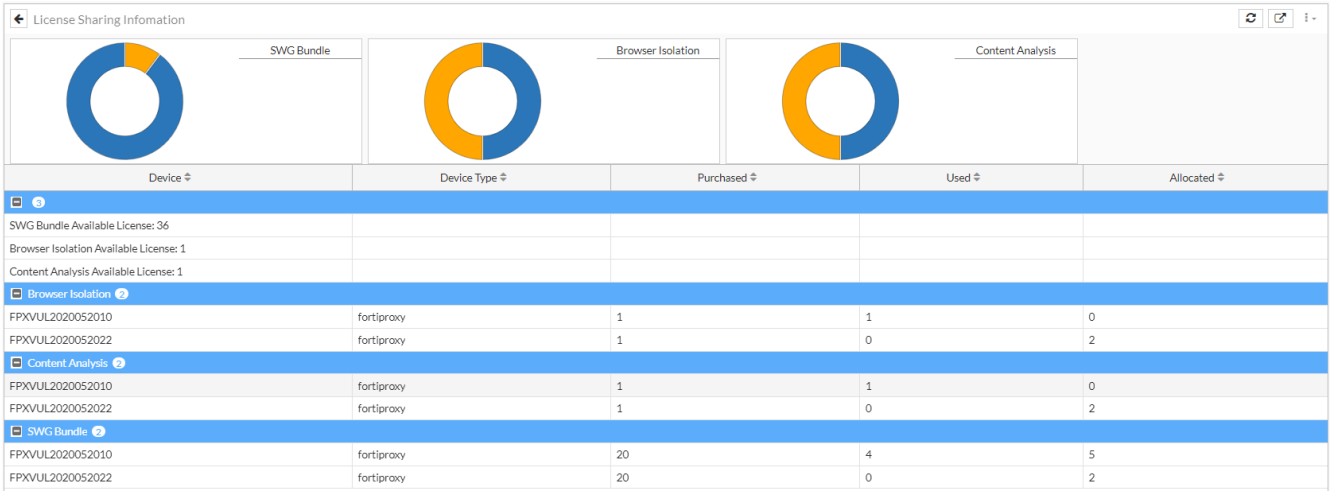
- *pending*—Initial state of all forward servers. A pending forward server can mean one of the following:

  - The state of the forward server is unknown, which means no connection has been established yet or the state has not been updated yet.
  - The forward server is running but pending FQDN resolve. FQDN resolve failure triggers a state change to *down*.
- *try_once*—For forward servers in *down* state with *Health Monitor* disabled, FortiProxy periodically switches its state from *down* to *try_once* to verify the latest status of the server to avoid situations where a server in down state is ignored in all subsequent health state checks.
- *busy*—The forward server is running but unstable.
- *down*—The forward server is not running and connections are blocked.

See Create or edit a forwarding server on page 160 for more information about how to enable and configure health monitoring for the forward server.

License Sharing Information widget

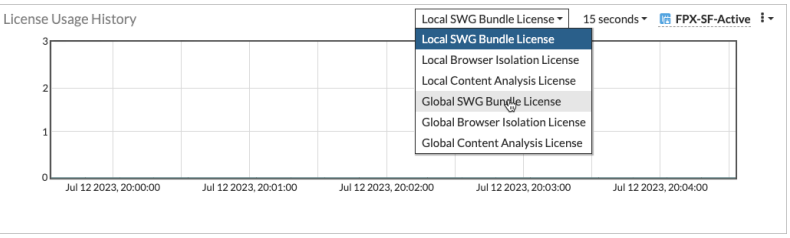
FortiProxy shares available seats among devices in HA on page 904 active-passive mode or in a Security Fabric on page 1016 group with license sharing enabled. The *License Sharing Information* widget displays the total number of available licenses of SWG Bundle, Browser Isolation (FNBI), and Content Analyses on page 719 (FCAS) license types and the numbers used by the devices in the license pool. Click on a specific section in the chart for more details about the license usage.



Device	Device Type	Purchased	Used	Allocated
3				
SWG Bundle Available License: 36				
Browser Isolation Available License: 1				
Content Analysis Available License: 1				
Browser Isolation 2				
FPXVUL2020052010	fortiproxy	1	1	0
FPXVUL2020052022	fortiproxy	1	0	2
Content Analysis 2				
FPXVUL2020052010	fortiproxy	1	1	0
FPXVUL2020052022	fortiproxy	1	0	2
SWG Bundle 2				
FPXVUL2020052010	fortiproxy	20	4	5
FPXVUL2020052022	fortiproxy	20	0	2

Refer to the FortiProxy datasheet for more information about different license types. See the FortiProxy License Sharing guide for more information about how license sharing works and how to configure license sharing to meet your needs.

License Usage History widget



The *License Usage History* widget displays the global or local license usage history of the following license types at a certain interval:

- SWG Bundle License
- Browser Isolation License
- Content Analysis License

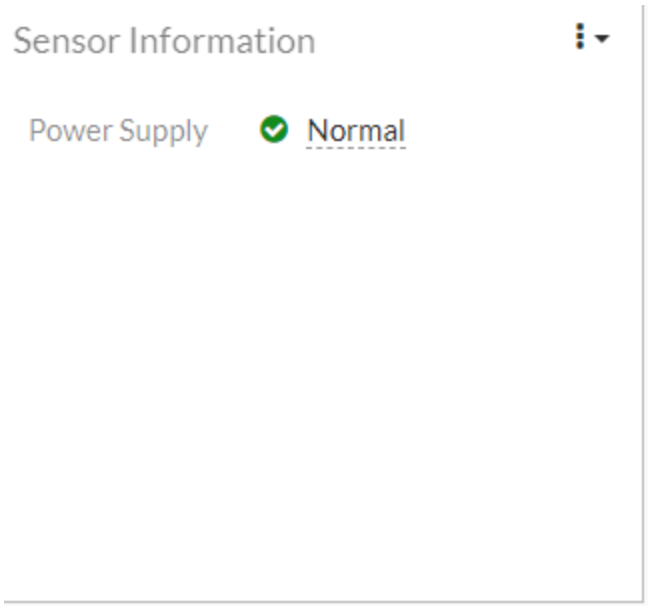
Use the filter at the top to display license usage data for a specific license type. Configure the interval at the top-right corner with the following options: 15 seconds, 5 minutes, 1 hour, 1 day, 1 week, 1 month, or 1 year.

For each timestamp, the widget displays the following values:

- **Min Usage**—Minimum number of license seats used during the past interval.
- **Max Usage**—Maximum number of license seats used during the past interval.
- **Average Usage**—Average number of license seats used during the past interval.

Refer to the FortiProxy datasheet for more information about different license types. See the FortiProxy License Sharing guide for more information about how license sharing works and how to configure license sharing to meet your needs.

Sensor Information widget



This widget allows you to view the status of power supply sensor in the hardware system. You can click on the status icon in the widget for more detailed information about the status, such as the real-time and expected power supply voltage values.

Sensor List - Power Supply

Name	Description	Status	Value
PSU1	Main 12V power supply #1	Normal	12.13 V
PSU2	Main 12V power supply #2	Normal	12.13 V
5VCC	Main 5V power supply	Normal	4.97 V
3.3VCC	Main 3.3V power supply	Normal	3.32 V
VBAT	Battery power supply	Normal	3.13 V
Vcpu1	CPU #1 voltage	Normal	1.8 V
Vcpu2	CPU #2 voltage	Normal	1.8 V
VDIMMAB	Memory channel 1 voltage	Normal	1.19 V
VDIMMCD	Memory channel 2 voltage	Normal	1.18 V
VDIMMEF	Memory channel 3 voltage	Normal	1.19 V
VDIMMGH	Memory channel 4 voltage	Normal	1.19 V
5VSB	5V standby	Normal	5.05 V
3.3VSB	3.3V standby	Normal	3.4 V
1.5V PCH	1.5V platform controller voltage	Normal	1.52 V
1.2V BMC	1.2V baseboard controller voltage	Normal	1.21 V
1.05V PCH	1.05V platform controller voltage	Normal	1.04 V

This widget is available only for FPX-2000E/4000E/2000G/4000G/400G units.

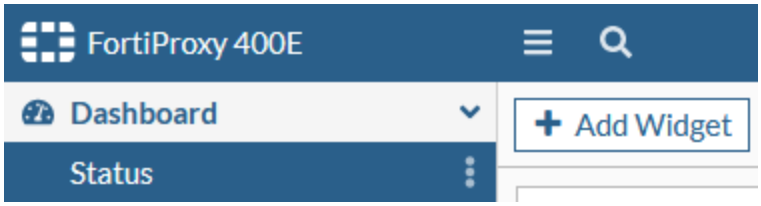
User dropdown menu

In the right corner of the FortiProxy title bar, the user dropdown menu provides the following actions:

- Reboot the system.
- Shut down the system.
- Upload a new version of the FortiProxy firmware or restore an older firmware version.
- Back up your FortiProxy configuration.
- Restore a saved FortiProxy configuration.
- Check the available versions of your saved FortiProxy configurations.
- Upload or run a script.
- Change your password.
- Log out.

GUI-based global search

The global search option in the GUI allows users to search for keywords appearing in objects and navigation menus to quickly access the object and configuration page. Click the magnifying glass icon in the top-left corner of the banner to access the global search.



The global search includes the following features:

- Keep a history of frequent and recent searches
- Sort results alphabetically by increasing or decreasing order, and relevance by search weight
- Search by category
- Search in Security Fabric members (accessed by the Security Fabric members dropdown menu in the banner)

FortiView

FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view on your FortiProxy unit. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

FortiView allows you to use multiple filters within the consoles, enabling you to narrow your view to a specific time (up to 24 hours in the past), by user ID or local IP address, by application, and in many more ways.

FortiView can be used to investigate traffic activity, such as user uploads/downloads or videos watched on YouTube, on a network-wide, user group, and individual-user level, with information relayed in both text and visual format. FortiView makes it easy to get an actionable picture of your network's Internet activity.

This section covers the following topics:

- FortiView dependencies on page 98
- FortiView interface on page 101
- FortiView consoles on page 101

FortiView dependencies

By default, FortiView is enabled on FortiProxy units. You will find the FortiView consoles in the main menu.

Most FortiView consoles require the user to enable several features to produce data. The following table summarizes the dependencies:

FortiView Console	Dependencies
FortiView Applications	• Application control profile added to a policy • Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Cloud Applications	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy • Full SSL inspection enabled for all protocols in an SSL/SSH Inspection profile • Application Control profile and Full SSL Inspection profile added to the same policy
FortiView Countries/Regions	• Logging device set up and enabled • Historical FortiView enabled

FortiView Console	Dependencies
	• Traffic logging enabled in a policy
FortiView Destination Firewall Objects	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Destination Interfaces	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Destination Owners	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Destinations	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Interface Pairs	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Policies	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Search Phrases	• FortiGuard categories enabled in a Web Filter profile • Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy • Log all search keywords enabled in a Web Filter profile • Profile-based NGFW mode
FortiView Servers	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Sessions	• Disk logging enabled • Traffic logging enabled in a policy
FortiView Source Firewall Objects	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Source Interfaces	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Sources	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy

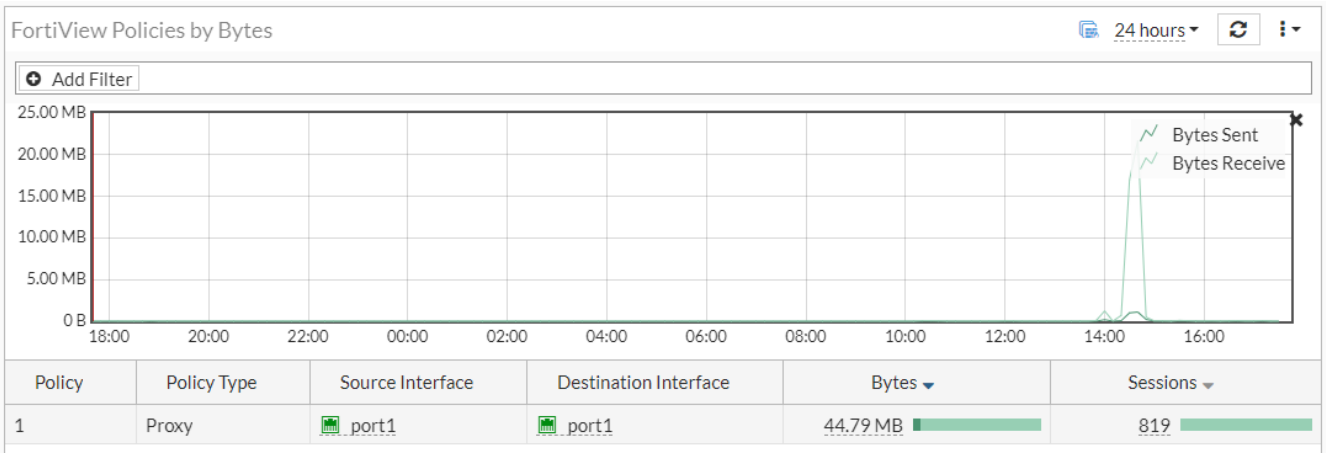
FortiView Console	Dependencies
FortiView Sources - WAN	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Traffic Shaping	• Enable traffic-shaping feature • Disk logging enabled • Historical FortiView enabled
FortiView Web Categories	• FortiGuard categories enabled in a Web Filter profile • Web Filter profile added to a policy • Traffic logging enabled in a policy • Logging device set up and enabled • Historical FortiView enabled
FortiView Web Sites	• FortiGuard categories enabled in a Web Filter profile • Web Filter profile added to a policy • Traffic logging enabled in a policy • Logging device set up and enabled • Historical FortiView enabled
FortiView VPN	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy

To enable disk logging and historical FortiView:

1. Go to *Log & Report* > *Log Settings*.
2. Under *Local Log*, enable *Disk* and *Enable Historical FortiView*.
3. Click *Apply*.

FortiView interface

FortiView lets you access information about the traffic activity on your FortiProxy unit, visually and textually. FortiView is broken up into several consoles, each of which features a top menu bar and a graph window, as seen in the following image:



Depending on the FortiView console, the top menu bar contains various controls:

- *Refresh* button, which updates the data displayed
- *Add Filter* button, for filtering the data by category
- Filter buttons to select what data to view
- View drop-down menu to select *Table View* or *Bubble Chart*
- Time Display drop-down menu (options: *5 minutes*, *1 hour*, or *24 hours*; if you are using FortiAnalyzer, you can select longer time periods)
- Dashboard widget drop-down menu
- *Settings* button
- Information icon

FortiView consoles

This section briefly describes the consoles available in FortiView:

- FortiView Applications console on page 102 displays applications used on the network that have been recognized by Application Control and allows you to view what sort of applications individual employees are using.
- FortiView Cloud Applications console on page 103 displays Web/Cloud Applications used on the network and allows you to access detailed data on cloud application usage, for example, YouTube.
- FortiView Countries/Regions console on page 103 provides a geographical display of threats, in real time, from international sources as they arrive at your FortiProxy unit.
- FortiView Destination Firewall Objects console on page 103 displays the top traffic sessions aggregated by destination object.

- FortiView Destination Interfaces console on page 104 displays the number of destination interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring.
- FortiView Destination Owners console on page 104 displays the top traffic sessions aggregated by owner.
- FortiView Destinations console on page 104 displays the top traffic sessions aggregated by destination.
- FortiView Interface Pairs console on page 104 displays the top traffic sessions aggregated by interface pair.
- FortiView Policies console on page 104 displays what policies are in affect on your network, what their source and destination interfaces are, how many sessions are in each policy, and what sort of traffic is occurring.
- FortiView Search Phrases console on page 105 displays the top traffic sessions aggregated by website search phrase.
- FortiView Servers console on page 105 displays the top servers aggregated by server address.
- FortiView Sessions console on page 105 displays complete information on all FortiProxy sessions, with the ability to filter sessions by port number and application type.
- FortiView Source Firewall Objects console on page 106 displays the top traffic sessions aggregated by source object.
- FortiView Source Interfaces console on page 106 displays the number of source interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring.
- FortiView Sources console on page 107 displays detailed information on the sources of traffic passing through the FortiProxy unit so that you can investigate an unusual spike in traffic to determine which user is responsible.
- FortiView Sources - WAN console on page 107 displays the top traffic sessions for interfaces with a role of WAN, aggregated by source.
- FortiView VPN console on page 107 displays the top traffic sessions aggregated by VPN user.
- FortiView Web Categories console on page 107 displays the top traffic sessions aggregated by website category.
- FortiView Web Sites console on page 107 displays web sites visited as part of network traffic that have been recognized by Web Filtering so that you can investigate instances of proxy avoidance, which is the act of circumventing blocks using proxies.

FortiView Applications console

The *FortiView Applications* console provides information about the applications being used on your network.

This console can be sorted by sessions or bytes. The data can be filtered by 5 minutes, 1 hour, or 24 hours. You can select which applications are displayed.



For information to appear in the *FortiView Applications* console, Application Control must be enabled in a policy.

FortiView Cloud Applications console

The *FortiView Cloud Applications* console provides information about the cloud applications being used on your network. This includes information such as:

- The names of videos viewed on YouTube (visible by hovering the cursor over the session entry)
- Filed uploaded and downloaded from cloud hosting services such as Dropbox
- Account names used for cloud services

Two different views are available for the Cloud Applications: *Applications* and *Users* (located in the top menu bar next to the time periods). *Applications* shows a list of the programs being used. *Users* shows information on the individual users of the cloud applications, including the username, if the FortiProxy unit was able to view the login event.

You can sort the data by bytes, sessions, or files (up or down). The data can be filtered by 5 minutes, 1 hour, or 24 hours. You can select which cloud applications are displayed.



For information to appear in the Cloud Applications console, an application control profile (that has Deep Inspection of Cloud Applications enabled) must be enabled in a policy, and SSL Inspection must use deep-inspection.

FortiView Countries/Regions console

The *FortiView Countries/Regions* console displays network activity by geographic region. Threats from various international destinations will be shown, but only those arriving at your destination, as depicted by the FortiProxy unit. You can place your cursor over the FortiProxy's location to display the device name, IP address, and the city name/location.

The color gradient of the darts on the map indicate the traffic risk, where red indicates the more critical risk.

This console can be sorted by bytes, sessions, or threat scores. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Destination Firewall Objects console

The *FortiView Destination Firewall Objects* console displays the top destination firewall objects. You can drill down by destination object.

This console leverages UUIDs to resolve firewall object address names for improved usability, which requires address objects' UUIDs to be logged.

To enable address object UUID logging in the CLI:

```
config system global
   set log-uuid-address enable
end
```

This console can be sorted by sessions or bytes. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Destination Interfaces console

The *FortiView Destination Interfaces* console lists the total number of destination interfaces connected to your network, how many sessions there are in each interface, and the number of bytes sent.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Destination Owners console

The *FortiView Destination Owners* console displays the top destination owners. This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Destinations console

The *FortiView Destinations* console provides information about the destination IP addresses of traffic on your FortiProxy unit, as well as the application used. You can select the country/region, destination device, or destination IP address to display.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

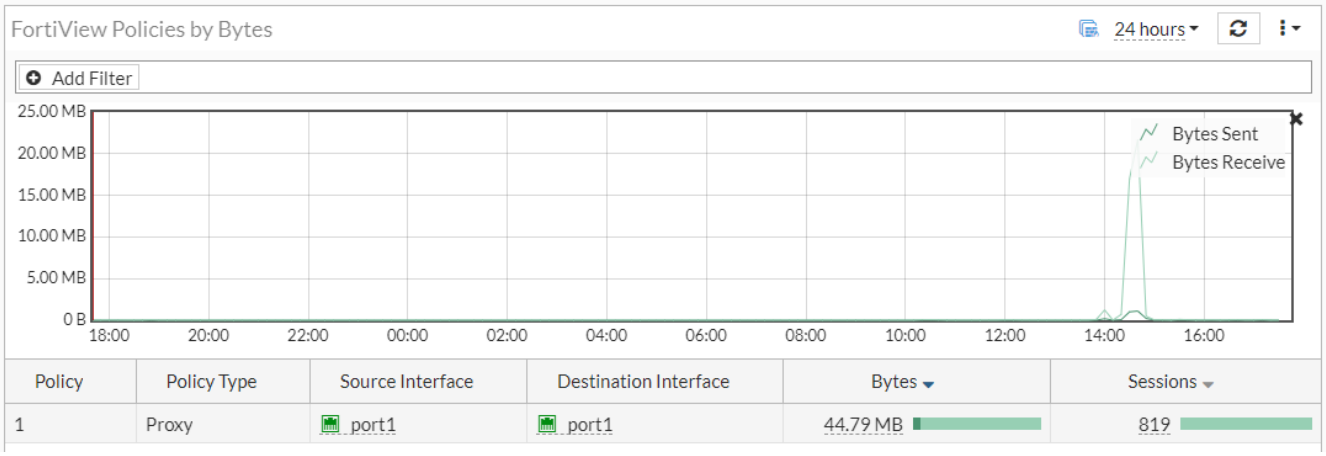
FortiView Interface Pairs console

The *FortiView Interface Pairs* console displays the top traffic sessions aggregated by the interface pair. You can select the destination interface or the source interface to display.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Policies console

The *FortiView Policies* console shows what policies are in affect on your network, what their source and destination interfaces are, how many sessions are in each policy, and what sort of traffic is occurring, represented in bytes sent and received. You can select which policies to display.



This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Search Phrases console

The *FortiView Search Phrases* console displays the top search phrases, sorted by count. You can drill down by search phrase.

The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Servers console

The *FortiView Servers* console displays the top servers. You can drill down by the server address. You can select the country/region, destination device, or destination IP address to display.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Sessions console

The *FortiView Sessions* console displays the top sessions by traffic source and can be used to end sessions.

This console has the greatest number of column options to choose from. To choose which columns you want to view, select the column settings cog at the far right of the columns and select your desired columns. They can then be clicked and dragged in the order that you wish them to appear.

Some of the columns available in FortiView are only available in All Sessions. For example, the Action column displays the type of response taken to a security event. This function can be used to review what sort of threats were detected, whether the connection was reset due to the detection of a possible threat, and so on. This would be useful to display alongside other columns such as the Source, Destination, and Bytes (Sent/Received) columns, as patterns or inconsistencies can be analyzed.

Similarly, there are a number of filters that are only available in All Sessions, one of which is Protocol. This allows you to display the protocol type associated with the selected session, for example, TCP, FTP, HTTP, HTTPS, and so on.

The *FortiView Sessions* console is useful when verifying open connections. For example, if you have a web browser open to browse the Fortinet website, you would expect a session entry from your computer on port 80 to the IP address for the Fortinet website. You can also use a session table to investigate why there are too many sessions for the FortiProxy unit to process.

You can also view the session data in the CLI.

To view session data using the CLI:

```
# diagnose sys session list
```

The session table output in the CLI is very large. You can use the supported filters in the CLI to show only the data you need.

To view session data with filters using the CLI:

```
# diagnose sys session filter {sintf | dintf | src | nsrc | dst | proto | sport | nport | dport |
policy | clear}
```

FortiView Source Firewall Objects console

The *FortiView Source Firewall Objects* console displays the top source firewall objects. You can drill down by source object.

This console leverages UUIDs to resolve firewall object address names for improved usability, which requires address objects' UUIDs to be logged.

To enable address object UUID logging in the CLI:

```
config system global
   set log-uuid-address enable
end
```

This console can be sorted by sessions or bytes. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Source Interfaces console

The *FortiView Source Interfaces* console lists the total number of source interfaces connected to your network, how many sessions there are in each interface, and the number of bytes sent.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Sources console

The *FortiView Sources* console provides information about the sources of traffic on your FortiProxy unit.

You can select which source devices and source IP addresses are displayed. This console can be sorted by bytes, sessions, or threat scores. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Sources - WAN console

The *FortiView Sources - WAN* console displays the top traffic sessions for interfaces with a role of WAN, aggregated by source.

You can select which source devices and source IP addresses are displayed. This console can be sorted by bytes, sessions, or threat scores. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView VPN console

The *FortiView VPN* console displays the top traffic sessions aggregated by VPN user.

You can select which user names and VPN types are displayed. This console can be sorted by connections or bytes. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Web Categories console

The *FortiView Web Categories* console displays the top web categories. You can drill down by category.

You can select which domains and web categories are displayed. This console can be sorted by browsing time, threat score, bytes, or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.



For information to appear in the *FortiView Web Categories* console, web filtering must be enabled in a policy, with FortiGuard categories enabled.

FortiView Web Sites console

The *FortiView Web Sites* console lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be selected to see a description of the category and several example sites, with content loaded from FortiGuard on demand.

You can select which domains and web categories are displayed. This console can be sorted by browsing time, threat score, bytes, or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.



For information to appear in the *FortiView Web Sites* console, web filtering must be enabled in a policy, with FortiGuard categories enabled.

Using the process monitor

The *Process Monitor* displays running processes with their CPU and memory usage levels. Administrators can sort, filter, and terminate processes within the *Process Monitor* pane.

To access the process monitor:

1. Go to *Dashboard* > *Status*:
   - Left-click in the *CPU* or *Memory* widget and select *Process Monitor*.
   - Click the user name in the upper right-hand corner of the screen, then go to *System* > *Process Monitor*.

   The *Process Monitor* appears, which includes a line graph, donut chart, and process list.
2. Click the *+* beside the search bar to view which columns can be filtered.

To kill a process within the process monitor:

1. Select a process.
2. Click the *Kill Process* dropdown.
3. Select one of the following options:
   - *Kill*: the standard kill option that produces one line in the crash log (`diagnose debug crashlog read`).
   - *Force Kill*: the equivalent to `diagnose sys kill 9 <pid>`. This can be viewed in the crash log.
   - *Kill & Trace*: the equivalent to `diagnose sys kill 11 <pid>`. This generates a longer crash log and backtrace. A crash log is displayed afterwards.

Proxy Settings

For more information about web proxy and explicit web proxy, see Deployments on page 67.

This section covers the following topics:

- Explicit Proxy on page 109
- Web Proxy Setting on page 143
- Web Proxy Profile on page 145
- Forwarding Server on page 159
- Server URL on page 166
- FTP Proxy on page 169
- Proxy Options on page 171
- SSL Keyring on page 179

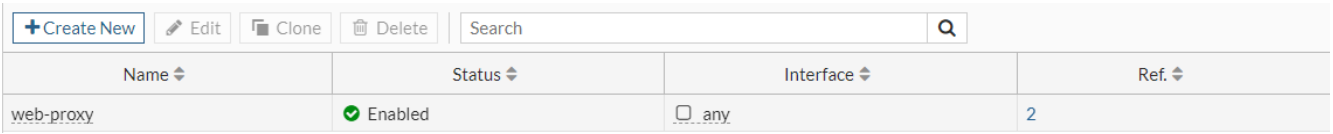
Explicit Proxy

Use the explicit web proxy configuration to enable the explicit HTTP proxy on one or more Fortinet interfaces. IPv6 is supported.



IP pools support the explicit web proxy, allowing such traffic to be sourced from a range of IP addresses.

To configure the explicit web proxy configuration, go to *Proxy Settings* > *Explicit Proxy*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

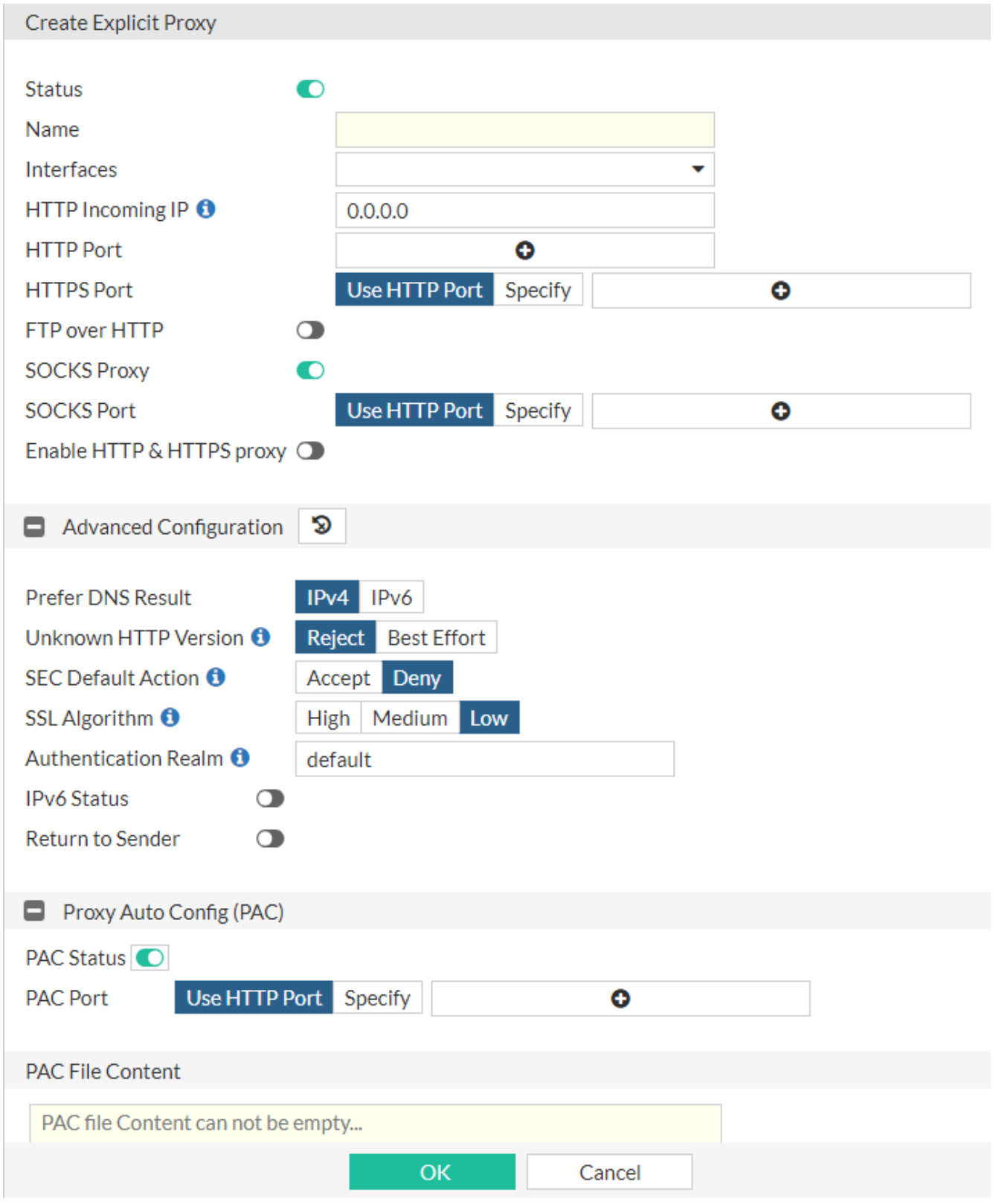
The following options are available:

Create New	Create an explicit web proxy configuration. See Create or edit an explicit proxy on page 110.
Edit	Modify settings to an explicit web proxy configuration. See Create or edit an explicit proxy on page 110.
Clone	Copies an existing explicit web proxy configuration.

Delete	Remove a proxy from the list.
Search	Enter a search term to find in the list.
Name	The name of the explicit web proxy configuration.
Status	The status of the explicit web proxy configuration.
Interface	The interface to which the proxy applies.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an explicit proxy

Select *Create New* to open the *Create Explicit Proxy* window.



Select an explicit proxy configuration and then click *Edit* to open the *Edit Explicit Proxy* window.

Configure the following settings in the *Explicit Proxy* window and then click *OK*:

Status	This explicit web proxy configuration is enabled by default. Toggle to disable this explicit web proxy configuration.
Name	Enter the name of the explicit web proxy configuration.
Interfaces	Select the interface or interfaces that are being monitored by the explicit web proxy from the drop-down list.
HTTP Incoming IP	Select an HTTP cncoming IP from the drop-down list. This field restricts the explicit HTTP proxy to accept sessions only from the specified IP address.
HTTP Port	Enter the port number that HTTP traffic from client web browsers use to connect to the explicit proxy for the specific protocol. Explicit proxy users must configure their web browser's protocols proxy settings to use this port. The default port is 8080. You can enter a maximum of eight ports. Separate multiple ports with a comma. The range of values is 1-65535.
HTTPS Port	Select *Use HTTP Port* or select *Specify* and then enter the port number that HTTPS traffic from client web browsers use to connect to the explicit proxy for the specific protocol. Explicit proxy users must configure their web browser's protocols proxy settings to use this port. You can enter a maximum of eight ports. Separate multiple ports with a comma. The range of values is 1-65535.
FTP Over HTTP	Select this checkbox to enable FTP over HTTP for the explicit web proxy. Then select *Use HTTP Port* or select *Specify* and enter the port number.  The FTP over HTTP proxy engine supports PORT mode, FTP over HTTP CONNECT, and uploads through PUT (UTM scanning).
SOCKS Proxy	Select this checkbox to enable the SOCKS proxy. Then select *Use HTTP Port* or select *Specify* and enter the port number.
Enable HTTP/HTTPS proxy	Select this option to enable HTTP/HTTPS proxy. The default is enabled.
Prefer DNS Result	Select whether the DNS result uses an *IPv4* or *IPv6* address.
Unknown HTTP Version	You can select the action to take when the proxy server must handle an unknown HTTP version request or message. Set the unknown HTTP version to *Best Effort*, *Reject*, or *Tunnel*. • *Best Effort* attempts to handle the HTTP traffic as best as it can. • *Reject* treats known HTTP traffic as malformed and drops it.
SEC Default Action	Accept or deny explicit web proxy sessions when no web proxy firewall policy exists.

SSL Algorithm	Select the strength of the encryption algorithms accepted in HTTPS deep scan.
Authentication Realm	Enter an authentication realm to identify the explicit web proxy. The realm can be any text string of up to 63 characters. If the realm includes spaces, you need to enclose it in quotes. When a user authenticates with the explicit web proxy, the HTTP authentication dialog box includes the realm so that you can use the realm to identify the explicitly web proxy for your users.
IPv6 Status	Toggle this setting if you want to use IPv6 addresses.
Return to Sender	Toggle this setting to allow the FortiProxy to remember the MAC address of the last hop and send responses to that MAC address instead of the default gateway.
PAC Status	Toggle this setting to use a proxy auto-config (PAC) file to define how web browsers can choose a proxy server for receiving HTTP content. PAC files include the FindProxyForURL(url, host) JavaScript function that returns a string with one or more access method specifications. These specifications cause the web browser to use a particular proxy server or to connect directly.
PAC Port	Select *Use HTTP Port* or select *Specify* and then enter the port number that traffic from client web browsers use to connect to the explicit proxy for the specific protocol. Explicit proxy users must configure their web browser's protocols proxy settings to use this port.
PAC File Content	Select *Edit* to make changes to a PAC file that was previously uploaded or select *Download* and then select *Save* to save a copy of the PAC file.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Secure explicit proxy

Secure explicit web proxy with HTTPS connections is supported between web clients and the FortiProxy.

```
config web-proxy explicit-proxy
    set secure-web-proxy {disable | enable | secure}
    set secure-web-proxy-cert <certificate1> <certificate2> ...
    set ssl-dh-bits {768 | 1024 | 1536 | 2048}
end
```

`secure-web-proxy {disable | enable | secure}`	Enable/disable/require the secure web proxy for HTTP and HTTPS session. • `disable`: disable secure web proxy (default) • `enable`: enable secure web proxy access, allowing both HTTPS and HTTP connections to the explicit proxy • `secure`: require secure web proxy access, allowing only HTTPS connections to the explicit proxy
`secure-web-proxy-cert <certificate1> <certificate2> ...`	Enter the names of the server certificates in the local certificate store of the FortiProxy used to establish a TLS connection between the user's browser and the FortiProxy. Multiple server certificates can be configured, and different certificate types can be used. The SNI tries to match the right server certificate for the connection. If the SNI cannot not match with the certificates' CN or SAN, the first server certificate will be offered.
`ssl-dh-bits {768 | 1024 | 1536 | 2048}`	Set the bit size of Diffie-Hellman (DH) prime used in the DHE-RSA negotiation. • `768`: use 768-bit Diffie-Hellman prime • `1024`: use 1024-bit Diffie-Hellman prime • `1536`: use 1536-bit Diffie-Hellman prime • `2048`: use 2048-bit Diffie-Hellman prime (default)

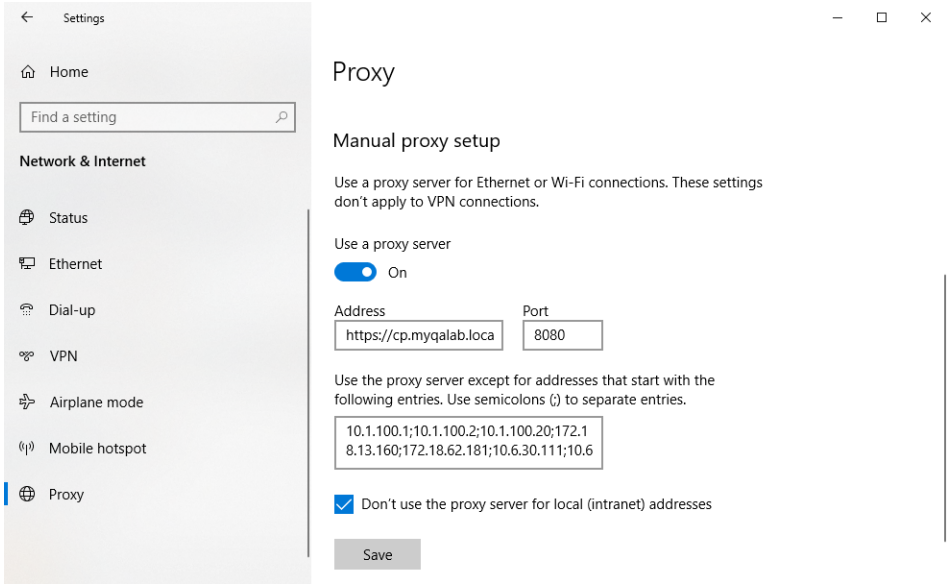
Example

In this example, a Windows PC user configures an HTTPS URL (https://cp.myqalab.local) as the proxy address for the explicit web proxy. When the user opens a browser (such as Edge or Chrome), the browser will use the HTTPS URL to connect to the explicit web proxy and send any HTTP requests to the proxy over HTTPS. The certificate (server_cert) contains the explicit web proxy's name (cp.myqalab.local) as its CN, so the browser will accept this certificate for the TLS connection.



To configure the Windows proxy settings:

1. On the Windows PC, go to *Settings* > *Network & Internet* > *Proxy*.
2. In the *Manual proxy setup* section configure the following:
   a. Enable *Use a proxy server*.
   b. Set the *Address* to *https://cp.myqalab.local*.
   c. Set the *Port* to *8080*.
   d. If needed, enter any addresses to exempt in the text box (use a semicolon to separate entries).
   e. Enable *Don't use the proxy server for local (intranet) addresses*.



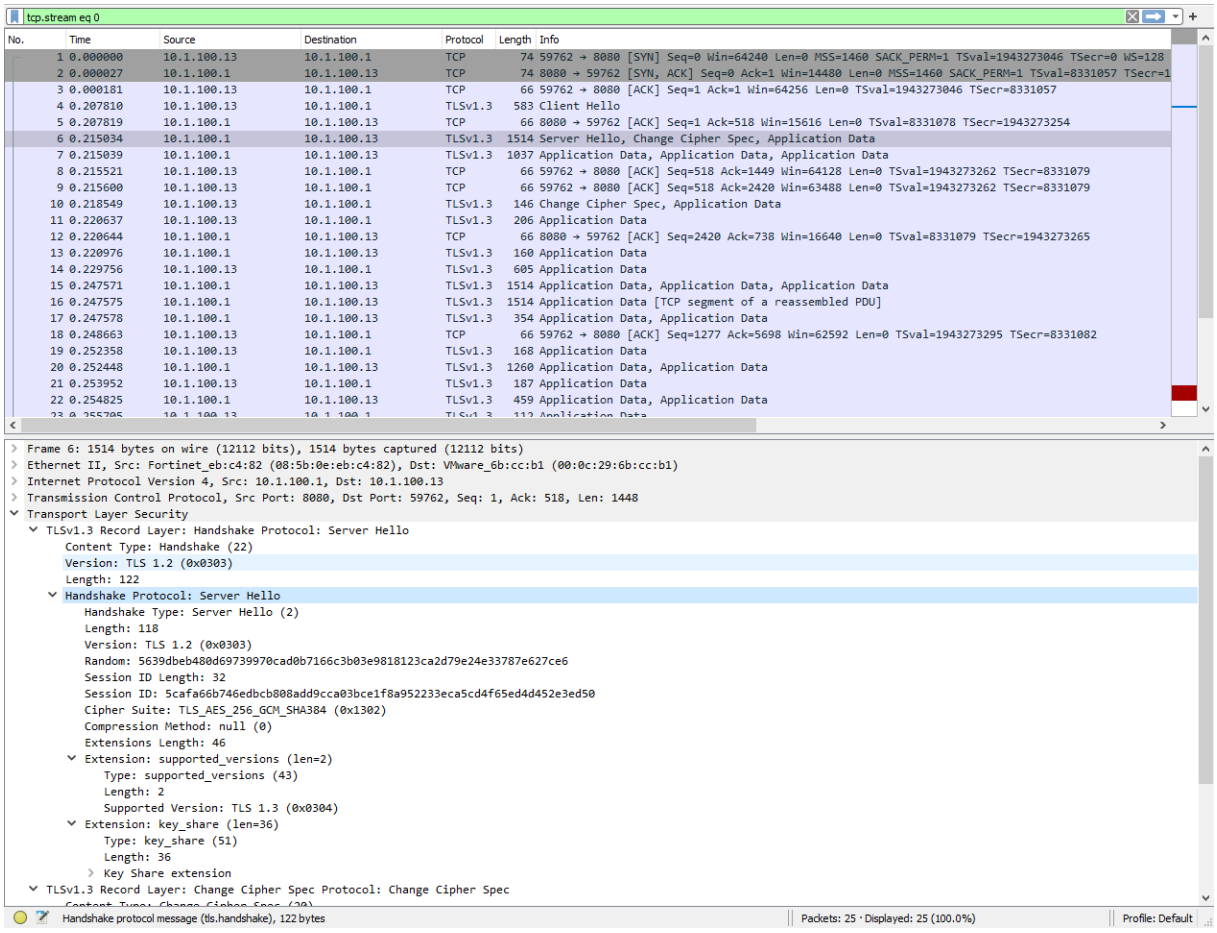
3. Click *Save*.

To configure the secure explicit web proxy:

```
config web-proxy explicit-proxy
    set status enable
    set secure-web-proxy enable
    set ftp-over-http enable
    set socks enable
    set http-incoming-port 8080
    set secure-web-proxy-cert "server_cert"
    set socks-incoming-port 1080
    set ipv6-status enable
    set unknown-http-version best-effort
    set pac-file-server-status enable
    set pac-file-data "function FindProxyForURL(url, host) {
   // testtest
   return \"PROXY 10.1.100.1:8080\";
}
"
    set pac-file-through-https enable
end
```

To verify the TLS connection:

1. Perform a packet capture of HTTPS traffic between the web client and the web server. Wireshark is used in this example.
2. Locate the exchange between the web client (10.1.100.13) and the explicit web proxy (10.1.100.1:8080):



After the client initiates the TLS connection to the explicit web proxy with a client hello packet, the web proxy is able to respond appropriately with a server hello packet to establish a TLS connection first before any HTTP messages are exchanged, and all HTTP messages will be protected by the TLS connection.

Proxy chaining

For explicit web proxy, you can configure proxy chaining by setting up a series of forwarding servers to redirect HTTP/HTTPS, FTP, and SOCKS proxy sessions from the FortiProxy unit to a remote network or other proxy servers on your network, including a remote FortiProxy unit with explicit proxy enabled. You can use proxy chaining to integrate the FortiProxy explicit proxy with a proxy solution that you already have in place.

You can deploy the explicit proxy with proxy chaining in an enterprise environment consisting of small satellite offices and a main office. If each office has a FortiProxy unit, users at each of the

satellite offices can use their local FortiProxy unit as an explicit proxy server. The satellite office FortiProxy units can forward explicit proxy sessions to an explicit proxy server at the central office. From here the sessions can connect to web servers on the Internet.



FortiProxy proxy chaining does not support proxies in the proxy chain authenticating each other.

To configure proxy chaining:

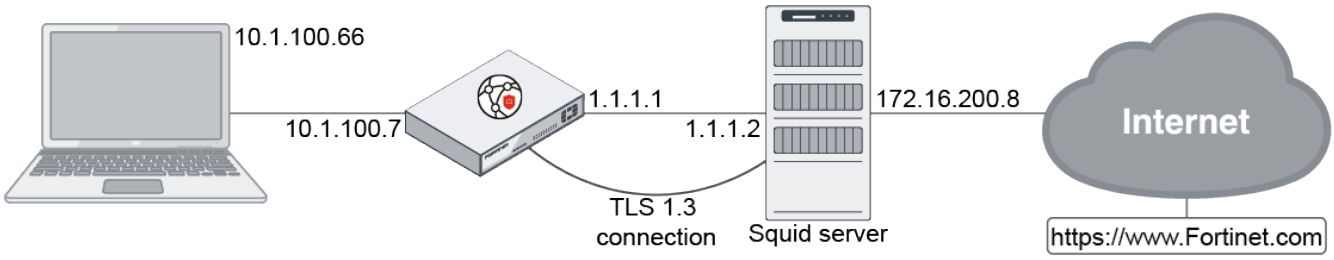
1. Make sure explicit proxy is enabled:
   - **GUI**—Navigate to the *System > Feature Visibility* page and check the *Explicit Proxy* option in the *Core Features* column.
   - **CLI**—Enable the `set explicit-web-proxy` (for HTTP/HTTPS and SOCKS) and `set explicit-ftp-proxy` (for FTP) options in the `config system interface` command.
2. If you do not have an explicit proxy already, configure one and make sure it is enabled:
   - **GUI**—Refer to Create or edit an explicit proxy on page 110 for HTTP/HTTPS/SOCKS. Refer to FTP Proxy on page 169 for FTP.
   - **CLI**—Use the `config web-proxy explicit-proxy` command.
3. Create a Forwarding Server on page 159:
   - **GUI**—Refer to Create or edit a forwarding server on page 160. You cannot set the protocol of the forwarding server in GUI. HTTP/HTTPS and SOCKS are enabled by default. To set the protocol to FTP, use the `set protocol ftp` option under the `config web-proxy forward-server` command.
   - **CLI**—Use the `config web-proxy forward-server` command. HTTP/HTTPS and SOCKS are enabled by default. To set the protocol to FTP, use the `set protocol ftp` option.
4. Repeat step 3 for each additional forwarding server you want to add to the proxy chain. Make sure you configure the forwarding servers in sequence so that each one acts as the destination of the previous server and source of the next server.
5. **(Optional)** Use the `config web-proxy forward-server-group` command to create a forwarding server group to host all the forwarding servers you just created. Doing so saves some management overhead, especially in case of a large number of forwarding servers. Refer to Grouping forwarding servers and load balancing traffic to the servers on page 165 for more details.
6. Configure an explicit policy and add the forwarding servers or forwarding server group to the policy:
   - **GUI**—See Create or edit a policy on page 387. For HTTP/HTTPS/SOCKS, select the *Explicit* type. For FTP, select the *FTP* type. To add the forwarding servers or forwarding server group to the policy, use the *Web Proxy Forwarding Server* option for HTTP/HTTPS/SOCKS. For FTP, the forwarding servers or group can only be added using the `set webproxy-forward-server` option under the `config firewall policy` command.
   - **CLI**—Use the `config firewall policy` command.

   All explicit proxy traffic accepted by this policy will then be forwarded to the specified forwarding server or server group. For example, the following configuration adds a policy that allows all users on the `10.31.101.0` subnet to use the explicit proxy for connections through the `wan1` interface to the Internet. The policy forwards proxy sessions to a remote forwarding server named *fwd-srv*.

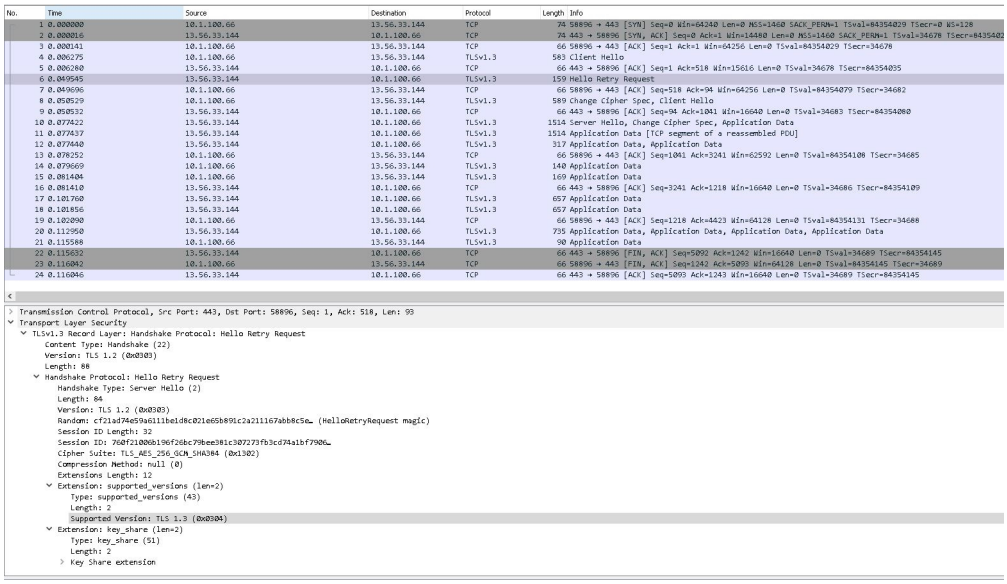
```
config firewall policy
        edit 0
                set type explicit-web
                set dstintf "wan1"
                set srcaddr "Internal_subnet"
                set dstaddr "all"
                set service "webproxy"
                set action accept
                set schedule "always"
                set webproxy-forward-server "fwd-srv"
        next
end
```

Example: Using TLS 1.3 with chaining proxy forwarding servers

The following example involves a proxy chain of the Squid server and the FortiProxy, both of which can handle TLS 1.3 traffic.



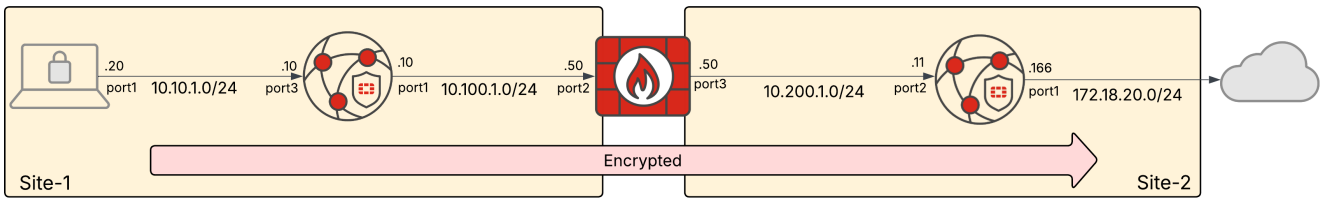
The following output from the Squid server demonstrates that the FortiProxy forwards the hello retry request back to the client PC. The client PC then sends the client hello again, and the connection is successfully established.



Proxy chaining over IPsec tunnel

You can configure proxy chaining over an IPsec VPN tunnel to ensure that all traffic forwarded from the inside to the outside proxy is encrypted.

Network Topology



To configure an IPsec VPN tunnel:

Refer to Basic site-to-site VPN with pre-shared key on page 780 to create the Site-1 and Site-2 IPsec site-to-site tunnels based on the network topology.

To configure Site-2:

1. Configure the interface as follows:

```
config system interface
   edit "port1" <<-outside-interface
      set vdom "root"
      set ip 172.18.20.166 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric ftm
          speed-test
      set type physical
      set explicit-web-proxy enable
      set explicit-ftp-proxy enable
      set alias "Site-2-External"
      set snmp-index 1
      next
   edit "port2" <<-inside-interface
      set vdom "root"
      set ip 10.200.1.11 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric ftm
          speed-test
      set type physical
      set explicit-web-proxy enable
      set explicit-ftp-proxy enable
      set alias "Site-2-Internal"
      set snmp-index 3
      next
   edit "to-site-1"
      set vdom "root"
      set type tunnel
      set explicit-web-proxy enable
      set explicit-ftp-proxy enable
      set snmp-index 4
```

```
      set interface "port2"
   next
end
```

2. Configure the IPsec tunnel as follows:

```
config vpn ipsec phase1-interface
    edit "to-site-1"
        set interface "port2" <<- inside-interface
        set peertype any
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: to-site-1 (Created by VPN wizard)"
        set remote-gw 10.100.1.10 <<- outside interface of Site-1 device
        set psksecret ENC
      Im/HjW6abJFHgpclP7XYqJcreuVNxJZLDT32LOJDwXnNprNtQJ9n3N2VDM6Q9kxuviUPaiRA9Wq+dodgs5PKhhmmE2
      LzGMlsi6kNas8ZMw6Q1uF3iJkLcvzZap7M9m5+8Ay8zMzR97m4zpgt80RculvXt26q6pU7UIsjTOtf1FDnnf7T0RCz
      U4n/WiTe2LbUJ2VKs1lmMjY3dkVA
    next
end
config vpn ipsec phase2-interface
    edit "to-site-1"
        set phase1name "to-site-1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
      chacha20poly1305
        set comments "VPN: to-site-1 (Created by VPN wizard)"
        set src-addr-type name
        set dst-addr-type name
        set src-name "to-site-1_local"
        set dst-name "to-site-1_remote"
    next
end
```

3. Configure the static route as follows:
   - Route to the outside interface/subnet of the Site-1 proxy via the inside interface
   - Route to the Site-1 inside explicit proxy address/subnet via the VPN tunnel
   - Default route via the outside interface

```
config router static
    edit 1
        set gateway 172.18.20.1
        set device "port1"
    next
    edit 2
        set dst 10.100.1.0 255.255.255.0
        set gateway 10.200.1.50
        set device "port2"
    next
    edit 3
        set device "to-site-1"
        set comment "VPN: to-site-1 (Created by VPN wizard)"
        set dstaddr "to-site-1_remote"
    next
end
```

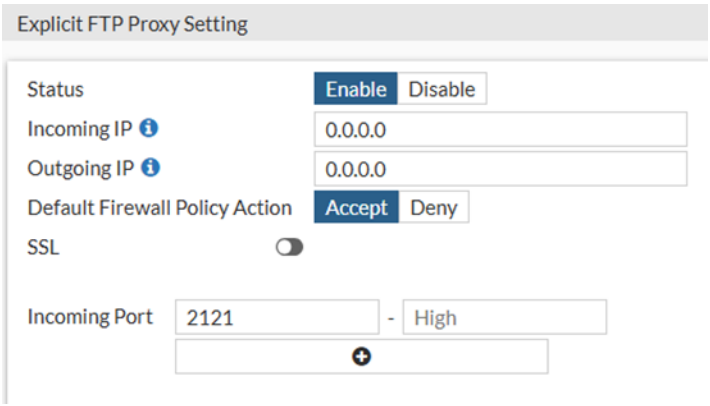
4. Configure the explicit proxy as follows:

```
config web-proxy explicit-proxy
    edit "web-proxy"
        set status enable
        set interface "to-site-1"
        set http-incoming-port 8080
```

```
        set https-incoming-port 8080
    next
end
```

5. Configure the explicit FTP proxy as follows:

```
config ftp-proxy explicit
    set status enable
    set incoming-port 2121
    set outgoing-ip 0.0.0.0
    set sec-default-action accept
end
```



6. Configure the firewall proxy policy as follows:

```
config firewall policy
    edit 1
        set type explicit-web
        set name "Upstream proxy in Site-2"
        set uuid f8aac3fa-1005-51f0-f549-57daac806021
        set dstintf "port1" <<-outside interface
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "webproxy"
        set explicit-web-proxy "web-proxy"
        set webproxy-profile "XFF-Site-2"
        set logtraffic all
        set log-http-transaction enable
    next
    edit 3
        set type explicit-ftp
        set name "ftp-proxy-policy"
        set uuid 3a1cbbfa-10aa-51f0-c416-4cd82a72e04f
        set dstintf "port1" <<-outside interface
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set logtraffic all
    next
end
```

7. Configure DNS service as follows:

```
config system dns-server
    edit "to-site-1"
```

```
    next
end
```

To configure Site-1:

1. Configure the interface as follows:

```
config system interface
    edit "port2" <<-outside-interface
        set vdom "root"
        set ip 10.100.1.10 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
      ftm speed-test
        set type physical
        set alias "to_site-2"
        set snmp-index 3
    next
    edit "port3" <<-inside-interface
        set vdom "root"
        set ip 10.10.1.10 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric
      ftm speed-test
        set type physical
        set explicit-web-proxy enable
        set explicit-ftp-proxy enable
        set snmp-index 4
    next
    edit "to-site-2"
        set vdom "root"
        set type tunnel
        set snmp-index 5
        set interface "port2"
    next
end
```

2. Configure the IPsec tunnel as follows:

```
config vpn ipsec phase1-interface
    edit "to-site-2"
        set interface "port2" <<-outside-interface
        set peertype any
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: to-site-2 (Created by VPN wizard)"
        set remote-gw 10.200.1.11 <<-inside interface of Site-2 device
        set psksecret ENC
      MAmDuLLv4/T5ydYd4qglW6fcNyfbSlq1LMl25rDwAaFe4XhXwW8Ryec7fRXHagbGF4Dvn2Ccr4wYdSjIYkbDY9Dwz3
      wEuYCXKHzqHx+FST1oU5DQb4KpcPsR7BgGjShNkeLVnV1HUTUhpIJDyxJzb04wMu0OFljY6ru4rNcMUy7lxxUreJgV
      oMdCbWLrCcETY+TDyFlmMjY3dkVA
    next
end
config vpn ipsec phase2-interface
    edit "to-site-2"
        set phase1name "to-site-2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
      chacha20poly1305
        set comments "VPN: to-site-2 (Created by VPN wizard)"
        set src-addr-type name
        set dst-addr-type name
        set src-name "to-site-2_local"
```

```
        set dst-name "to-site-2_remote"
    next
end
```

3. Configure the static route as follows:
   - Route to the inside interface/subnet of the Site-2 proxy via the outside interface
   - Route to the outside interface/subnet of the Site-2 proxy via the VPN tunnel
   - Configure "preferred-source" as Site-1 FPX inside interface ip (10.10.1.10) under VPN tunnel route.

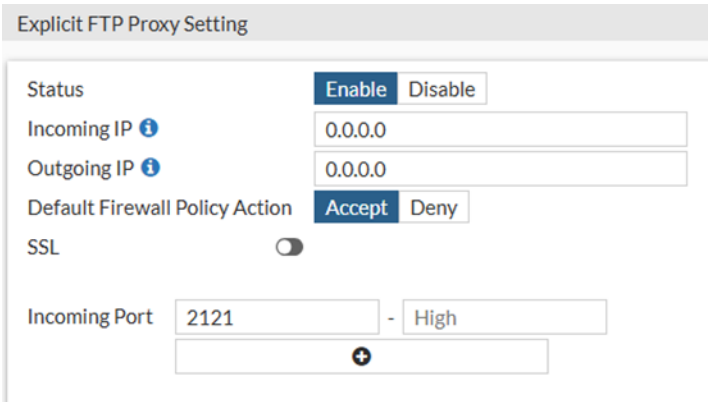
```
config router static
    edit 1
        set dst 10.200.1.0 255.255.255.0
        set gateway 10.100.1.50
        set device "port2"
    next
    edit 2
        set preferred-source 10.10.1.10
        set device "to-site-2"
        set comment "VPN: to-site-2 (Created by VPN wizard)"
        set dstaddr "to-site-2_remote"
    next
end
```

4. Configure the explicit policy as follows:

```
config web-proxy explicit-proxy
    edit "web-proxy"
        set status enable
        set interface "port3"
        set http-incoming-port 8080
        set https-incoming-port 8080
        set incoming-ip 10.10.1.10 <<-port3 ip address
    next
end
```

5. Configure the explicit FTP proxy as follows:

```
config ftp-proxy explicit
    set status enable
    set incoming-port 2121
    set outgoing-ip 0.0.0.0
    set sec-default-action accept
end
```



6. Configure the forward server as follows:

```
config web-proxy forward-server
```

```
    edit "http-to-site-2"
        set ip 172.18.20.166 <<-outside interface IP address of Site-2 proxy
        set port 8080
        set protocol http
    next
    edit "ftp-to-site-2"
        set ip 172.18.20.166 <<- outside interface IP address of Site-2 proxy
        set port 2121
        set protocol ftp
    next
end
```

7. Configure the server list as follows:

```
config web-proxy url-match
    edit "www.fortinet.com"
        set explicit-web-proxy "web-proxy"
        set url-pattern "www.fortinet.com"
        set forward-server "http-to-site-2"
    next
end
```

8. Configure the firewall proxy server as follows:

```
config firewall policy
     edit 4
        set type explicit-ftp
        set name "ftp-proxy-chaining"
        set uuid a36d1baa-10a9-51f0-7706-d06775cd89be
        set dstintf "to-site-2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set logtraffic all
        set logtraffic-start enable
        set webproxy-forward-server "ftp-to-site-2"
    next
    edit 1
        set type explicit-web
        set name "server-url-match-forward"
        set uuid eb97a0d0-1004-51f0-01f6-2c7c369110d4
        set dstintf "to-site-2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "webproxy"
        set explicit-web-proxy "web-proxy"
        set logtraffic all
        set log-http-transaction enable
     next
 end
```

9. Configure FortiGuard as follows:

```
 config system autoupdate tunneling
     set status enable
     set address "172.18.20.166"
     set port 8080
 end
```

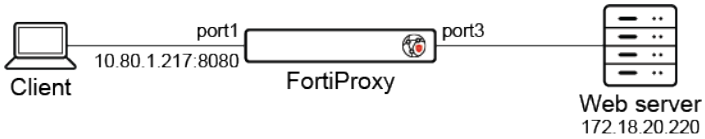
Forward HTTPS requests to a web server without the need for an HTTP CONNECT message

An explicit web proxy can forward HTTPS requests to a web server without the need for an HTTP CONNECT message. The FortiProxy explicit web proxy can be configured to detect the HTTPS scheme in the request line of a plain text HTTP request and forward it as an HTTPS request to the web server. This allows applications that cannot use the CONNECT message for sending an HTTPS request to communicate with the web server through an explicit web proxy.

```
config firewall policy
    edit <id>
        set detect-https-in-http-request {enable | disable}
    next
end
```

Example

Based on the following topology, an HTTPS request is sent to a web server through an explicit web proxy.



To enable detection of HTTPS in an HTTP request:

1. Configure the explicit web proxy:

```
config web-proxy explicit-proxy
    set status enable
    set interface "any"
    set http-incoming-port 8080
    set https-incoming-port 8080
    set unknown-http-version best-effort
end
```

2. Enable the explicit web proxy on port1:

```
config system interface
    edit "port1"
        set ip 10.80.1.217 255.255.255.0
        set explicit-web-proxy enable
    next
end
```

3. Configure the firewall policy:

```
config firewall policy
    edit 4
        set type explicit-web
        set name "expp"
        set uuid 6461ddca-d87f-51ec-d47a-ceb0934db42e
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "webproxy"
        set explicit-web-proxy "web-proxy"
        set utm-status enable
        set logtraffic all
        set log-http-transaction all
        set extended-log enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "default"
        set detect-https-in-http-request enable
    next
end
```



An SSL-SSH profile with deep inspection must be applied in order to decrypt the server response in HTTPS and forward the response to the client by HTTP.

4. Using Telnet, send an HTTP request with an HTTPS scheme as follows:

```
telnet 10.80.1.217 8080
Trying 10.80.1.217...
Connected to 10.80.1.217.
Escape character is '^]'.
POST https://172.18.20.220/ HTTP/1.1
Host: 172.18.20.220
User-Agent: curl/7.68.0
Accept: */*
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

HTTP/1.1 200 OK
```

5. Verify the traffic log. The HTTP request is forwarded to the server successfully by HTTPS:

```
# execute log filter category 3
...
2: date=2024-04-23 time=10:01:34 eventtime=1713891694636926727 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.80.1.57 srcport=46486
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.18.20.220 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=1035953713
service="
HTTPS" proxyapptype="web-proxy" proto=6 action="accept" policyid=4 policytype="proxy-policy"
```

```
poluuid="6461ddca-d87f-51ec-d47a-ceb0934db42e" policyname="expp" trandisp="snat"
transip=10.80.1.217 transport=20300 clientip=10.80.1.57 duration=123121 wanin=12791
rcvdbyte=12791 wanout=773 lanin=172 sentbyte=172 lanout=11229 appcat="unscanned"
utmaction="allow"
```

HTTP connection coalescing and concurrent multiplexing for explicit proxy

HTTP connection coalescing and concurrent multiplexing allows multiple HTTP requests to share the same TCP three-way handshake when the destination IP is the same.

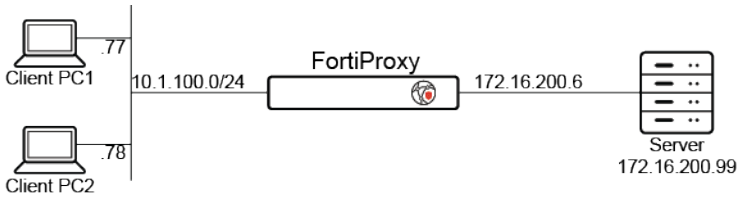
To configure the explicit web proxy:

```
config web-proxy explicit
    set http-connection-mode {static | multiplex | serverpool}
end
```

`http-connection-mode {static | multiplex | serverpool}`	Set the HTTP connection mode: • static: only one server connection exists during the proxy session (default). • multiplex: hold established connections until the proxy session ends. • serverpool: share established connections with other proxy sessions.

Example

In this example, multiple clients submit requests in HTTP. The requests hit the VIP address, and then FortiProxy opens a session between itself (172.16.200.6) and the server (172.16.200.99). The coalescing occurs in this session as the multiple streams share the same session to connect to the same destination server.



To configure connection coalescing and concurrent multiplexing with an explicit proxy:

1. Configure the explicit web proxy:

```
config web-proxy explicit
    set status enable
```

```
    set http-incoming-port 8080
    set http-connection-mode serverpool
end
```

2. Enable explicit web proxy on port2:

```
config system interface
    edit "port2"
        set ip 10.1.100.6 255.255.255.0
        set explicit-web-proxy enable
    next
end
```

3. Configure the policy:

```
config firewall policy
    edit 1
        set proxy explicit-web
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set service "web"
        set action accept
        set schedule "always"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set utm-status enable
        set profile-protocol-options "default-clone"
        set ssl-ssh-profile "deep-inspection-clone"
    next
end
```

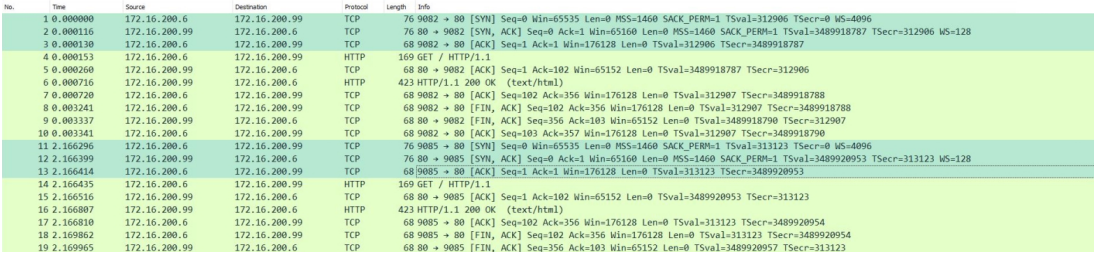
4. Get the clients to access the server through the explicit web proxy (10.1.100.6:8080). The FortiProxy shares the first connection TCP three-way handshake with later connections that connect to same destination address.
5. Verify the sniffer packet capture on the FortiProxy server side. There is one TCP three-way handshake, but there are two HTTP connections.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.200.6	172.16.200.99	TCP	76	8874 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=288652 TSecr=0 WS=4096
2	0.000099	172.16.200.99	172.16.200.6	TCP	76	80 → 8874 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3489676249 TSecr=288652 WS=128
3	0.000114	172.16.200.6	172.16.200.99	TCP	68	8874 → 80 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=288652 TSecr=3489676249
4	0.000137	172.16.200.6	172.16.200.99	HTTP	169	GET / HTTP/1.1
5	0.000208	172.16.200.99	172.16.200.6	TCP	68	80 → 8874 [ACK] Seq=1 Ack=102 Win=65152 Len=0 TSval=3489676249 TSecr=288652
6	0.000503	172.16.200.99	172.16.200.6	HTTP	423	HTTP/1.1 200 OK (text/html)
7	0.000507	172.16.200.6	172.16.200.99	TCP	68	8874 → 80 [ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=288652 TSecr=3489676249
8	2.148158	172.16.200.6	172.16.200.99	HTTP	169	GET / HTTP/1.1
9	2.148419	172.16.200.99	172.16.200.6	HTTP	399	HTTP/1.1 200 OK (text/html)
10	2.148430	172.16.200.6	172.16.200.99	TCP	68	8874 → 80 [ACK] Seq=203 Ack=687 Win=176128 Len=0 TSval=288867 TSecr=3489678397

6. Change the HTTP connection mode to static:

```
config web-proxy explicit
    set status enable
    set http-incoming-port 8080
    set http-connection-mode static
end
```

7. Verify the sniffer packet capture. This time, the FortiProxy establishes a TCP connection for each client.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.200.6	172.16.200.99	TCP	76	9082 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=312906 TSecr=0 WS=4096
2	0.000116	172.16.200.99	172.16.200.6	TCP	76	80 → 9082 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3489918787 TSecr=312906 WS=128
3	0.000130	172.16.200.6	172.16.200.99	TCP	68	9082 → 80 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=312906 TSecr=3489918787
4	0.000153	172.16.200.6	172.16.200.99	HTTP	169	GET / HTTP/1.1
5	0.000260	172.16.200.99	172.16.200.6	TCP	68	80 → 9082 [ACK] Seq=1 Ack=102 Win=65152 Len=0 TSval=3489918787 TSecr=312906
6	0.000716	172.16.200.99	172.16.200.6	HTTP	423	HTTP/1.1 200 OK (text/html)
7	0.000720	172.16.200.6	172.16.200.99	TCP	68	9082 → 80 [ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=312907 TSecr=3489918788
8	0.003241	172.16.200.6	172.16.200.99	TCP	68	9082 → 80 [FIN, ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=312907 TSecr=3489918788
9	0.003337	172.16.200.99	172.16.200.6	TCP	68	80 → 9082 [FIN, ACK] Seq=356 Ack=103 Win=65152 Len=0 TSval=3489918790 TSecr=312907
10	0.003341	172.16.200.6	172.16.200.99	TCP	68	9082 → 80 [ACK] Seq=103 Ack=357 Win=176128 Len=0 TSval=312907 TSecr=3489918790
11	2.166296	172.16.200.6	172.16.200.99	TCP	76	9085 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=313123 TSecr=0 WS=4096
12	2.166399	172.16.200.99	172.16.200.6	TCP	76	80 → 9085 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3489920953 TSecr=313123 WS=128
13	2.166414	172.16.200.6	172.16.200.99	TCP	68	9085 → 80 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=313123 TSecr=3489920953
14	2.166435	172.16.200.6	172.16.200.99	HTTP	169	GET / HTTP/1.1
15	2.166516	172.16.200.99	172.16.200.6	TCP	68	80 → 9085 [ACK] Seq=1 Ack=102 Win=65152 Len=0 TSval=3489920953 TSecr=313123
16	2.166807	172.16.200.99	172.16.200.6	HTTP	423	HTTP/1.1 200 OK (text/html)
17	2.166810	172.16.200.6	172.16.200.99	TCP	68	9085 → 80 [ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=313123 TSecr=3489920954
18	2.169862	172.16.200.6	172.16.200.99	TCP	68	9085 → 80 [FIN, ACK] Seq=102 Ack=356 Win=176128 Len=0 TSval=313123 TSecr=3489920954
19	2.169965	172.16.200.99	172.16.200.6	TCP	68	80 → 9085 [FIN, ACK] Seq=356 Ack=103 Win=65152 Len=0 TSval=3489920957 TSecr=313123

Secure explicit proxy with client certificates

The explicit web proxy policy can use client certificates for validation. In this example, a CA signs a client certificate. The client certificate is installed on an endpoint, and the root CA is imported to FortiGate. A web proxy policy is configured to require the client certificate.

When the user accesses a web site, the explicit web proxy policy uses the client certificate from the endpoint device to authenticate the user and grant access to the web site.

To configure client certificates with explicit proxies:

1. Prepare the certificate:
   a. Use a CA to sign the client certificate.
   b. Import the root CA certificate that signed the client certificate to FortiProxy. In this scenario, the certificate is Fortinet_SSL.
   c. Install the client certificate on an endpoint.
2. Configure the explicit web-proxy policy to request the client certificate from the endpoint.

```
config web-proxy explicit-proxy
                                        edit "web-proxy"
                                    set status enable
                                    set interface "any"
                                    set secure-web-proxy enable
                                    set http-incoming-port 8080
                                    set secure-web-proxy-cert "Fortinet_SSL"
                                    next
                                end
```

```
config firewall access-proxy
                                    edit "httpsvip"
                                    set vip "httpsvip"
                                    set client-cert enable
                                    set empty-cert-action block
                                    config api-gateway
                                    edit 1
                                    config realservers
                                    edit 1
                                    set ip 10.100.1.78
                                    next
                                    end
```

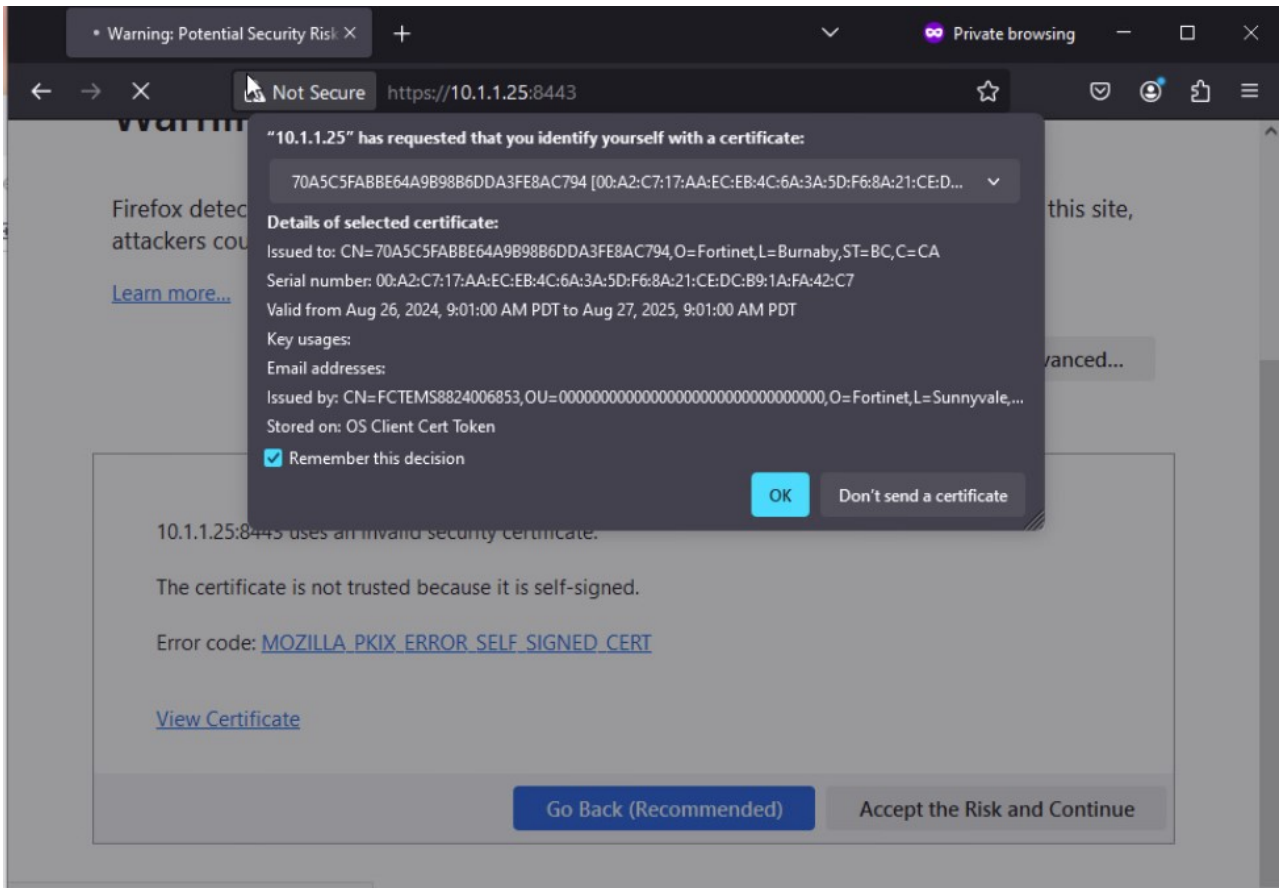
```
                                        next
                                        end
                                        next
                                        end
```

3. Configure verification of the client certificate with the Fortinet_SSL CA.

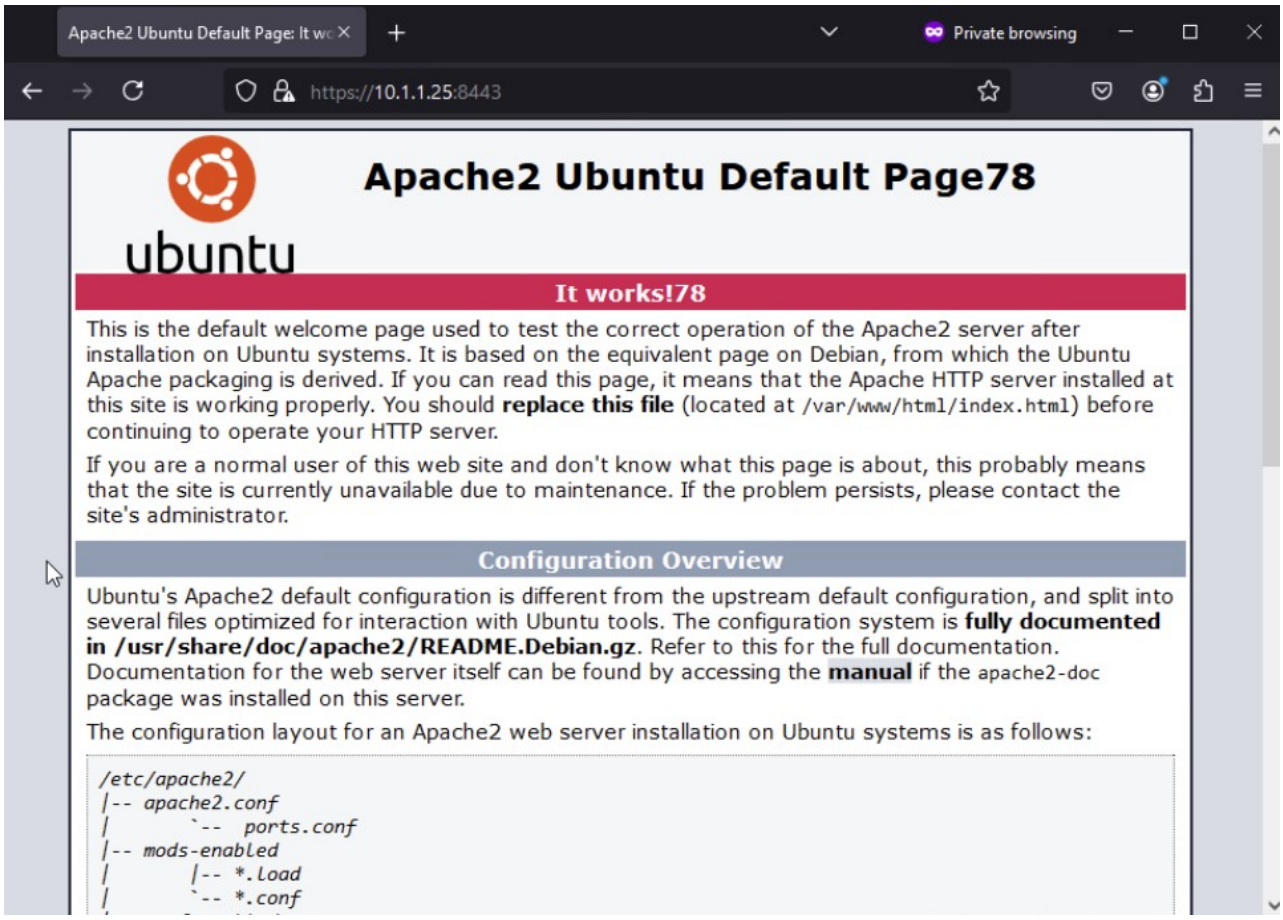
```
config authentication setting
                                              set user-cert-ca "Fortinet_CA_SSL"
                                end
```

When the user accesses a web site:

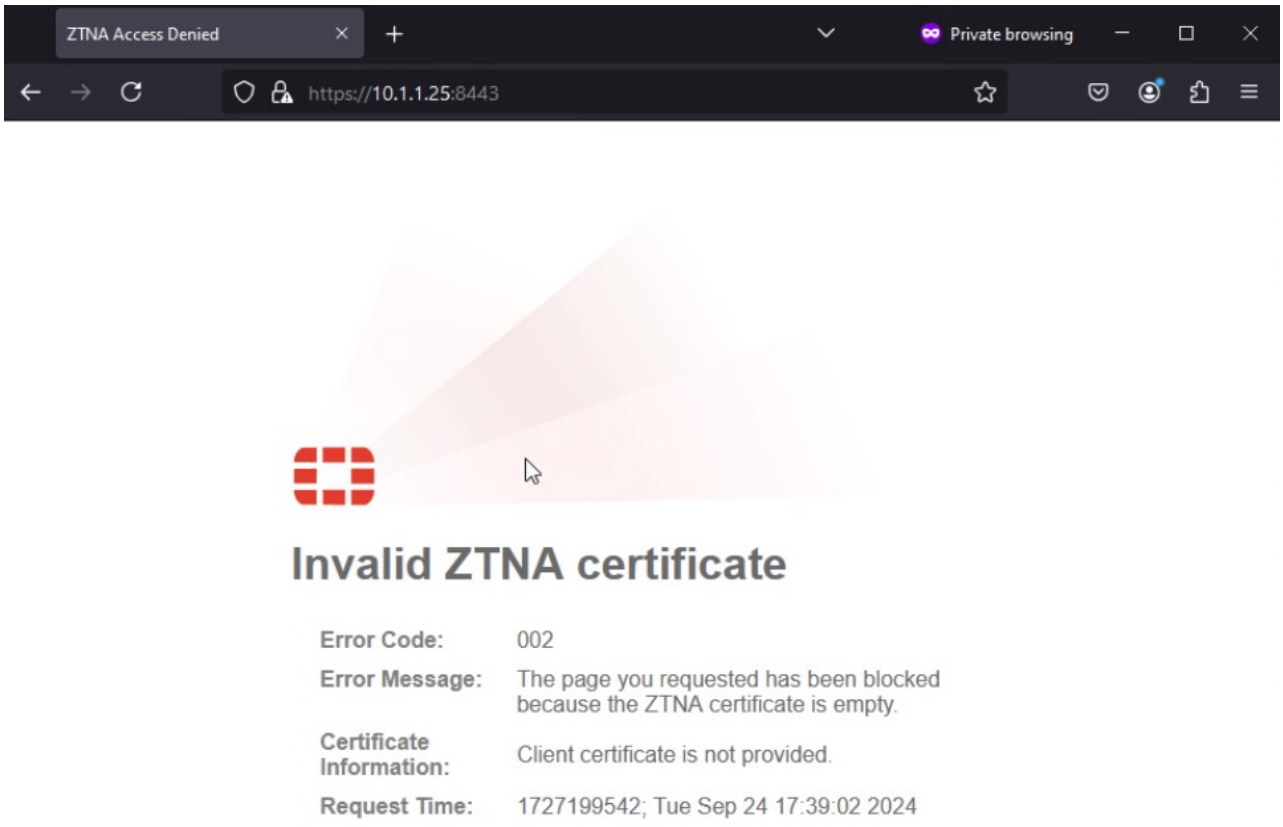
1. FortiProxy requests client certificate authentication, and the web browser displays the available certificates. The user selects a client certificate and clicks *OK*.



2. Once the client certificate is successfully verified against the root CA certificate imported on the FortiProxy, access to the web site is granted.



When the endpoint device fails to present a client certificate, a message is displayed, and access to the web site is blocked.



Display CORS content in explicit proxy

Webpages can properly display Cross-Origin Resource Sharing (ORS) content in an explicit proxy environment when using session-based, cookie-enabled, and captive portal assisted authentication.

```
config authentication rule
    edit <name>
        set web-auth-cookie enable
        set cors-stateful {enable | disable}
        set cors-depth <integer>
    next
end
```

`cors-stateful {enable | disable}`	Enable/disable allowing CORS access (default = disable). This setting is only available when `web-auth-cookie` is enabled.
`cors-depth <integer>`	Set the depth to allow CORS access (1 - 8, default = 3). For example, when visiting domain A, the returned web page may refer the browser to a cross-origin domain B (depth of 1). When the browser visits domain B, the returned web content may further refer the browser to another cross-origin domain C (depth of 2).

Example

CORS access is enabled in this example. When a user access the Microsoft *Sign in* page using an explicit proxy, the page appears and the user can log in. This example assumes the web proxy and user group have already been configured, and that the proxy captive portal setting has been enabled on the appropriate interface.

To view CORS content in an explicit proxy environment:

1. Configure the authentication scheme:

```
config authentication scheme
    edit "form"
        set method form
        set user-database "local-user-db"
    next
end
```

2. Configure the authentication rule:

```
config authentication rule
    edit "form"
        set srcaddr "all"
        set ip-based disable
        set active-auth-method "form"
        set web-auth-cookie enable
        set cors-stateful enable
        set cors-depth 3
    next
end
```

3. Configure the captive portal:

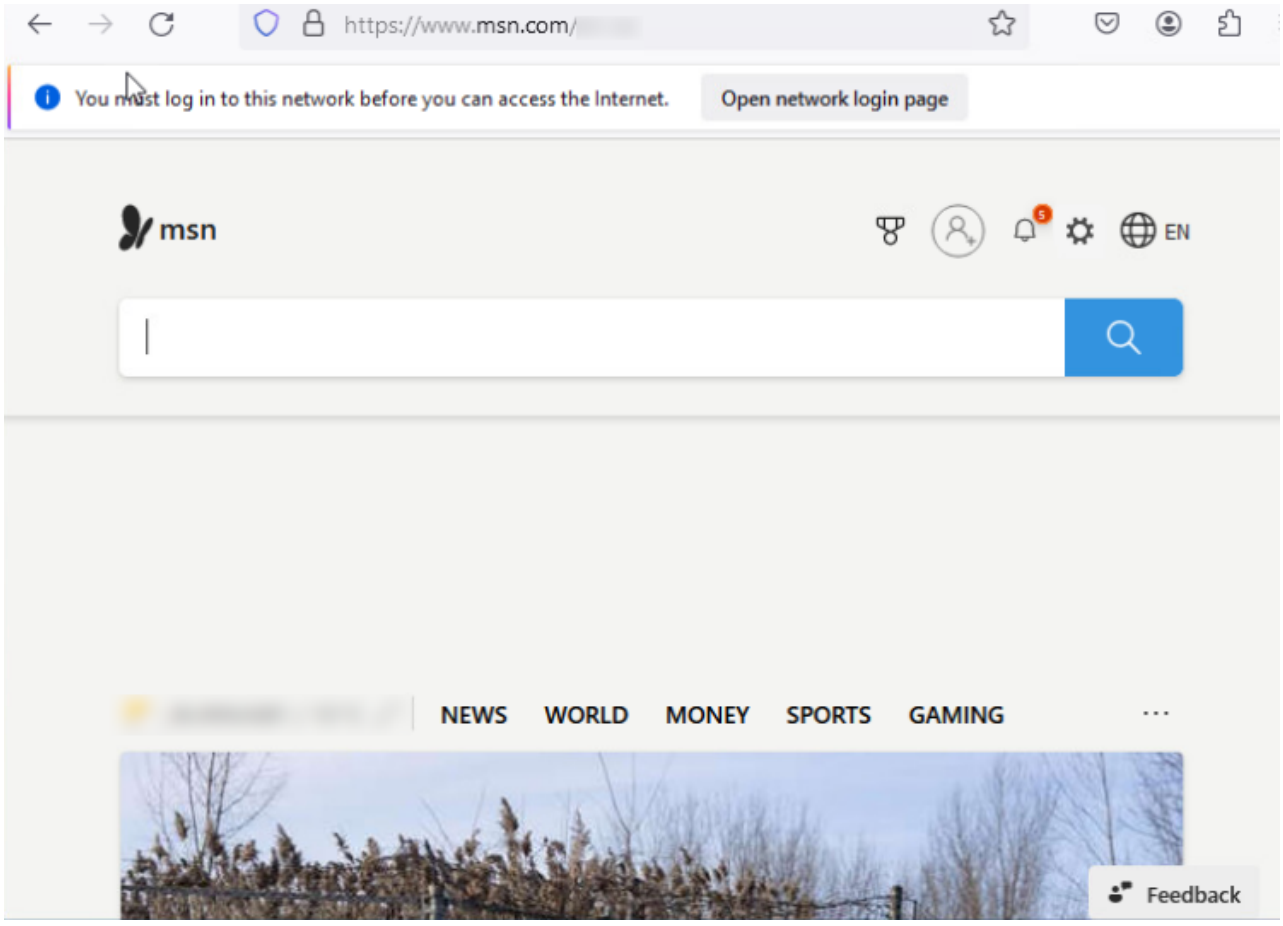
```
config authentication setting
    set captive-portal-type ip
 set captive-portal-ip 10.120..209
end
```

4. Configure the policy:

```
config firewall policy
    edit 1
        set type explicit-web
        set uuid 921737c8-d81a-51ee-76db-dcd160b8695d
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set schedule "always"
        set explicit-web-proxy "web-proxy"
```

```
        set logtraffic all
        set logtraffic-start enable
        set log-http-transaction all
        set extended-log enable
        set groups "localgroup"
        set utm-status enable
        set ssl-ssh-profile "deep-custom"
        set av-profile "av"
    next
end
```

5. Get a user to access `www.msn.com` through the explicit web proxy. The website loads CORS content.



If CORS access (`cors-stateful`) was disabled, the browser would display an incomplete page with CORS content hidden.



Explicit proxy logging

Explicit proxy traffic logging can be used to troubleshoot the HTTP proxy status for each HTTP transaction with the following:

- Monitor HTTP header requests and responses in the http transaction log. This requires an SSL deep inspection profile to be configured and extented-log enabled in the corresponding firewall policy.
- Log the explicit web proxy forward server name using `set log-forward-server`, which is disabled by default.

```
config web-proxy global
    set log-forward-server {enable | disable}
end
```

- Log TCP connection failures in the traffic log when a client initiates a TCP connection to a remote host through the FortiProxy, and the remote host is unreachable.

Basic configuration

The following FortiProxy configuration is used in the three explicit proxy traffic logging use cases in this topic.

To configure the FortiProxy:

1. Configure the web proxy profile:

```
config web-proxy profile
    edit "header"
        config headers
            edit 1
                set name "test_request_header"
                set action monitor-request
            next
            edit 2
                set name "ETag"
                set action monitor-response
            next
        end
    next
end
```

2. Enable forward server name logging in traffic:

```
config web-proxy global
    set proxy-fqdn "100D.qa"
    set log-forward-server enable
end
```

3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port10"
        set dstintf "port9"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set webproxy-profile "header"
        set webproxy-forward-server "227"
        set ssl-ssh-profile "deep-inspection"
        set logtraffic all
        set log-http-transaction enable
        set extended-log enable
    next
end
```

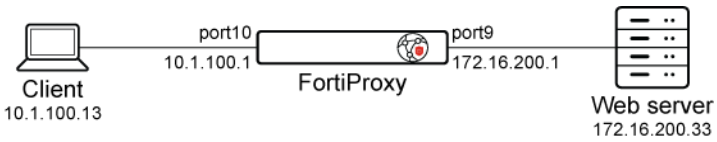


A firewall policy is used in this basic configuration example and the specific examples that follow. This feature also works for the explicit web proxy or transparent web proxy with proxy policies, and the configurations are similar:

- Example 1: apply the `web-proxy profile` to the proxy policy.
- Example 2: apply the `webproxy-forward-server`.

Example 1: monitoring HTTP header requests

In this example, the user wants to monitor some HTTP headers in HTTP messages forwarded through a FortiProxy proxy (either transparent or explicit proxy. When the monitored headers are detected, they will be logged in the http transaction log.



In the web proxy profile configuration, the following HTTP headers are monitored:

- `test_request_header`: this is a user-customized HTTP header.
- `ETag`: this is a HTTP header returned by the web server's 200 OK response.

The monitored headers in the web proxy profile will be logged when the HTTP response received by the FortiProxy. The `extended-log` setting must be enabled.

The following settings are required in the firewall policy:

- `set webproxy-profile "header"`
- `set ssl-ssh-profile "deep-inspection"`
- `set extended-log enable`

To verify the configuration:

1. Send a HTTP request from the client:

   ```
   curl -kv https://172.16.200.33 -H "test_request_header: aaaaa"
   ```

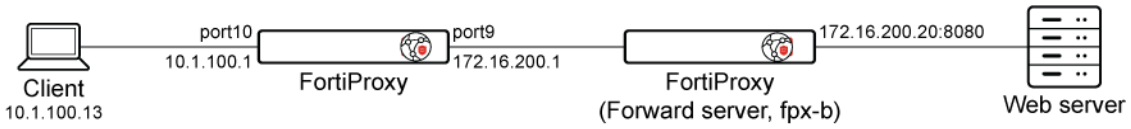
   This command sends a HTTP request with the header `test_request_header: aaaaa` through the FortiProxy.
2. On the FortiProxy, check the http-transaction logs:

   ```
   2: date=2024-09-26 time=16:44:02 eventtime=1727394241416669139 tz="-0700" logid="0010000099"
   type="traffic" subtype="http-transaction" level="notice" vd="root" srcip=10.45.1.41
   dstip=172.18.20.226 clientip=10.45.1.41 scheme="https" srcport=36552 dstport=443
   hostname="172.18.20.226" url="https://172.18.20.226/files/card.docx" prefetch=0 policyid=3
   sessionid=1853239712 transid=16777218 reqlength=134 resplength=1736 rcvdbyte=3881 sentbyte=753
   resptype="normal" httpmethod="GET" agent="curl/7.76.1" statuscode="200" rawdata="Time=-
   1726977ms|[REQ] Host=172.18.20.226|test_request_header=aaaaa|| |[RESP] Content-
   Type=application/vnd.openxmlformats-officedocument.wordprocessingml.document|ETag=\\\"595-
   5fca03fb77091\\\"" reqtime=1727394241 resptime=1727394241 respfinishtime=1727394241
   duration=416 appcat="unscanned" utmaction="allow" countweb=1 utmref=65533-104484
   ```

   This log is for the HTTP reqest and response that contain both monitored headers, `test_request_header` and `ETag`, and their values, `aaaaa` and `595-5fca03fb77091`, respectively.

Example 2: logging the explicit web proxy forward server name

In this example, the user wants to see the name of the web proxy forward server in the traffic log when the traffic is forwarded by a web proxy forward server.



In the global web proxy settings, `log-forward-server` must be enabled.

The following settings are required in the firewall policy:

- `set webproxy-forward-server`
- `set logtraffic all`

When a HTTP request is sent through the FortiProxy proxy, the request will be forwarded by the FortiProxy to the upstream proxy, and the forward server's name will be logged in the traffic log.

To verify the configuration:

1. Send a HTTP request from the client:

```
curl -kv https://www.google.com
```

2. On the FortiProxy, check the traffic logs:

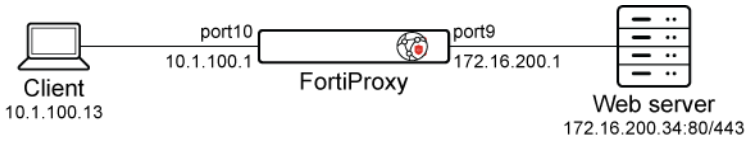
```
# execute log filter category 31: date=2024-09-25 time=15:16:55 eventtime=1727302615474066335
tz="-0700" logid="0000000010" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.40.1.1 srcport=52636 srcintf="port1" srcintfrole="undefined" dstcountry="United
States" srccountry="Reserved" dstip=34.107.221.82 dstport=80 dstintf="port1"
dstintfrole="undefined" sessionid=1533148235 service="HTTP" fwdsrv="227" proxyapptype="web-
proxy" proto=6 action="accept" policyid=1 policytype="proxy-policy" poluuid="1a61a9c0-79e6-
51ef-a968-b5799a9ec837" trandisp="snat+dnat" tranip=10.40.1.227 tranport=8080 transip=0.0.0.0
transport=0 clientip=10.40.1.1 duration=184 wanin=1192 rcvdbyte=1192 wanout=1240 lanin=1336
sentbyte=1336 lanout=1192 appcat="unscanned" utmaction="allow" countweb=4 utmref=65534-33278
```

Example 3: logging TCP connection failures

In this example, a client initiates a TCP connection to a remote network node through the FortiProxy. The connection fails because the IP address or port of the remote node is unreachable. A `Connection Failed` message appears in the logs.

Based on the basic FortiProxy configuration used in examples 1 and 2, the forward server may need to be removed from the policy if the forward server's TCP IP port is actually reachable. If the forward server proxy tries to set up back-to-back TCP connections with the downstream FortiProxy and the remote server as in the case of deep-inspection, then when the client tries to connect to a remote node (even if the IP address or port is unreachable), the downstream FortiProxy is able to establish a TCP connection with the upstream forward server, so there will be no `Connection Failed` message in the downstream FortiProxy's log.

Currently, the `Connection Failed` message in the downstream FortiProxy's log is visible for the case when there is an unreachable TCP port only when explicit web proxy with a proxy policy is configured. Therefore, the following example that makes use of a firewall policy demonstrates this log message is only supported for the unreachable IP address case.



To verify the configuration:

1. Send a HTTP request from the client to an unreachable IP:

```
curl -kv https://172.16.200.34
```

2. On the FortiProxy, check the traffic logs:

```
# execute log filter category 3
5: date=2024-09-26 time=17:42:54 eventtime=1727397774498700894 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.40.1.226 srcport=45020
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.18.20.23 dstport=80 dstintf="port1" dstintfrole="undefined" sessionid=1853239900
service="HTTP" proxyapptype="web-proxy" proto=6 action="timeout" policyid=1 policytype="proxy-
policy" poluuid="1a61a9c0-79e6-51ef-a968-b5799a9ec837" trandisp="snat" transip=10.40.1.229
transport=50970 clientip=10.40.1.226 duration=3 wanin=0 rcvdbyte=0 wanout=0 lanin=125
sentbyte=125 lanout=30331 appcat="unscanned" utmaction="allow" msg="Connection Failed"
crscore=5 craction=262144 crlevel="low"
```

Configuring fast fallback for explicit proxy

The fast fallback (also named "Happy Eyeballs") algorithm, as outlined in RFC 8305, is now supported for explicit web proxy. This feature operates by attempting to connect to a web server that is available at multiple IPv4 and IPv6 addresses, either sequentially or simultaneously. As a result, the web server can be connected with reduced user-visible delay, which enhances the overall browsing experience.

```
config web-proxy fast-fallback
    edit <name>
        set status {enable | disable}
        set connection-mode {sequentially | simultaneously}
        set protocol {IPv4-first | IPv6-first | IPv4-only | IPv6-only}
        set connection-timeout <integer>
    next
end
```

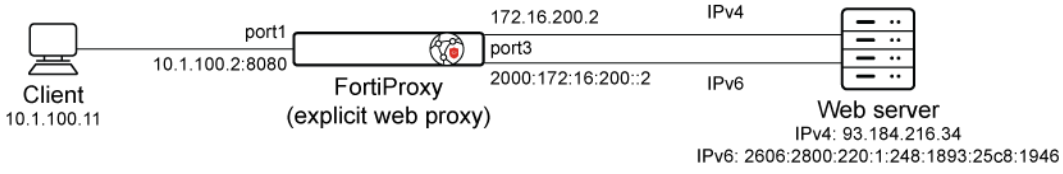
`status {enable | disable}`	Enable/disable the fast fallback entry (default = `enable`).
`connection-mode {sequentially | simultaneously}`	Set the connection mode for multiple destinations. • `sequentially`: connect the different destinations sequentially (default). • `simultaneously`: connect the different destinations simultaneously.
`protocol {IPv4-first | IPv6-first | IPv4-only | IPv6-only}`	Set the connection protocols for multiple destinations. • `IPv4-first`: connect IPv4 destinations first (default). • `IPv6-first`: connect IPv6 destinations first. • `IPv4-only`: connect IPv4 destinations only. • `IPv6-only`: connect IPv6 destinations only.
`connection-timeout <integer>`	Start another connection if a connection takes longer than the timeout value, in milliseconds (200 - 1800000, default = 200).

Based on the settings for `connection-mode` and `protocol`, the explicit web proxy will try connecting to the web server in different ways:

- If the `connection-mode` is set to `sequential` (default), then the explicit web proxy will try connecting to the web server by IPv4 first, or by IPv6 first depending on the `protocol` setting. If the connection attempt over IPv4 or IPv6 succeeds, then the connection is kept; but if the connection fails, then it falls back to try a connection over IPv6 or IPv4 instead.
- If the `connection-mode` is set to `simultaneously`, then the explicit web proxy will try connecting to the web server by IPv4 and IPv6 at the same time. If the connection over IPv4 is established first, then the connection is kept for the session and the IPv6 connection is discarded and vice-versa.
- If the user only wants to connect by IPv4 but not IPv6, or by IPv6 but not IPv4, then the `protocol` option can be set to `IPv4-only` or `IPv6-only` accordingly. The explicit web proxy will try connecting to the web server only by IPv4 or IPv6, even though both IPv4 and IPv6 may work.

Example

In this example, a client visits a web server through a FortiProxy explicit web proxy that has IPv4 and IPv6 connections to the web server (www.example.com), which can resolve to IPv4 address 93.184.216.34 and IPv6 address 2606:2800:220:1:248:1893:25c8:1946.



The configuration uses sequential connection mode, the IPv4 first protocol, and the default connection timeout (200 ms).

To configure the FortiProxy:

1. Configure the IPv4 static route:

```
config router static
    edit 1
        set gateway 172.16.200.251
        set device "port3"
    next
end
```

2. Configure the IPv6 static route:

```
config router static6
    edit 1
        set gateway 2000:172:16:200::254
        set device "port3"
    next
end
```

3. Configure the proxy destination connection fast fallback:

```
config web-proxy fast-fallback
    edit "ffbk"
        set status enable
        set connection-mode sequentially
        set protocol IPv4-first
        set connection-timeout 200
    next
end
```

4. Configure the exempt URL of the web server from web proxy forwarding and caching:

```
config web-proxy url-match
    edit "ffbk"
        set url-pattern "example.com"
        set fast-fallback "ffbk"
    next
end
```

5. Configure the proxy policy:

```
config firewall proxy-policy
    edit 1
        set proxy explicit-web
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
```

```
        set schedule "always"
        set logtraffic all
        set srcaddr6 "all"
        set dstaddr6 "all"
        set utm-status enable
        set ssl-ssh-profile "deep-custom"
        set av-profile "av"
    next
end
```

Verifying the connection

Scenario 1:

The TCP connection from the explicit web proxy to the web server is established successfully over IPv4 within 200 ms.

As shown in the forward traffic log, the web session data is transmitted over IPv4 between the explicit web proxy and the web server.

```
2: date=2024-09-24 time=18:46:18 eventtime=1687830378260927765 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.1.100.11 srcport=33304
srcintf="port1" srcintfrole="undefined" dstcountry="United States" srccountry="Reserved"
dstip=93.184.216.34 dstport=80 dstintf="port3" dstintfrole="undefined" sessionid=1688881487
service="HTTP" proxyapptype="web-proxy" proto=6 action="accept" policyid=1 policytype="proxy-
policy" poluuid="560d8520-fa7b-51ed-e06a-df05ec145542" trandisp="snat" transip=0.0.0.0 transport=0
clientip=10.1.100.11 duration=0 wanin=0 rcvdbyte=0 wanout=0 lanin=131 sentbyte=131 lanout=1591
appcat="unscanned"
```

Scenario 2:

The TCP connection from the explicit web proxy to the web server is not established over IPv4 within 200 ms and falls back to IPv6 successfully.

The IPv4 path to the server is interrupted, and the TCP connection between the explicit web proxy and web server cannot be established. The explicit web proxy waits until the 200 ms connection timeout timer expires, then attempts to connect to the server by IPv6, which is successful. The web session data is transmitted over IPv6, as shown in the forward traffic log.

```
2: date=2024-09-24 time=18:47:27 eventtime=1687830447277653089 tz="-0700" logid="0000000010"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.1.100.11 srcport=44392
srcintf="port1" srcintfrole="undefined" srccountry="United States"
dstip=2606:2800:220:1:248:1893:25c8:1946 dstport=80 dstintf="port3" dstintfrole="undefined"
sessionid=803961034 service="HTTP" proxyapptype="web-proxy" proto=6 action="accept" policyid=1
policytype="proxy-policy" poluuid="aa49f750-6c3e-51ef-8eb6-01a4e14a9dbe" trandisp="snat"
transport=0 clientip=10.1.100.11 duration=0 wanin=0 rcvdbyte=0 wanout=0 lanin=131 sentbyte=131
lanout=728 appcat="unscanned"
```

Web Proxy Setting

Use the web proxy setting to change the global configuration of explicit web proxies.

Go to *Proxy Settings* > *Web Proxy Setting* to change the global explicit web proxy settings.

Configure the following settings and then click *Apply*:

Proxy FQDN	The FQDN for the global proxy server. This is the domain name to enter into browsers to access the proxy server.
Max HTTP request length	The maximum length of an HTTP request that can be cached, in KB. Larger requests are rejected. The default is 8 KB.
Max HTTP message length	The maximum length of an HTTP message that can be cached, in KB. Larger messages are rejected. The default is 32 KB.
Realm	You can enter an authentication realm to identify the explicit web proxy. The realm can be any text string of up to 63 characters. If the realm includes spaces, enclose it in quotes. When a user authenticates with the explicit web proxy, the HTTP authentication dialog box includes the realm, so you can use the realm to identify the explicitly web proxy for your users.
Explicit Outgoing IP	Enter the IP address to use as the source address for outgoing HTTP requests by explicit web proxy. Select + to enter another IP address.
Webproxy Profile	Enter the name of the web proxy profile that will be applied when explicit proxy traffic is allowed by default and traffic is accepted that does not match an explicit proxy policy.
Default CA Certificate	Select which certificate to use as a default. The default certificate is Fortinet_CA_SSL.
Forward Server Affinity Timeout	Enter the number of minute before the traffic from the source IP address is no longer assigned to the forwarding server. The default is 30 minutes. The range is 6-60 minutes.
Fast Policy Match	The fast policy match function improves the performance of IPv4 explicit and transparent web proxies on FortiProxy units. When enabled, after the proxy policies are configured, the FortiProxy unit builds a fast searching table based on the different proxy policy matching criteria. When fast policy matching is disabled, web proxy traffic is compared to the policies one at a time from the beginning of the policy list.
LDAP User Cache	Enable or disable the LDAP user cache.
Strict Web Check	Enable or disable (by default) the blocking of web sites that send incorrect headers that don't conform to HTTP 1.1 (see RFC 2616 for more information). Enabling this option may block some commonly used websites.

Forward Proxy Auth	Enable or disable (by default) the forwarding of proxy authentication headers. Note that this option is only practical when in explicit mode, because proxy authentication headers are always forwarded when in transparent mode. By default, in explicit mode, proxy authentication headers are blocked by the explicit web proxy. Therefore, enable this entry if you need to allow proxy authentication through the explicit web proxy.
Strict Guest	Enable or disable whether the explicit web proxy uses strict guest user checking.
HTTPS Replacement Message	Enable or disable whether a replacement message is displayed for HTTPS requests.
Message Upon Server Error	Enable or disable whether a replacement message is displayed when a server error is detected.
Trace Auth No Resp	Enable or disable whether timed-out authentication requests are logged.
Extended Log	Enable or disable the recording of extended log for implicit policies. The extended log includes the useragent, referralurl, httpmethod, and statuscode fields.
Log HTTP Transaction	Configure the logging of HTTP transactions: • *Enable*—Enable HTTP transaction log. • *Disable* (default)—Disable HTTP transaction log. When enabled, you can find the HTTP transaction logs under *Log & Report > HTTP Transaction*. See Types of logs on page 1138.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Logging client IP for forward traffic and HTTP transaction

The HTTP transaction and Forward session logs include the ClientIP column that records the client IP address based on the `learn-client-ip` configuration. By default, the `original-source-ip` is recorded.

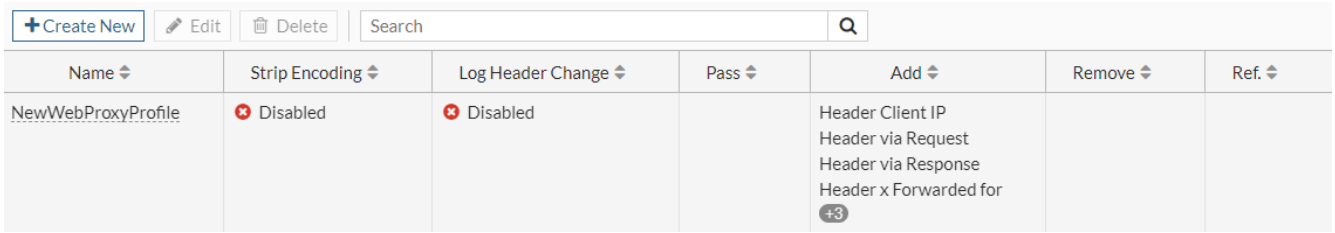
```
config web-proxy global
    set learn-client-ip {enable | disable}
    set learn-client-ip-from-header {true-client-ip x-real-ip x-forwarded-for}
    set learn-client-ip-srcaddr <address>
    set learn-client-ip-srcaddr6 <address>
end
```

`learn-client-ip {enable | disable}`	Enable/disable learning the client's IP address from headers (default = disable).
`learn-client-ip-from-header {true-client-ip | x-real-ip | x-forwarded-for}`	Learn client IP address from the specified headers: True-Client-IP, X-Real-IP, and X-Forwarded-For.
`learn-client-ip-srcaddr(6) <address>`	Source address name (srcaddr or srcaddr6 must be set).

Web Proxy Profile

You can create web proxy profiles that can add, remove, and change HTTP headers. The web proxy profile can be added to the web proxy global configuration.

Go to *Proxy Settings* > *Web Proxy Profile* to change the web proxy profiles.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

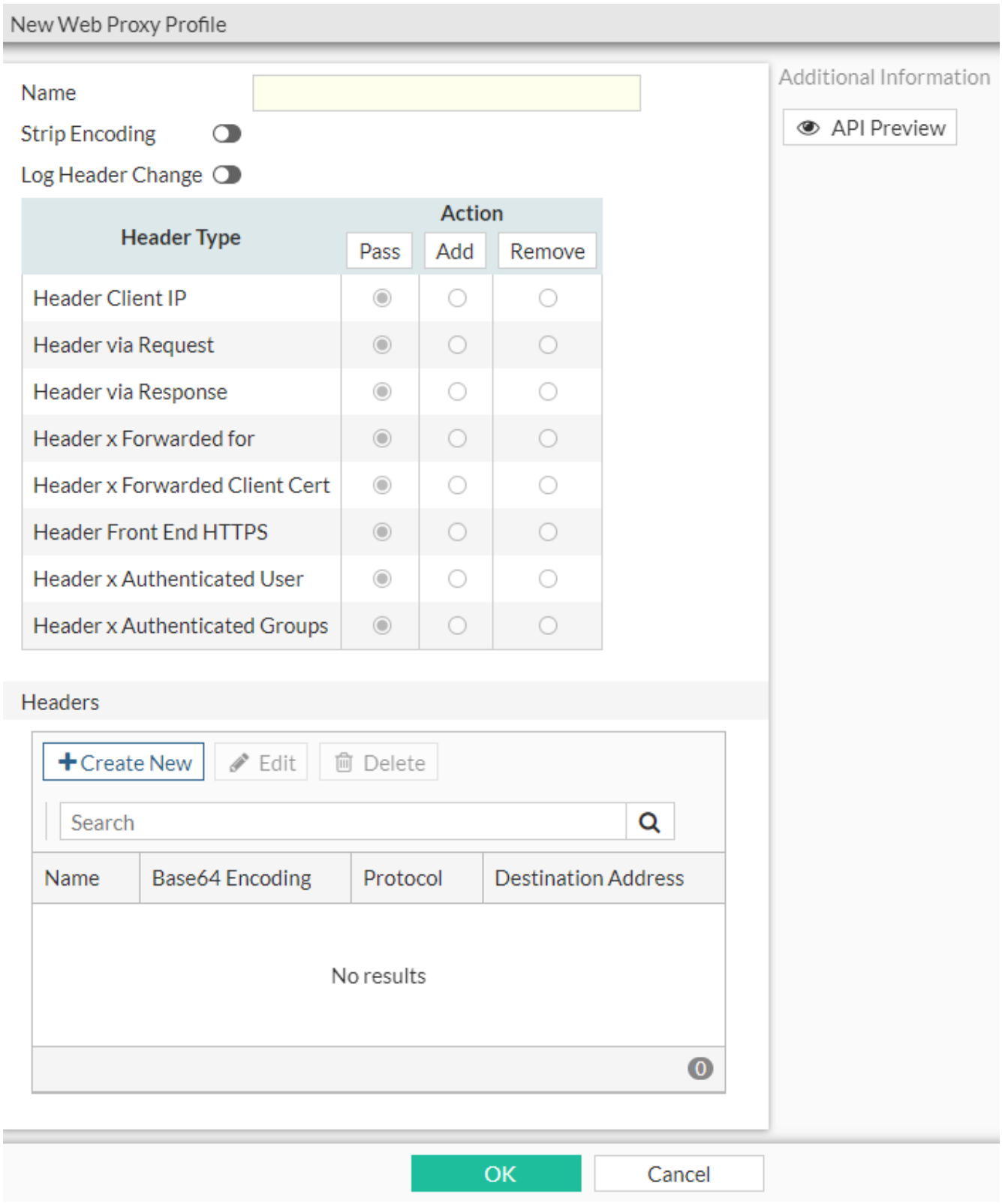
The following options are available:

Create New	Create a web proxy profile. See Create or edit a web proxy profile on page 146.
Edit	Edit the selected web proxy profile. See Create or edit a web proxy profile on page 146.
Delete	Remove the selected web proxy profile.
Search	Enter a search term to find in the list.
Name	The name of the web proxy profile.

Strip Encoding	Whether the profile strips out unsupported encoding from request headers and correctly block banned words.
Log Header Change	Whether the profile allows changes to the log header.
Pass	Which HTTP headers will be forwarded in forwarded requests.
Add	Which HTTP headers will be added in forwarded requests.
Remove	Which HTTP headers will be removed from forwarded requests.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.

Create or edit a web proxy profile

Select *Create New* to open the *New Web Proxy Profile* window.



To open the *Edit Web Proxy Profile* window, select a web proxy profile and then click *Edit*.

Configure the following settings in the *New Web Proxy Profile* window or *Edit Web Proxy Profile* window and then click *OK*:

Name	Enter the name of the new web proxy profile.
Strip Encoding	Toggle whether to strip out unsupported encoding from request headers and correctly block banned words. This option can resolve issues when attempting to successfully block content using Google Chrome.
Log Header Change	Toggle whether to allow changes to the log header.
Header Client IP	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header via Request	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header via Response	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header x Forwarded for	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header x Forwarded Client Cert	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header Front End HTTPS	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header x Authenticated User	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header x Authenticated Groups	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Create New	Select to add a new header. See Create or edit an HTTP header on page 149.
Edit	Select to change an existing header. See Create or edit an HTTP header on page 149.
Delete	Select to remove an existing header.
Search	Enter a search term to find in the list.
Name	The name for the HTTP forwarded header.
Base64 Encoding	Whether base64 encoding is enabled or disabled.
Protocol	Whether the new header uses HTTP, HTTPS, or both.
Destination Address	The destination addresses and destination address groups for the HTTP forwarded header.
Action	The action for the HTTP forwarded header: *add-to-request*, *add-to-response*, *remove-from-request*, or *remove-from-response*.
Add Option	How the new header is added: *append*, *new-on-not-found*, or *new*.
Header Content	The content of the HTTP header.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown for the CMDB API that creates the explicit proxy configuration.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create or edit an HTTP header

You can change the following HTTP headers:

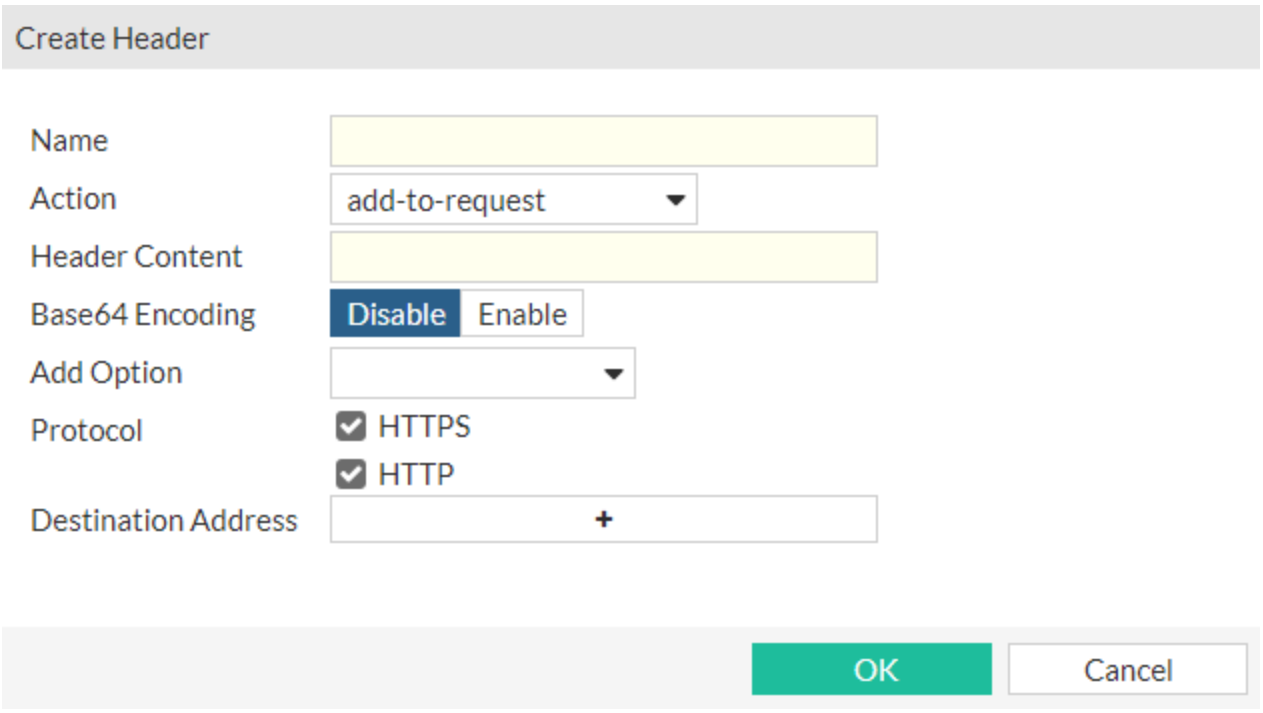
- Header Client IP
- Header via Request
- Header via Response
- Header x Forwarded For
- header-x-forwarded-client-cert
- Header Front End HTTPS
- Header x Authenticated User
- Header x Authenticated Groups

For each of these headers, you can set the action to the following:

- Forward (pass) the same HTTP header
- Add the HTTP header
- Remove the HTTP header

The web proxy can add or remove custom headers from requests or responses. If you are adding a header, you can specify the content to be included in the added header.

Select *Create New* to open the *Create Header* window.



To open the *Edit Header* window, select a header and then click *Edit*.

Configure the following settings in the *Create Header* window or *Edit Header* window and then click *OK*:

Name	Enter a name for the HTTP forwarded header.
Action	Select the action for the HTTP forwarded header: *add-to-request*, *add-to-response*, *remove-from-request*, or *remove-from-response*.
Header Content	Enter the content of the HTTP header.
Base64 Encoding	Enable or disable base64 encoding.
Add Option	Select how the new header is added: *append*, *new-on-not-found*, or *new*.
Protocol	Select whether the new header uses HTTP, HTTPS, or both.
Destination Address	Select + to add destination addresses and destination address groups.

To create a web proxy profile and header from the CLI:

```
config web-proxy profile
   edit <name>
      set header-client-ip {add | pass | remove}
      set header-via-request {add | pass | remove}
      set header-via-response {add | pass | remove}
      set header-x-forwarded-for {add | pass | remove}
      set header-front-end-https {add | pass | remove}
      set header-x-authenticated-user {add | pass | remove}
      set header-x-authenticated-groups {add | pass | remove}
```

```
        set strip-encoding {enable | disable}
        set log-header-change {enable | disable}
        config headers
           edit <id>
              set action {add-to-request | add-to-response | remove-from-request | remove-from-
                   response}
              set content <string>
              set name <name>
           end
        end
     next
end
```

Restricted SaaS access

Large organizations may want to restrict SaaS access to resources like Microsoft Office 365, Google Workspace, and Dropbox by tenant to block non-company login attempts and secure the users from accessing non-approved cloud resources. Many cloud vendors enable this by applying tenant restrictions for access control. For example, users accessing Microsoft 365 applications with tenant restrictions through the corporate proxy will only be allowed to log in as the company's tenant and access the organization's applications.

To implement this, access requests from the clients pass through the company's web proxy, which inserts headers to notify the SaaS service to apply tenant restrictions with the permitted tenant list. Users are redirected the SaaS service login page, and are only allowed to log in if they belong to the permitted tenant list.

For more information, refer to the vendor-specific documentation:

- Office 365: Restrict access to a tenant
- Google Workspace: Block access to consumer accounts
- Dropbox: Network control

Basic configuration

A web proxy profile can specify access permissions for Microsoft Office 365, Google Workspace, and Dropbox by inserting vendor-defined headers that restrict access to the specific accounts. Custom headers can also be inserted for any destination. The web proxy profile can then be applied to a policy to control the header's insertion.

To implement Office 365 tenant restriction, Google Workspace account access control, and Dropbox network access control:

1. Create or edit a web proxy profile on page 146 according to the vendors' specifications:
   a. Set the header name (defined by the service provider).
   b. Set the traffic destination (the service provider).
   c. Set the HTTP header content to be inserted into the traffic (defined by your settings).

```
config web-proxy profile
       edit <name>
        config headers
        edit <id>
               set name <string>
               set dstaddr <address>
               set action add-to-request
               set base64-encoding disable
               set add-option new
               set protocol https http
               set content <string>
       next
 end
 next
end
```

2. Apply the web proxy profile to a policy. SSL deep inspection must be used in the firewall policy:

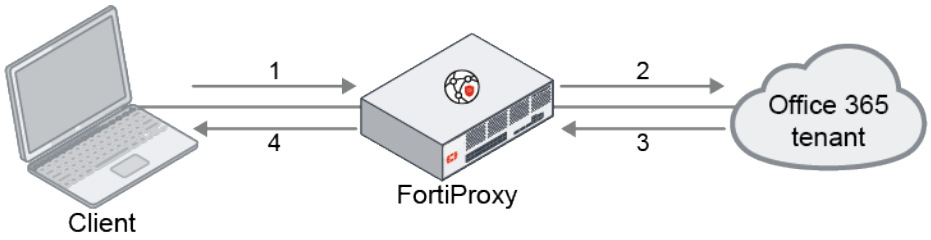
The following table lists the vendor-specific `config headers` settings that must be configured in the web proxy profile (`config web-proxy profile`):

Setting	Vendor specification		
	Microsoft Office 365	Google Workspace	Dropbox
`name <string>`	• `Restrict-Access-To-Tenants` • `Restrict-Access-Context`	• `X-GoogApps-Allowed-Domains`	• `X-Dropbox-allowed-Team-Ids`
`dstaddr <address>`	• Use the built-in `Microsoft Office 365` address.	• Use the built-in `G Suite` address.	• Use the built-in `wildcard.dropbox.com` address.
`content <string>`	• Enter the domain for `Restrict-Access-To-Tenants`. • Enter the directory ID for `Restrict-Access-Context`.	• Enter the domain.	• Enter the Dropbox team ID.

Due to vendors' changing requirements, these settings may no longer comply with the vendors' official guidelines. See the vendor documentation for more details.

Microsoft Office 365 example

In this example, a web proxy profile is created to control permissions for Microsoft Office 365 to allow corporate domains and deny personal accounts, such as Hotmail and Outlook that are accessed through login.live.com.



1. When a user attempts to access login.microsoftonline.com, login.microsoft.com, or login.windows.net, the traffic will match a proxy inspection mode policy with the assigned web proxy profile.
2. The web proxy profile adds new headers to the customer tenant, indicating the allowed domain and restricted access for personal accounts. Next, the FortiProxy starts a new connection with the Microsoft Office 365 domain controller including the new headers.
3. The Microsoft Office 365 domain controller assesses this data and will allow or deny this access, then sends a reply to the FortiProxy.
4. The FortiProxy sends a reply to the client.

The FortiProxy will only indicate the correct domains to be allowed or denied through the headers to Microsoft. The custom sign-in portal in the browser is generated by Microsoft.

Configuration summary

The following must be configured in FortiOS:

- An FQDN address for login.live.com
- An SSL inspection profile that uses deep inspection with an exemption for login.live.com



Ensure that the firewall certificate is installed on the client machines. A company certificate signed by an internal CA is recommended.

- A web filter profile in proxy mode with static URL filters for the SNI URLs
- A web proxy profile that adds new headers to the customer tenant
- A policy that applies the configured SSL SSL inspection, web filter, and web proxy profiles

The `Restrict-Access-To-Tenants` and `Restrict-Access-Context` headers are inserted for incoming requests to: login.microsoftonline.com, login.microsoft.com, and login.windows.net, which are part of the `Microsoft Office 365` address group.

To restrict access to personal accounts using the login.live.com domain, the `sec-Restrict-Tenant-Access-Policy` header is inserted and uses `restrict-msa` as the header content.

Before configuring the FortiProxy, collect the information related to the company domain in the Office 365 contract.

- `Restrict-Access-To-Tenants`: your <domain.com>
- `Restrict-Access-Context`: Directory ID



To find the Directory ID related to the domain, locate it in the Azure portal, or use the whatismytenantid.com open tool.

To configure the FortiProxy:

1. Add the FQDN address for login.live.com:

```
config firewall address
    edit "login.live.com"
        set type fqdn
        set fqdn "login.live.com"
    next
end
```

2. Configure the SSL inspection profile. In this example, the `deep-inspection` profile is cloned, and the `live.com` FQDN is removed from the exemption list.
   a. Clone the `deep-inspection` profile:

```
config firewall ssl-ssh-profile
    clone "deep-inspection" to "Tenant"
end
```

   b. Edit the `Tenant` profile and remove `live.com` from the `config ssl-exempt` list.
3. Configure the URL filter list:

```
config webfilter urlfilter
    edit 1
        set name "Auto-webfilter-urlfilter"
        config entries
            edit 1
                set url "login.microsoftonline.com"
                set action allow
            next
            edit 2
                set url "login.microsoft.com"
                set action allow
            next
            edit 3
                set url "login.windows.net"
                set action allow
            next
            edit 4
                set url "login.live.com"
                set action allow
            next
        end
    next
end
```

4. Configure the web filter profile:

```
config webfilter profile
    edit "Tenant"
        set comment "Office 365"
        config web
```

```
            set urlfilter-table 1
        end
    next
end
```

5. Configure the web proxy profile (enter the header names exactly as shown):

```
config web-proxy profile
    edit "SaaS-Tenant-Restriction"
        set header-client-ip pass
        set header-via-request pass
        set header-via-response pass
        set header-x-forwarded-for pass
        set header-x-forwarded-client-cert pass
        set header-front-end-https pass
        set header-x-authenticated-user pass
        set header-x-authenticated-groups pass
        set strip-encoding disable
        set log-header-change disable
        config headers
            edit 1
                set name "Restrict-Access-To-Tenants"
                set dstaddr "login.microsoft.com" "login.microsoftonline.com"
"login.windows.net"
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content <domain>
            next
            edit 2
                set name "Restrict-Access-Context"
                set dstaddr "login.microsoftonline.com" "login.microsoft.com"
"login.windows.net"
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content <directory_ID>
            next
            edit 3
                set name "sec-Restrict-Tenant-Access-Policy"
                set dstaddr "login.live.com"
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content "restrict-msa"
            next
        end
    next
end
```

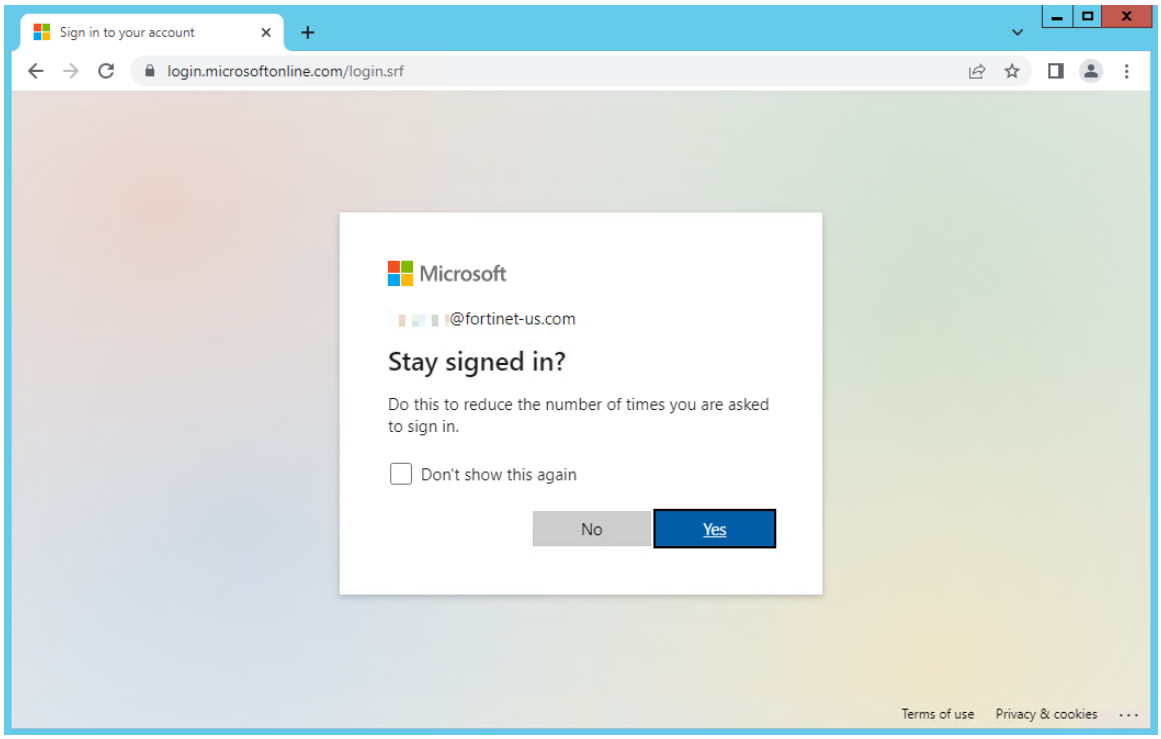
6. Configure the policy:

```
config firewall policy
    edit 10
        set name "Tenant"
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "users-lan"
        set dstaddr "login.microsoft.com" "login.microsoftonline.com" "login.windows.net"
"login.live.com"
        set schedule "always"
        set service "HTTP" "HTTPS"
        set utm-status enable
        set inspection-mode proxy
        set webproxy-profile "SaaS-Tenant-Restriction"
        set ssl-ssh-profile "Tenant"
        set webfilter-profile "Tenant"
        set logtraffic all
    next
end
```

Testing the access

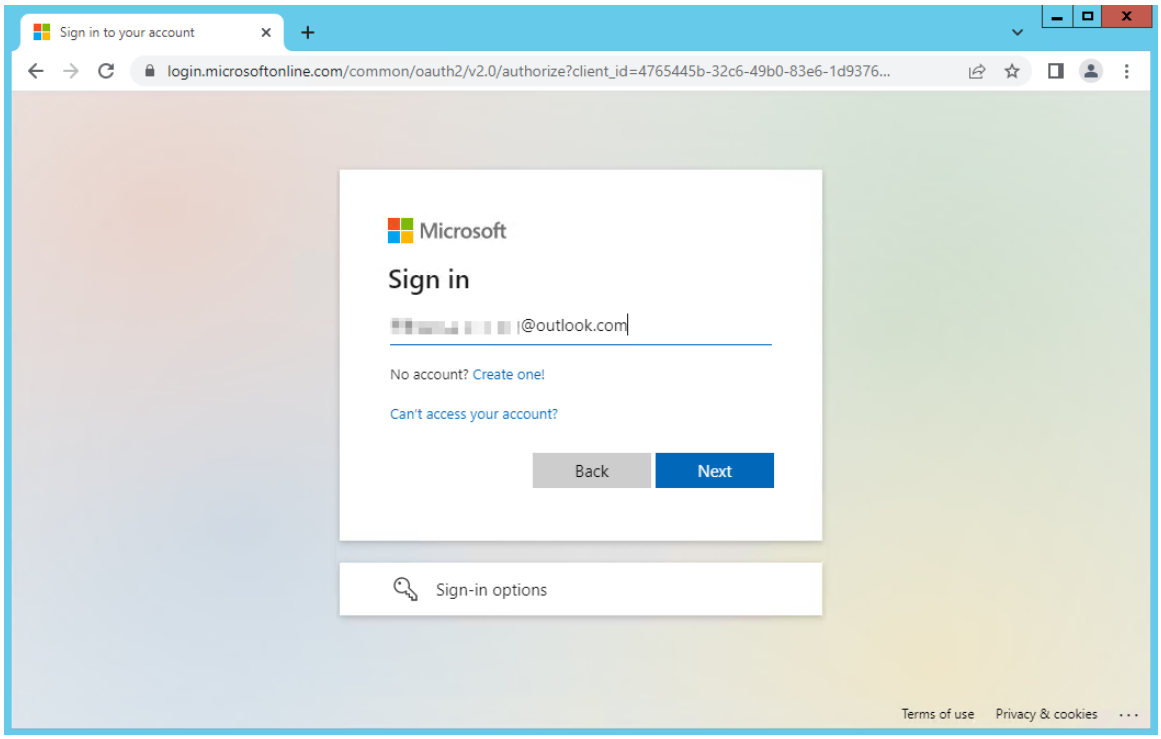
To test the access to corporate domains and personal accounts:

1. Get a client to log in with their corporate email using the login.microsoftonline.com domain.

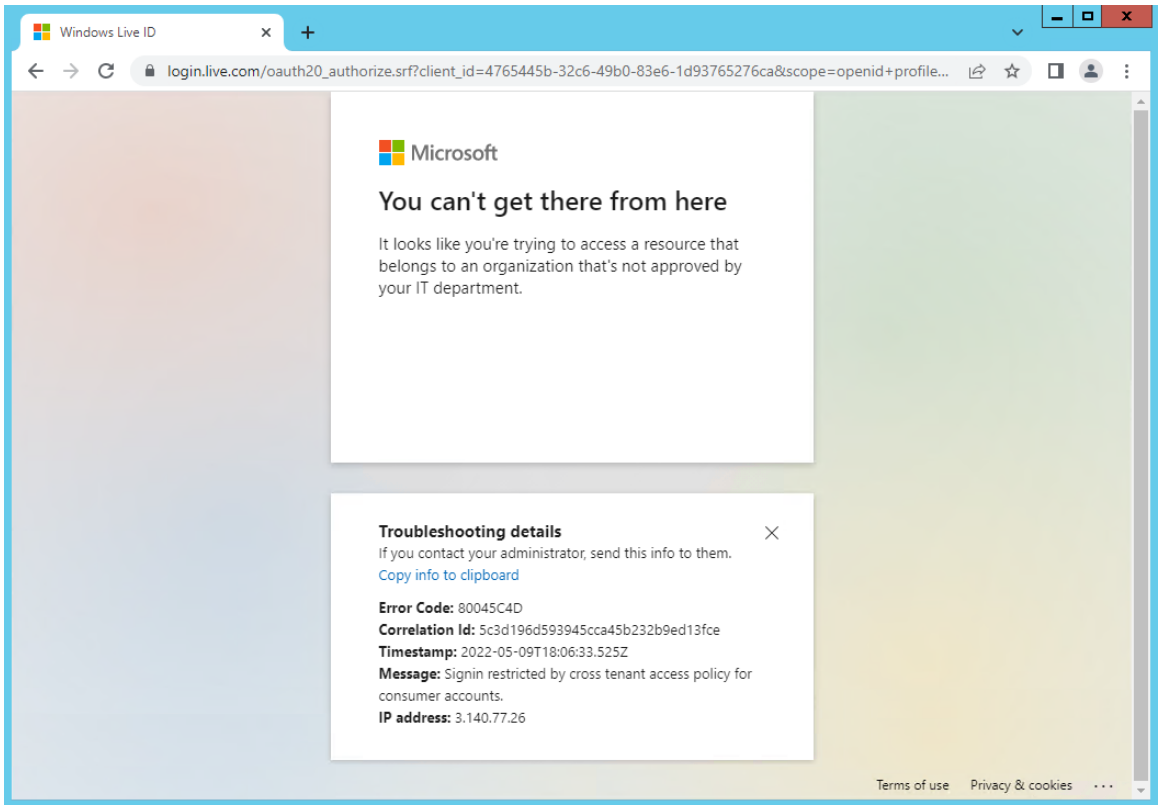


2. The client is able to enter their credentials and log in successfully.

3. Get a client to log in to their personal Outlook account.



4. After the client enters their credentials, a message appears that they cannot access this resource because it is restricted by the cross-tenant access policy.



Verifying the header insertion

To verify the header insertion for corporate domains and personal accounts:

1. On the FortiProxy, start running the WAD debugs:

```
# diagnose wad debug enable category http
# diagnose wad debug enable level info
# diagnose debug enable
```

2. After a client attempts to access corporate domains, verify that the header information is sent to the Microsoft Active Directory:

```
[I][p:234][s:2481][r:33] wad_dump_fwd_http_req             :2567  hreq=0x7fc75f0cd468 Forward
request to server:
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Connection: keep-alive
Content-Length: 1961
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
hpgrequestid: d7f706a8-1143-4cdd-ad52-1cc69dc7bb00
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/101.0.4951.54 Safari/537.36
client-request-id: 5c3d196d-5939-45cc-a45b-232b9ed13fce
...
Restrict-Access-To-Tenants: fortinet-us.com
Restrict-Access-Context: ********-****-452f-8535-************
```

3. After a client attempts to access a personal account, verify that the header information is sent to the Microsoft Active Directory:

```
[I][p:234][s:2519][r:34] wad_dump_fwd_http_req             :2567  hreq=0x7fc75f0ce6a8 Forward
request to server:
GET /oauth20_authorize.srf?client_id=4765445b-32c6-49b0-83e6-
1d93765276ca&scope=openid+profile+https%3a%2f%2fwww.office.com%2fv2%2fOfficeHome.All&redirect_
uri=https%3a%2f%2fwww.office.com%2flandingv2&response_type=code+id_
token&state=7tAtndYhcA3132S--UOTyLVEtyIZs8FgndTpeYM9mJ1EeA-
X5nfqrSalnnPH41cHxfHGug6N5cbliK676v6xZgszgH_
JARVKrptZwBvjI2cbnZ4mttYNNdK1FTlbEtu5VBjgtBOX2u6v3F_
9g7UikCpGTnBRGhvO2pyTndT3EEIyAHvhg9LsKRtY3kxce8dQkfk1iDjLcc3q-01r4rpxSx2xZSbwg_
KkAN3kCRQ9uLfE0ziHAcpvunuKmzGBWKnBhC4sJJkXrMEfXwCg4nsOjg&response_mode=form_
post&nonce=637877163655610380.MjNjZmM4NzQtOTU5My00OGZlLTk0NTItZTE5NDU2YjVlODdjNjViOTQwYmUtOTZl
MS00M2Y5LTkyN2MtN2QyMjgwNjcxY2Uz&x-client-SKU=ID_NETSTANDARD2_0&x-client-
Ver=6.12.1.0&uaid=5c3d196d593945cca45b232b9ed13fce&msproxy=1&issuer=mso&tenant=common&ui_
locales=en-US&epct=AQABAAAAAAD--DLA3VO7QrddgJg7WevrfA6SLaDsJUcjb1Bg9OKonF3d_
lfNJsdDAIH5hlJdUSGejEBIqsko-A7JX67PzaGdEJgOIGa37VhJzGTYBZ-KgATe9FHssnNmLjM_
dojr0dAT83xDhiqQTN2-UcYdcP2s3vPainF7Nqes5ecXRaEoE9Vw9-
sN7jfASOkPRWW03aI6buz0niABvA860YOWDb98vdJWPGkWE-euDr6n8_
zI5iAA&jshs=0&username=***************%40outlook.com&login_hint=***************%40outlook.com
HTTP/1.1
Host: login.live.com
```

```
Connection: keep-alive
...
Referer: https://login.microsoftonline.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
sec-Restrict-Tenant-Access-Policy: restrict-msa
```

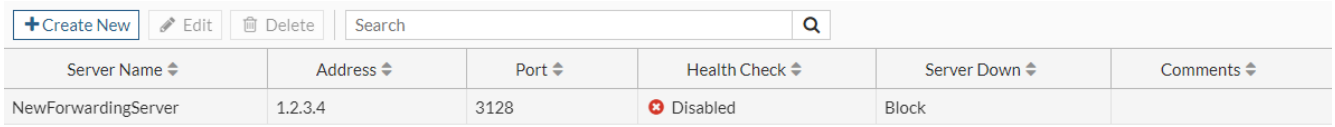
Forwarding Server

By default, the FortiProxy unit monitors a web proxy forwarding server by forwarding a connection to the remote server every 10 seconds. If the remote server does not respond, it is assumed to be down. Checking continues until, when the server does send a response, the server is assumed to be back up. If health checking is enabled, the FortiProxy unit attempts to get a response from a web server by connecting through the remote forwarding server every 10 seconds.

You can enable health checking for each remote forwarding server and specify a different web site to check for each one. Use the Forward Server Monitor widget in the dashboard to monitor the health status of the forwarding servers.

If the remote server is down, you can configure the FortiProxy unit to either block sessions until the server comes back up or allow sessions to connect to their destination using the original server. You cannot configure the FortiProxy unit to fail over to another remote forwarding server.

To configure the server-down action and enable health monitoring, go to *Proxy Settings* > *Forwarding Server*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

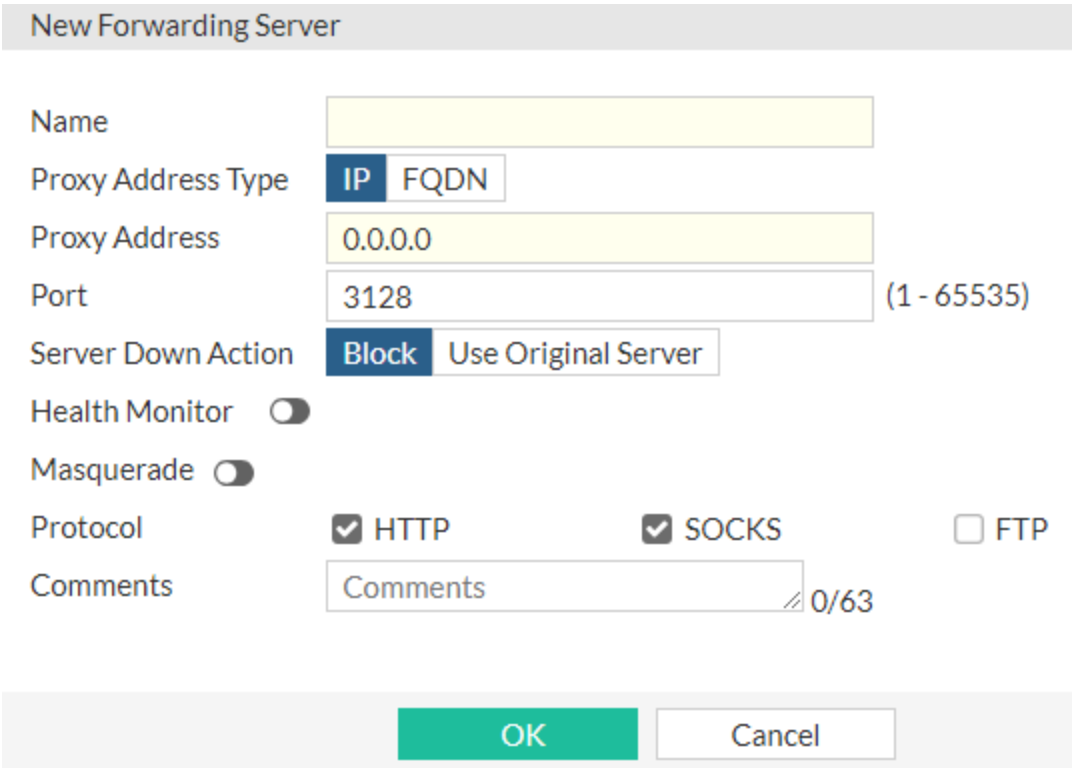
The following options are available:

Create New	Create a forwarding server. See Create or edit a forwarding server on page 160.
Edit	Edit a forwarding server. See Create or edit a forwarding server on page 160.
Delete	Remove a forwarding server from the list.
Search	Enter a search term to find in the list.
Server Name	The name of the forwarding server.
Address	The IP address of the forwarding server.

Port	The port number of the forwarding server.
Health Check	Indicates whether the health check is disabled or enabled for that forwarding server.
Server Down	The action that the FortiProxy unit takes when the server is down.
Comments	Optional description of the forwarding server.

Create or edit a forwarding server

Select *Create New* to open the *New Forwarding Server* window.



To open the *Edit Forwarding Server* window, select a forwarding server and then click *Edit*.

Configure the following settings in the *New Forwarding Server* window or *Edit Forwarding Server* window and then click *OK*:

Name	Enter the name of the forwarding server.
Proxy Address Type	Select the type of IP address of the forwarding server, either *IP* or *FQDN*.
Proxy Address	Enter the IP address or the fully qualified domain name of the forwarding server.
Port	Enter the port number of the forwarding server.

Server Down Action	Select what action the FortiProxy unit will take if the forwarding server is down, either *Block* or *Use Original Server*.
Health Monitor	Enable or disable health check monitoring. This option behaves differently when the forward server is configured with different protocols: **Protocol** / **Behavior** FTP / When *Health Monitor* is enabled, health check is performed against the explicit FTP proxy server. You cannot configure Health Check Monitor Site. HTTP or HTTP + HTTPS / When *Health Monitor* is enabled, health check is performed with HTTP only. SOCKS only / The *Health Monitor* option is not available. No health check is performed. Use the Forward Server Monitor widget in the dashboard to monitor the health status of the forwarding server.
Health Check Monitor Site	If you enabled *Health Monitor*, enter the URL address of the health check monitoring site. This option is unavailable when the protocol of the forward server is FTP.
Masquerade	Enable or disable whether the web proxy uses the device address to connect to the proxy server.
Protocol	Configure the protocol of the forwarding server. The following protocols are supported: • HTTP • SOCKS • FTP HTTP and SOCKS are enabled by default, which means both HTTP and SOCKS traffic is forwarded. Traffic with a disabled or unsupported protocol will not be forwarded. For example, when the forward server is configured with HTTP as supported protocol, SOCKS or FTP traffic will not be forwarded. You can configure a forward server group with different types of SOCKS/HTTP/FTP servers so that the load balancing algorithm can pick a server that supports the protocol within the group automatically. If none of the configured servers supports the protocol of incoming traffic, the forward server group is ignored. See Grouping forwarding servers and load balancing traffic to the servers on page 165 for more details.

Comments	Enter an optional description of the forwarding server.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown for the CMDB API that creates the explicit proxy configuration.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

To create a forwarding server in the CLI:

```
config web-proxy forward-server
    edit <server_name>
        set addr-type {ip | fqdn}
        set ip <IPv4_address>
        set fqdn <FQDN>
        set port <1-65535>
        set healthcheck {disable | enable}
        server-down-option {block | pass}
        set comment <string>
        set authentication {disabled | immediately | upon-challenge}
        set masquerade {enable | disable}
    next
end
```

Selectively forward web requests to a transparent web proxy

Web traffic over HTTP/HTTPS can be forwarded selectively by the FortiProxy unit's transparent web proxy to an upstream web proxy to avoid overwhelming the proxy server. Traffic can be selected by specifying the proxy address (`set webproxy-forward-server`), which can be based on a FortiGuard URL category.



The FortiGuard web filter service must be enabled on the downstream FortiProxy unit.

Forwarding behavior

The forward server will be ignored if the proxy policy matching for a particular session needs the FortiProxy unit to see authentication information inside the HTTP (plain text) message. For example, assume that user authentication is required and a forward server is configured in the transparent web proxy, and the authentication method is an active method (such as basic). When the user or client sends the HTTP request over SSL with authentication information to the FortiProxy unit, the request cannot be forwarded to the upstream proxy. Instead, it will be forwarded directly to the original web server (assuming deep inspection and `http-policy-redirect` are enabled in the firewall policy).

The FortiProxy unit will close the session before the client request can be forwarded if all of the following conditions are met:

- The certificate inspection is configured in the firewall policy that has the `http-policy-redirect` option enabled.
- A previously authenticated IP-based user record cannot be found by the FortiProxy unit's memory during the SSL handshake.
- Proxy policy matching needs the FortiProxy unit to see the HTTP request authentication information.

Use the following best practices to enable user authentication and use `webproxy-forward-server` in the transparent web proxy policy at the same time:

- In the firewall policy that has the `http-policy-redirect` option enabled, set `ssl-ssh-profile` to use the `deep-inspection` profile.
- Use IP-based authentication rules; otherwise, the `webproxy-forward-server` setting in the transparent web proxy policy will be ignored.
- Use a passive authentication method such as FSSO. With FSSO, once the user is authenticated as a domain user by a successful login, the web traffic from the user's client will always be forwarded to the upstream proxy as long as the authenticated user remains unexpired. If the authentication method is an active authentication method (such as basic, digest, NTLM, negotiate, form, and so on), the first session containing authentication information will bypass the forward server, but the following sessions will be connected through the upstream proxy.

Sample configuration

On the downstream FortiProxy proxy, there are two category proxy addresses used in two separate transparent web proxy policies as the destination address:

- In the policy with `upstream_proxy_1` as the forward server, the proxy address `category_infotech` is used to match URLs in the information technology category.
- In the policy with `upstream_proxy_2` as the forward server, the proxy address `category_social` is used to match URLs in the social media category.

To configure forwarding requests to transparent web proxies:

1. Configure the proxy forward servers:

```
config web-proxy forward-server
    edit "upStream_proxy_1"
        set ip 172.16.200.20
```

```
    next
    edit "upStream_proxy_2"
        set ip 172.16.200.46
    next
end
```

2. Configure the web proxy addresses:

```
config firewall proxy-address
    edit "category_infotech"
        set type category
        set host "all"
        set category 52
    next
    edit "category_social"
        set type category
        set host "all"
        set category 37
    next
end
```

3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "av"
    next
end
```

4. Configure the proxy policies:

```
config firewall policy
    edit 1
        set type transparent
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "category_infotech"
        set action accept
        set schedule "always"
        set logtraffic all
        set webproxy-forward-server "upStream_proxy_1"
        set utm-status enable
```

```
        set ssl-ssh-profile "deep-inspection"
        set av-profile "av"
    next
    edit 2
        set type transparent
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "category_social"
        set action accept
        set schedule "always"
        set logtraffic all
        set webproxy-forward-server "upStream_proxy_2"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "av"
    next
end
```

Grouping forwarding servers and load balancing traffic to the servers

You can add multiple forwarding servers to a forwarding server group and then add the server group to an explicit policy instead of adding a single server. Forwarding server groups can only be created from the FortiProxy CLI using the `config web-proxy forward-server-group` command but can be added to policies from the GUI (or CLI).

When you create a forwarding server group, you can select a load balancing method to control how sessions are load balanced to the forwarding servers in the server group. Two load balancing methods are available:

- *Weighted* load balancing sends more sessions to the servers with higher weights. You can configure the weight for each server when you add it to the group.
- *Least-session* load balancing sends new sessions to the forwarding server that is processing the fewest sessions.

When you create a forwarding server group you can also enable *affinity*. Enable affinity to have requests from the same client processed by the same server. This can reduce delays caused by using multiple servers for a single multi-step client operation. Affinity takes precedence over load balancing.

You can also configure the behavior of the group if all of the servers in the group are down. You can select to block traffic or you can select to have the traffic pass through the FortiProxy explicit proxy directly to its destination instead of being sent to one of the forwarding servers.

Example

The following example adds a forwarding server group that uses weighted load balancing to load balance traffic to three forwarding servers. Server weights are configured to send most traffic to

server2. The group has affinity enabled and blocks traffic if all of the forward servers are down.

```
config web-proxy forward-server
    edit server_1
        set ip 172.20.120.12
        set port 8080
    next
    edit server_2
        set ip 172.20.120.13
        set port 8000
    next
    edit server_3
        set ip 172.20.120.14
        set port 8090
    next
end
```

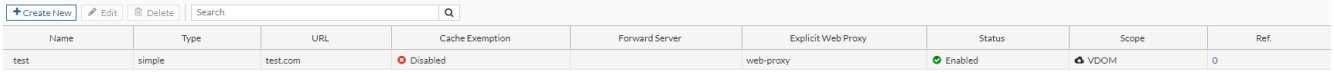
```
config web-proxy forward-server-group
    edit New-fwd-group
        set affinity enable
        set ldb-method weighted
        set group-down-option block
        config server-list
            edit server_1
                set weight 10
            next
            edit server_2
                set weight 40
            next
            edit server_3
                set weight 10
            next
        end
    next
end
```

Server URL

The URL match list is used to exempt URLs from caching and to enable forwarding specific URLs to a web proxy server. URLs, URL patterns, and numeric IP addresses can be added to the match list.

For example, if your users access web sites that are not compatible with FortiProxy web caching, you can add the URLs of these web sites to the web caching exempt list, and all traffic accepted by a web cache policy for these websites will not be cached.

To see the available URL match entries, go to *Proxy Settings* > *Server URL*.



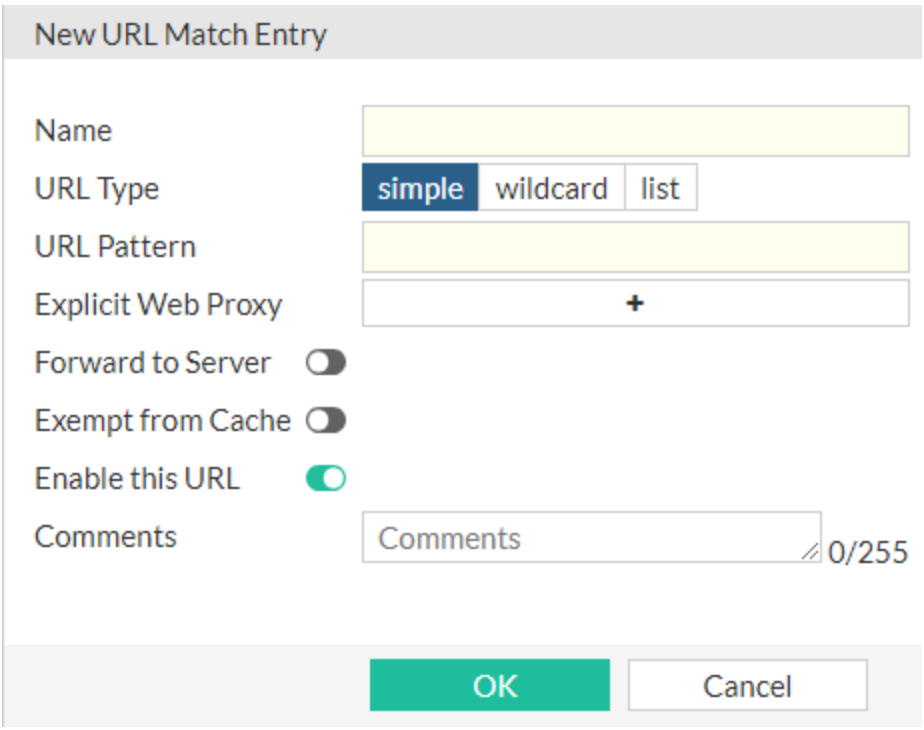
Hover over the leftmost edge of the column heading to display the Configure Table icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings or rows to change the order.

The following options are available:

Create New	Create a URL match entry. See Create or edit a URL match entry on page 167.
Edit	Edit a URL match entry. See Create or edit a URL match entry on page 167.
Delete	Remove a URL match entry from the list.
Search	Enter a search term to find in the list.
Name	The name for the URL match entry.
Type	URL match type, which can be one of the following: • simple—The URL match entry is a simple URL. • wildcard—The URL match entry is defined as a set of URLs with a wildcard in it. • list—The URL match entry is defined as a list of URLs.
URL	The URL pattern or list to match.
Cache Exemption	Whether the URL is exempt from caching.
Forward Server	Name of the forwarding server that the URL is forwarded to. To create a forwarding server, see Create or edit a forwarding server on page 160.
Explicit Web Proxy	Explicit proxy that the URL match entry applies to.
Status	The status is either *enable* or *disable*.
Scope	Scope that the URL match entry applies to. For example, it can be the VDOM where the URL match entry is created.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Comments	Optional description of the URL match entry.

Create or edit a URL match entry

Select *Create New* to open the *New URL Match Entry* window.



To open the *Edit URL Match Entry* window, select a URL match entry and then click *Edit*.

Configure the following settings in the *New URL Match Entry* window or *Edit URL Match Entry* window and then click *OK*.

Name	Enter a name for the URL match entry.
URL Type	URL match type, which can be one of the following: • simple—The URL match entry is a simple URL. • wildcard—The URL match entry is defined as a set of URLs with a wildcard in it. • list—The URL match entry is defined as a list of URLs.
URL Pattern/List	The URL pattern or list to match.
Explicit Web Proxy	Select the explicit proxy that the URL match entry applies to.
Forward to Server	If you want to forward the URL to a web proxy server, enable *Forward to Server* and select the server from the drop-down list. To create a forwarding server, see Forwarding Server on page 159.
Exempt from Cache	Enable this option to exempt the URL from caching.
Enable this URL	Enable this option to make the URL match entry active.
Comments	Enter an optional description of the URL match entry.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To create a URL match entry in the CLI:

```
config web-proxy url-match
   edit <name>
      set status {enable | disable}
      set type [simple|wildcard|...]
      set url-pattern <value>
      set url-list {string}
      set forward-server <forwarding_server_name>
      set cache-exemption {enable | disable}
      set comment <optional_string>
   next
end
```

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown for the CMDB API that creates the explicit proxy configuration.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

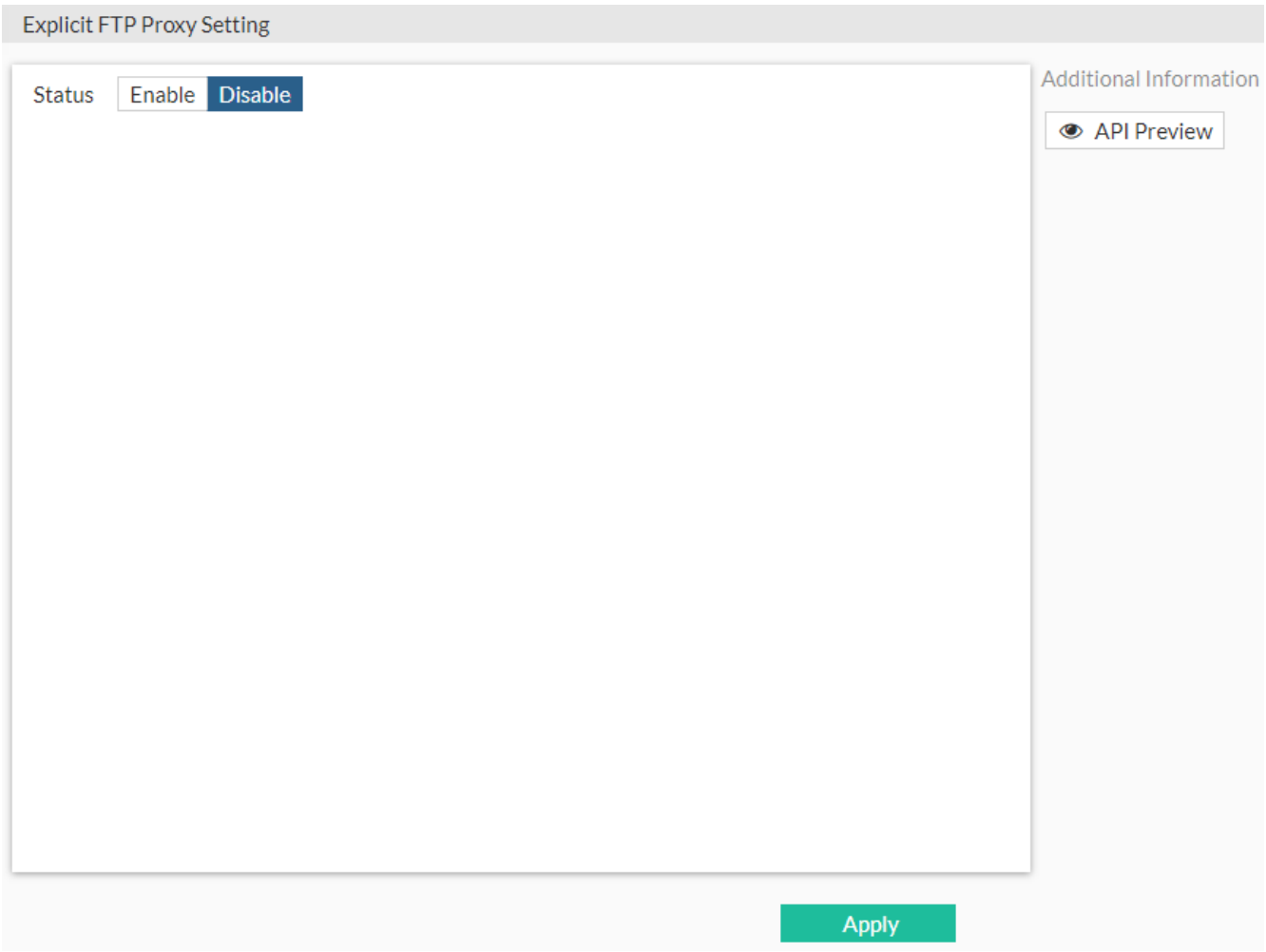
FTP Proxy

You can enable the explicit FTP proxy on one or more FortiProxy interfaces. The explicit web and FTP proxies can be operating at the same time on the same or on different FortiProxy interfaces.



Enabling the explicit FTP proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

To configure the explicit FTP proxy, go to *Proxy Settings* > *FTP Proxy*.



Configure the following settings and then click *Apply*:

Status	Select *Enable* to make the explicit FTP proxy active.
Incoming IP	Enter the incoming IP address.
Outgoing IP	Enter the outgoing IP address.
Default Firewall Policy Action	If *Default Firewall Policy Action* is set to *Deny*, traffic sent to the explicit FTP proxy that is not accepted by an explicit FTP proxy policy is dropped. If *Default Firewall Policy Action* is set to *Allow*, all FTP proxy sessions that do not match a policy are allowed.
Incoming Port	Enter the range of incoming port numbers. Click + to add another range.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown for the CMDB API that creates the explicit proxy configuration.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

FTPS handling

When `explicit-ftp-tls` is enabled in the FTP protocol options, FTP control sessions are proxied to enforce deep inspection so that the proxy can understand FTP control commands after STARTTLS and open a pinhole for FTP data sessions regardless of FTPS deep inspection and/or UTM status.

```
config firewall profile-protocol-options
    edit "test"
        config ftp
            set ports 21
            set status enable
            set explicit-ftp-tls {disable | enable}
        end
    next
end
```

When deep inspection is enabled, transparent policy FTP is always redirected.

Proxy Options

Certain inspections defined in security profiles require that the traffic be held in proxy while the inspection is carried out. When a security profile requiring the use of a proxy is enabled in a policy, the *Proxy Options* field is displayed. The proxy options define the parameters of how the traffic will be processed and to what level the traffic will be processed. There can be multiple security profiles of a single type. There can also be a number of unique proxy option profiles. As the requirements for a policy differ from one policy to the next, a different proxy option profile for each individual policy can be configured or one profile can be repeatedly applied.

The proxy options refer to the handling of the following protocols:

- HTTP
- SMTP
- POP3
- IMAP
- FTP
- NNTP

- MAPI
- DNS
- CIFS

The configuration for each of these protocols is handled separately.

Just like other components of the FortiProxy unit, different proxy option profiles can be configured to allow for granular control of the FortiProxy unit. In the case of the proxy option profiles, you need to match the correct profile to a firewall policy that is using the appropriate protocols. If you are creating a proxy option profile that is designed for policies that control SMTP traffic into your network, you only want to configure the settings that apply to SMTP. You do not need or want to configure the HTTP components.

To view the available proxy option profiles, go to *Proxy Settings* > *Proxy Options*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a proxy option profile. See Create or edit a proxy option profile on page 175 and Create a CIFS proxy option on page 178.
Edit	Modify the selected proxy option profile. See Create or edit a proxy option profile on page 175.
Clone	Make a copy of the selected proxy option profile.
Delete	Remove the selected proxy option profile.
Search	Enter a search term to find in the proxy option profile list.
Name	The name of the proxy option profile.
Read Only	The `default` proxy option profile is read only. It cannot be changed or deleted.
Comments	An optional description of the proxy option profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Video streaming splitting

The following are the most popular audio/video streaming protocols:

1. Real-time Transport Protocol (RTP)
2. Real Time Streaming Protocol (RTSP)
3. MPEG-Dynamic Adaptive Streaming over HTTP (DASH)
4. Apple HTTP Live Streaming (HLS)
5. Adobe HTTP Dynamic Streaming (HDS)
6. Microsoft Smooth Streaming (MSS)

To deliver streams smoothly and transmit as much information as possible, video stream splitting splits streams into fragments, and their size is negotiated dynamically between the client and server. Sometimes, the fragment is kept unchanged. The default fragment sizes are 64 bytes for audio data and 128 bytes for video data and most other data types. Fragments from different streams can then be interleaved and multiplexed over a single connection. Streams can carry, for example, video and one or more audio channels, next to a control channel to control the streams. This is like an FTP command versus data session.

FortiProxy supports Apple HLS and MPEG-DASH stream splitting, which can be transferred over HTTP (S) or TCP port 1935.

Configuring TCP windows

Some file transfer applications can negotiate large TCP windows. For example, WinSCP can negotiate an initial TCP window size of about 2 GB.

The TCP window options can be used to prevent overly large initial TCP window sizes, helping avoid channel flow control issues. It allows stream-based scan's flow control to limit peers from sending data that exceeds a policy's configured oversize limit.

To configure TCP window size options:

```
config firewall profile-protocol-options
    edit <string>
        config {ftp | ssh}
            ...
            set stream-based-uncompressed-limit <integer>
            set tcp-window-type {auto-tuning | system | static | dynamic}
            set tcp-window-size <integer>
            set tcp-window-minimum <integer>
            set tcp-window-maximum <integer>
            ...
        end
    next
end
```

`{ftp | ssh}`	• `ftp`: Configure FTP protocol options.

	• ssh: Configure SFTP and SCP protocol options.
stream-based-uncompressed-limit <integer>	The maximum stream-based uncompressed data size that will be scanned, in MB (default = 0 (unlimited)). Stream-based uncompression used only under certain conditions.).
tcp-window-type {auto-tuning | system | static | dynamic}	The TCP window type to use for this protocol. • auto-tuning: Allow the system to automatically tune the TCP window size (default). When memory usage reaches the threshold of 80%, FortiProxy automatically changes the value to system to protect memory usage. • system: Use the system default TCP window size for this protocol. • static: Manually specify the TCP window size. • dynamic: Vary the TCP window size based on available memory within the limits configured in tcp-window-minimum and tcp-window-maximum.
tcp-window-size <integer>	The TCP static window size (65536 - 33554432, default = 262144). This option is only available when tcp-window-type is static.
tcp-window-minimum <integer>	The minimum TCP dynamic window size (65536 - 1048576, default = 131072). This option is only available when tcp-window-type is dynamic.
tcp-window-maximum <integer>	The maximum TCP dynamic window size (1048576 - 33554432, default = 8388608). This option is only available when tcp-window-type is dynamic.

Handling SSL offloaded traffic from an external decryption device

In scenarios where the FortiProxy unit is sandwiched between load-balancers and SSL processing is offloaded on the external load-balancers, the FortiProxy unit can perform scanning on the unencrypted traffic by specifying the ssl-offloaded option in firewall profile-protocol-options.

To configure SSL offloading:

```
config firewall profile-protocol-options
    edit <name>
        config http
            set ports <1-65535>
            set ssl-offloaded {no | yes}
        end
        config ftp
            set ports <1-65535>
            set ssl-offloaded {no | yes}
        end
```

```
        config imap
            set ports <1-65535>
            set ssl-offloaded {no | yes}
        end
        config pop3
            set ports <1-65535>
            set ssl-offloaded {no | yes}
        end
        config smtp
            set ports <1-65535>
            set ssl-offloaded {no | yes}
        end
        config ssh
            set ports <1-65535>
            set ssl-offloaded {no | yes}
        end
    next
end
```

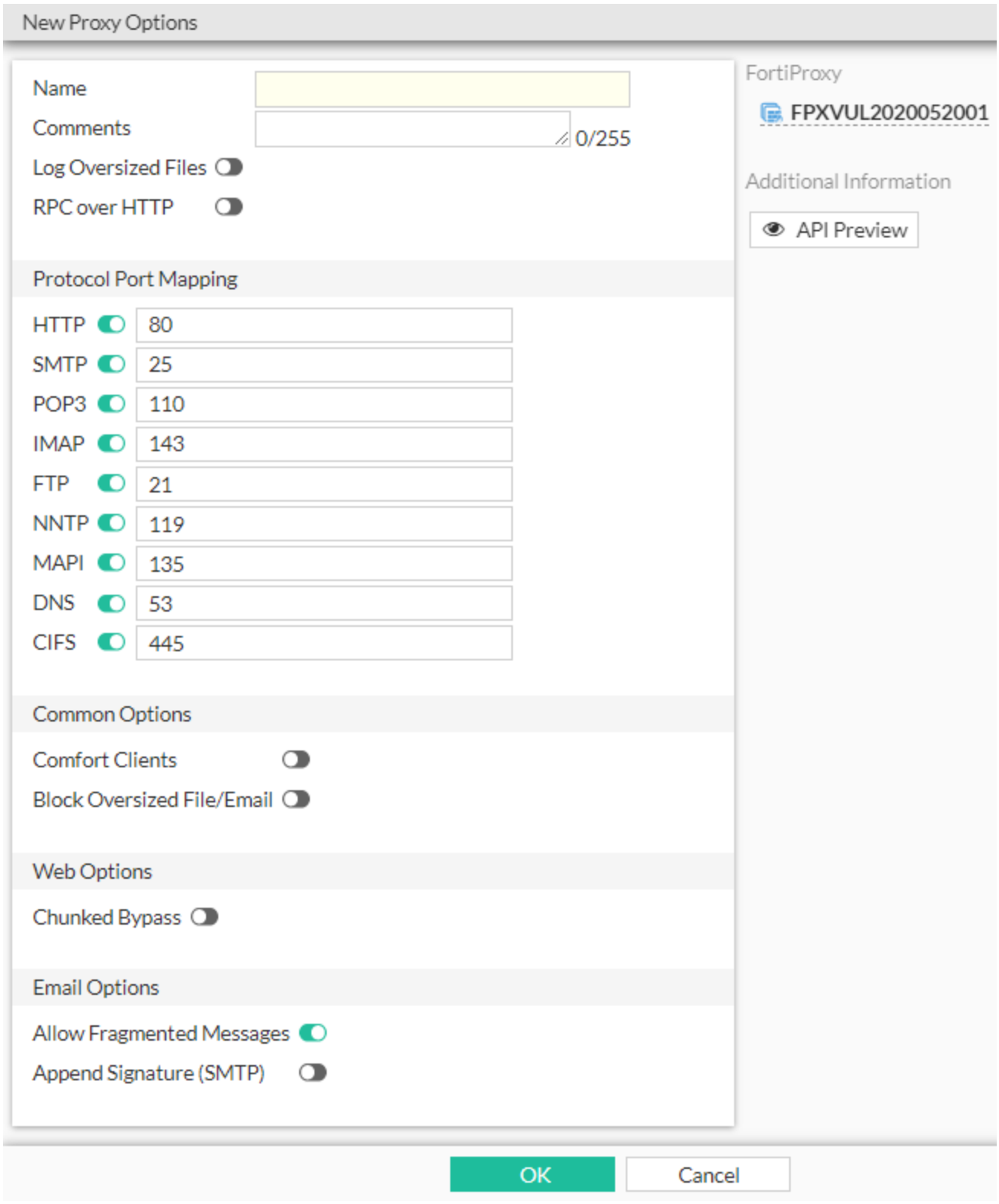
HTTP domain fronting blocking

To block HTTP domain fronting:

```
config firewall profile-protocol-options
    edit <name>
        config http
            set domain-fronting block
        end
    next
end
```

Create or edit a proxy option profile

To configure a new proxy option profile, go to *Proxy Settings* > *Proxy Options* and click *Create New*. The *New Proxy Options* page is displayed.


New Proxy Options
Name
Comments
0/255
Log Oversized Files
RPC over HTTP
Protocol Port Mapping
HTTP 80
SMTP 25
POP3 110
IMAP 143
FTP 21
NNTP 119
MAPI 135
DNS 53
CIFS 445
Common Options
Comfort Clients
Block Oversized File/Email
Web Options
Chunked Bypass
Email Options
Allow Fragmented Messages
Append Signature (SMTP)
FortiProxy
FPXVUL2020052001
Additional Information
API Preview
OK
Cancel

Configure the following settings and then click *OK* to save your changes:

Name	The name of the proxy option profile.
Comments	Optional description of the proxy option profile.
Log Oversized Files	Enable this setting to log when oversized files are processed. The setting does not change how the files are processed. It only enables the FortiProxy unit to log that they were either blocked or allowed through. A common practice is to allow larger files through without antivirus processing. This practice allows you to get an idea of how often this happens and decide on whether to alter the settings relating to the treatment of oversized files.
RPC over HTTP	Enable or disable the inspection of RPC over HTTP.
Protocol Port Mapping	To optimize the resources of the unit, enable or disable the mapping and inspection of protocols. When you enable a protocol, the default port numbers are automatically filled in, but you can change them.
Common Options	
Comfort Clients	When proxy-based antivirus scanning is enabled, the FortiProxy unit buffers files as they are downloaded. After the entire file is captured, the FortiProxy unit begins scanning the file. During the buffering and scanning procedure, the user must wait. After the scan is completed, if no infection is found, the file is sent to the next step in the process flow. If the file is a large one this part of the process can take some time. In some cases enough time that some users may get impatient and cancel the download. The *Comfort Clients* feature mitigates this potential issue by feeding a trickle of data while waiting for the scan to complete. The user then knows that processing is taking place and that there hasn't been a failure in the transmission. The slow transfer rate continues until the antivirus scan is complete. After the file has been successfully scanned and found to be clean of any viruses, the transfer will proceed at full speed. Enable and then configure the following: • *Interval (seconds)*—Enter the interval time in seconds. The default is 10. • *Amount (bytes*—Enter the amount in bytes. The default is 1.
Block Oversized File/Email	You can block files or emails that are larger than a specified size. Enable and then enter the threshold size in megabytes of the files and emails to block.
Web Options	

Chunked Bypass	The HTTP section allows the enabling of Chunked Bypass. This refers to the mechanism in version 1.1 of HTTP that allows a web server to start sending chunks of dynamically generated output in response to a request before actually knowing the actual size of the content. Where dynamically generated content is concerned, enabling this feature means that there is a faster initial response to HTTP requests. From a security stand point, enabling this feature means that the content is not held in the proxy as an entire file before proceeding. Enable or disable the chunked bypass setting.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create a CIFS proxy option

CIFS can be configure in the GUI by creating or editing a proxy option under *Proxy Settings* > *Proxy Options*, and in the CLI using the `config firewall profile-protocol-options` command. The `cifs-profile` command is no longer available from the `firewall policy` options.

The CIFS proxy option can then be used in a policy.

To create a CIFS proxy option:

```
config firewall profile-protocol-options
    edit <option>
        config cifs
            set ports <port>
            set status {enable | disable}
            set options <string>
            set oversize-limit <integer>
            set uncompressed-oversize-limit <integer>
            set uncompressed-nest-limit <integer>
            set scan-bzip2 {enable | disable}
            set tcp-window-type {auto-tuning | system | static | dynamic}
            set server-credential-type {none | credential-replication | credential-keytab}
        end
```

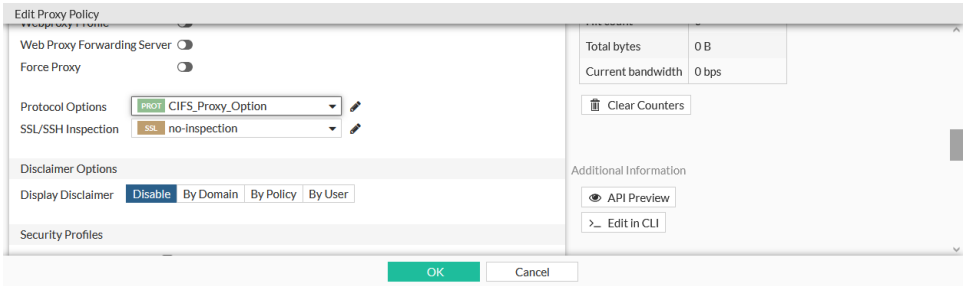
```
    next
end
```

To use the CIFS proxy option in a policy:

- In the CLI, select the option using the set `profile-protocol-options <option>` command:

```
config firewall policy
    edit 1
        set profile-protocol-options <option>
    next
end
```

- In the GUI, select the option in the *Protocol Options* field when editing a policy.



SSL Keyring

The FortiProxy keyring file includes a list of SSL client certificates (maximum 240,000) or certificate chains in PEM format. The file is stored on the FortiProxy disk and is encrypted using aes256 gsm and a random salt. You can upload the file using the GUI or SCP.

The keyring list must start with `#keyring`, and uses the following format:

```
#keyring:1
<private_key_1>
<certificate_1>
<optional_certificate_chain_1>
#keyring:2
<private_key_2>
<certificate_2>
<optional_certificate_chain_2>
....
```

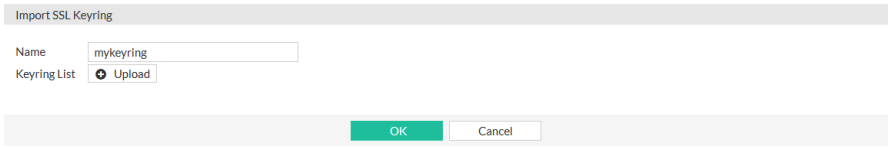
For example:

```
#keyring:1
-----BEGIN PRIVATE KEY-----
MC4CAQ...arfLXfXrEve+Yb8zQ
-----END PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
MII...SDg==
-----END CERTIFICATE-----
#keyring:2
-----BEGIN EC PARAMETERS-----
Bg...Bw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHc...onQ==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MII...4Dh
-----END CERTIFICATE-----
```

To upload a keyring list in the GUI:

1. Go to *Proxy Settings* > *SSL Keyring* and click *Create New*.
2. Enter a name for the list.



3. Click *Upload* to upload the list from the management computer.
4. Click *OK*.

To upload a keyring list from the management computer using SCP:

```
scp <keyring-file-path> admin@<FPX address>:keyring-list:<optional profile name>
```

For example:

```
scp mykeyring admin@10.10.10.1:keyring-list:mykeyring
```

Network

The *Network* menu allows you to configure the unit to operate on the network. This menu provides features for configuring and viewing basic network settings, such as the unit's interfaces, Domain Name System (DNS) options, and routing table.

This section describes the following:

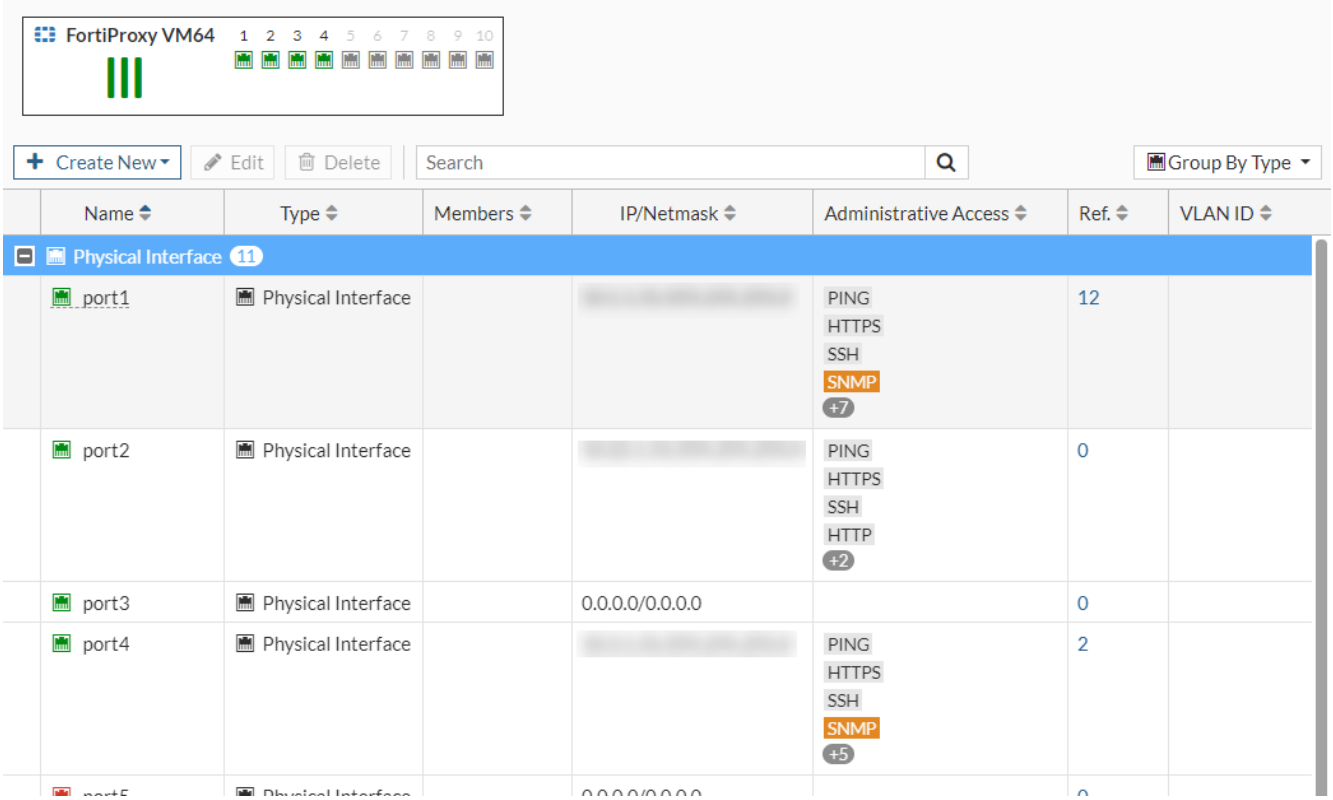
- Interfaces on page 181
- GRE Tunnel on page 196
- DNS Settings on page 199
- DNS Service on page 207
- Diagnostics on page 218
- Static routes on page 224
- Policy routes on page 227
- VXLAN on page 230

Interfaces



Unless stated otherwise, the term *interface* refers to a physical FortiProxy interface.

In *Network* > *Interfaces*, you can configure the interfaces that handle incoming and outgoing traffic.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

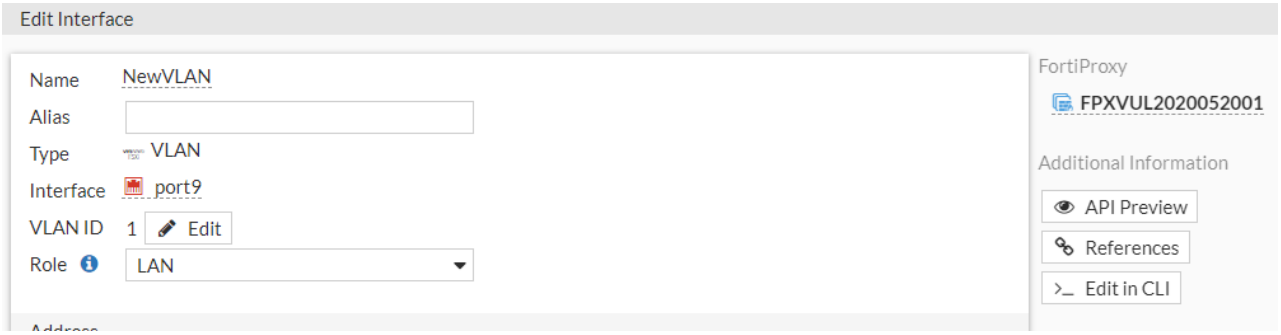
The following options are available:

Create New	Select to create an interface or a zone. See Create or edit an interface on page 188 and Create or edit a zone on page 194.
Edit	Modifies settings within the interface or zone. See Create or edit an interface on page 188 and Create or edit a zone on page 194.
Delete	Removes an interface from the list. To remove multiple interfaces, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Search	Enter a search term to find in the list.
Grouping	Select *Group By Type*, *Group By Role*, *Group By Status*, *Group By Zone*, or *No Grouping* to change how the rows are displayed on the interface list.
Status	The administrative status for the interface. If the administrative status is green, the interface is up and can accept network traffic. If the administrative status is red, the interface is administratively down and cannot accept traffic. To change the administrative status of an interface, right-click the icon and select the *Set Status* setting for the interface.

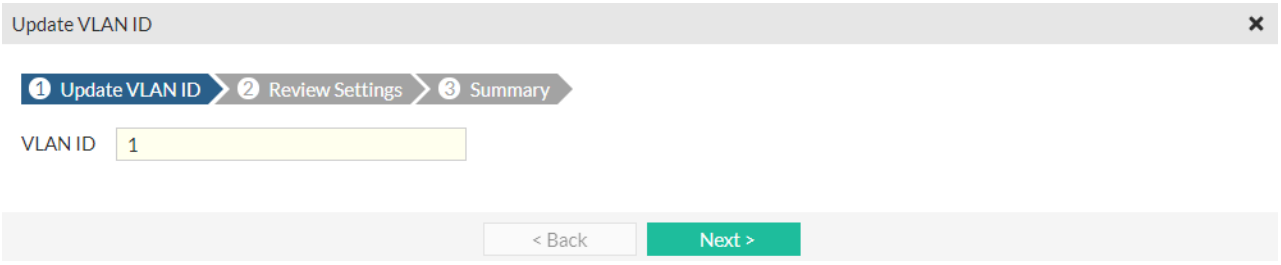
Name	The names of the physical interfaces on your FortiProxy unit. The names include any alias names that have been configured.
Type	The type of the interface, such as *Physical Interface*.
Members	Interfaces that belong to the virtual interface of the software switch.
IP/Netmask	The current IP address/netmask of the interface. When IPv6 Support is enabled on the GUI, IPv6 addresses are displayed in this column.
Administrative Access	The administrative access configuration for the interface.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Bytes	The number of bytes being used.
Description	A description of the interface.
DHCP Clients	If the interface has been configured as a DHCP client.
DHCP Ranges	The range of IPv4 addresses.
Errors	Any errors detected.
IPv6 Access	The types of administrative access permitted for IPv6 connections to this interface.
IPv6 Address	The IPv6 address/subnet mask for the interface.
IPv6 DHCP Clients	If the interface has been configured as a DHCP client.
IPv6 DHCP Ranges	The range of IPv6 addresses.
Link Status	The status is *Up* when a valid cable is plugged in. The status is *Down* when an invalid cable is plugged in.
MAC Address	The MAC address of the interface.
Packets	The total number of packets that have been sent and received. Hover over the bar chart to see the separate packet numbers.
Role	The role can be *LAN*, *WAN*, *DMZ*, or *Undefined*.
Secondary IP(s)	The secondary IPv4 addresses added to the interface.
Secondary IPv6 Addresses	The secondary IPv6 addresses added to the interface.
Security Mode	The mode is either *None* or *Captive Portal*.
VLAN ID	The configured VLAN ID for VLAN subinterfaces.
VRRP	Whether the Virtual Router Redundancy Protocol is being used.
Zone	The name of the zone that the interface belongs to.

To change the VLAN ID:

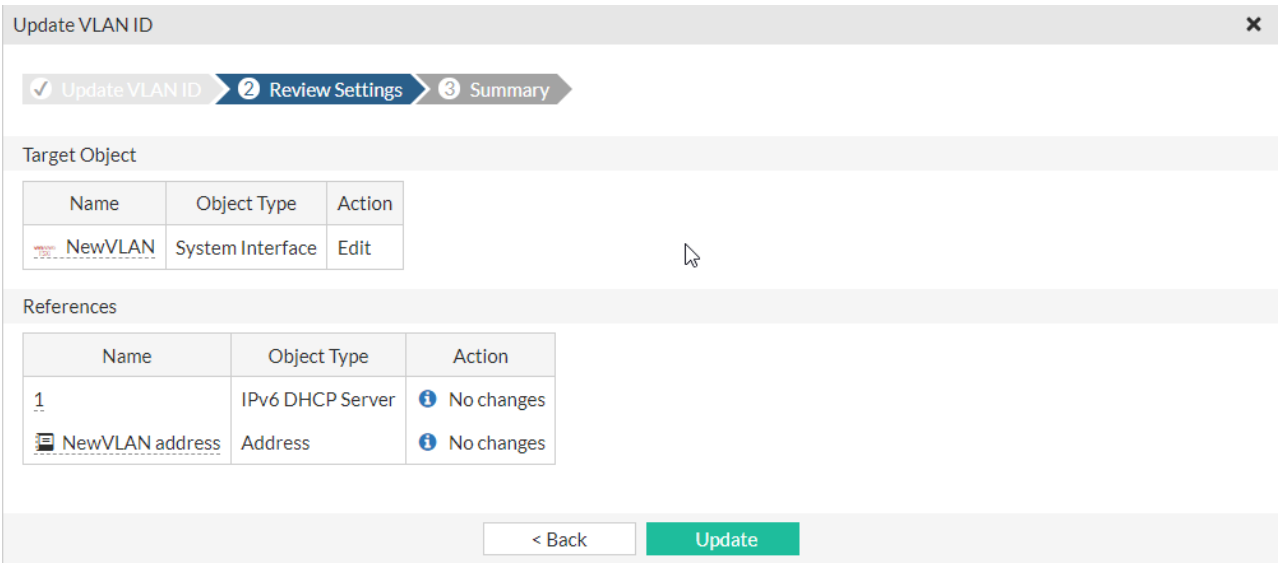
1. Go to *Network* > *Interfaces*, select a VLAN, and then click *Edit*.
2. Beside the *VLAN ID* field, click *Edit*. The *Update VLAN ID* window opens.



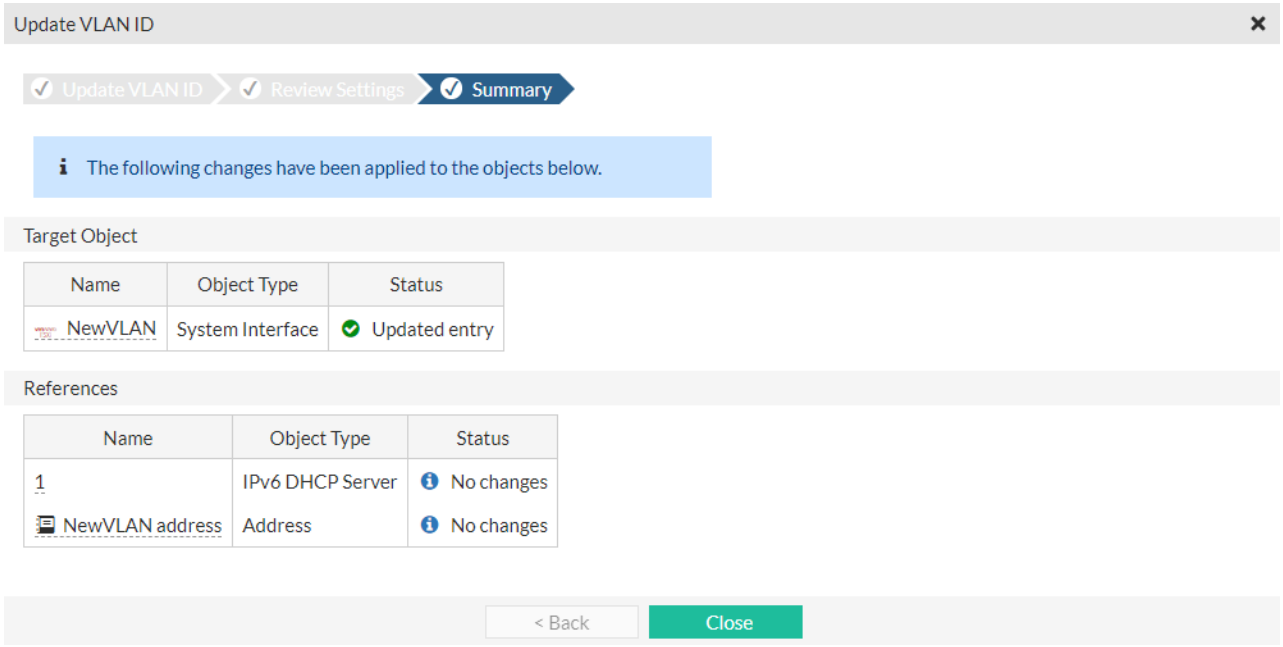
3. Enter the new ID and click *Next*.



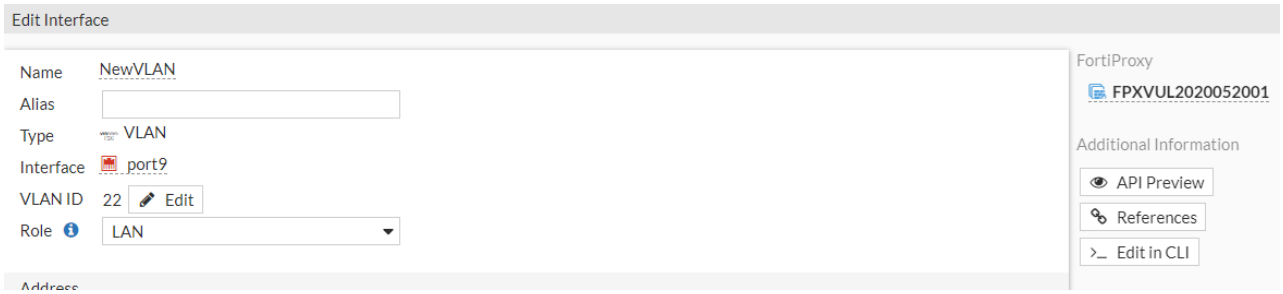
4. Verify the changes and then click *Update* and *OK*.



5. The target object status changes to *Updated entry*. Click *Close*.



In the interface settings, the new VLAN ID is displayed.



Link health monitor

A link health monitor confirms the connectivity of the device's interface. You can detect possible routing loops with link health monitors. You can configure the FortiProxy unit to ping a gateway at regular intervals to ensure that it is online and working. When the gateway is not accessible, that interface is marked as down.

Set the `interval` (how often to send a ping) and `failtime` (how many lost pings are considered a failure). A smaller `interval` and smaller number of lost pings results in faster detection but creates more traffic on your network. You might also want to log CPU and memory usage, as a network outage causes your CPU activity to spike.

To configure a link health monitor using the CLI:

```
config system link-monitor
   edit <link_monitor_name>
      set srcintf <interface_name>
      set server <server_IP_address>
      set protocol {ping | tcp-echo | udp-echo | http | twamp}
      set gateway-ip <gateway_IPv4_address>
```

```
      set source-ip <IPv4_address>
      set interval <seconds>
      set timeout <seconds>
      set failtime <retry_attempts>
      set recoverytime <number_of_successful_responses>
      set ha-priority <priority>
      set update-cascade-interface {enable | disable}
      set update-static-route {enable | disable}
      set status {enable | disable}
   next
end
```

CLI option	Description
srcintf	The name of the interface to add the link health monitor to.
server	One or more IP addresses of the servers to be monitored. If the link health monitor cannot connect to all of the servers, remote IP monitoring considers the link to be down. You can add multiple IP addresses to a single link monitor to monitor more than one IP address from a single interface. If you add multiple IP addresses, the health checking will be with all of the addresses at the same time. The link monitor only fails when no responses are received from all of the addresses.
protocol	One or more protocols to be used to test the link. The default is ping.
gateway-ip	The IPv4 address of the remote gateway that the link monitor must communicate with to contact the server. Only required if there is no other route on for this communication.
source-ip	Optionally add a source IPv4 address for the monitoring packets. Normally the source address is the address of the source interface. You can add a different source address if required.
interval	The time between sending link health check packets. The default is 5 seconds. The range is 1 to 3600 seconds.
timeout	The time to wait before receiving a response from the server. The default is 1 second. The range is 1 to 255 seconds.
failtime	The number of times that a health check can fail before a failure is detected (the failover threshold). The default is 5. The range is 1 to 10.
recoverytime	The number of times that a health check must succeed after a failure is detected to verify that the server is back up. The default is 5. The range is 1 to 10.
ha-priority	The priority of this link health monitor when the ling health monitor is part of a remote link monitor configuration. The default is 1. The range is 1 to 50.
update-cascade-interface	Enable to bring down the source interface if the link health monitor fails. Disable to keep the interface up if the link health monitor fails.

CLI option	Description
	The default is enable.
update-static-route	Enable to remove static routes from the routing table that use this interface if the link monitor fails. The default is enable.
status	Enable or disable this link monitor. The default is enable.

Selecting the source interface and address for Telnet and SSH

The execute telnet-options and execute ssh-options commands allow administrators to set the source interface and address for their connection:

```
# execute telnet-options {interface <outgoing interface> | reset | source <source interface IP> |
view-settings}
```

```
# execute ssh-options {interface <outgoing interface> | reset | source <source interface IP> |
view-settings}
```

To edit the Telnet options:

```
# execute telnet-options interface port1
```

```
# execute telnet-options source 1.1.1.1
```

To confirm that the Telnet packets are using the configured port and address:

```
# diagnose sniffer packet any "port 23" 4
4.070426 port1 out 1.1.1.1.13938 -> 15.15.15.2.23: syn 400156130
4.070706 port1 in 15.15.15.2.23 -> 1.1.1.1.13938: syn 2889776642 ack 400156131
```

To edit the SSH options:

```
# execute ssh-options interface port1
```

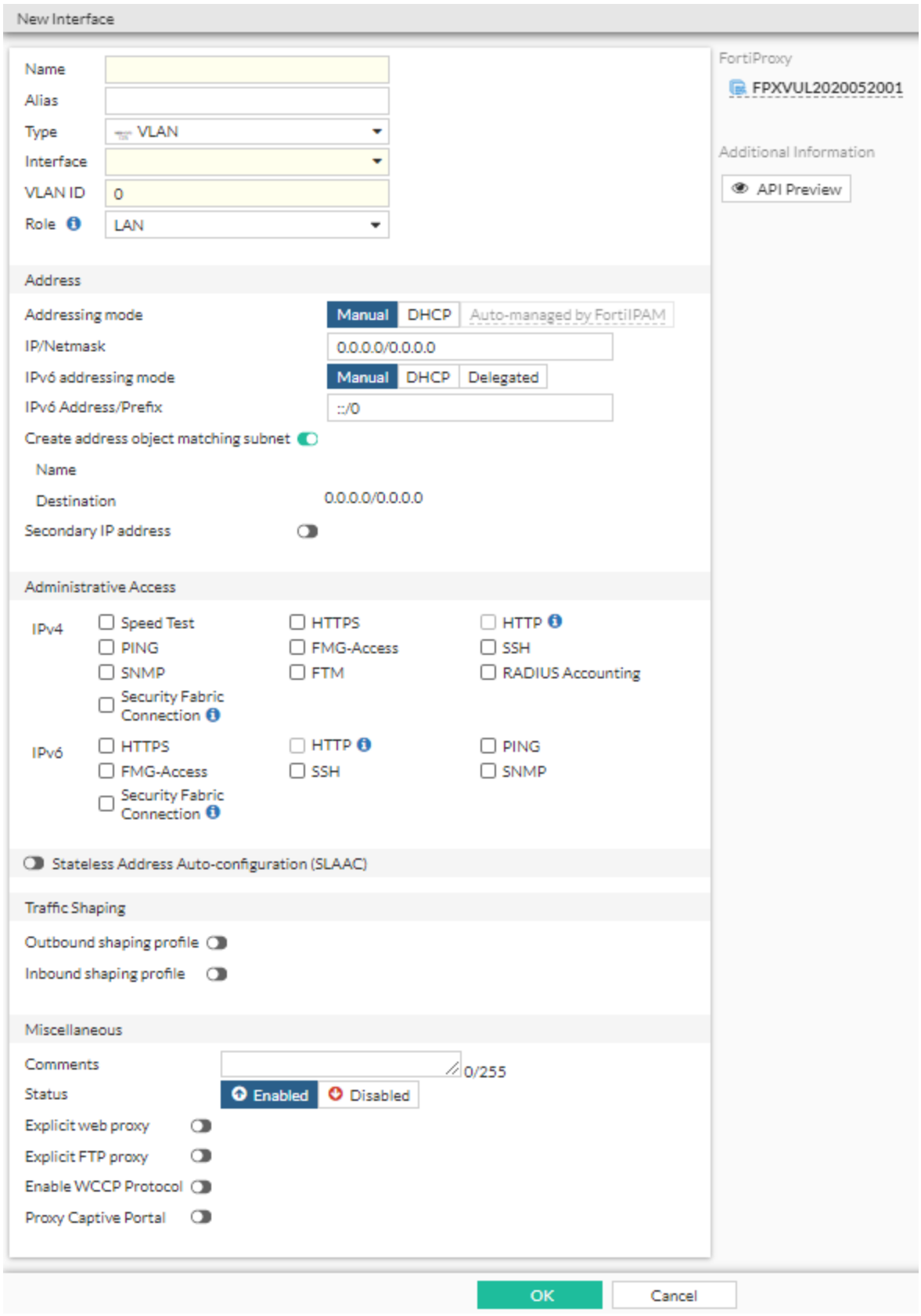
```
# execute ssh-options source 1.1.1.1
```

To confirm that the SSH packets are using the configured port and address:

```
# diagnose sniffer packet any "port 22" 4
6.898985 port1 out 1.1.1.1.20625 -> 15.15.15.2.22: syn 1704095779
6.899286 port1 in 15.15.15.2.22 -> 1.1.1.1.20625: syn 753358246 ack 1704095780
```

Create or edit an interface

Selecting *Create New* > *Interface* opens the *New Interface* page, which provides settings for configuring a new interface.


New Interface
Name
Alias
Type
VLAN
Interface
VLAN ID
0
Role
LAN
FortiProxy
FPXVUL2020052001
Additional Information
API Preview
Address
Addressing mode
Manual
DHCP
Auto-managed by FortiIPAM
IP/Netmask
0.0.0.0/0.0.0.0
IPv6 addressing mode
Manual
DHCP
Delegated
IPv6 Address/Prefix
::/0
Create address object matching subnet
Name
Destination
0.0.0.0/0.0.0.0
Secondary IP address
Administrative Access
IPv4
Speed Test
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric Connection
IPv6
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
Security Fabric Connection
Stateless Address Auto-configuration (SLAAC)
Traffic Shaping
Outbound shaping profile
Inbound shaping profile
Miscellaneous
Comments
0/255
Status
Enabled
Disabled
Explicit web proxy
Explicit FTP proxy
Enable WCCP Protocol
Proxy Captive Portal
OK
Cancel

Selecting an interface and then selecting *Edit* opens the *Edit Interface* page.

Configure the following settings in the *New Interface* page or *Edit Interface* page and click *OK*:

Name	Enter a name for the interface. Physical interface names cannot be changed. If VLAN pooling is enabled, the maximum name length is 10 characters. You cannot edit the interface name after you create the interface.
Alias	Enter an alternate name for a physical interface on the FortiProxy unit. The alias can be a maximum of 25 characters. The alias name does not appear in logs. This field appears when editing an existing physical interface.
Type	Select the type of the interface: *VLAN*, *802.3ad Aggregate*, or *Redundant Interface*. Refer to Aggregation on page 193 for more information about the Aggregate interface type.
Interface Members	Select the ports to be included in the interface if the *Type* is *802.3ad Aggregate* or *Redundant Interface*.
Interface	This field is available when *Type* is set to *VLAN*. Select the name of the physical interface that you want to add a VLAN interface to. After it is created, the VLAN interface is listed below its physical interface in the Interface list. You cannot change the physical interface of a VLAN interface.
VLAN ID	This field is available when *Type* is set to *VLAN*. Enter the VLAN ID. You cannot change the VLAN ID except when you add a new VLAN interface. The VLAN ID must be a number between 1 and 4094. It must match the VLAN ID that the IEEE 802.1Q-compliant router or switch that is connected to the VLAN subinterface adds.
Role	Set the role setting for the interface. Different settings will be shown or hidden when editing an interface depending on the role. • *LAN*: Used to connected to a local network of endpoints • *WAN*: Used to connected to the internet. • *DMZ*: Used to connected to the DMZ. When selected, DHCP server and Security mode are not available. • *Undefined*: The interface has no specific role.
Estimated bandwidth	The estimated WAN bandwidth. Enter the upstream and downstream bandwidth. These values are used to estimate WAN usage.
Addressing mode	Select the addressing mode for the interface: • Select *Manual* and add an IPv4 address and network mask for the interface. If IPv6 configuration is enabled, you can add both an IPv4 and an IPv6 IP address. • Select *DHCP* to get the interface IP address and other network settings from a DHCP server.

	• Select *Auto-managed by FortiIPAM* if you have FortiIPAM Cloud. The FortiIPAM (IP Address Management) service automatically assigns subnets to the FortiProxy unit to prevent duplicate IP addresses from overlapping within the same Security Fabric. FortiIPAM is a paid service and must be registered to the FortiProxy unit in FortiCare.
IP/Netmask	Enter an IPv4 address and subnet mask for the interface. FortiProxy interfaces cannot have IP addresses on the same subnet. This option is available only if *Addressing mode* is set to *Manual*.
Retrieve default gateway from server	Enable this to retrieve a default gateway IP address from the DHCP server. The default gateway is added to the static routing table. This option is available only if *Addressing mode* is set to *DHCP*.
Distance	Enter the administrative distance for the default gateway retrieved from the DHCP server. The administrative distance is an integer from 1 to 255, and specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. This option is available only if *Addressing mode* is set to *DHCP* and *Retrieve default gateway from server* is enabled.
Override internal DNS	Enable this to use the DNS addresses retrieved from the DHCP server instead of the DNS server IP addresses on the DNS page. This option is available only if *Addressing mode* is set to *DHCP*.
IPv6 Addressing mode	Select the addressing mode for the interface: • Select *Manual* and add an IP address and network mask for the interface. • Select *DHCP* to get the interface IP address and other network settings from a DHCP server. • Select *Delegated* to select an *IPv6 upstream interface* that has DHCPv6 prefix delegation enabled and enter an *IPv6 subnet* if needed. The interface will get the IPv6 prefix from the upstream DHCPv6 server that is connected to the IPv6 upstream interface and form the IPv6 address with the subnet configured on the interface.
IPv6 Address/Prefix	If *Addressing Mode* is set to *Manual* and IPv6 support is enabled, enter an IPv6 address and subnet mask for the interface. A single interface can have an IPv4 address, IPv6 address, or both.
Create address object matching subnet	This option is available when *Role* is set to *LAN* or *DMZ*. Enable this option to automatically create an address object that matches the interface subnet.
Secondary IP address	Add additional IPv4 addresses to this interface.

IPv6 Address/Prefix	If IPv6 support is enabled on the GUI, enter an IPv6 address and subnet mask for the interface. A single interface can have both an IPv4 and IPv6 address or just one or the other. This option is available only if *IPv6 Addressing mode* is set to *Manual*.
IPv4 IPv6	Select the types of administrative access permitted for IPv4 and IPv6 connections to this interface.
Speed Test	Allows speed tests to be executed on the interface.
HTTPS	Allow secure HTTPS connections to the GUI through this interface.
HTTP	HTTP traffic is automatically redirected to HTTPS.
PING	Interface responds to pings. Use this setting to verify your installation and for testing.
FMG-Access	Allow FortiManager to access this interface.
SSH	Allow SSH connections to the CLI through this interface.
SNMP	Allow a remote SNMP manager to request SNMP information by connecting to this interface.
FTM	Allow FTM Push notifications, for when users are attempting to authenticate through a VPN and/or RADIUS (with FortiAuthenticator as the RADIUS server).
RADIUS Accounting	Allow RADIUS accounting records that the server forwards (originating from the RADIUS client). These records include the user's IP address and user group.
Security Fabric Connection	Allow Security Fabric access. This access enables CAPWAP and FortiTelemetry.
Stateless Address Auto-configuration	Enable to provide IPv6 addresses to connected devices using SLAAC.
IPv6 prefix list	Enable to provide a list of IPv6 prefixes.
IPv6 prefix	Enter the IPv6 prefix.
Outbound shaping profile	Enable or disable traffic shaping on the interface. This allows you to enforce bandwidth limits on individual interfaces.
Outbound bandwidth	Enable to specify the outbound bandwidth.
Inbound shaping profile	Enable or disable traffic shaping on the interface. This allows you to enforce bandwidth limits on individual interfaces.
Inbound bandwidth	Enable to specify the inbound bandwidth.
Comments	Enter a description of the interface of up to 255 characters.
Status	Enable or disable the interface.
Explicit web proxy	Select this to enable explicit web proxying on this interface.

Explicit FTP proxy	Enable or disable explicit FTP proxying on this interface.
Enable WCCP Protocol	The Web Cache Communication Protocol (WCCP) can be used to provide web caching with load balancing and fault tolerance. In a WCCP configuration, a WCCP server receives HTTP requests from a user's web browsers and redirects the requests to one or more WCCP clients. The clients either return cached content or request new content from the destination web servers before caching it and returning it to the server, which in turn returns the content to the original requester. If a WCCP configuration includes multiple WCCP clients, the WCCP server load balances traffic among the clients and can detect when a client fails and failover sessions to still operating clients. WCCP is described by the Web Cache Communication Protocol Internet draft.
Proxy Captive Portal	Enable or disable proxy captive portal on this interface.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To add secondary IP addresses:

1. Go to *Network > Interfaces* and select *Create New > Interface*.
2. Enable *Secondary IP Address*.
3. Select *Create New*.
4. Enter the IPv4 address and network mask.
5. Select the types of administrative access to allow.
6. Click *OK*. The new IP address is added to the table.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Aggregation

Link aggregation (IEEE 802.3ad) enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link uses the total bandwidth of the functioning links in the group, up to eight. If a link in the group fails, traffic is transferred automatically to the remaining interfaces. The only noticeable effect is reduced bandwidth.

Only physical interfaces can be used in an aggregated (combined) link. You cannot aggregate VLAN interfaces, subinterfaces, or HA heartbeat interfaces. Each physical interface can belong to only one

aggregated interface. If VDOM is enabled, all interfaces in the aggregated interface must be in the same VDOM.

Interfaced included in an aggregate interface are not listed under *Network > Interfaces* and cannot be configured individually with an IP address, DHCP, or PPPoE. They also cannot not be referenced in security policies, VIPs, IP pools, routing, or multicast policies. While you can see such interfaces in the CLI, configurations for those interfaces do not take effect.

Example configuration

This example creates an aggregate interface on a FortiProxy using ports 3-5 with an internal IP address of 10.1.1.123, as well as the administrative access to HTTPS and SSH.

To create an aggregate interface in the GUI:

1. Go to *Network > Interfaces* and select *Create New > Interface*.
2. Set *Name* to *aggregate*.
3. Set *Type* to *802.3ad Aggregate*.
4. Set *Interface members* to *port4*, *port5*, and *port6*.
5. Set *Addressing mode* to *Manual*.
6. Set *IP/Netmask* to *10.1.1.123/24*.
7. For *Administrative Access*, select *HTTPS* and *SSH*.
8. Click *OK*.

See Create or edit an interface on page 188 for more information.

To create an aggregate interface in the CLI:

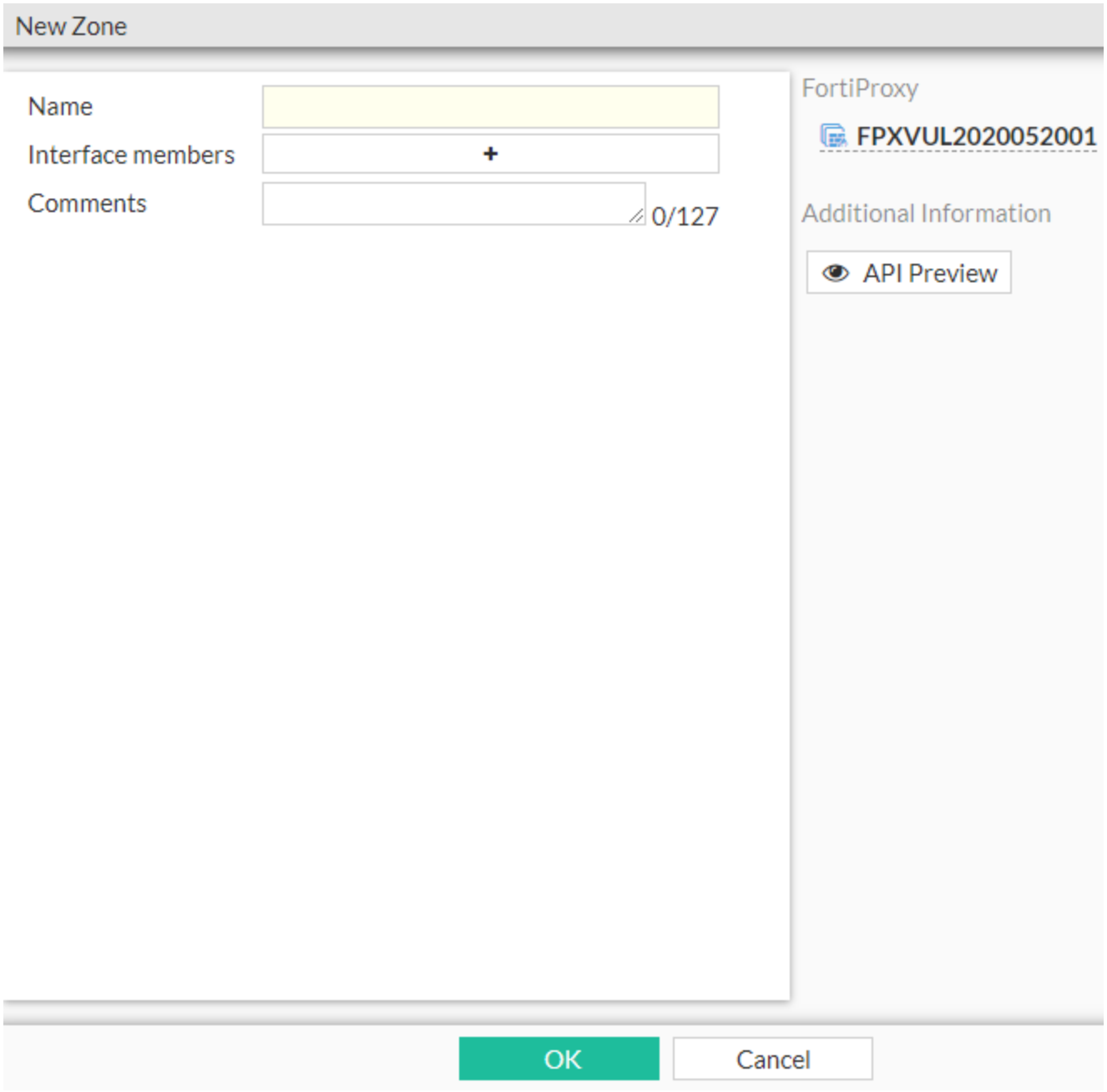
```
config system interface
    edit "aggregate"
        set vdom "root"
        set ip 10.1.1.123 255.255.255.0
        set allowaccess https ssh
        set type aggregate
        set member "port4" "port5" "port6"
        set snmp-index 45
    next
end
```

See `config system interface` for more information.

Create or edit a zone

Zones are a group of one or more physical or virtual FortiProxy interfaces that you can apply security policies to control inbound and outbound traffic. Grouping interfaces into zones simplifies the creation of security policies where a number of network segments can use the same policy settings and protection profiles. Interfaces that are included in a zone must not be assigned to another zone or have firewall policies defined.

Selecting *Create New* > *Zone* opens the *New Zone* page, which provides settings for configuring a new zone.



Selecting a zone and then selecting *Edit* opens the Edit Zone page.

Configure the following settings in the New Zone page or Edit Zone page and click *OK*:

Name	Enter a name for the zone. You can change the name of the zone after creating it.
Interface Members	Select the ports to be included in the zone.

Comments	Enter a description up to 255 characters to describe the zone.
API Preview	Select the ports to be included in the zone.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

To create a zone:

```
config system zone
   edit <zone_name>
      set description <string>
      set interface <interface_names>
   next
end
```

Verification

When a client visits a HTTP website, the client will be redirected to the captive portal for authentication by HTTPS. For example, the client could be redirected to a URL by a HTTP 303 message similar to the following:

HTTP/1.1 303 See Other

Connection: close

Content-Type: text/html

Cache-Control: no-cache

Location: https://fpx.fortinetqa.local:7831/XX/YY/ZZ/cpauth?scheme=http&4Tmthd=0&host=172.16.200.46&port=80&rule=75&uri=Lw==&

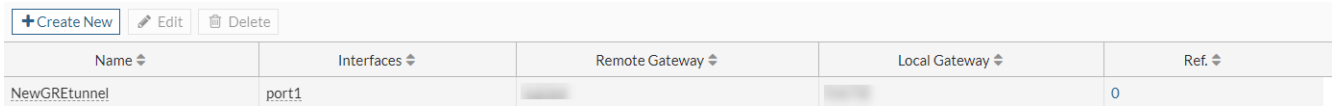
Content-Length: 0

The captive portal URL used for authentication is *https://fpx.fortinetqa.local:7831/...*. After the authentication is complete with all user credentials protected by HTTPS, the client is redirected to the original HTTP website it intended to visit.

GRE Tunnel

The Generic Routing Encapsulation (GRE) tunnel allows direct communication between two nodes on a network.

Go to *Network* > *GRE Tunnel* to see which GRE tunnels have been configured.



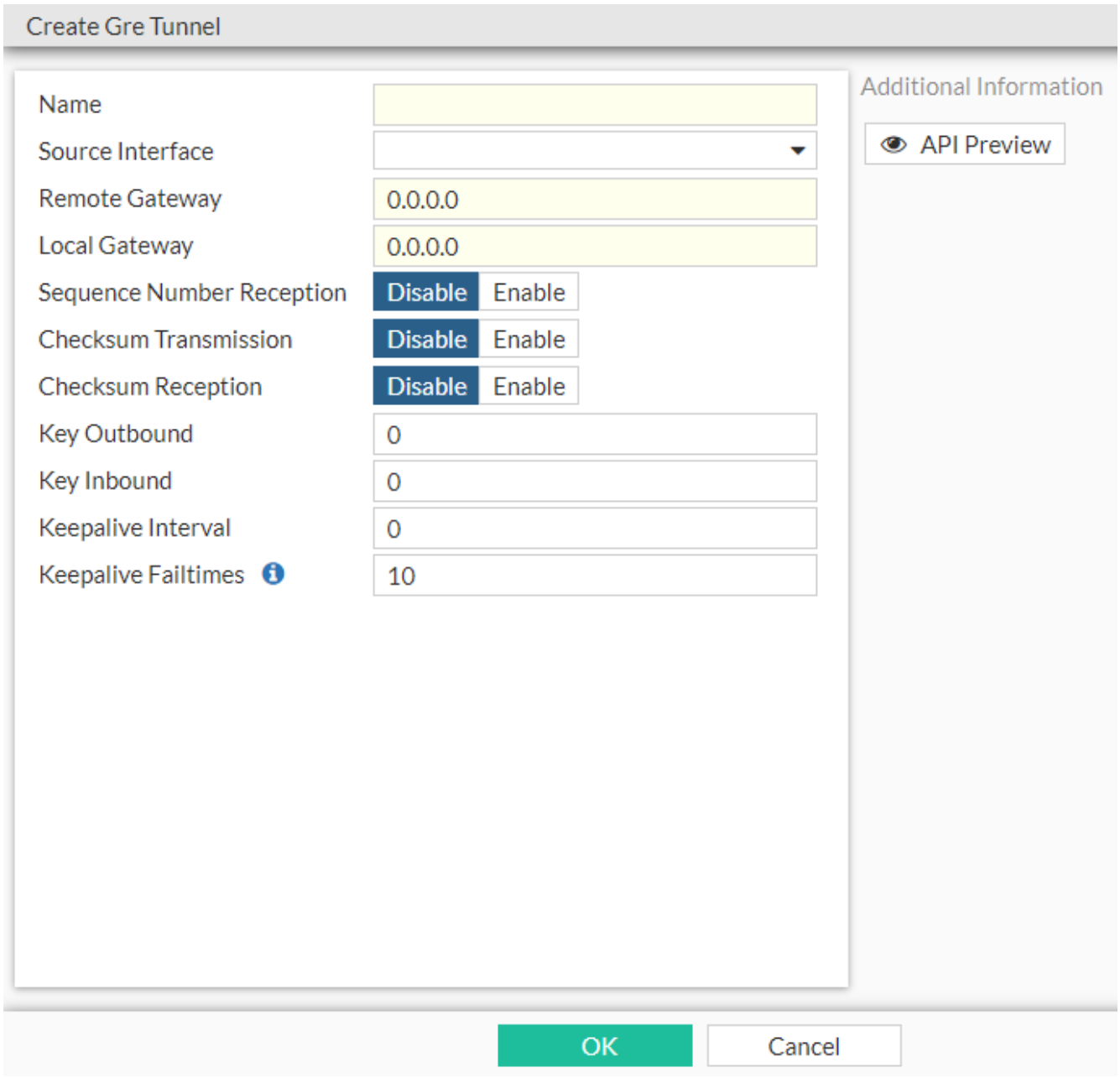
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Select to create a GRE tunnel. See Create or edit a GRE tunnel on page 197.
Edit	Modifies settings for the selected GRE tunnel. When you click *Edit*, the Edit GRE Tunnel page opens.
Delete	Removes the selected GRE tunnel.
Name	The name of the GRE tunnel.
Interfaces	Name of the source interface.
Remote Gateway	IP address of the remote gateway.
Local Gateway	IP address of the local gateway.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a GRE tunnel

Select *Create New* to open the *Create Gre Tunnel* page.



Select a GRE tunnel and then click *Edit* to open the *Edit Gre Tunnel* page.

Configure the following settings in the *Create Gre Tunnel* page or *Edit Gre Tunnel* page and then click *OK*:

Name	Enter the name to identify the GRE tunnel. You cannot edit the name after you create the GRE tunnel.
Source Interface	Name of the source interface. There is no default value.
Remote Gateway	IP address of the remote gateway. The default is 0.0.0.0.

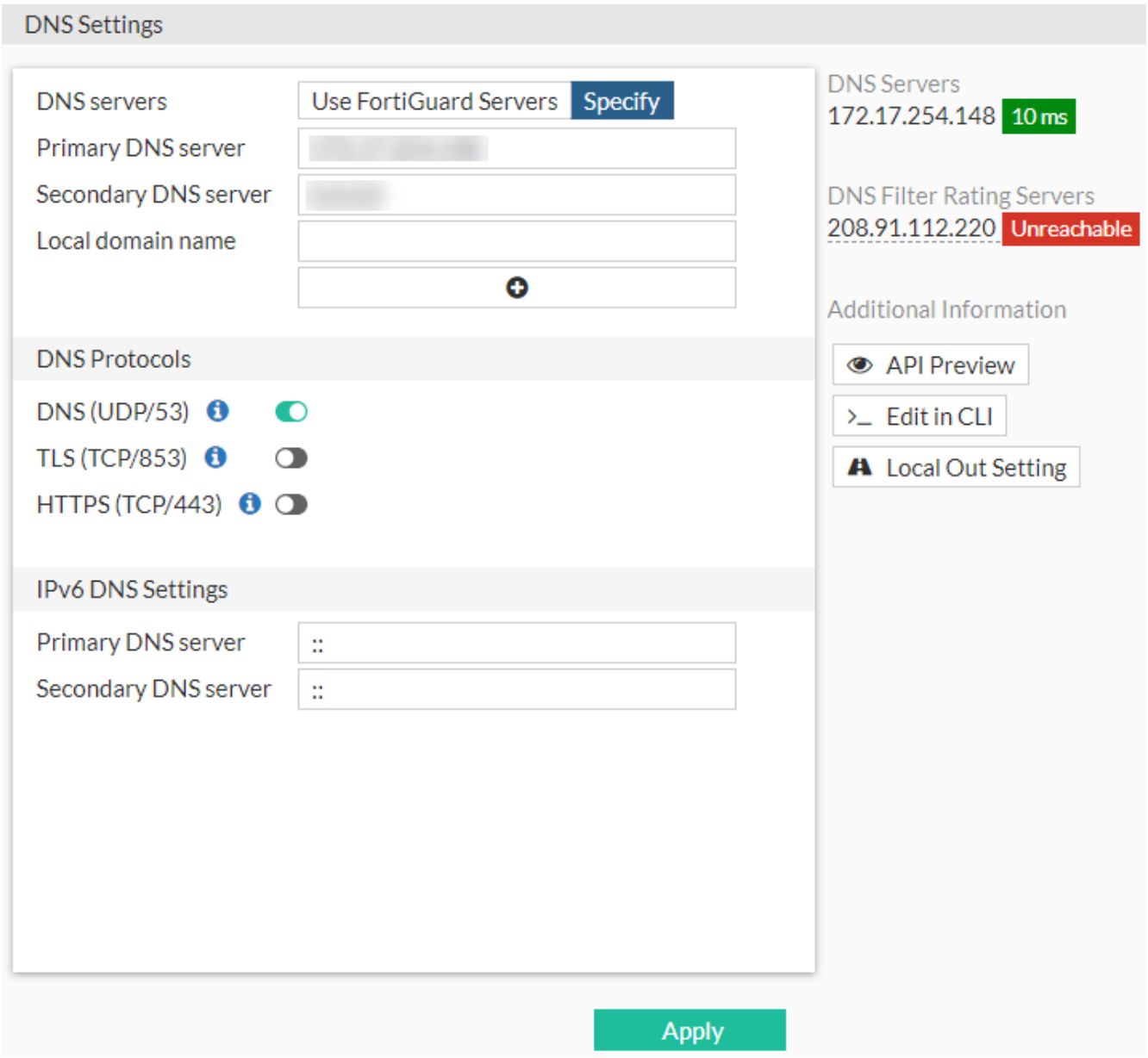
Local Gateway	IP address of the local gateway. The default is 0.0.0.0.
Sequence Number Reception	Enable or disable whether sequence numbers are validated in the received GRE packets. The default is disable.
Checksum Transmission	Enable or disable whether checksums are included in transmitted GRE packets. The default is disable.
Checksum Reception	Enable or disable whether checksums are validated in received GRE packets. The default is disable.
Key Outbound	Enter the key to be included in transmitted GRE packets. The range is 0 to 4,294,967,295. The default is 0.
Key Inbound	Enter the key that is required to be in received GRE packets. The range is 0 to 4,294,967,295. The default is 0.
Keepalive Interval	Specify how many minutes pass before a GRE keep-alive message is sent. The range is 0 to 32,767. Enter 0 to disable this feature. The default is 0.
Keepalive Failtimes	How many times the GRE keep-alive message fails before the GRE connection is considered down. The range is 1-255. The default is 10.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

DNS Settings

Several FortiProxy functions use DNS, including alert email. You can specify the IP addresses of the DNS servers that your unit connects to. DNS server IP addresses are usually supplied by your ISP. To configure DNS settings, go to *Network > DNS Settings*.



Configure the following settings and select *Apply*:

DNS Servers	Select *Use FortiGuard Servers* or *Specify*. If you select *Specify*, enter the IP addresses for the primary and secondary DNS servers. See also Use DNS over TLS for default FortiGuard DNS servers on page 205.
Primary DNS Server	Enter the IPv4 or IPv6 address for the primary DNS server.
Secondary DNS Server	Enter the IPv4 or IPv6 address for the secondary DNS server.
Local Domain Name	Enter the domain name to append to addresses with no domain portion when performing DNS lookups.

DNS (UDP/53)	Enable or disable the use of clear-text DNS over port 53.
TLS (TCP/853)	Enable or disable the use of DNS over TLS (DoT).
HTTPS (TCP/443)	Enable or disable the use of DNS over HTTPS (DoH).
SSL certificate	Select which SSL certificate or click *Create* to import a certificate.
Server hostname	Enter the host name of the DNS server.

To enable DoT and DoH DNS in the CLI:

```
config system dns
   set primary <IP_address>
   set secondary <IP_address>
   set protocol {cleartext | dot | doh}
end
```

Important DNS CLI commands

DNS settings can be configured with the following CLI command:

```
config system dns
    set primary <ip_address>
    set secondary <ip_address>
    set protocol {cleartext dot doh}
    set ssl-certificate <string>
    set server-hostname <hostname>
    set domain <domains>
    set ip6-primary <ip6_address>
    set ip6-secondary <ip6_address>
    set timeout <integer>
    set retry <integer>
    set dns-cache-limit <integer>
    set dns-cache-ttl <integer>
    set cache-notfound-responses {enable | disable}
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
    set source-ip <class_ip>
    set server-select-method {least-rtt | failover}
    set alt-primary <ip_address>
    set alt-secondary <ip_address>
    set log {disable |error | all}
    set fqdn-cache-ttl <integer>
    set fqdn-min-refresh <integer>
    set fqdn-max-refresh <integer>
end
```

For a FortiProxy with multiple logical CPUs, you can set the DNS process number from 1 to the number of logical CPUs. The default DNS process number is 1.

```
config system global
    set dnsproxy-worker-count <integer>
end
```

DNS protocols

The following DNS protocols can be enabled:

- `cleartext`: Enable clear text DNS over port 53 (default).
- `dot`: Enable DNS over TLS.
- `doh`: Enable DNS over HTTPS.

cache-notfound-responses

When enabled, any DNS requests that are returned with `NOT FOUND` can be stored in the cache. The DNS server is not asked to resolve the host name for `NOT FOUND` entries. By default, this option is disabled.

dns-cache-limit

Set the number of DNS entries that are stored in the cache (0 to 4294967295, default = 5000). Entries that remain in the cache provide a quicker response to requests than going out to the Internet to get the same information.

dns-cache-ttl

The duration that the DNS cache retains information, in seconds (60 to 86400 (1 day), default = 1800).

fqdn-cache-ttl

FQDN cache time to live (TTL), in seconds (0 - 86400, default = 0).

This is the amount of time an FQDN's address record can live if not refreshed. This setting applies globally, across all VDOMs, to FQDNs that have unspecified firewall address `cache-ttl` settings. If the `cache-ttl` value is configured for an FQDN address, it will supersede the `fqdn-cache-ttl` setting for that address.

For example, configure the FQDN cache TTL on the global VDOM:

```
config system dns
    set fqdn-cache-ttl 2000
end
```

```
# diagnose test application dnsproxy 6
```

```
...
vfid=0 name=test.bb.com ver=IPv4 wait_list=0 timer=985 min_ttl=1000 cache_ttl=2000 slot=-1 num=1
wildcard=0
         1.1.1.1 (ttl=1000:991:1991)
vfid=0 name=*.google.com ver=IPv4 wait_list=0 timer=0 min_ttl=0 cache_ttl=2000 slot=-1 num=0
wildcard=
...
```

Change the cache TTL in a VDOM for a specific address:

```
config firewall address
    edit "test.bb.com"
        set cache-ttl 1000
    next
end
```

```
# sudo global diagnose test application dnsproxy 6
...
vfid=0 name=test.bb.com ver=IPv4 wait_list=0 timer=864 min_ttl=1000 cache_ttl=1000 slot=-1 num=1
wildcard=0
1.1.1.1 (ttl=1000:870:1870)
vfid=0 name=*.google.com ver=IPv4 wait_list=0 timer=0 min_ttl=0 cache_ttl=2000 slot=-1 num=0
wildcard=1
...
```

fqdn-min-refresh

FQDN cache minimum refresh time, in seconds (10 - 3600, default = 60).

An FQDN normally requeries for updates according to the lowest TTL interval returned from all the DNS records in a DNS response. The FortiProxy has a default minimum refresh interval of 60 seconds; if a TTL interval is shorter than 60 seconds, it still requires a minimum of 60 seconds for the FortiProxy to requery for new addresses. The `fqdn-min-refresh` setting changes the interval. The settings could be shortened if there are FQDNs that require fast resolutions based on a short TTL interval.

For example, if `fqdn_min_refresh` is unspecified:

```
# diagnose test application dnsproxy 3
worker idx: 0
...
FQDN: min_refresh=60 max_refresh=3600
...
```

```
# diagnose test application dnsproxy 6
worker idx: 0
vfid=0 name=aa.com ver=IPv4 wait_list=0 timer=28 min_ttl=20 cache_ttl=0 slot=-1 num=1 wildcard=0
         23.202.195.114 (ttl=20:0:0)
```

The `min_refresh` is the default value of 60 seconds. Although the `min_ttl` (TTL returned) value is shorter, the FortiProxy only requeries for updates based on the `min_refresh` value. the `timer` value is

the countdown until the next refresh is triggered. The FortiProxy triggers a refresh slightly earlier than the larger of the `min_refresh` or `min_ttl` value.

If `fqdn_min_refresh` is configured:

```
config system dns
    set fqdn-min-refresh 20
end
```

```
# diagnose test application dnsproxy 3
worker idx: 0
...
FQDN: min_refresh=20 max_refresh=3600
...
```

```
# diagnose test application dnsproxy 6
worker idx: 0
vfid=0 name=aa.com ver=IPv4 wait_list=0 timer=8 min_ttl=20 cache_ttl=0 slot=-1 num=1 wildcard=0
         23.202.195.114 (ttl=20:14:14)
```

This setting can be used in combination with `fqdn-cache-ttl` and `cache-ttl` to send more frequent queries and store more resolved addresses in cache. This is useful in scenarios where the FQDN has many resolutions and changes very frequently.

fqdn-max-refresh

FQDN cache maximum refresh time, in seconds (3600 - 86400, default = 3600).

The `fqdn-max-refresh` setting is used to control the global upper limit of the FQDN refresh timer. FQDN entries with a TTL interval that is longer than the `fqdn-max-refresh` value will have their refresh timer reduced to this upper limit. This allows the FortiProxy to dictate the upper limit in querying for DNS updates for its FQDN addresses.

VDOM DNS

When the FortiProxy is in multi-vdom mode, DNS is handled by the management VDOM. However in some cases, administrators may want to configure custom DNS settings on a non-management VDOM. For example, in a multi-tenant scenario, each VDOM might be occupied by a different tenant, and each tenant might require its own DNS server. For more information on VDOM DNS, see Interfaces in non-management VDOMs as the source IP address of the DNS conditional forwarding server on page 216.

To configure a custom VDOM within a non-management VDOM:

```
config vdom
edit <vdom>
config system vdom-dns
    set vdom-dns enable
```

```
    set primary <primary_DNS>
    set secondary <secondary_DNS>
    set protocol {cleartext dot doh}
    set ip6-primary <primary_IPv6_DNS>
    set ip6-secondary <secondary_IPv6_DNS>
    set source-ip <IP_address>
    set interface-select-method {auto | sdwan | specify}
end
```

Using the FortiProxy unit as an IPv6 DDNS client for generic DDNS

When configuring the generic DDNS service provider as a DDNS server, the server type and address type can be set to IPv6. This allows the FortiProxy unit to connect to an IPv6 DDNS server and provide the FortiProxy unit's IPv6 interface address for updates.

```
config system ddns
    edit <ID>
        set ddns-server genericDDNS
        set server-type {ipv4 | ipv6}
        set ddns-server-addr <address>
        set addr-type {ipv4 | ipv6}
        set monitor-interface <port>
    next
end
```

To configure an IPv6 DDNS client with generic DDNS:

```
config system ddns
    edit 1
        set ddns-server genericDDNS
        set server-type ipv6
        set ddns-server-addr "2004:16:16:16::2" "16.16.16.2" "ddns.genericddns.com"
        set ddns-domain "test.com"
        set addr-type ipv6
        set monitor-interface "port3"
    next
end
```

Use DNS over TLS for default FortiGuard DNS servers

When using FortiGuard servers for DNS, the FortiProxy unit defaults to using DNS over TLS (DoT) to secure the DNS traffic. New FortiGuard DNS servers are added as primary and secondary servers.



Because DNS servers probably do not support low encryption DES, low encryption devices do not have the option to select DoT or DoH. The devices default to cleartext (UDP/53) instead.

The FortiGuard DNS server certificates are signed with the globalsdns.fortinet.net hostname by a public CA. The FortiProxy unit verifies the server hostname using the `server-hostname` setting.

To view the FortiGuard server DNS settings in the GUI:

1. Go to *Network > DNS Settings*.
2. For *DNS servers*, select *Use FortiGuard Servers*.
   The *Primary DNS server* is *96.45.45.45*, and the *Secondary DNS server* is *96.45.46.46*. *DNS Protocols* is set to *TLS* and cannot be modified.

To view the FortiGuard server DNS settings in the CLI:

```
# show system dns
config system dns
    set primary 96.45.45.45
    set secondary 96.45.46.46
    set protocol dot
    set server-hostname "globalsdns.fortinet.net"
end
```



The `protocol` and `server-hostname` settings should not be modified when using the default FortiGuard servers.

Alternate DNS servers

The alternate DNS servers are used only when DNS resolution of the primary or secondary DNS servers return a name error (NXDOMAIN). They are not used as failover DNS servers. If the query in the primary list times out, no alternate DNS server is contacted.

To configure the alternate DNS servers:

```
config system dns
    set alt-primary <ip_address>
    set alt-secondary <ip_address>
end
```

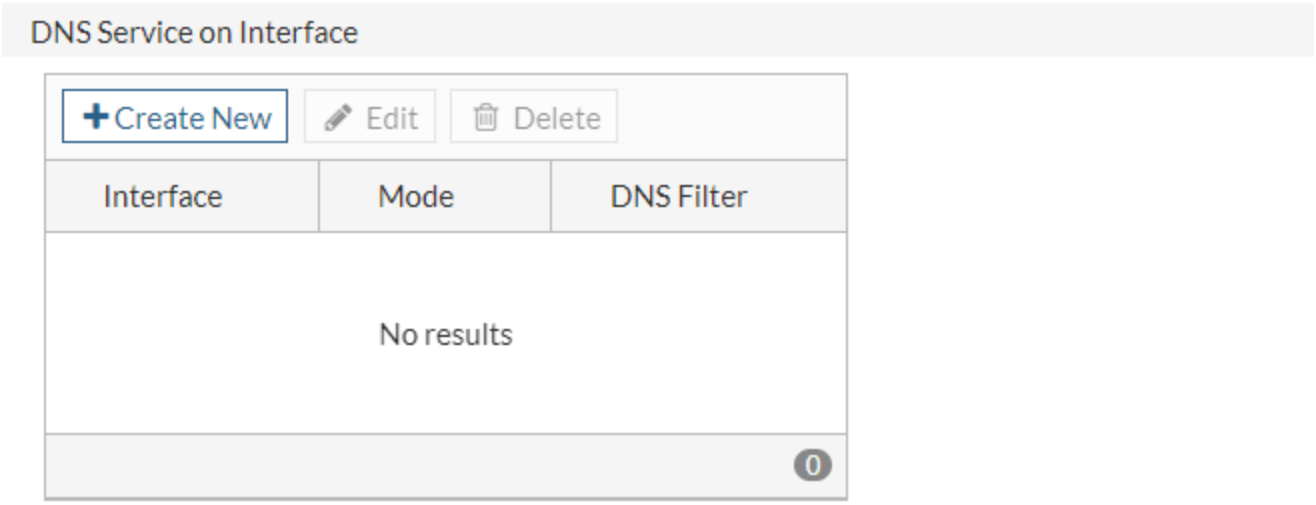
`alt-primary <ip_address>`	Alternate primary DNS server. This is not used as a failover DNS server.
`alt-secondary <ip_address>`	Alternate secondary DNS server. This is not used as a failover DNS server.

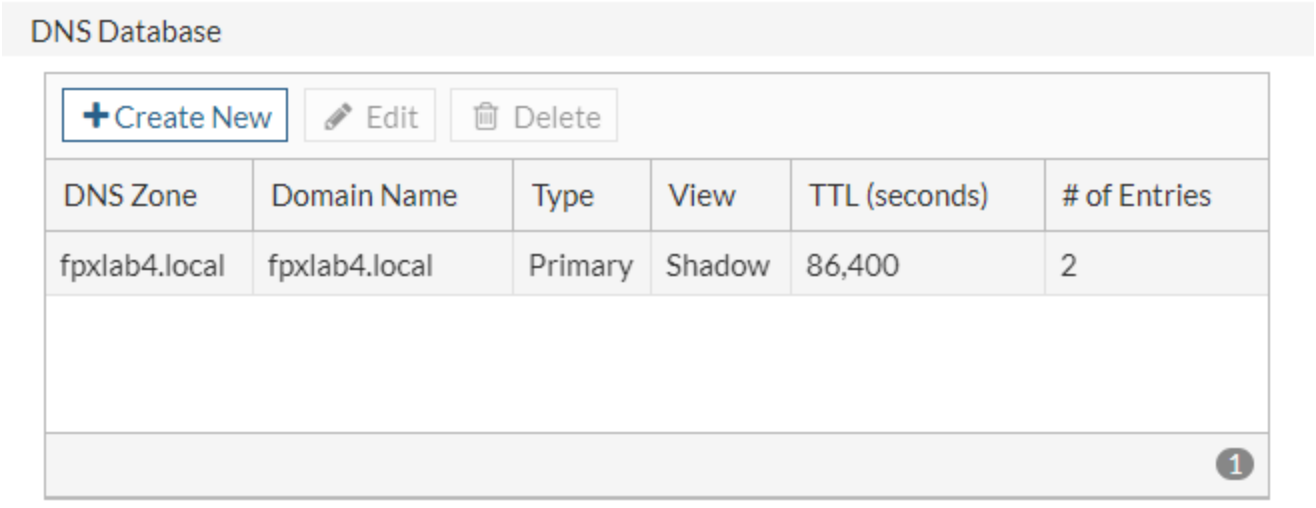
DNS Service

You can create local DNS servers for your network. Depending on your requirements, you can manually maintain your entries (primary DNS server) or use it as a jumping point, where the server refers to an outside source (secondary DNS server). A local primary DNS server works similarly to the DNS server addresses configured in *Network > DNS Settings*, but you must manually add all entries. This allows you to add a local DNS server to include specific URL and IP address combinations.

You can set an option to ensure this type of DNS server is not the authoritative server. When configured as a recursive DNS, the FortiProxy unit will check its internal DNS server (primary or secondary). If the request cannot be fulfilled, it will look to the external DNS servers. This is known as a split DNS configuration.

To configure DNS servers and zones, go to *Network > DNS Service*.





Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

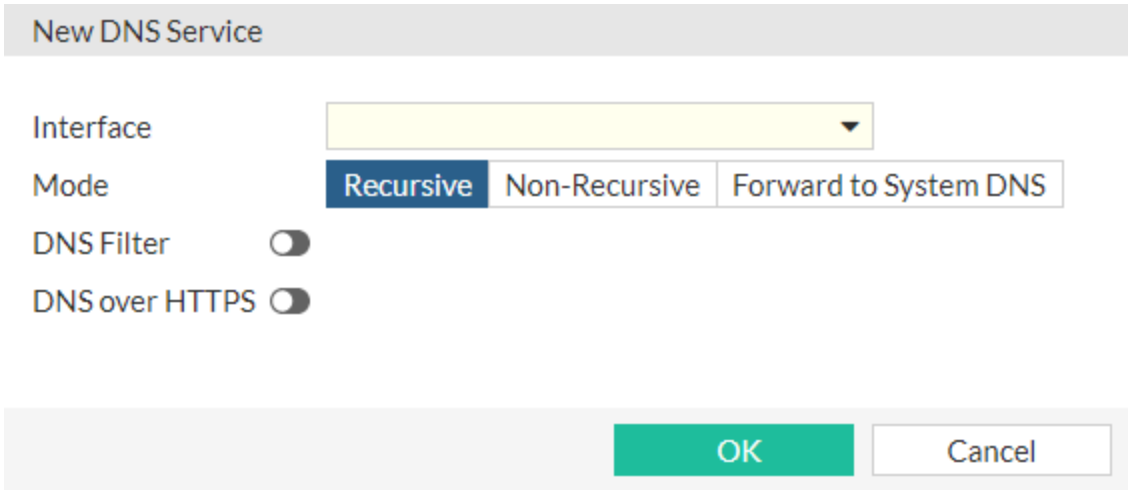
From the *DNS Service* page, you can do the following:

- Create or edit a DNS service on page 208
- Create or edit a DNS zone on page 209

Create or edit a DNS service

To add a DNS service on a specific interface:

1. Go to *Network* > *DNS Service* and, under *DNS Service on Interface*, select *Create New*.



2. Select an interface.
3. Select *Recursive*, *Non-Recursive*, or *Forward to System DNS*.
4. Enable *DNS Filter* if you want to use a DNS filter and select the DNS filter to use.
5. Enable *DNS over HTTPS* if you want to use DNS over HTTPS.
6. Click *OK*. The new DNS service is added to the table.

To edit a DNS service:

1. Go to *Network* > *DNS Service* and, under *DNS Service on Interface*, select a DNS service.
2. Select *Edit*.
3. Make your changes.
4. Click *OK*.

To enable DNS over HTTPS (DoH) on the DNS server in the CLI:

```
config system dns-server
   edit {<DNS_server_name> | <interface_name>}
      set dnsfilter-profile {<profile_name> | default}
      set doh enable
   next
```

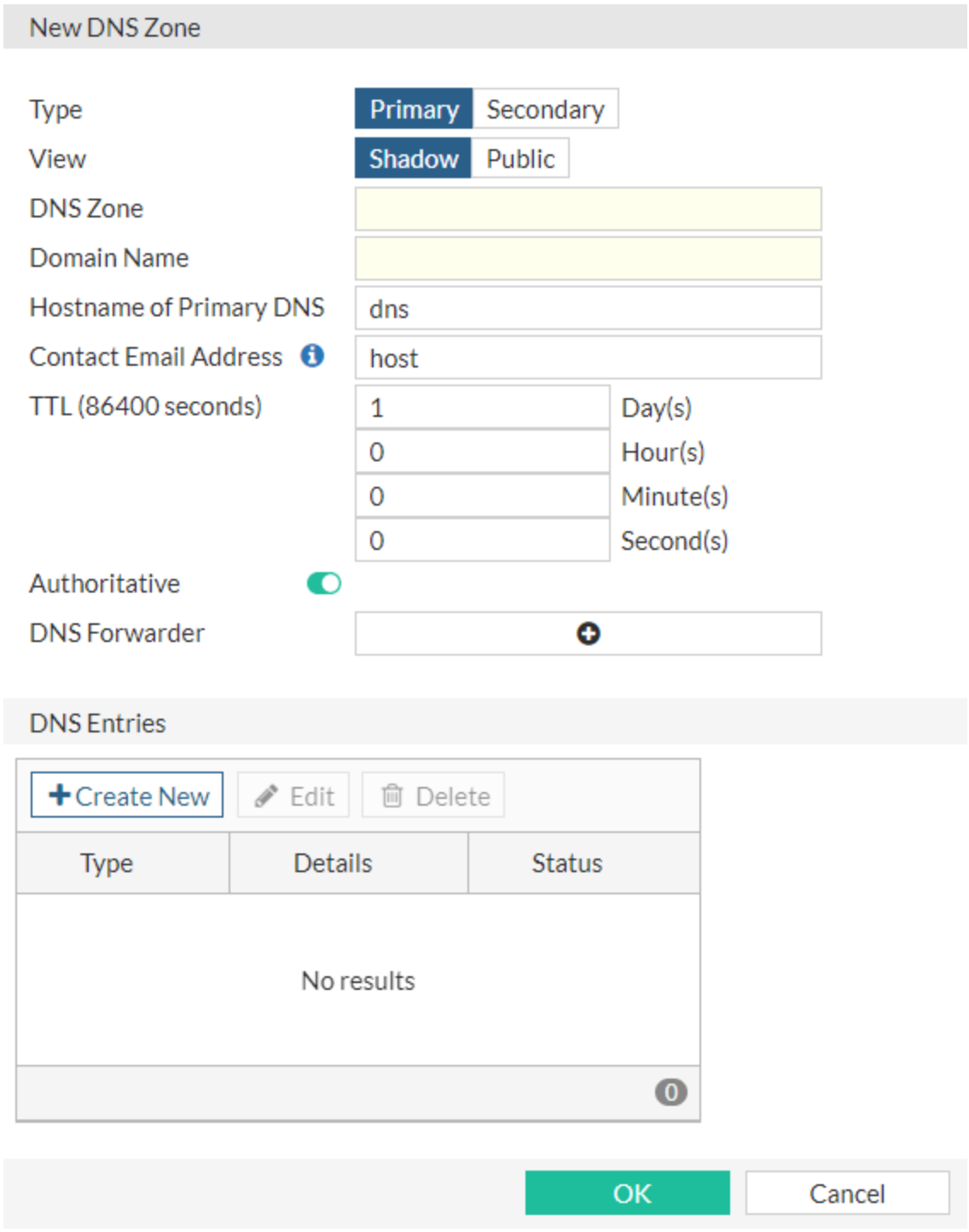
```
end
```

Create or edit a DNS zone

You can create a primary or secondary DNS zone.

To create a primary DNS zone:

1. Go to *Network* > *DNS Service* and, under *DNS Database*, select *Create New*.



2. Select *Primary* for the type of DNS zone.
3. Select the accessibility of the DNS server. If you select *Public*, external users can use the DNS server. If you select *Shadow*, only internal users can use it.
4. Enter a name for the DNS zone.

5. Enter the domain name.
6. Enter the host name of the primary DNS server.
7. Enter the contact email address for the administrator, for example, `admin@example.com`.
8. Enter how long the DNS zone should exist in days, hours, minutes, and seconds. The maximum time to live (TTL) is 86,400 seconds.
9. Enable *Authoritative* if you want an authoritative zone.
10. Enter the IP address for the DNS zone forwarder.
11. Select or create a DNS entry. See Create or edit a DNS entry on page 211.
12. Click *OK* to save your new DNS zone. The new DNS zone is added to the table.

To create a secondary DNS zone:

1. Go to *Network* > *DNS Service* and, under *DNS Database*, select *Create New*.
2. Select *Secondary* for the type of DNS zone.
3. Select the accessibility of the DNS server. If you select *Public*, external users can use the DNS server. If you select *Shadow*, only internal users can use it.
4. Enter a name for the DNS zone.
5. Enter the domain name.
6. Enter the IP address of the primary DNS zone.
7. Enable *Authoritative* if you want an authoritative zone.
8. Enter the IP address for the DNS zone forwarder.
9. Click *OK* to save your new DNS zone. The new DNS zone is added to the table.

To edit a DNS zone:

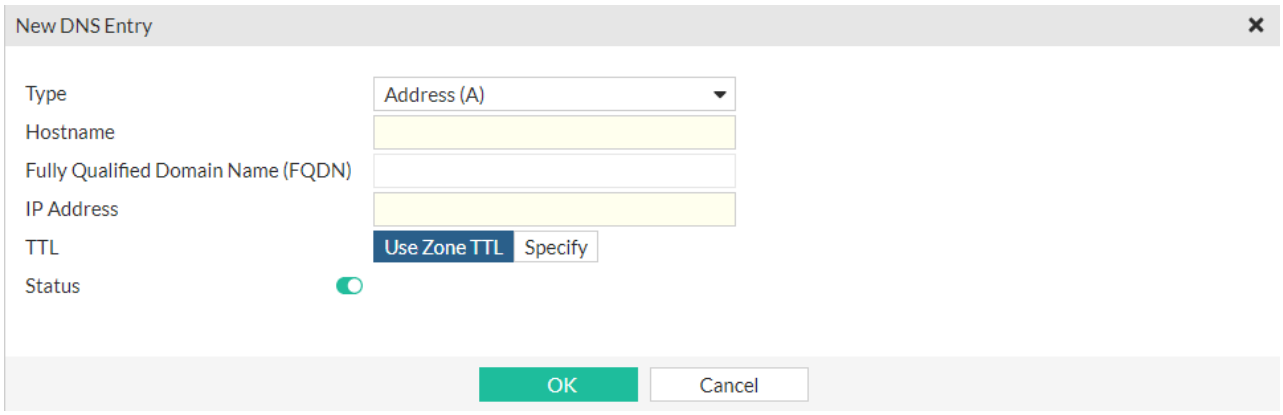
1. Go to *Network* > *DNS Service* and, under *DNS Database*, select a DNS zone.
2. Select *Edit*.
3. Make your changes.
4. Click *OK* to save your changes.

Create or edit a DNS entry

You can create or edit a DNS entry for the DNS service.

To create a DNS entry:

1. Go to *Network* > *DNS Service* and, under *DNS Database*, select a DNS zone and then click *Edit*.
2. In the *Edit DNS Zone* page, select *Create New*.



3. Select the type of DNS entry, one of *Address (A)*, *Name Server (NS)*, *Canonical Name (CNAME)*, *Mail Exchange (MX)*, *IPv6 Address (AAAA)*, *IPv4 Pointer (PTR)*, or *IPv6 Pointer (PTR)*.
4. Enter the host name for the DNS entry.
5. Enter the fully qualified domain name for the DNS entry.
6. Enter the IP address for the DNS entry.
7. For the time to live (TTL), select *Use Zone TTL* or *Specify*. If you select *Specify*, enter the number of days, hours, minutes, and seconds, up to a maximum of 86,400 seconds.
8. Enable or disable *Status* to make the DNS entry active or inactive.
9. Click *OK* to save your new DNS entry. The new DNS entry is added to the table.
10. Click *OK* to save your changes to the DNS zone.

To edit a DNS entry:

1. Go to *Network* > *DNS Service* and, under *DNS Database*, select a DNS zone and then click *Edit*.
2. Select a DNS entry and then click *Edit*.
3. In the *Edit DNS Entry* page, make your changes.
4. Click *OK* to save your changes to the DNS entry.
5. Click *OK* to save your changes to the DNS zone.

Transparent conditional DNS forwarder

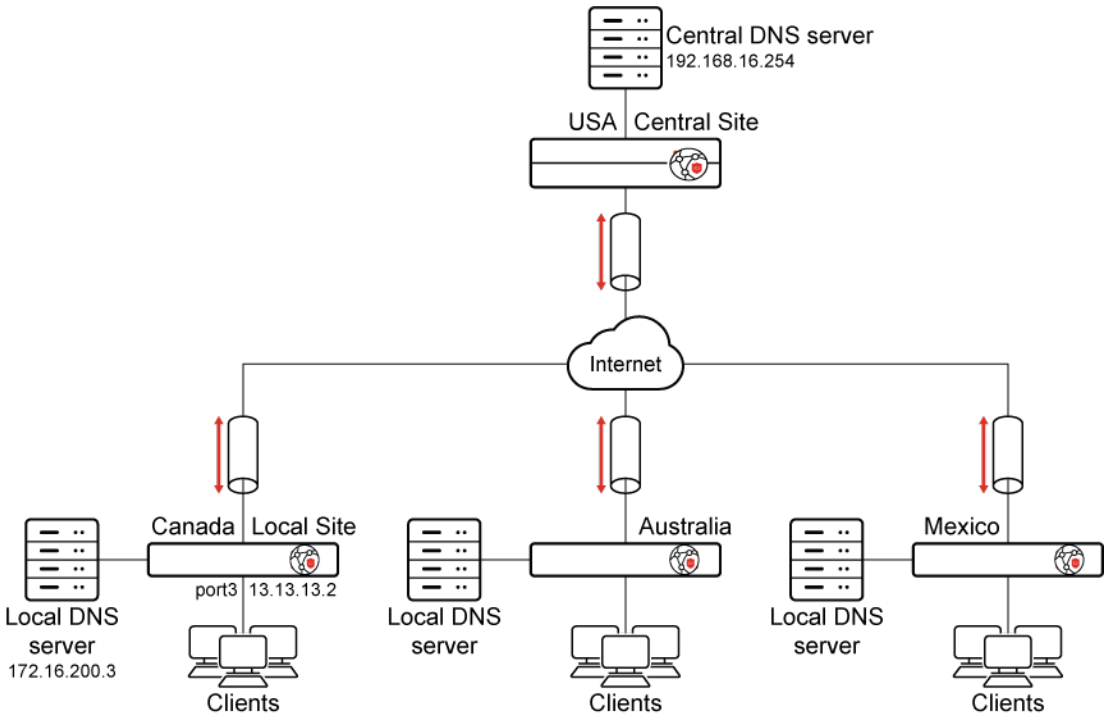
The transparent conditional DNS forwarder allows the FortiProxy to intercept and reroute DNS queries for specific domains to a specific DNS server. For example, when a client's DNS is located in a distant location, in order to resolve destination addresses (such as SaaS applications) to the closest application server, the FortiProxy can intercept and reroute the requests to a local DNS to resolve.

This is done by parsing entries and creating a list of filters based on the domain names of zones. When a DNS request matches one of these filters, the DNS proxy will retrieve the zone's data. The DNS request will then be handled based on the zone's forwarder settings and whether a local answer is available. It may be forwarded to the original destination address, the forwarder address, or not forwarded at all if a local answer is available.

This provides greater control over DNS requests, especially when the administrator is not managing the DNS server configuration of the client devices. This can improve network efficiency and performance by resolving IPs local to the client's PCs rather than IPs local to the central DNS server.

Example

In this example, FortiProxies at various locations are connected to a central site by VPN tunnels where the corporate DNS server is located. Typically, DNS queries from different sites are sent to the central DNS server and resolved to an IP local to the central site, which might cause latency and performance issues for certain destinations, such as SaaS applications.



The Local Site FortiProxy is configured with the Microsoft domain and a local DNS entry. Traffic matching the Microsoft domain is either forwarded to the local DNS server or resolved by the FortiProxy, which resolves it to an IP local to the Local Site, thus improving performance.

This example assumes the following have been configured:

- A successfully operational site-to-site VPN between the Local Site and the Central Site FortiProxies.
- Appropriate routing and network interfaces.
- The client PCs are configured to use the Central DNS Server.

By default, DNS server options are not available in the GUI.

To enable DNS server options in the GUI:

1. Go to *System* > *Feature Visibility*.
2. In the *Additional Features* section, enable *DNS Database*.
3. Click *Apply*.

To configure the DNS zone and local DNS entries on the Local Site FortiProxy in the GUI:

1. Go to *Network > DNS Service*.
2. In the *DNS Database* table, click *Create New*.
3. Enter a *DNS Zone* name (*SaaS_applications*).
4. Enter a *Domain Name* (*microsoft.com*).
5. Disable the *Authoritative* setting.
6. In the *DNS Forwarder* field, click the *+* and enter the DNS Forwarder address (*172.16.200.3*).
7. Configure the DNS entry:
   a. In the *DNS Entries* table, click *Create New*.
   b. Set the *Type* to *Address (A)*.
   c. Enter a *Hostname* (*office*).
   d. Configure the remaining settings as needed. The options vary depending on the selected *Type*.
   e. Click *OK*.
   f. Optionally, add more DNS entries if needed.
8. In the CLI, configure the source IP:

```
config system dns-database
                                        edit "SaaS_applications"
                                        set source-ip 13.13.13.2
                                        next
                                end
```



If the DNS server is accessed over a VPN, it may be necessary to specify a source IP for the FortiProxy to reach the DNS server.

Site-to-site VPN is not a mandatory requirement for this feature to work and is only applicable to this example.

To configure the DNS zone and local DNS entries on the Local Site FortiProxy in the CLI:

```
config system dns-database
                        edit "SaaS_applications"
                        set domain "microsoft.com"
                        set authoritative disable
                        set forwarder "172.16.200.3"
                        set source-ip 13.13.13.2
                        config dns-entry
                        edit 1
                        set hostname "office"
                        set ip 172.16.200.55
                        next
                        end
                        next
                        end
```

To add the DNS database to a DNS filter profile:

```
config dnsfilter profile
                        edit "SaaS"
                        set transparent-dns-database "SaaS_applications"
                        next
                        end
```



Multiple DNS databases can be selected for `transparent-dns-database`.

After selecting a DNS database, users are not permitted to modify the domain name of the zone. Before making any changes to the domain name, remove the reference from the `dnsfilter profile`.

To apply the DNS filter profile in a firewall policy in the GUI:

1. Go to *Policy & Objects* > *Policy* and edit the outbound policy towards the IPsec VPN tunnel.
2. In the *Security Profiles* section, enable *DNS Filter* and select the profile created in the previous procedure (*SaaS*).
3. In the *Logging Options* section, enable *Log Allowed Traffic*.
4. Configure the remaining settings as needed.
5. Click *OK*.

To apply the DNS filter profile to the outbound policy towards the IPsec VPN tunnel in the CLI:

```
config firewall policy
                        edit 1
                        set name "outbound_VPN"
                        ...
                        set dnsfilter-profile "SaaS"
                        set logtraffic enable
                        ...
                        next
                end
```

To verify the configuration:

From one of the Windows client desktops, use the `nslookup` command to send various DNS queries.

1. Send a DNS query for a DNS entry configured locally on the Local Site FortiProxy:

```
C:\Users\demo>nslookup office.microsoft.com
                                        Server:  Unknown
                                        Address:  192.168.16.254
                                        Non-authoritative answer:
                                        Name:     osiprod-wus-pineapple-100.westus.cloudapp.azure.com
                                    Address:  172.16.200.55
```

   The query is resolved to the IP address configured on the Local Site FortiProxy.

2. Send a DNS query for the domain configured on the Local Site FortiProxy:

```
C:\Users\demo>nslookup teams.microsoft.com
                                        Server:  Unknown
                                        Address:  192.168.16.254
                                        Non-authoritative answer:
                                        Name:     s-0005.s-msedge.net
                                        Address:  172.16.200.254
```

   The query is resolved by the local DNS server.

3. Send a DNS query for a domain that is not configured on the Local Site FortiProxy:

```
C:\Users\demo>nslookup facebook.com
                                        Server:  Unknown
                                        Address:  192.168.16.254
                                        Non-authoritative answer:
                                        Name:    facebook.com
                                        Addresses:  157.240.249.35
```

   The query is resolved by the central DNS server.

IPv6 support for conditional DNS forwarder

The configuration for IPv6 is similar to an IPv4 conditional DNS forwarder. When configuring the DNS forwarder address, the IPv6 address must be specified.

To configure a DNS forwarder:

```
config system dns-database
                        edit <name>
                        set source-ip6 <IPv6_address>
                        set forwarder6 <IPv6_address>
                        next
                end
```



If the DNS server is accessed over a VPN, it may be necessary to specify a source IP for the FortiProxy to reach the DNS server.

Interfaces in non-management VDOMs as the source IP address of the DNS conditional forwarding server

Interfaces that are in non-management VDOMs can be the source IP address of the DNS conditional forwarding server.

- When vdom-dns is enabled in a VDOM, only the IP addresses of interfaces in that VDOM can be configured as the source-ip.
- When vdom-dns is disabled (default), only the IP address of interfaces in the management VDOM can be configured as the source-ip.

In this example:

- vdom1 is a non-management VDOM
- port8 is assigned to vdom1 and has IP address 13.13.13.13
- port1 is assigned to the management VDOM (root) and has IP address 172.16.200.1

To configure the interfaces:

```
config global
    config system interface
        edit "port8"
            set vdom "vdom1"
            set ip 13.13.13.13 255.255.255.0
        next
        edit "port1"
            set vdom "root"
            set ip 172.16.200.1 255.255.255.0
        next
    end
end
```

To test configuring a source IP address when vdom-dns is disabled:

```
config vdom
    edit vdom1
        config system vdom-dns
            set vdom-dns disable
        end
    next
end
```

- port8 cannot be used as the source IP address in a DNS database because it is assigned to vdom1, and not to a management VDOM:

```
config vdom
    edit vdom1
        config system dns-database
            edit "1"
                set source-ip 13.13.13.13
13.13.13.13 does not match any interface ip in vdom root.
node_check_object fail! for source-ip 13.13.13.13
```

- port1 can be used as the source IP address in a DNS database because it is assigned to the management VDOM:

```
config vdom
    edit vdom1
        config system dns-database
            edit "1"
                set source-ip 172.16.200.1
            next
        end
    next
end
```

To test configuring a source IP address when `vdom-dns` is enabled:

```
config vdom
    edit vdom1
        config system vdom-dns
            set vdom-dns enable
        end
    next
end
```

- `port8` can be used as the source IP address in a DNS database because it is assigned to the `vdom1`:

```
config vdom
    edit vdom1
        config system dns-database
            edit "1"
                set source-ip 13.13.13.13
            next
        end
    next
end
```

- `port1` cannot be used as the source IP address in a DNS database because it is assigned to the management VDOM, and not to `vdom1`:

```
config vdom
    edit vdom1
        config system dns-database
            edit "1"
                set source-ip 172.16.200.1
172.16.200.1 does not match any interface ip in vdom vdom1.
node_check_object fail! for source-ip 172.16.200.1
```

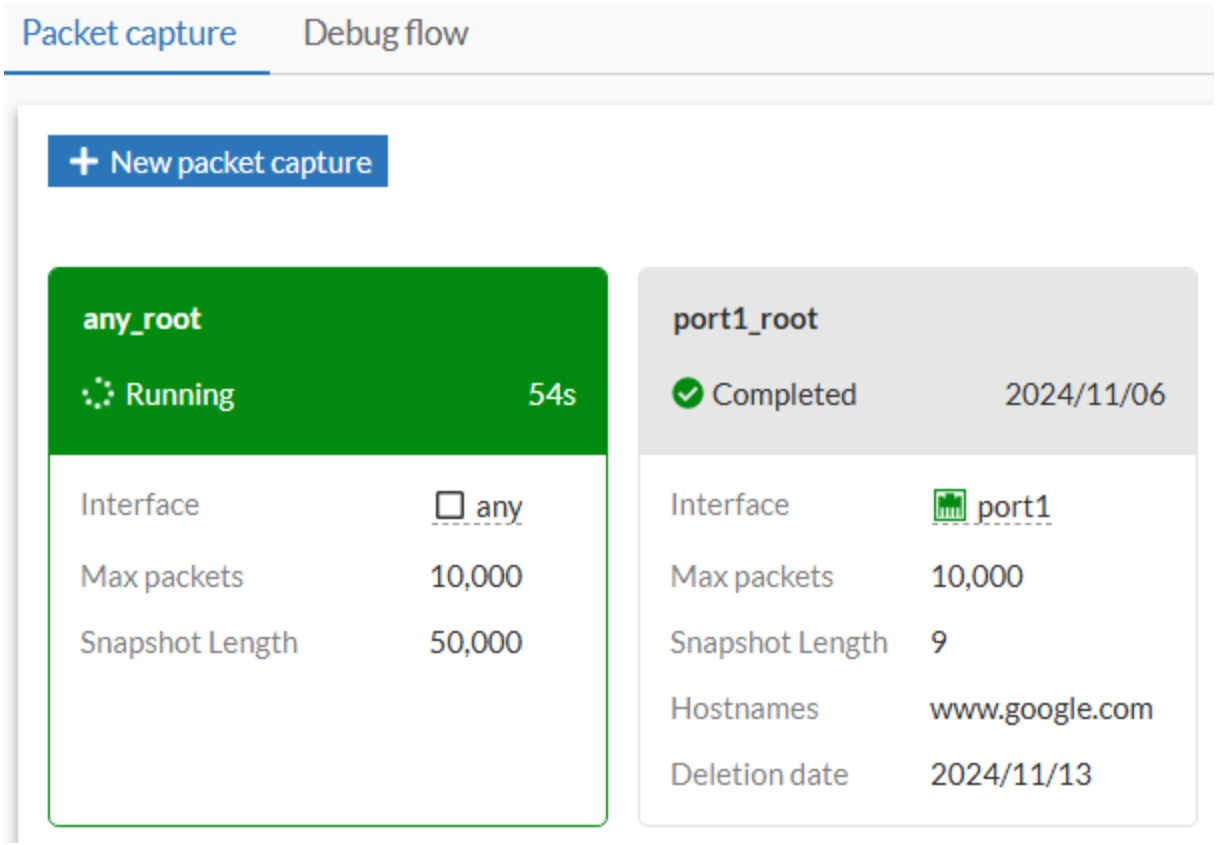
Diagnostics

Administrators can use the *Diagnostics* page to create a filter on an interface to capture a specified number of packet streams to examine in real-time with header and payload information. Once completed, packets can be filtered by various fields or through the search bar. The capture can be

saved as a PCAP file that you can use with a third-party application, such as Wireshark, for further analysis. Recent capture criteria is saved after the packet capture, and you can select and use the same criteria again. You can also save the capture criteria without starting the capture by clicking *Save settings for later* after configuring the packet capture criteria.

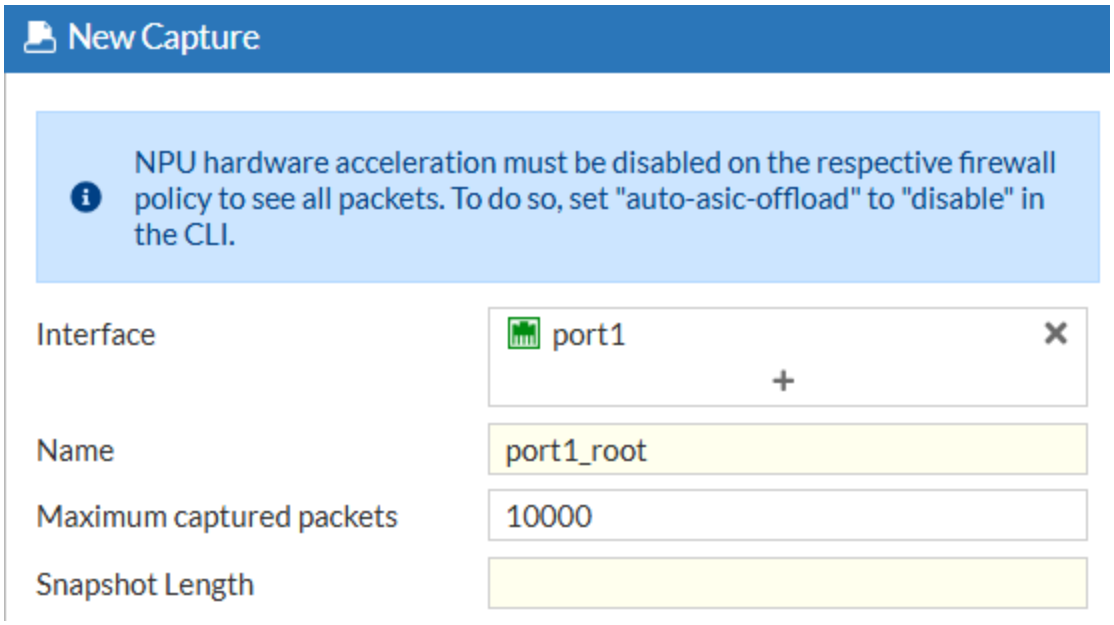
Capture cards in the *Network* > *Diagnostics* page are sorted in alphabetical order of the configured name and colored depending on state:

- Green: The packet capture is running.
- Gray: The packet capture has not started yet, has completed, or the capture files have been deleted.



To capture packets in the GUI:

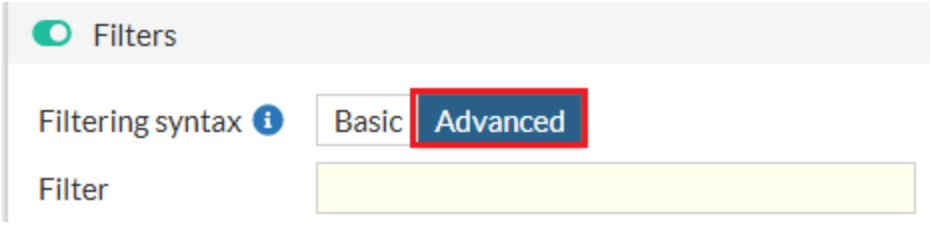
1. Go to *Network* > *Diagnostics* and select the *Packet Capture* tab.
2. Select one or multiple interfaces (default is *any*).



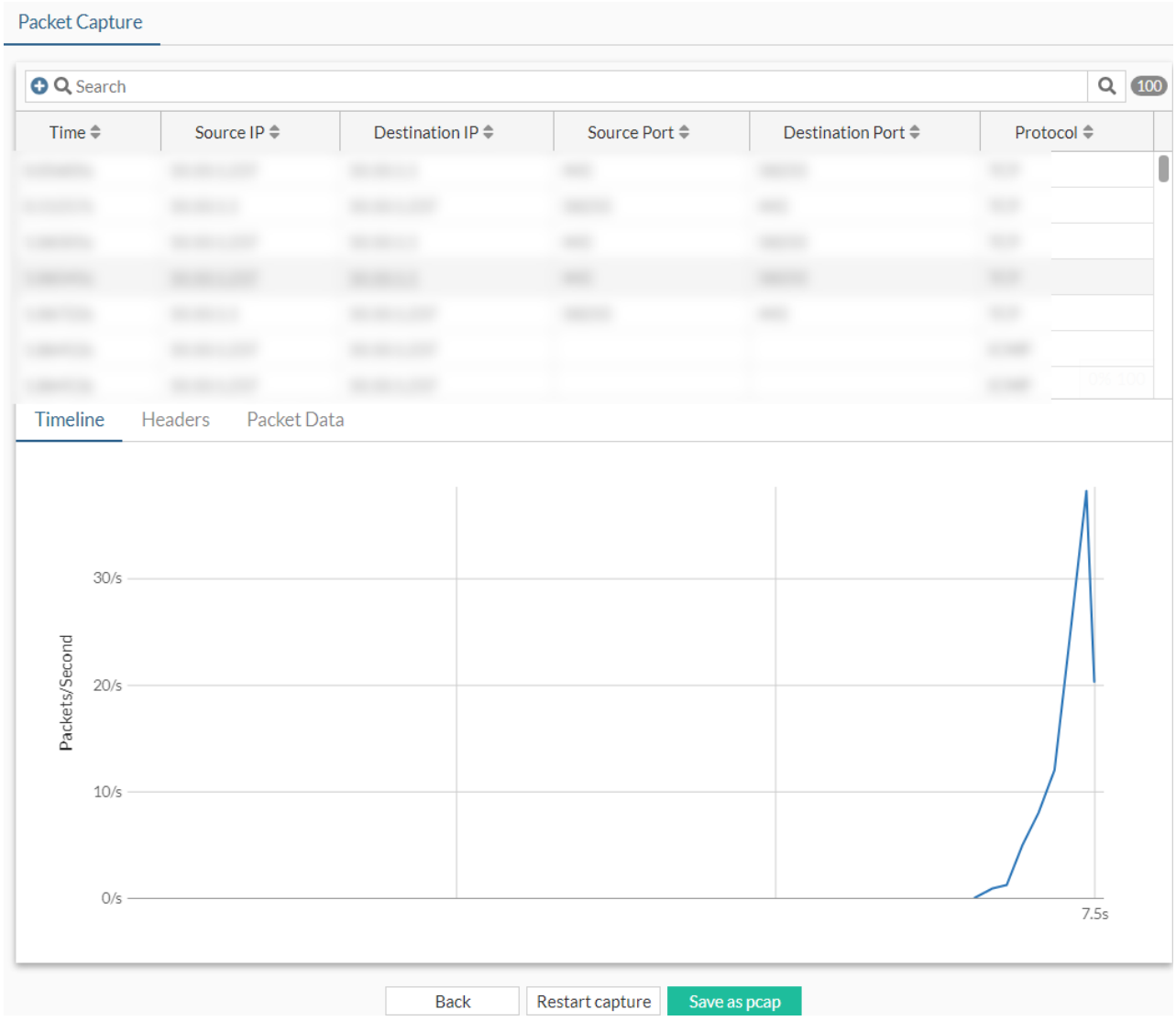
3. Specify the name in the *Name* field. The name must be unique for the packet capture criteria being configured.
4. Optionally, enable *Maximum captured packets* and enter a number which is the maximum number of packets that the FortiProxy will capture. The default is 10000. When disabled, the FortiProxy automatically stops after capturing 50,000 packets to preserve memory.
5. Optionally, enable *Filters* and select a *Filtering syntax*:
   a. *Basic*: enter criteria for the *Host*, *Hostname*, *Port*, and *Protocol number*.



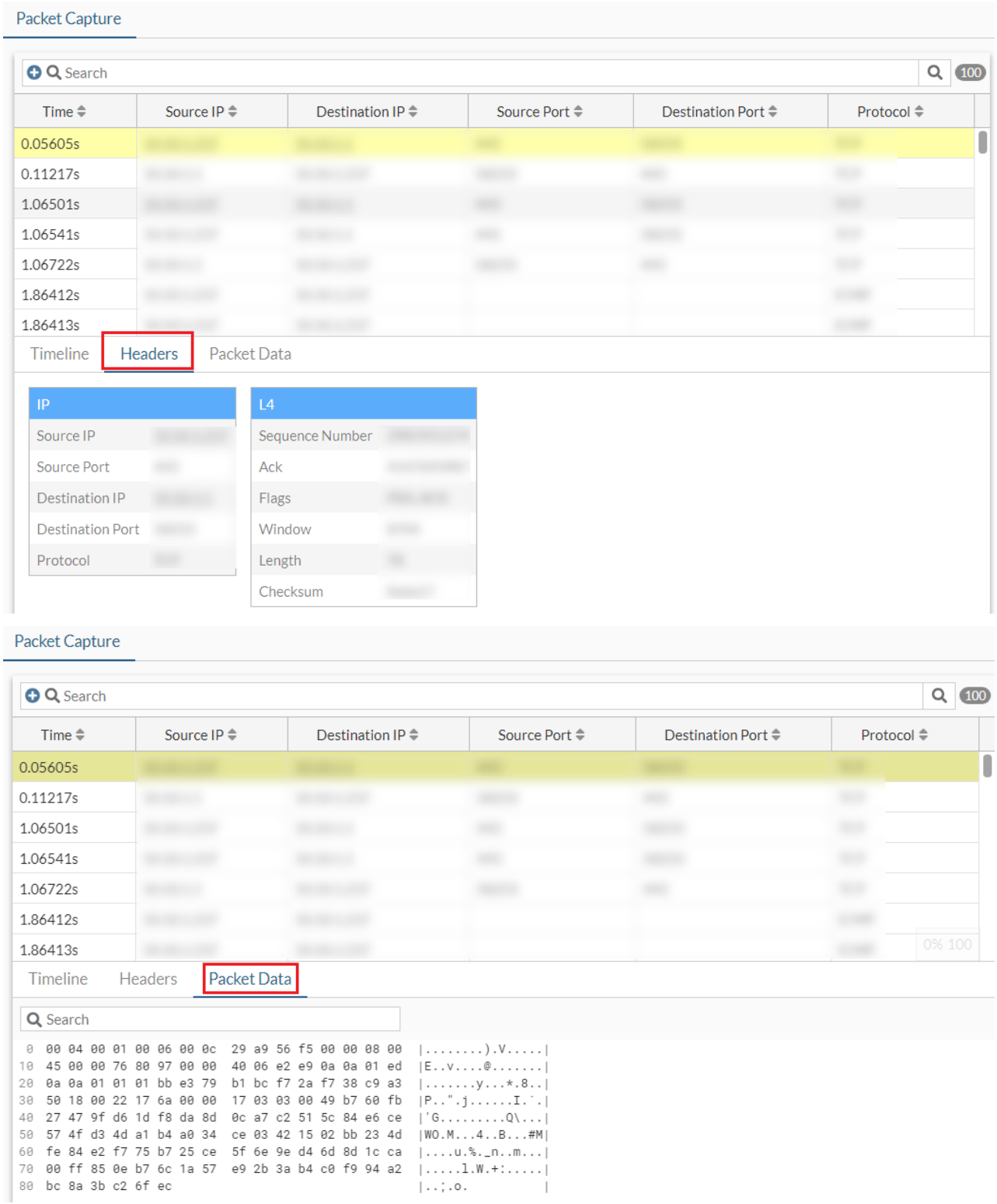
b. *Advanced*: enter a string, such as *src host 172.16.200.254 and dst host 172.16.200.1 and dst port 443*.



6. Click *Start capture*. The capture is visible in real-time.



7. While the capture is running, select a packet, then click *View* to see more information in the *Headers* or *Packet Data* tabs.



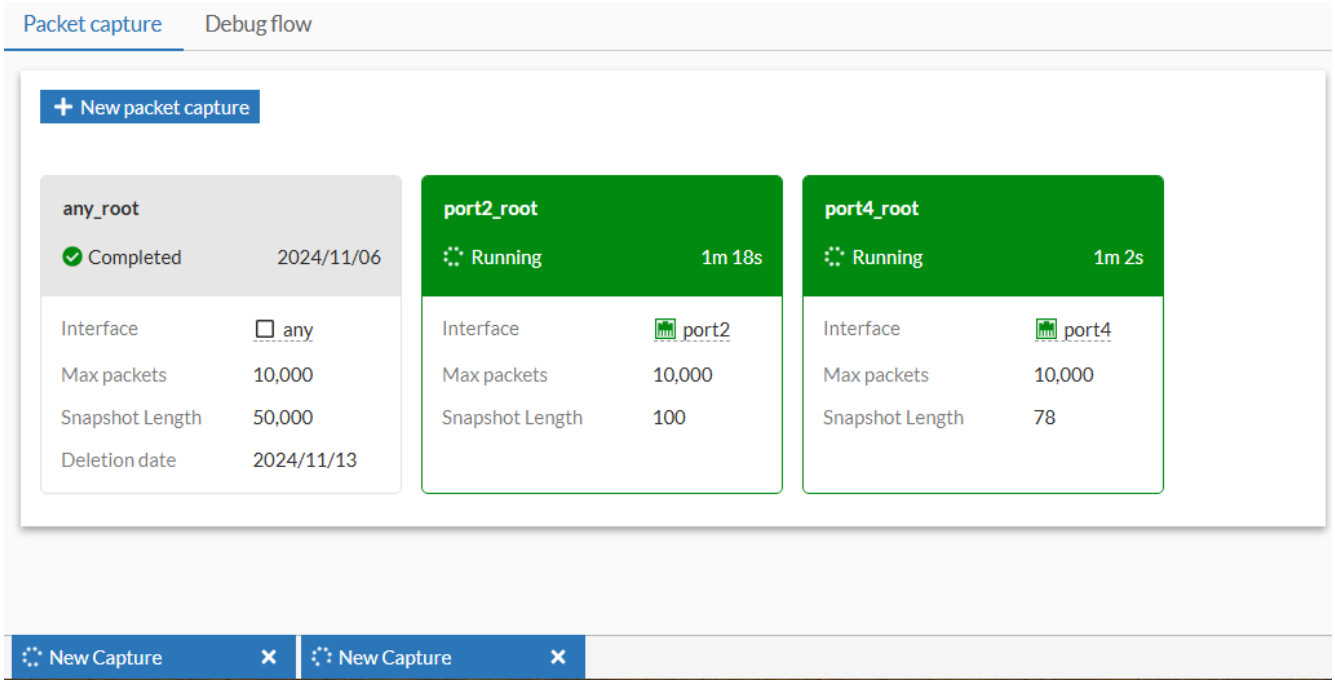
8. When the capture is finished, click *Save as pcap*. The PCAP file is automatically downloaded.
9. Optionally, use the *Search* bar or the column headers to filter the results further.

For more granular sniffer output with various verbose settings, use `diagnose sniffer packet <interface> <'filter'> <verbose> <count> <tsformat>`.

Multiple packet captures

Multiple packet captures can be run simultaneously for when many packet captures are needed for one situation. For example, ingress and egress interfaces can be captured at the same time to compare traffic or the physical interface and VPN interface can be captured using different filters to see if packets are leaving the VPN.

The packet capture dialog can be docked and minimized to run in the background. The minimized dialog aligns with other CLI terminals that are minimized.



To run multiple packet captures at the same time:

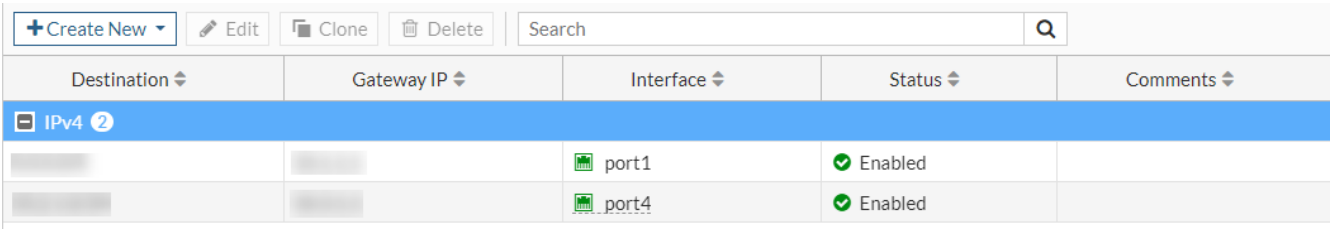
1. Go to *Network* > *Diagnostics*.
2. Configure the first packet capture:
   a. Click *New packet capture*. The *Packet Capture (1)* dialog is displayed.
   b. Select the *Interface* and configure other settings as needed.
   c. Click *Start capture*. The first packet capture begins.
3. Minimize the packet capture. The packet capture continues to run.
4. Configure the second packet capture:
   a. Click *New packet capture*. The *Packet Capture (2)* dialog is displayed.
   b. Select the *Interface* and configure other settings as needed.

c. Click *Start capture*. The second packet capture begins.

5. When the captures are complete, expand the dialog and select *Save as pcap* for each packet capture.

Static routes

To see a list of static routes that control the flow of traffic through the unit, go to *Network* > *Static Routing*



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

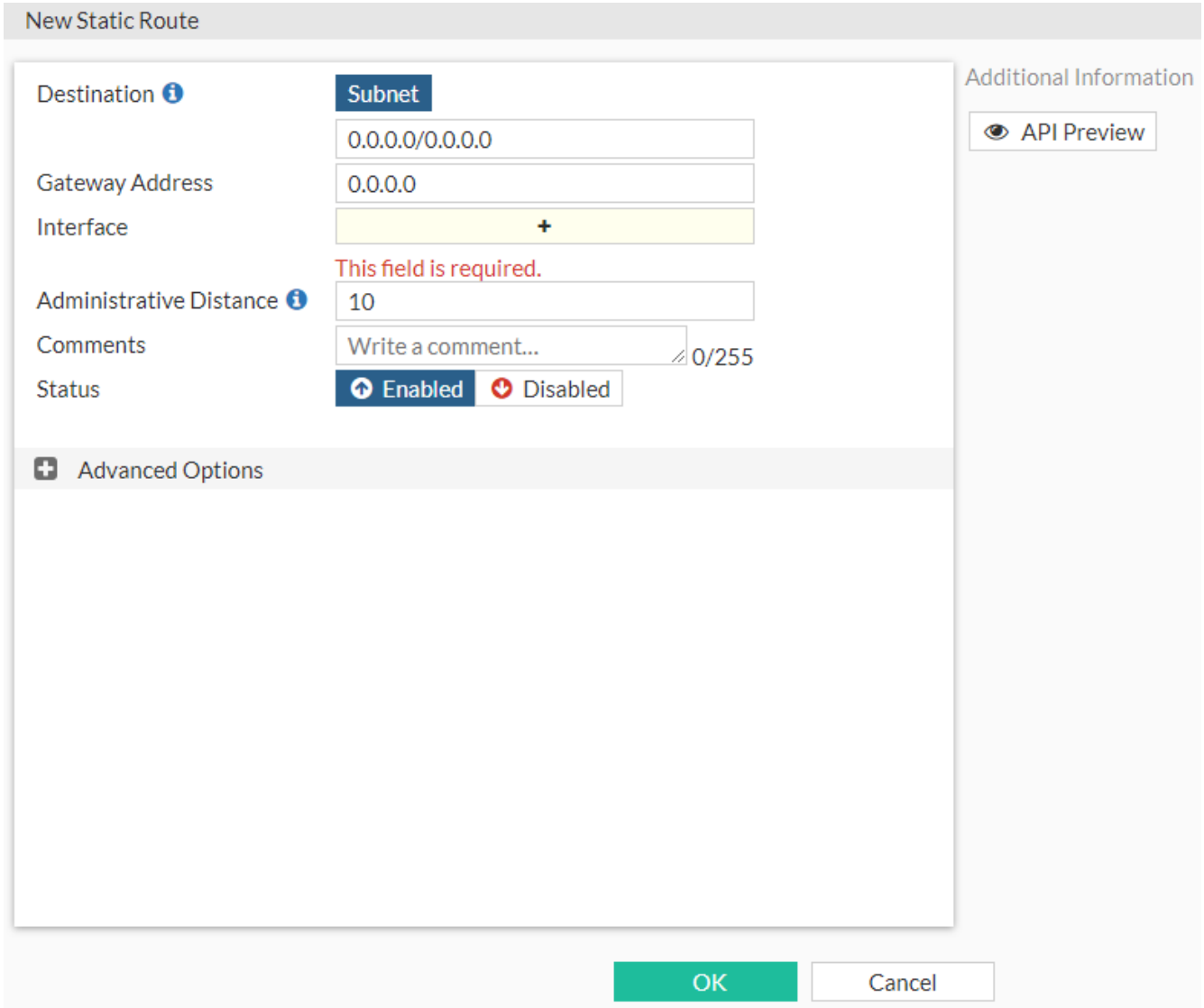
The following options are available:

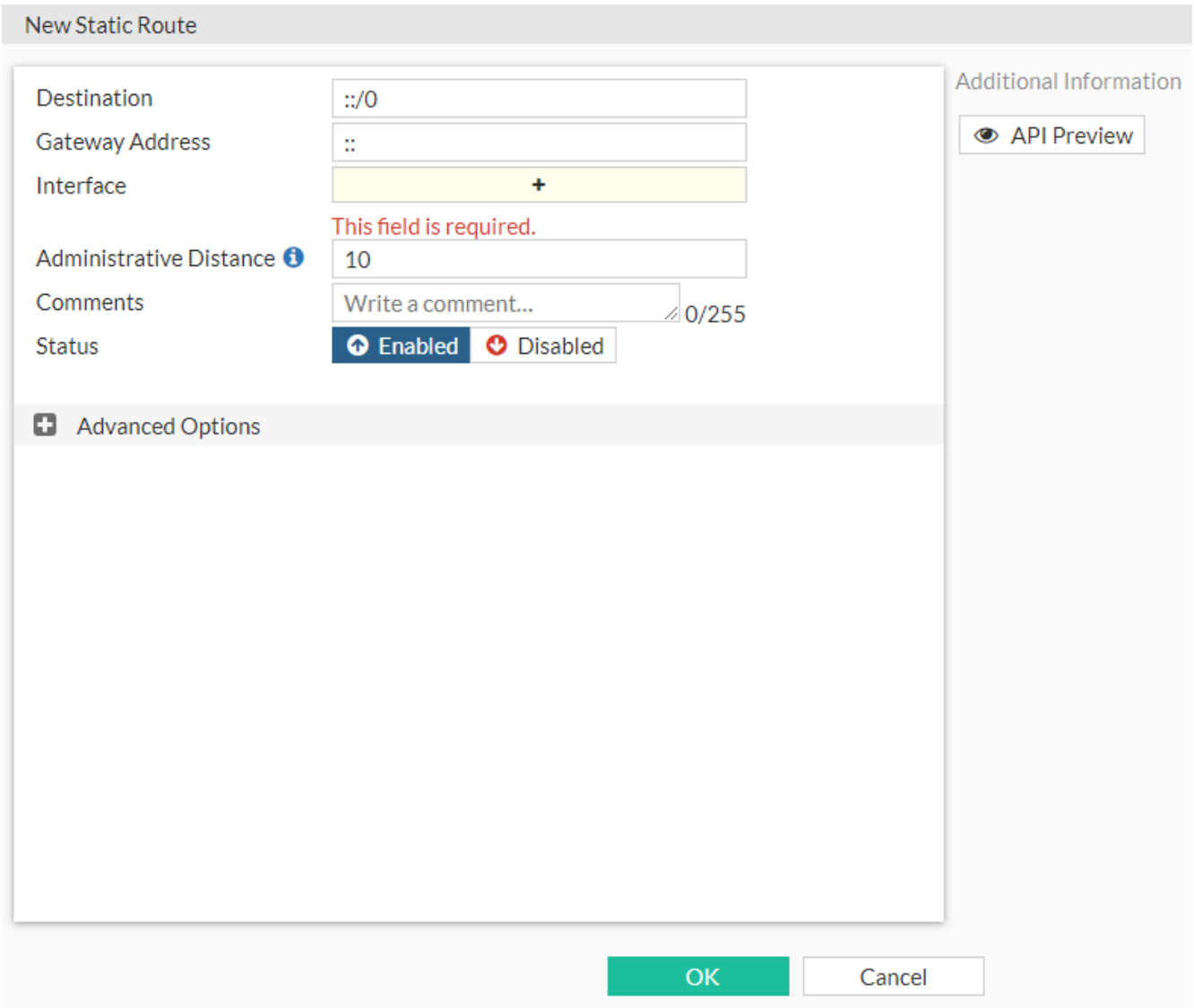
Create New	Creates an IPv4 or IPv6 static route. See Create or edit a static route on page 225.
Edit	Modifies settings within the static route. See Create or edit a static route on page 225.
Clone	Copies an existing route.
Delete	Removes a static route from the list. To remove multiple static routes, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Search	Enter a search term to find in the list.
Destination	The destination IP addresses and network masks of packets that the FortiProxy unit intercepts.
Gateway IP	The IP addresses of the next-hop routers to which intercepted packets are forwarded.
Interface	The interface or port number the static route is configured to.
Status	The static route is either enabled or disabled.
Comments	A description of the route (optional).
Distance	The number of hops the static route has to the configured gateway. Routes with the same distance will be considered as equal-cost multi-path (ECMP)

Priority	A number for the priority of the static route. Routes with a larger number will have a lower priority. Routes with the same priority are considered as ECMP.

Create or edit a static route

Select *Create New* > *IPv4 Static Route* or *Create New* > *IPv6 Static Route* to open the New Static Route page and create a static route.





Select a static route and then click *Edit* to change a static route.

Configure the following settings in the *New Static Route* page or *Edit Static Route* page and click *OK*:

Destination	Enter the IPv4 or IPv6 address and netmask of the new static route.
Gateway Address	Enter the gateway IP address for those packets that you intend the unit to intercept.
Interface	Select the static route's interface, port number, or *Blackhole.*

	A blackhole route is a route that drops all traffic sent to it. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator will not discover any information from the target network. Blackhole routes can also limit traffic on a subnet. If some subnet addresses are not in use, traffic to those addresses, which may be valid or malicious, can be directed to a blackhole for added security and to reduce traffic on the subnet.
Administrative Distance	The administrative distance is used to determine the cost of the route. Smaller distances are considered as a "better" route that should be used when multiple paths exist to the same destination. The routes with the same distance are considered as equal-cost multi-path routing (ECMP).
Comments	Enter a description up to 255 characters to describe the new static route.
Status	Select *Enabled* or *Disabled* to set the status of the new static route.
Advanced Options	Click + to show the *Priority* option.
Priority	Enter a number for the priority of the static route. Routes with a larger number have a lower priority. Routes with the same priority are considered as ECMP.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Policy routes

Policy routing allows you to specify an interface to route traffic. This is useful when you need to route certain types of network traffic differently than you would if you were using the routing table. You can use the incoming traffic's protocol, source or destination address, source interface, or port number to determine where to send the traffic. Policy routes are sometimes referred to as Policy-based routes (PBR).

When a packet arrives, the FortiProxy starts at the top of the policy route list and attempts to match the packet with a policy. For a match to be found, the policy must contain enough information to route the packet. At a minimum, this requires the outgoing interface to forward the traffic, and the gateway to route the traffic to. If one or both of these are not specified in the policy route, then the FortiProxy searches the routing table to find the best active route that corresponds to the policy route. If no routes are found in the routing table, then the policy route does not match the packet. The FortiProxy continues down the policy route list until it reaches the end. If no matches are found, then the FortiProxy does a route lookup using the routing table.

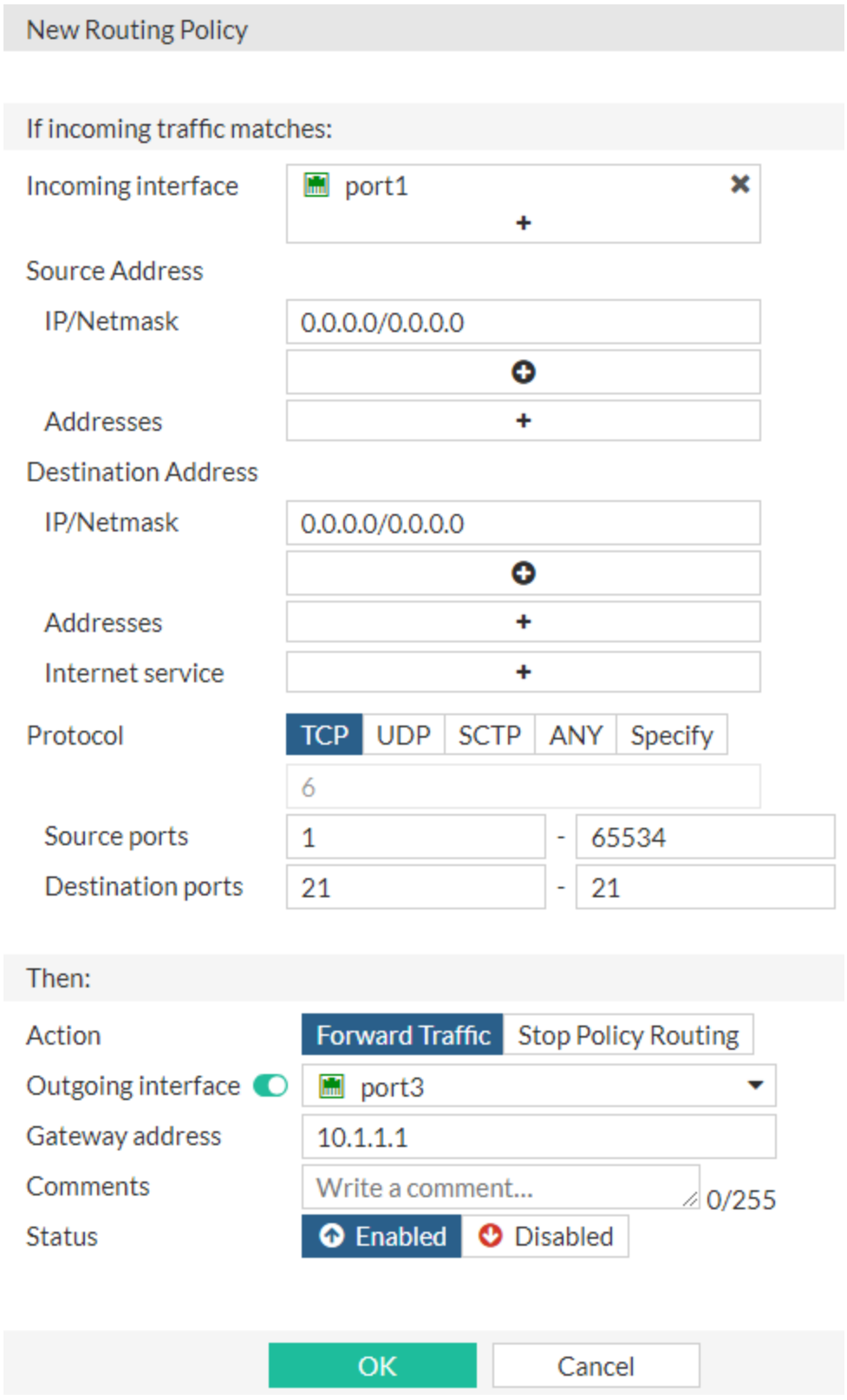
Configuring a policy route

In this example, a policy route is configured to send all FTP traffic received at port1 out through port3 and to a next hop router at 10.1.1.1. To route FTP traffic, the protocol is set to TCP (6) and the destination ports are set to 21 (the FTP port).

To configure a policy route in the GUI:

1. Go to *Network* > *Policy Routes* and click *Create New*.
2. Configure the following fields:

Incoming interface	port1
Source Address	0.0.0.0/0.0.0.0
Destination Address	0.0.0.0/0.0.0.0
Protocol	TCP
Destination ports	21 - 21
Outgoing interface	Enable and select port3
Gateway address	10.1.1.1


New Routing Policy
If incoming traffic matches:
Incoming interface
port1
Source Address
IP/Netmask
0.0.0.0/0.0.0.0
Addresses
Destination Address
IP/Netmask
0.0.0.0/0.0.0.0
Addresses
Internet service
Protocol
TCP
UDP
SCTP
ANY
Specify
6
Source ports
1
65534
Destination ports
21
21
Then:
Action
Forward Traffic
Stop Policy Routing
Outgoing interface
port3
Gateway address
10.1.1.1
Comments
Write a comment...
0/255
Status
Enabled
Disabled
OK
Cancel

3. Click *OK*.

To configure a policy route in the CLI:

```
config router policy
    edit 1
        set input-device "port1"
        set src "0.0.0.0/0.0.0.0"
        set dst "0.0.0.0/0.0.0.0"
        set protocol 6
        set start-port 21
        set end-port 21
        set gateway 10.1.1.1
        set output-device "port3"
    next
end
```

VXLAN

Virtual Extensible LAN (VXLAN) is a network virtualization technology used in large cloud computing deployments. It encapsulates layer 2 Ethernet frames within layer 3 IP packets using the standard destination port 4789. VXLAN endpoints that terminate VXLAN tunnels can be virtual or physical switch ports, and are known as VXLAN tunnel endpoints (VTEPs). For more information about VXLAN, see RFC 7348.

To configure VXLAN:

```
config system vxlan
    edit <name>
        set interface <interface>
        set vni <vxlan_network_id>
        set ip-version {ipv4_unicast | ipv6_unicast}
        set remote-ip <ipv4_address>
        set remote-ip6 <ipv6_address>
        set dstport <port>
    next
end
```

`interface <interface>`	Outgoing interface for VXLAN encapsulated traffic.
`vni <vxlan_network_id>`	VXLAN network ID (default = 0).
`ip-version {ipv4_unicast | ipv6_unicast}`	The IP address version to use for the VXLAN interface, and for communication over the VXLAN (default = ipv4_unicast).
`remote-ip <ip_address>` `remote-ip6 <ipv6_address>`	The IPv4 or IPv6 address of the VXLAN interface on the device at the remote end of the VXLAN.
`dstport <port>`	The VXLAN destination port (1 - 65535, default = 4789).

To view the VXLAN forwarding database list for an interface:

```
diagnose sys vxlan fdb list <interface>
```

Zero Trust Network Access

This section includes information about ZTNA related features:

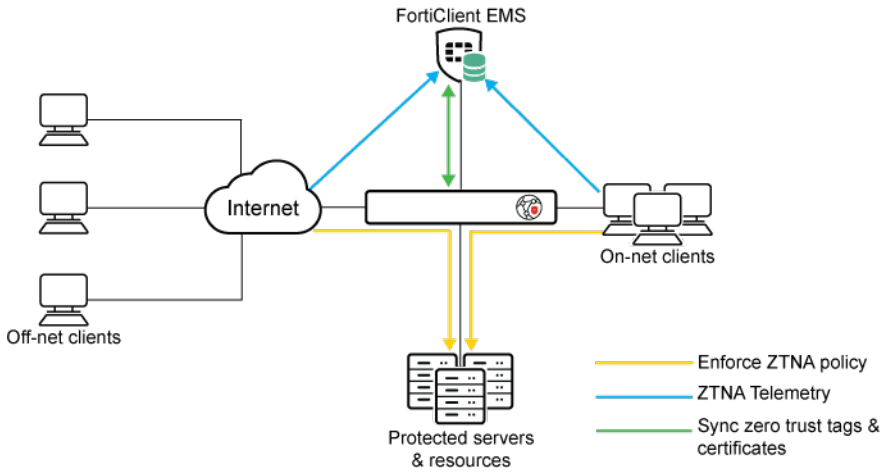
- Zero Trust Network Access introduction on page 232
  - Establish device identity and trust context with FortiClient EMS on page 235
  - SSL certificate based authentication on page 244
- Basic ZTNA configuration on page 246
- ZTNA advanced configurations on page 260
- ZTNA configuration examples on page 291
- ZTNA troubleshooting and debugging commands on page 367
- ZTNA troubleshooting scenarios on page 374

Zero Trust Network Access introduction

Zero Trust Network Access (ZTNA) is an access control method that uses client device identification, authentication, and Zero Trust tags to provide role-based application access. FortiProxy supports full ZTNA which allows users to securely access resources through a SSL encrypted access proxy. This simplifies remote access by eliminating the use of VPNs and gives administrators the flexibility to manage network access for On-net local users and Off-net remote users. Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using Zero Trust tags.

Traditionally, a user and a device have different sets of rules for on-net access and off-net VPN access to company resources. With a distributed workforce and access that spans company networks, data centers, and cloud, managing the rules can become complex. User experience is also affected when multiple VPNs are needed to get to various resources. ZTNA can improve this experience.

ZTNA telemetry, tags, and policy enforcement



When On-net and Off-net FortiClient endpoints register to FortiClient EMS, device information, log on user information, and security posture are all shared over ZTNA telemetry with the EMS server. Clients also make a certificate signing request to obtain a client certificate from the EMS that is acting as the ZTNA Certificate Authority (CA).

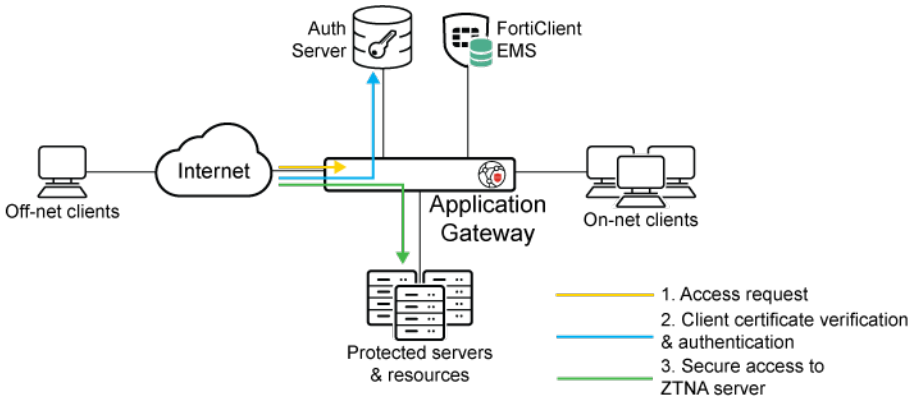
Based on the client information, EMS applies matching Zero Trust tagging rules to tag the clients. These tags, and the client certificate information, are synchronized with the FortiProxy unit in real-time. This allows the FortiProxy unit to verify the client's identity using the client certificate, and grant access based on the ZTNA tags applied in the ZTNA rule.

EMS ZTNA and endpoint tags are displayed in the *Device Inventory* widget, *FortiClient* widget, and the *Asset Identity Center* page. In the backend, EMS ZTNA tags, endpoint tags, and EMS serial numbers are in the user device query API and response.



The ZTNA tag name can be used as a search criterion in the *Asset* view of the *Asset Identity Center* page.

Application gateway



The FortiProxy application gateway can proxy HTTP and TCP traffic over secure HTTPS connections with the client. This enables seamless access from the client to the protected servers, without needing to form IPsec VPN tunnels.

HTTPS access proxy

The FortiProxy HTTPS access proxy works as a reverse proxy for the HTTP server. When a client connects to a webpage hosted by the protected server, the address resolves to the FortiProxy unit's access proxy VIP. The FortiProxy unit proxies the connection and takes steps to authenticate the user. It prompts the user for their certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from the EMS. If an authentication scheme, such as SAML authentication, is configured, the client is redirected to a captive portal for sign-on. If this passes, traffic is allowed based on the ZTNA rules, and the FortiProxy unit returns the webpage to the client.

TCP forwarding access proxy (TFAP)

TCP forwarding access proxy works as a special type of HTTPS reverse proxy. Instead of proxying traffic to a web server, TCP traffic is tunneled between the client and the access proxy over HTTPS, and forwarded to the protected resource. The FortiClient on the remote endpoint intercepts traffic destined for the protected resources and routes them to the FortiGate proxy gateway. An HTTPS connection is made to the FortiGate's access proxy VIP, where the client certificate is verified and access is granted based on the ZTNA policies. TCP traffic is forwarded from the FortiGate to the protected resource, and an end to end connection is established.

For an example configuration, see ZTNA TCP forwarding access proxy example on page 311.

Basic ZTNA configuration components

The following are the basic requirements for configuring full ZTNA on the FortiProxy unit:

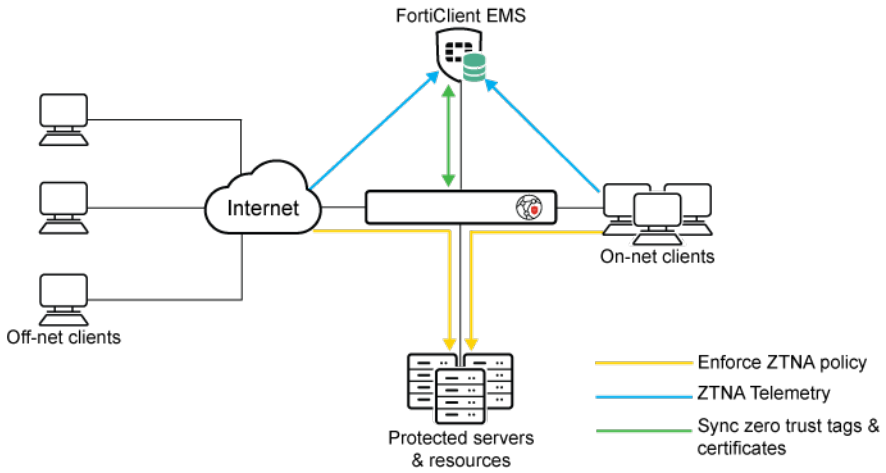
- FortiClient EMS fabric connector and ZTNA tags.
- FortiClient EMS running version 7.0.0 or later.

- FortiClient running 7.0.0 or later.
- ZTNA server
- ZTNA rule
- Firewall policy

For configuration details, see Basic ZTNA configuration on page 246.

Establish device identity and trust context with FortiClient EMS

How device identity is established through client certificates, and how device trust context is established between FortiClient, FortiClient EMS, and the FortiProxy, are integral to ZTNA.



Device roles

FortiClient

FortiClient endpoints provide the following information to FortiClient EMS when they register to the EMS:

- Device information (network details, operating system, model, and others)
- Logged on user information
- Security posture (On-net/Off-net, antivirus software, vulnerability status, and others)

It also requests and obtains a client device certificate from the EMS ZTNA Certificate Authority (CA) when it registers to FortiClient EMS. The client uses this certificate to identify itself to the FortiProxy.

FortiClient EMS

FortiClient EMS issues and signs the client certificate with the FortiClient UID, certificate serial number, and EMS serial number. The certificate is then synchronized to the FortiProxy. EMS also

shares its EMS ZTNA CA certificate with the FortiProxy, so that the FortiProxy can use it to authenticate the clients.

FortiClient EMS uses zero trust tagging rules to tag endpoints based on the information that it has on each endpoint. The tags are also shared with the FortiProxy. See Endpoint Posture Check Reference for a list of the endpoint posture checks that EMS can perform.



Each security posture tag creates two firewall addresses in all VDOMs on a FortiProxy. One firewall address is the IP address, and the other firewall address is the MAC address. Because each FortiProxy model has a global limit and a per-VDOM limit for the maximum number of supported firewall addresses, the FortiProxy model determines the maximum number of security posture tags allowable by that unit, which is the maximum number of firewall address divided by two. For each FortiProxy model's limit, see the Maximum Values table.

FortiProxy

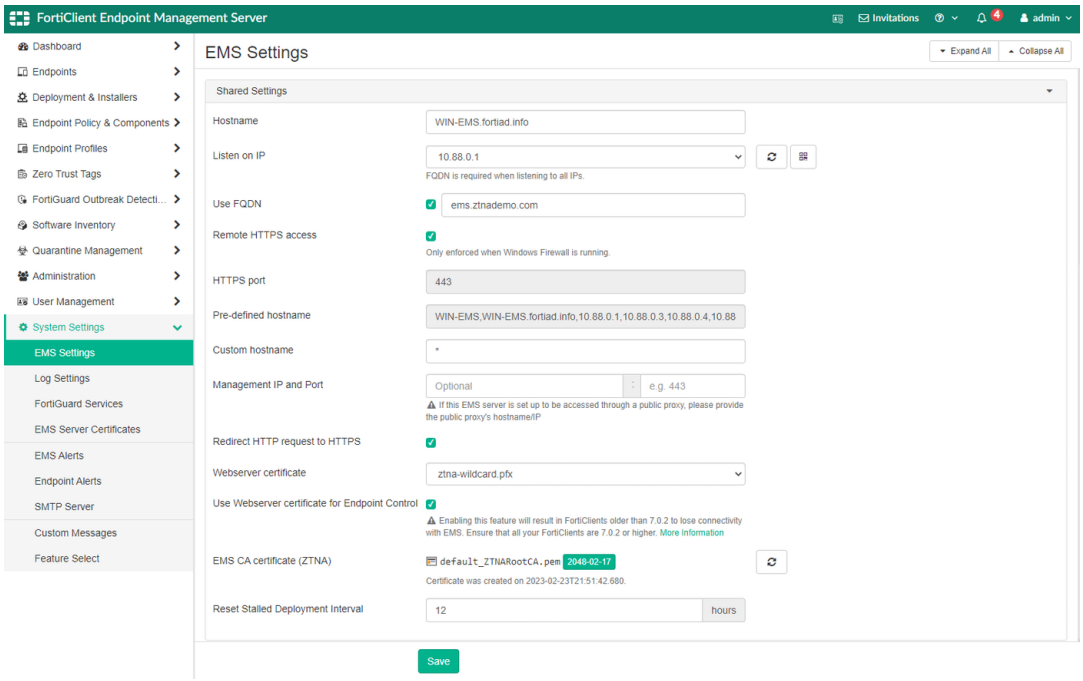
The FortiProxy maintains a continuous connection to the EMS server to synchronize endpoint device information, including primarily:

- FortiClient UID
- Client certificate SN
- EMS SN
- Device credentials (user/domain)
- Network details (IP and MAC address and routing to the FortiProxy)

When a device's information changes, such as when a client moves from on-net to off-net, or their security posture changes, EMS is updated with the new device information and then updates the FortiProxy. The FortiProxy's WAD daemon can use this information when processing ZTNA traffic. If an endpoint's security posture change causes it to no longer match the ZTNA policy criteria on an existing session, then the session is terminated.

Certificate management on FortiClient EMS

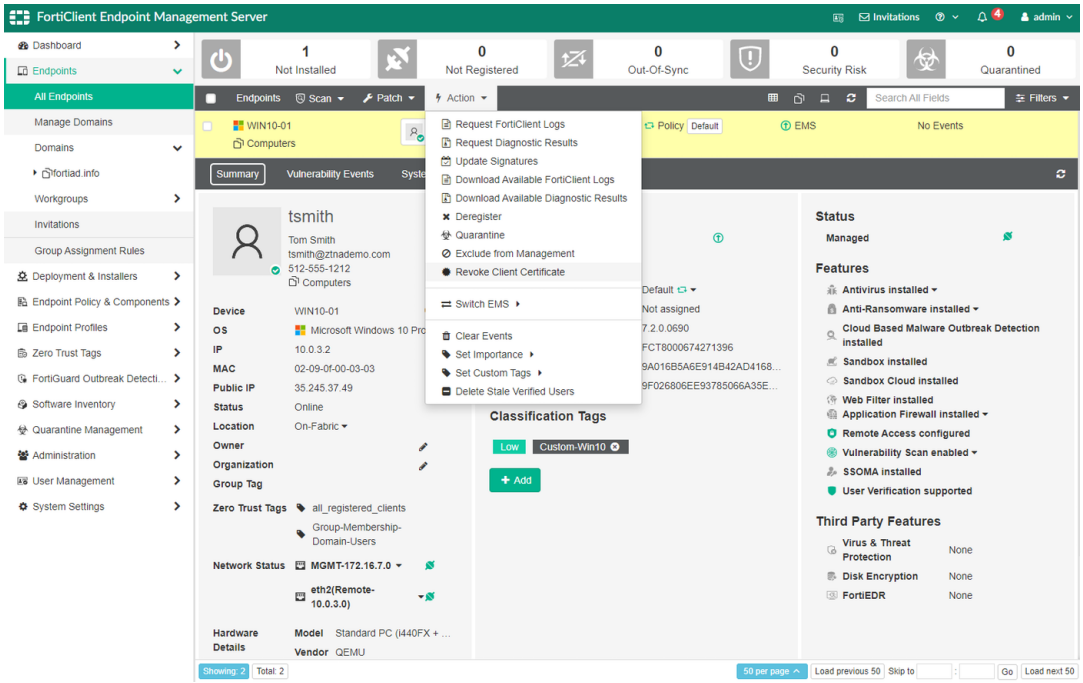
FortiClient EMS has a *default_ZTNARootCA* certificate generated by default that the ZTNA CA uses to sign CSRs from the FortiClient endpoints. Clicking the refresh button revokes and updates the root CA, forcing updates to the FortiProxy and FortiClient endpoints by generating new certificates for each client.





Do not confuse the EMS CA certificate (ZTNA) with the SSL certificate. The latter is the server certificate that is used by EMS for HTTPS access and fabric connectivity to the EMS server.

EMS can also manage individual client certificates. To revoke the current client certificate that is used by the endpoint: go to *Endpoint* > *All Endpoints*, select the client, and click *Action* > *Revoke Client Certificate*.



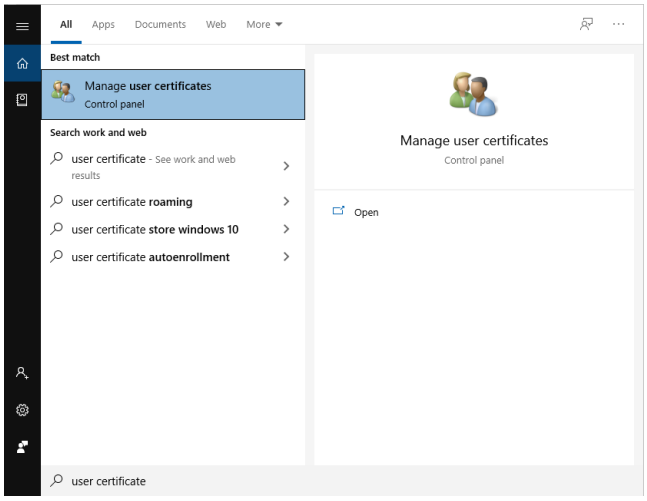
Locating and viewing the client certificate on an endpoint

In Windows, FortiClient automatically installs certificates into the certificate store. The certificate information in the store, such as certificate UID and SN, should match the information on EMS and the FortiProxy.

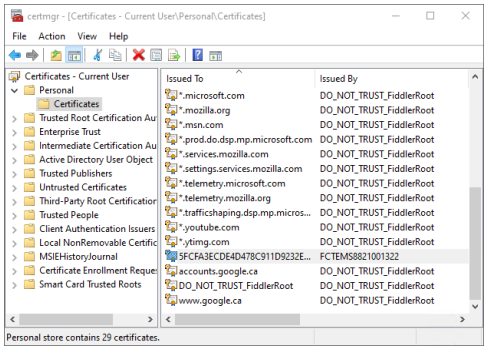
To locate certificates on other operating systems, consult the vendor documentation.

To locate the client certificate and EMS ZTNA CA certificate on a Windows PC:

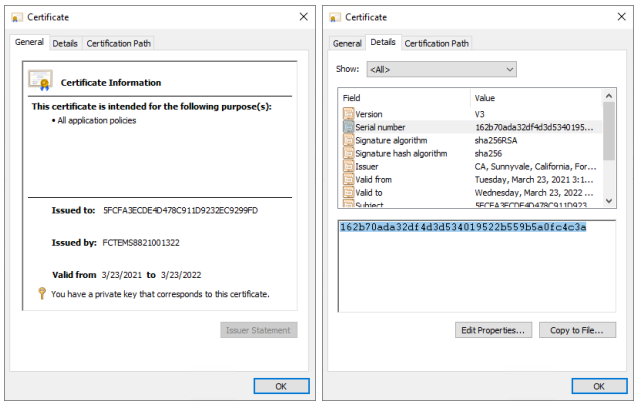
1. In the Windows search box, enter *user certificate* and click *Manage user certificates* from the results.



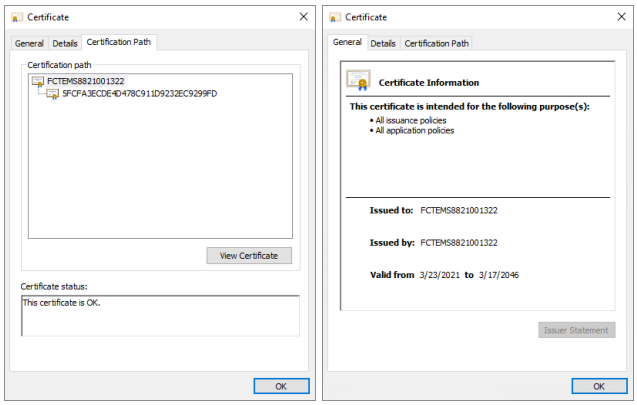
2. In the certificate manager, go to *Certificates - Current User* > *Personal* > *Certificates* and find the certificate that is issued by the FortiClient EMS.



3. Right-click on it and select Properties.
4. The *General* tab shows the client certificate UID and the issue and expiry dates. The *Details* tab show the certificate SN.



5. Go to the *Certificate Path* tab to see the full certificate chain.
6. Select the root CA and click *View Certificate* to view the details about the EMS ZTNA CA certificate.



Verifying that the client information is synchronized to the FortiProxy

The following diagnose commands help to verify the presence of matching endpoint record, and information such as the client UID, client certificate SN, and EMS certificate SN on the FortiProxy. If any of the information is missing or incomplete, client certificate authentication might fail because the corresponding endpoint entry is not found. More in-depth diagnosis would be needed to determine the reason for the missing records.

Command	Description
`# dia endpoint record list`	Show the endpoint record list. Optionally, add filters.
`# diagnose wad dev query-by uid <uid> <ems sn> <ems tenant id>`	Query from WAD diagnose command by UID.
`# diagnose wad dev query-by ipv4 <ip>`	Query from WAD diagnose command by IP address.
`# diagnose test application fcnacd 7`	Check the FortiClient NAC daemon ZTNA and route cache.

Command	Description
# diagnose test application fcnacd 8	
#diagnose test application fcnacd 5	Force a sync with the FortiClient EMS server.

To check the endpoint record list for IP address 10.100.1.58:

```
# dia endpoint record list 10.100.1.58
Record #1:
                IP Address = 10.100.1.58
                MAC Address = 00:0c:29:07:44:ab
                MAC list =
                VDOM = root (0)
                EMS serial number: FCTEMS8823005021
                EMS tenant id: 00000000000000000000000000000000
                Client cert SN: 77E6D29D582E05296DB4F78E10BEECD295BF5DEB
                Public IP address: 207.102.138.19
                Quarantined: no
                Online status: online
                Registration status: registered
                On-net status: on-net
                Gateway Interface: port2
                FortiClient version: 7.2.4
                AVDB version: 1.0
                FortiClient app signature version: 28.807
                FortiClient vulnerability scan engine version: 2.40
                FortiClient UID: F0D60B28FCAB464E81C725270B62BEC0
                Host Name: DESKTOP-2BGPITB
                OS Type: WIN64
                OS Version: Microsoft Windows 10 Professional Edition, 64-bit (build 14393)
                Host Description:
                Domain:
                Last Login User: guodong
                Owner:
                Host Model: VMware7,1
                Host Manufacturer: VMware, Inc.
                CPU Model: Intel(R) Xeon(R) CPU E5-2630 v2 @ 2.60GHz
                Memory Size: 8190
                AV Feature: 1
                FW Feature: 1
                WF Feature: 1
                AS Feature: 0
                VS Feature: 1
                VN Feature: 1
                Last vul message received time: N/A
                Last vul scanned time: N/A
                Last vul statistic: critical=0, high=0, medium=0, low=0, info=0
                Avatar fingerprint: e67ab4781b95573859127ca8a3e9dae913afc2b1
                Avatar source username:
                Avatar source email:
```

```
                Avatar source: OS
                Phone number:
                Number of Routes: (1)
                        Gateway Route #0:
                                - IP:10.100.1.58, MAC: 00:0c:29:07:44:ab, VPN: no
                                - Interface:port2, VFID:0, SN: FPXVULTM24000082
online records: 1; offline records: 0; quarantined records: 0; out-of-sync records: 0
```

To check the tags that are processed by the WAD daemon for a particular device:

```
# diagnose wad dev query-by uid F0D60B28FCAB464E81C725270B62BEC0 FCTEMS8823005021
00000000000000000000000000000000
Attr of type=0, length=83, value(ascii)=F0D60B28FCAB464E81C725270B62BEC0
Attr of type=4, length=0, value(ascii)=
Attr of type=6, length=1, value(ascii)=true
Attr of type=5, length=40, value(ascii)=77E6D29D582E05296DB4F78E10BEECD295BF5DEB
Attr of type=3, length=17, value(ascii)=EMS1_ZTNA_disk-en
Attr of type=3, length=21, value(ascii)=MAC_EMS1_ZTNA_disk-en
Attr of type=3, length=32, value(ascii)=EMS1_ZTNA_all_registered_clients
Attr of type=3, length=36, value(ascii)=MAC_EMS1_ZTNA_all_registered_clients
Attr of type=3, length=23, value(ascii)=EMS1_ZTNA_anti-virus-ok
Attr of type=3, length=27, value(ascii)=MAC_EMS1_ZTNA_anti-virus-ok
Response termination due to no more data
```

To check the FortiNAC daemon cache:

```
# diagnose test application fcnacd 7

ZTNA Cache V2:
Entry #1:

 - UID: F0D60B28FCAB464E81C725270B62BEC0
 - EMS Fabric ID: FCTEMS8823005021:00000000000000000000000000000000
 - Domain:
 - User: guodong
 - Owner:
 - Certificate SN: 77E6D29D582E05296DB4F78E10BEECD295BF5DEB
 - online: true
 - Routes (1):
  -- Route #0: IP=10.100.1.58, vfid=0
 - FWAddrNames (6):
  -- Name (#0): EMS1_ZTNA_disk-en
  -- Name (#1): MAC_EMS1_ZTNA_disk-en
  -- Name (#2): EMS1_ZTNA_all_registered_clients
  -- Name (#3): MAC_EMS1_ZTNA_all_registered_clients
  -- Name (#4): EMS1_ZTNA_anti-virus-ok
  -- Name (#5): MAC_EMS1_ZTNA_anti-virus-ok
lls_idx_mask = 0x00000001,
```

ZTNA scalability support for concurrent endpoints

ZTNA scalability supports up to 50 thousand concurrent endpoints. Communication between FortiProxy and FortiClient EMS has efficient queries that request incremental updates. Retrieved device information can be written to the FortiClient NAC daemon cache.

FortiProxy can receive tag information from the EMS common tags API. This feature requires FortiClient EMS 7.0.3 or later.

The APIs `api/v1/report/fct/uid_tags` and `api/v1/report/fct/tags` replace the API `api/v1/report/fct/host_tags`.

To use the common tags API capability:

1. Enable the common tags API when connecting the EMS:

```
config endpoint-control fctems
    edit 1
        set status enable
        set name "emstest"
        set server "10.120.1.24"
        set serial-number "FCTEMS8823005021"
        set tenant-id "00000000000000000000000000000000"
        set capabilities fabric-auth silent-approval websocket websocket-malware push-ca-certs
common-tags-api tenant-id
    next
```

```
end
```

2. The FortiProxy uses the new APIs to obtain device information from the EMS:

```
[ec_ems_context_submit_work:519] Call submitted successfully.
obj-id: 12, desc: REST API to get updates of tag endpoints., entry: api/v1/report/fct/tags.
[ec_ez_worker_base_prep_resolver:374] Outgoing interface index 0 for 1 (emstest).
[ec_ems_context_submit_work:519] Call submitted successfully.
obj-id: 13, desc: REST API to get updates of tags associated with FCT UID., entry:
api/v1/report/fct/uid_tags.
[ec_ez_worker_process:368] Processing call for obj-id: 13, entry: "api/v1/report/fct/uid_tags"
[_send_tags_to_info_store:166] Saving MAC and IP tag usergrp2
[_send_tags_to_info_store:166] Saving MAC and IP tag disk-en
[_send_tags_to_info_store:166] Saving MAC and IP tag all_registered_clients
[_send_tags_to_info_store:166] Saving MAC and IP tag anti-virus-ok
[_send_tags_to_info_store:166] Saving MAC and IP tag usergrp3
[_update_obj_stats:336] Storing (13, emstest, 0)
[ec_ez_worker_process:475] Call completed successfully.
obj-id: 13, desc: "REST API to get updates of tags associated with FCT UID.", entry:
"api/v1/report/fct/uid_tags".
[ec_ez_worker_base_prep_resolver:374] Outgoing interface index 0 for 1 (emstest).
[ec_ems_context_submit_work:519] Call submitted successfully.
obj-id: 8, desc: REST API to get updates about system info., entry: api/v1/report/fct/sysinfo.
[ec_ez_worker_process:368] Processing call for obj-id: 8, entry: "api/v1/report/fct/sysinfo"
[ec_mh_update:318] Error 22 opening mac_host.
```

```
[_update_obj_stats:336] Storing (8, emstest, 0)
[ec_ez_worker_process:475] Call completed successfully.
obj-id: 8, desc: "REST API to get updates about system info.", entry:
"api/v1/report/fct/sysinfo".
[ec_ez_worker_process:368] Processing call for obj-id: 12, entry: "api/v1/report/fct/tags"
[_update_obj_stats:336] Storing (12, emstest, 0)
[ec_ez_worker_process:475] Call completed successfully.
obj-id: 12, desc: "REST API to get updates of tag endpoints.", entry:
"api/v1/report/fct/tags".
(......)
```

3. Confirm that the device information from the EMS is written to the FortiClient NAC daemon cache:

```
# dia endpoint record list
    ...
          Avatar source: OS
                Phone number:
                Number of Routes: (1)
                        Gateway Route #0:
                                - IP:10.100.1.58, MAC: 00:0c:29:07:44:ab, VPN: no
                                - Interface:port2, VFID:0, SN: FPXVULTM24000082
online records: 1; offline records: 0; quarantined records: 0; out-of-sync records: 0
```

4. Use the tags that are pulled from the EMS in a firewall address:

```
config firewall address
    edit "EMS1_ZTNA_anti-virus-software"
        set uuid c4e5692c-283d-51ef-690b-af63889a4e89
        set type dynamic
        set sub-type ems-tag
        set obj-tag "anti-virus-software"
        set tag-type "zero_trust"
    next
end
```

5. Check the tags' resolved IP and MAC addresses:

```
# diagnose firewall fqdn getinfo-ip  EMS1_ZTNA_anti-virus-ok
getinfo EMS1_ZTNA_anti-virus-ok id:115 generation:7 count:1 data_len:20 flag 0

# diagnose firewall fqdn getinfo-mac MAC_EMS1_ZTNA_anti-virus-ok
getinfo MAC_EMS1_ZTNA_anti-virus-ok id:99 generation:5 count:1 data_len:6 flag 0

#  diagnose firewall dynamic address EMS1_ZTNA_anti-virus-ok
CMDB name: EMS1_ZTNA_anti-virus-ok
TAG name: anti-virus-ok
EMS1_ZTNA_anti-virus-ok: ID(115)
        ADDR(10.100.1.58)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 1.
# diagnose firewall dynamic address MAC_EMS1_ZTNA_anti-virus-ok
CMDB name: MAC_EMS1_ZTNA_anti-virus-ok
```

```
TAG name: anti-virus-ok
MAC_EMS1_ZTNA_anti-virus-ok: ID(99)
        MAC(00:0c:29:07:44:ab)
Total MAC dynamic addresses: 1.
```

SSL certificate based authentication

A client certificate is obtained when an endpoint registers to EMS. FortiClient automatically submits a CSR request and the FortiClient EMS signs and returns the client certificate. This certificate is stored in the operating system's certificate store for subsequent connections. The endpoint information is synchronized between the FortiProxy and FortiClient EMS. When an endpoint disconnects or is unregistered from EMS, its certificate is removed from the certificate store and revoked on EMS. The endpoint obtains a certificate again when it reconnects to EMS.

By default, client certificate authentication is enabled on the access proxy, so when the HTTPS request is received the FortiProxy"s WAD process challenges the client to identify itself with its certificate. The FortiProxye makes a decision based on the following possibilities:

1. If the client responds with the correct certificate that the client UID and certificate SN can be extracted from:
   - If the client UID and certificate SN match the record on the FortiProxy, the client is allowed to continue with the ZTNA proxy rule processing.
   - If the client UID and certificate SN do not match the record on the FortiProxy, the client is blocked from further ZTNA proxy rule processing.
2. If the client cancels and responds with an empty client certificate:
   - If `empty-cert-action` is set to `accept`, the client is allowed to continue with ZTNA proxy rule processing.
   - If `empty-cert-action` is set to `block`, the client is blocked from further ZTNA proxy rule processing.

To configure the client certificate actions:

```
config firewall access-proxy
    edit <name>
        set client-cert {enable | disable}
        set empty-cert-action {accept | block | accept-unmanageable}
    next
end
```

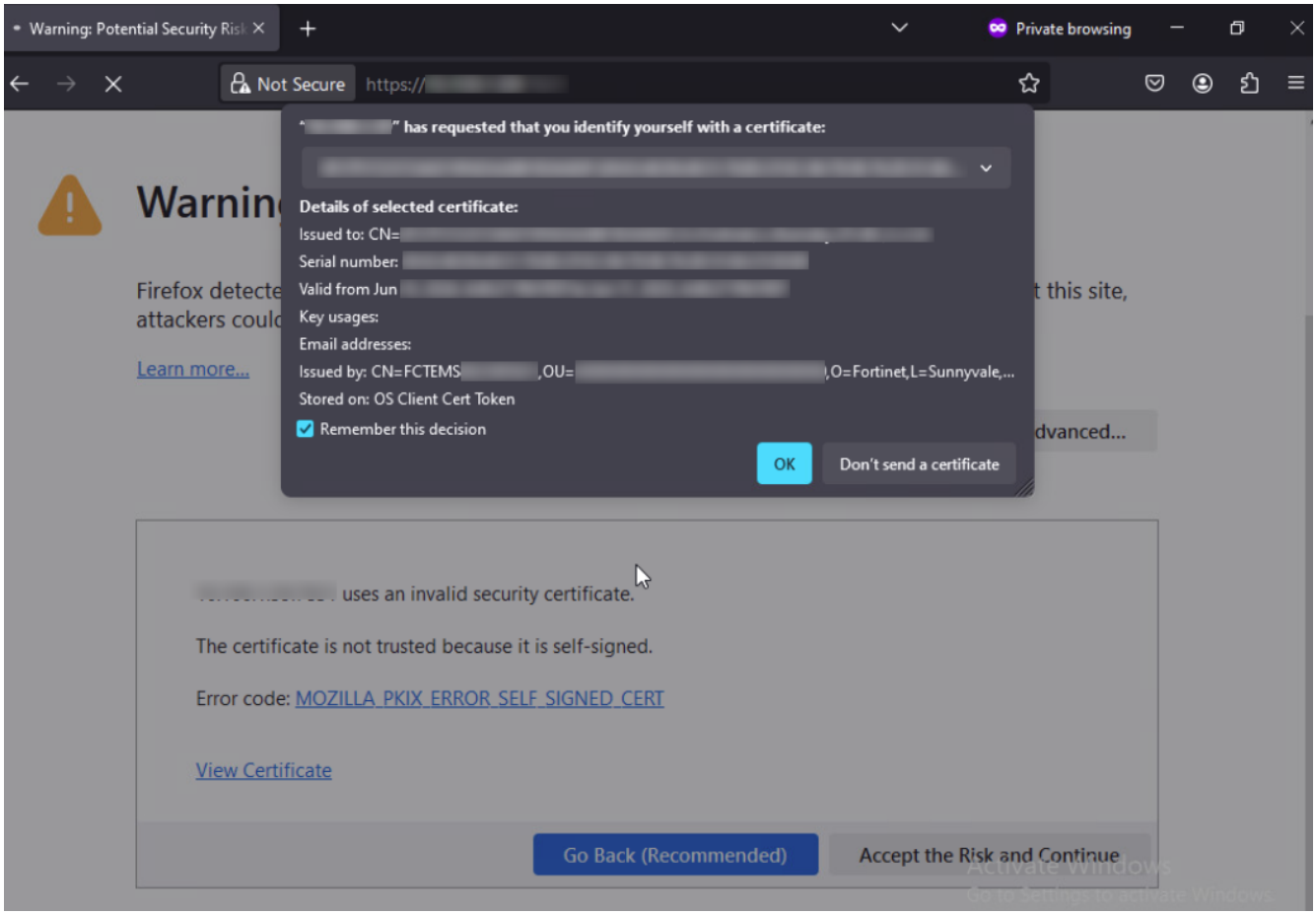
Example

In this example, a client connects to *qa.fortinet.com* and is prompted for a client certificate.

- `client-cert` is set to `enable`, and `empty-cert-action` is set to `block`.
- The ZTNA server is configured, and a ZTNA policy is set to allow this client.
- The domain resolves to the FortiProxy access proxy VIP.

Scenario 1:

When prompted for the client certificate, the client clicks *OK* and provides a valid certificate that is verified by the FortiProxy.

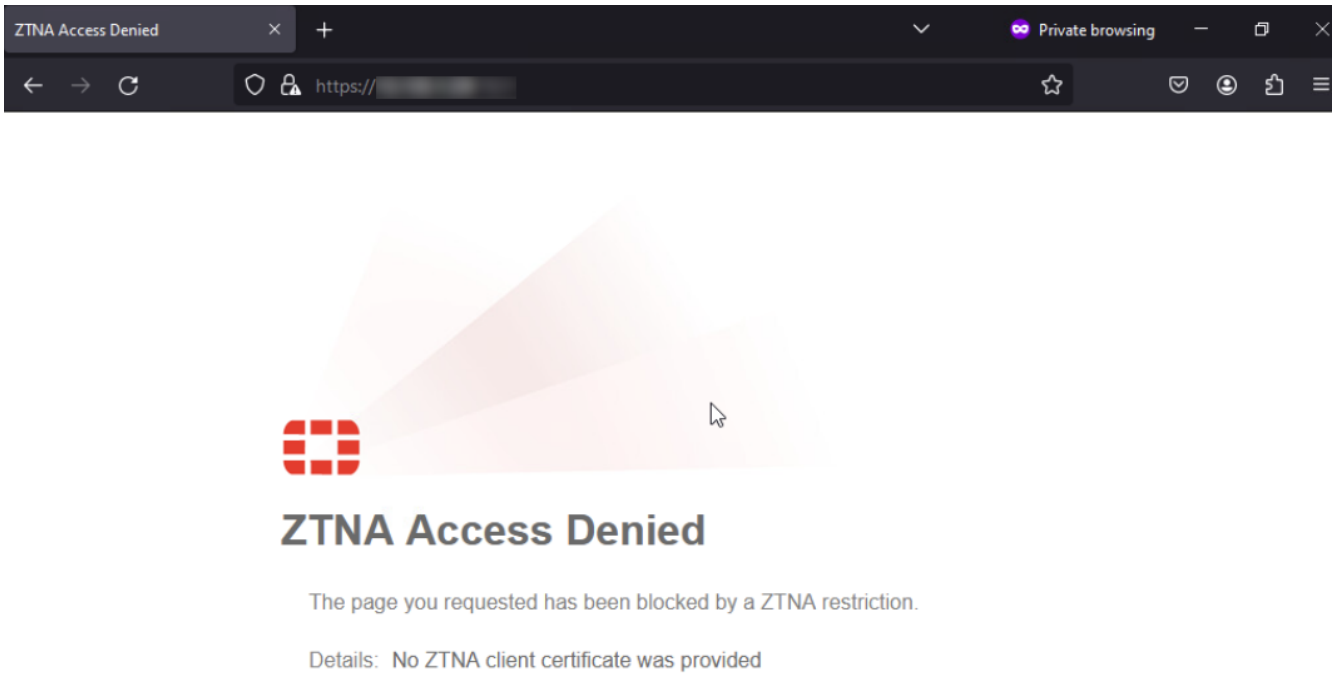


Result:

The client passes SSL certificate authentication and is allowed to access the website.

Scenario 2:

When prompted for the client certificate, the client clicks *Cancel*, resulting in an empty certificate response to the access proxy.



Result:

Because the certificate response is empty and `empty-cert-action` is set to `block`, the WAD daemon blocks the connection.

Currently, the Microsoft Edge, Google Chrome, and Safari browsers are supported by ZTNA.

Basic ZTNA configuration

To deploy full ZTNA, configure the following components on the FortiProxy unit:

1. Configure a FortiClient EMS connector on page 247
2. Configure a ZTNA server on page 250
3. Configure a ZTNA rule on page 254
4. Configure a firewall policy for full ZTNA on page 256
5. Optional authentication on page 258

To configure ZTNA in the GUI, go to *System* > *Feature Visibility* and enable *Zero Trust Network Access*.

Configure a FortiClient EMS connector

To add an on-premise FortiClient EMS server in the GUI:

1. Go to *Security Fabric* > *Fabric Connectors*.
2. Click *Create New* and click *FortiClient EMS*.
3. Enter a name for the connector and the IP address or FQDN of the EMS.
4. Click *OK*.
5. A window appears to verify the EMS server certificate. Click *Accept*.

To add an on-premise FortiClient EMS server in the CLI:

```
config endpoint-control fctems
    edit <id>
        set server <server IP or domain>
    next
end
```

A FortiProxy can connect a maximum of five EMS servers. An EMS ZTNA tag can resolve to a maximum of 100,000 IP addresses and 3,000 MAC addresses.

To verify address information, use the following diagnose commands: `# diagnose firewall fqdn <option>`.

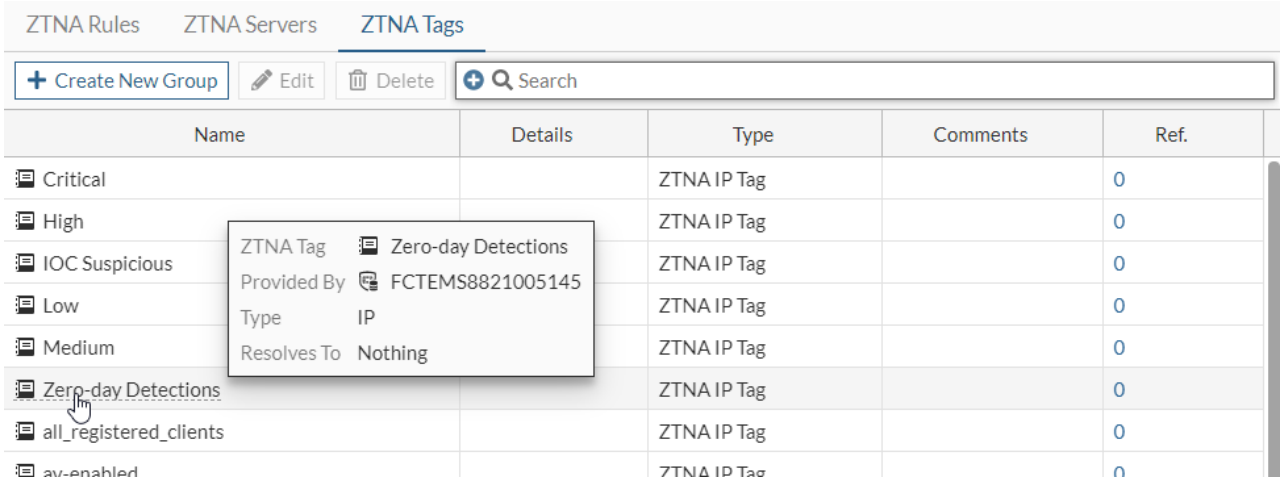
Option	Description
`list-ip`	List IP FQDN information.
`list-mac`	List MAC FQDN information.
`list-all`	List FQDN information.
`getinfo-ip`	Get information of IP FQDN address.
`getinfo-mac`	Get information of MAC FQDN address.
`get-ip`	Get and display one IP FQDN address.
`get-mac`	Get and display one MAC FQDN address.

ZTNA tags

After the FortiProxy unit connects to the FortiClient EMS, it automatically synchronizes ZTNA tags.

To view the synchronized ZTNA tags in the GUI:

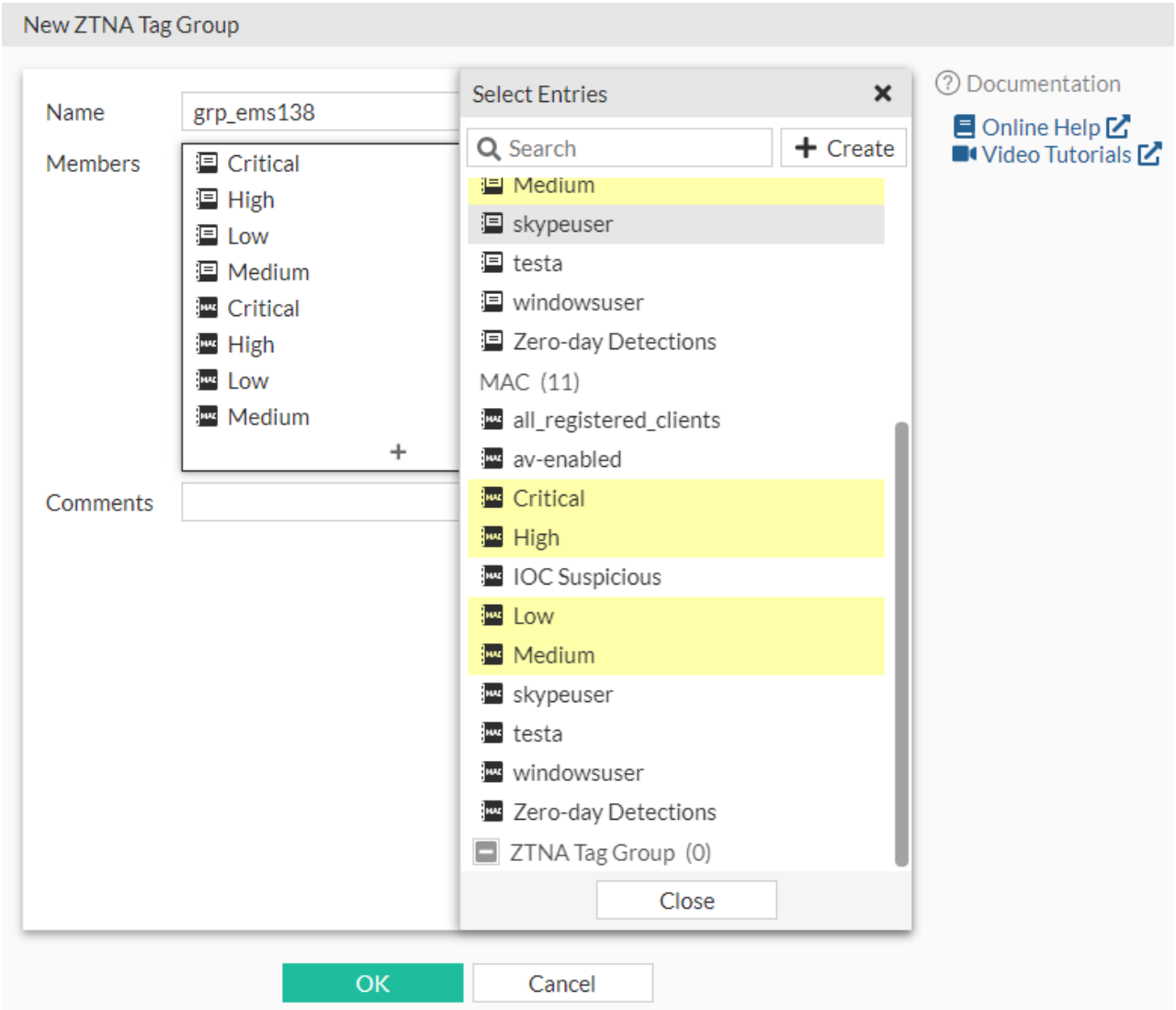
1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Tags* tab.
2. Hover the cursor over a tag name to view more information about the tag, such as its resolved addresses.



To create a ZTNA tag group in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Tags* tab.
2. Click *Create New Group*.

3. Enter a name for the group and select the group members.



4. Click *OK*.

To create a ZTNA tag group in the CLI:

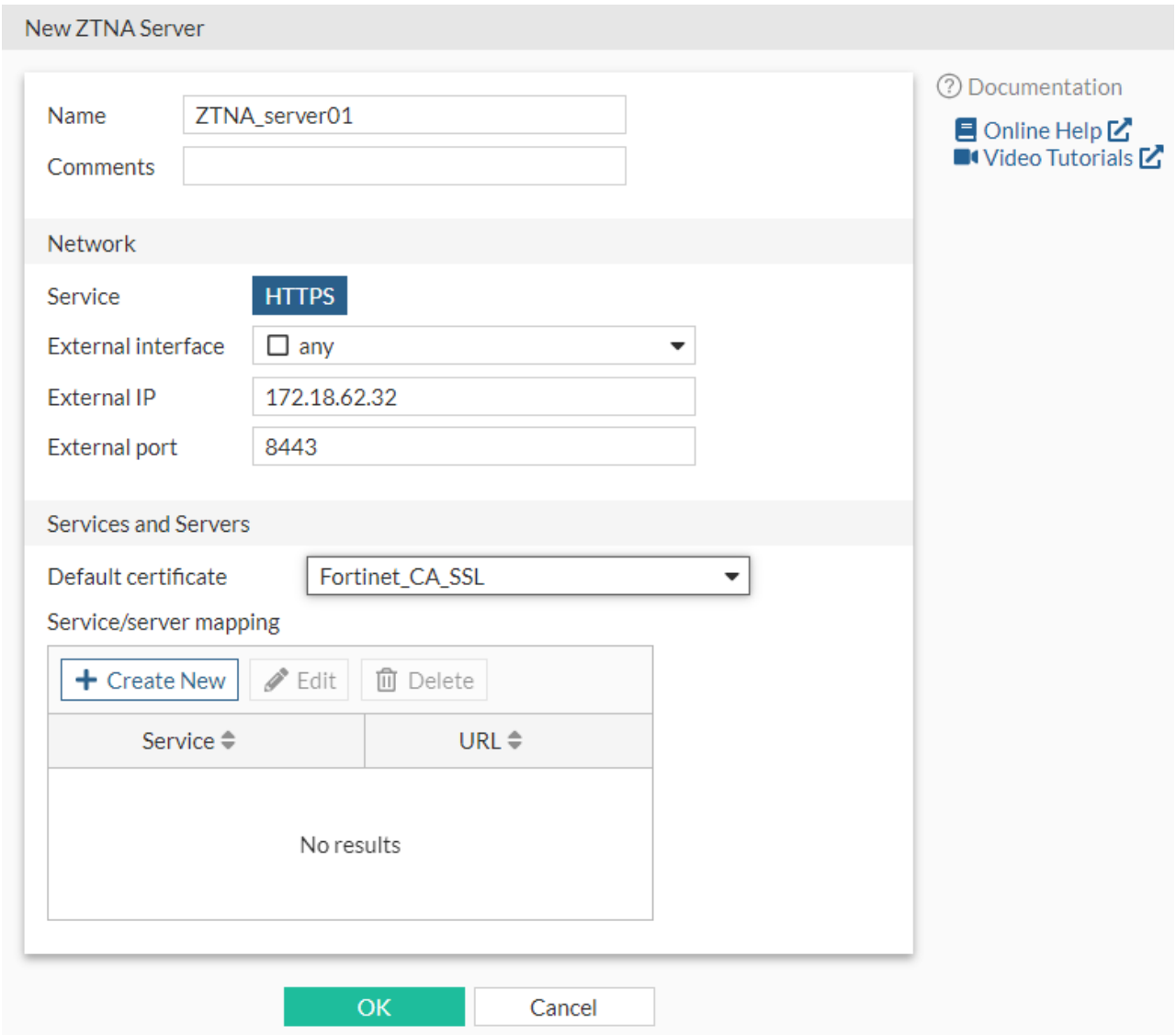
```
config firewall addrgrp
    edit <group name>
        set category ztna-ems-tag
        set member <members>
    next
end
```

Configure a ZTNA server

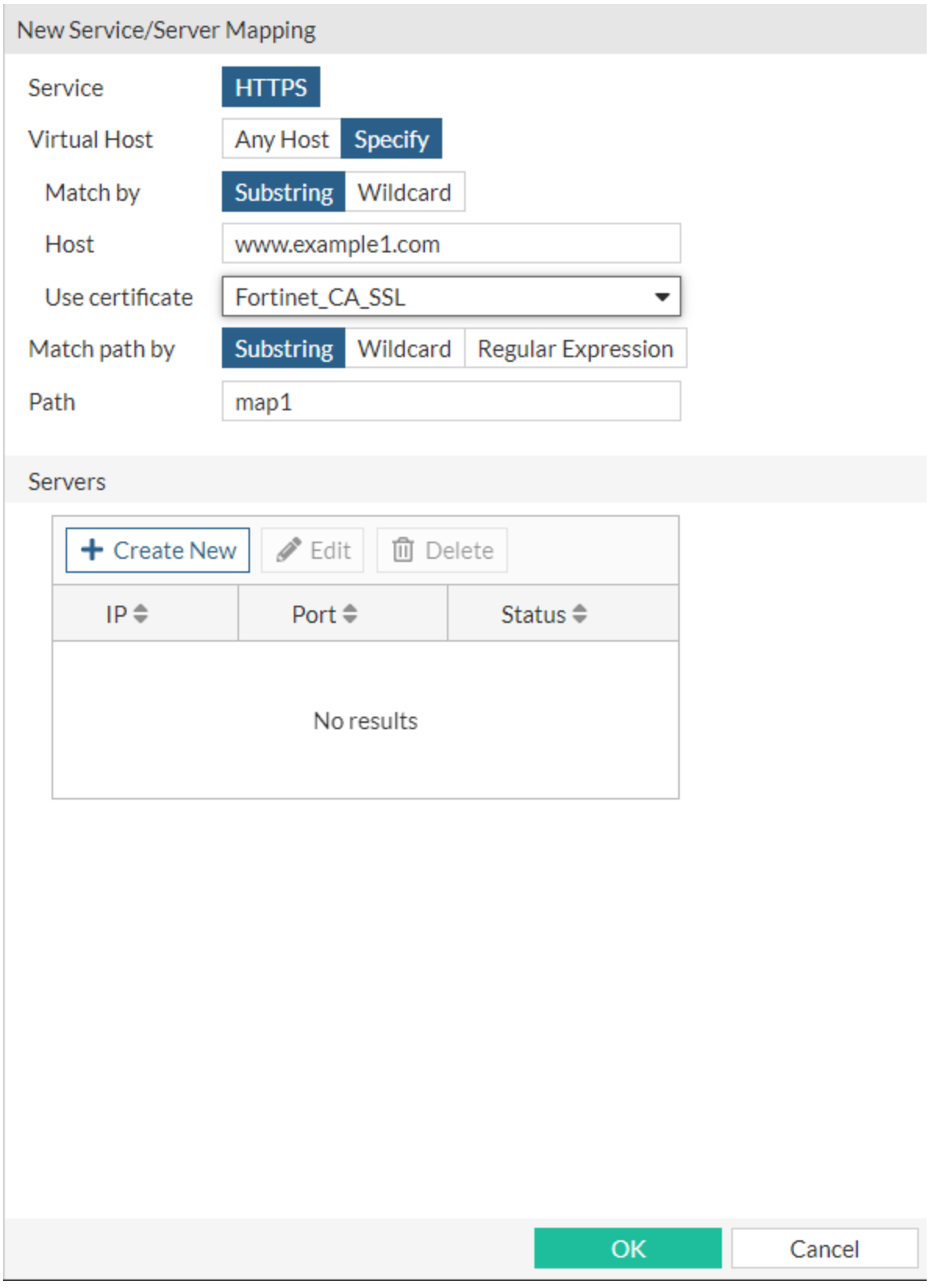
To configure a ZTNA server, define the access proxy VIP and the real servers that clients will connect to. The access proxy VIP is the FortiProxy ZTNA gateway that clients make HTTPS connections to. The service/server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

To create a ZTNA server and access proxy VIP in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Servers* tab.
2. Click *Create New*.
3. Enter a name for the server.
4. Select an external interface, enter the external IP address, and select the external port that the clients will connect to.
5. Select the *Default certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.



6. Add server mapping:
   a. In the *Service/server mapping* table, click *Create New*.
   b. Set *Virtual Host* to *Any Host* or *Specify*.
      - *Any Host*: Any request that resolves to the access proxy VIP will be mapped to your real servers. For example, if both www.example1.com and www.example2.com resolve to the VIP, then both requests are mapped to your real servers.
      - *Specify*: Enter the name or IP address of the host that the request must match. For example, if www.example1.com is entered as the host, then only requests to www.example1.com will match.
   c. Configure the path as needed.
      The path can be matched by substring, wildcard, or regular expression. For example, if the virtual host is specified as www.example1.com, and the path substring is map1, then www.example1/map1 will be matched.


New Service/Server Mapping
Service
HTTPS
Virtual Host
Any Host
Specify
Match by
Substring
Wildcard
Host
www.example1.com
Use certificate
Fortinet_CA_SSL
Match path by
Substring
Wildcard
Regular Expression
Path
map1
Servers
Create New
Edit
Delete
IP
Port
Status
No results
OK
Cancel

d. Add a server:
   i. In the *Servers* table, click *Create New*.
   ii. Enter the server IP address and port number.
   iii. Set the server status.
   iv. Click *OK*.
   v. Add more servers as needed.
e. Click *OK*.
f. Add more server mappings as needed.

7. Click *OK*.

To create a ZTNA server and access proxy VIP in the CLI:

1. Configure an access proxy VIP:

```
config firewall vip
    edit <name>
        set type access-proxy
        set extip <external_IP_address>
        set extintf <external interface>
        set server-type https
        set extport <external_port_number>
        set ssl-certificate <certificate>
    next
end
```

2. If the virtual host is specified, configure the virtual host:

```
config firewall access-proxy-virtual-host
    edit <auto generated when configured from GUI>
        set ssl-certificate <certificate>
        set host <host_name_or_IP_address>
        set host-type {sub-string | wildcard}
    next
end
```

3. Configure the server and path mapping:

```
config firewall access-proxy
    edit <name>
        set vip <virtual_IP_name>
        set client-cert {enable | disable}
        set empty-cert-action {accept | block}
        config api-gateway
            edit 1
                set url-map <mapped_path>
                set service {http | https | tcp-forwarding | samlsp}
                set virtual-host <name_of_virtual_host_if_specified>
                set url-map-type {sub-string | wildcard | regex}
                config realservers
                    edit 1
```

```
                        set ip <IP_address_of_real_server>
                        set port <port>
                        set status {active | standby | disable}
                        set health-check {enable | disable}
                    next
                end
                set ldb-method static
                set persistence none
                set ssl-dh-bits 2048
                set ssl-algorithm high
                set ssl-min-version tls-1.1
                set ssl-max-version tls-1.3
            next
        end
    next
end
```

The load balance method for the real servers can only be specified in the CLI.

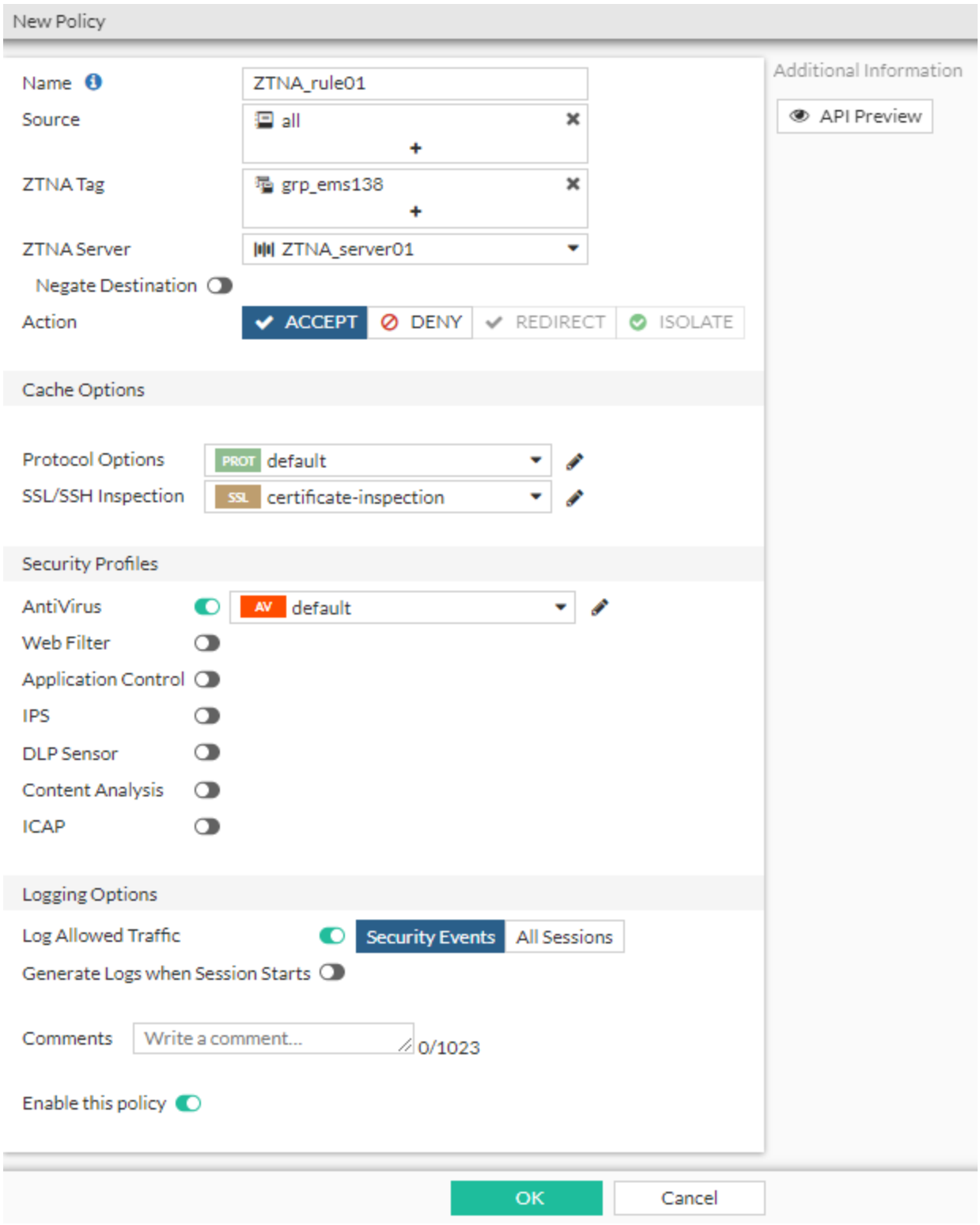
Configure a ZTNA rule

A ZTNA rule is a proxy policy used to enforce access control. ZTNA tags or tag groups can be defined to enforce zero trust role based access. Security profiles can be configured to protect this traffic.

To configure a ZTNA rule in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Rules* tab.
2. Click *Create New*.
3. Enter a name for the rule.
4. Add the ZTNA tags or tag groups that are allowed access.

5. Select the ZTNA server.



6. Configure the remaining options as needed.
7. Click *OK*.

To configure a ZTNA rule in the CLI:

```
config firewall policy
    edit 1
        set type access-proxy
        set name <ZTNA rule name>
        set access-proxy <access_proxy>
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag <ZTNA_tag(s)>
        set action accept
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set ssl-ssh-profile <inspection_profile>
    next
end
```

Configure a firewall policy for full ZTNA

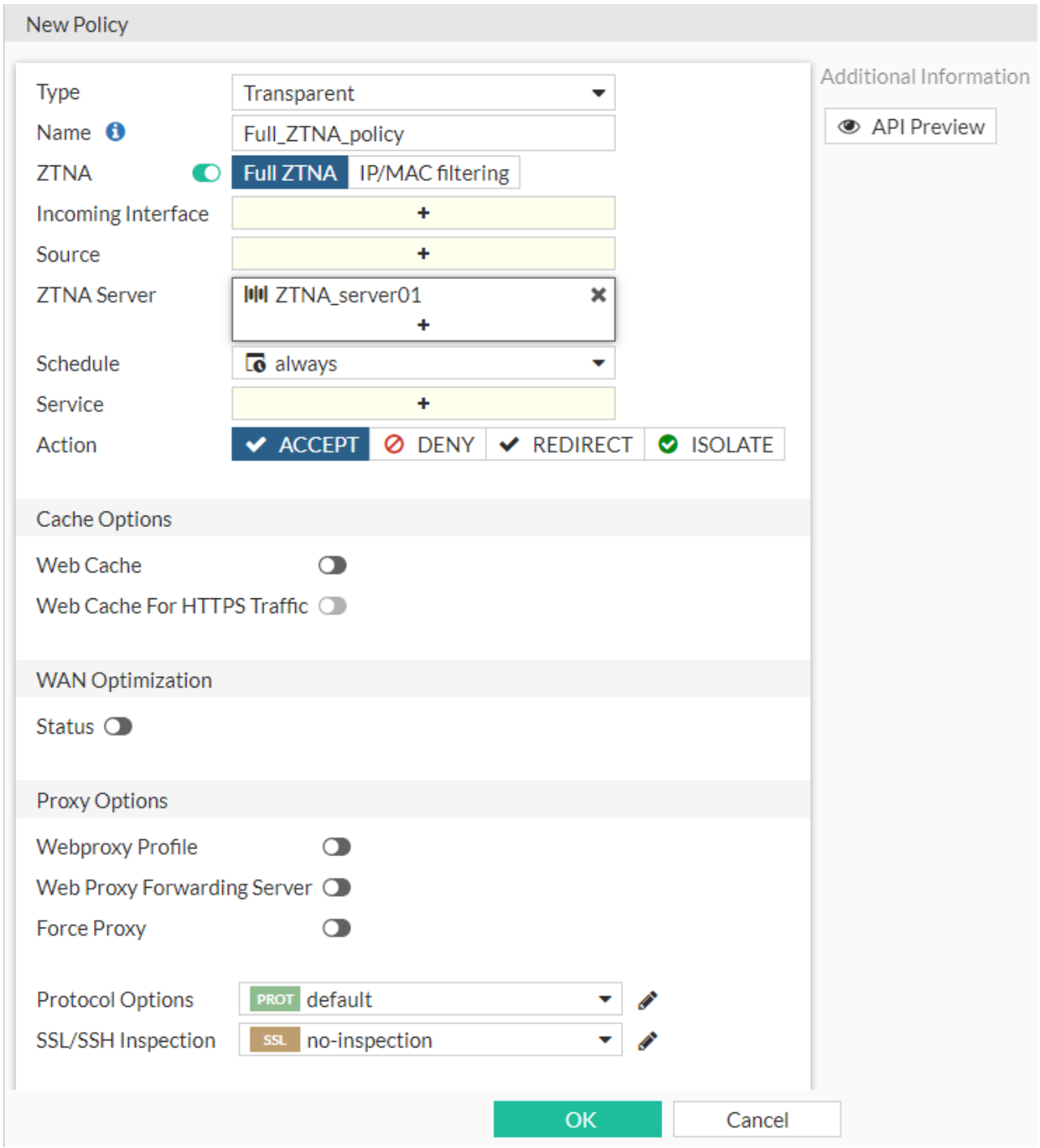
The firewall policy matches and redirects client requests to the access proxy VIP. The source interface and addresses that are allowed access to the VIP can be defined. By default, the destination is any interface, so once a policy is configured for full ZTNA, the policy list will be organized by sequence.

UTM processing of the traffic happens at the ZTNA rule.

To configure a firewall policy for full ZTNA in the GUI:

1. Go to *Policy & Objects* > *Policy* and click *Create New*.
2. Enter a name for the policy.
3. Enable *ZTNA* and select *Full ZTNA*.

4. Set *ZTNA Server* to the configured ZTNA server.



5. Configure the remaining settings as needed.
6. Click *OK*.

To configure a firewall policy for full ZTNA in the CLI:

```
config firewall policy
    edit <policy ID>
       set name <policy_name>
        set srcintf <source_interface>
        set dstintf "any"
        set srcaddr <source_address>
        set dstaddr <access_proxy_virtual_IP>
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

Optional authentication

To configure authentication to the access proxy, you must configure an authentication scheme and authentication rule in the CLI. They are used to authenticate proxy-based policies, similar to configuring authentication for explicit and transparent proxy.

The authentication scheme defines the method of authentication that is applied. For ZTNA, basic HTTP and SAML methods are supported. Each method has additional settings to define the data source to check against. For example, with basic HTTP authentication, a user database can reference an LDAP server, RADIUS server, local database, or other supported authentication servers that the user is authenticated against.

The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. For ZTNA, active authentication method is supported. The active authentication method references a scheme where users are actively prompted for authentication, like with basic authentication.

After the authentication rule triggers the method to authenticate the user, a successful authentication returns the groups that the user belongs to. In the ZTNA rule and proxy policy you can define a user or user group as the allowed source. Only users that match that user or group are allowed through the proxy policy.

To configure a basic authentication scheme:

```
config authentication scheme
    edit <name>
        set method basic
        set user-database <authentication_server>
    next
end
```

To configure an authentication rule:

```
config authentication rule
    edit <name>
        set status enable
        set protocol http
        set srcintf <interface>
        set srcaddr <address>
        set dstaddr <address>
        set ip-based enable
        set active-auth-method <active_authentication_scheme>
    next
end
```

To apply a user group to a ZTNA rule in the GUI:

1. Go to *Policy & Objects > ZTNA* and select the *ZTNA Rules* tab.
2. Edit an existing rule or click *Create New* to create a new rule.
3. Click in the *Source* field, select the *User* tab, and select the users and user groups that will be allowed access.
4. Configure the remaining settings as required.
5. Click *OK*.

To apply a user group to a ZTNA rule in the CLI:

```
config firewall policy
    edit <policy ID>
        set name <ZTNA rule name>
        set type access-proxy
        set access-proxy <access proxy>
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag <ZTNA tags>
        set action accept
        set schedule "always"
        set logtraffic all
        set groups <user group>
        set utm-status enable
        set ssl-ssh-profile <inspection profile>
    next
end
```

The authentication rule and scheme defines the method used to authenticate users. With basic HTTP authentication, a sign in prompt is shown after the client certificate prompt. After the authentication passes, the returned groups that the user is a member of are checked against the user groups that are defined in the ZTNA rule. If a group matches, then the user is allowed access after passing a posture check.

ZTNA advanced configurations

This section includes the following ZTNA advanced configurations:

- ZTNA policy access control of unmanageable and unknown devices on page 260
- HTTP2 connection coalescing and concurrent multiplexing for ZTNA on page 264
- ZTNA traffic forwarding proxy on page 267
- ZTNA agentless web-based application access on page 279

ZTNA policy access control of unmanageable and unknown devices

The ZTNA application gateway can determine whether a client device that does not have FortiClient installed is a mobile device that is considered unmanageable, or is not a mobile device that is considered unknown. The ZTNA access proxy tags the device as either `EMS_ALL_UNMANAGEABLE_CLIENTS` or `EMS_ALL_UNKNOWN_CLIENTS` respectively. The FortiProxy WAD process achieves this by either matching device TLS fingerprints against a library or learning information from the HTTP User-Agent header if the `set user-agent-detect` setting is enabled.

Configuring the ZTNA access proxy and proxy policy

The `EMS_ALL_UNMANAGEABLE_CLIENTS` and `EMS_ALL_UNKNOWN_CLIENTS` tags allow for ZTNA access control of unmanageable and unknown devices using a proxy policy. The `accept-unmanageable` option for the `empty-cert-action` setting allows unmanageable clients to continue ZTNA proxy rule processing.

```
config firewall access-proxy
    edit <name>
        set client-cert enable
        set user-agent-detect {enable | disable}
        set empty-cert-action {accept | block | accept-unmanageable}
     next
end
```

`client-cert {enable | disable}`	Enable requesting client certificate.
`user-agent-detect {enable | disable}`	Enable/disable detecting the device type by HTTP User-Agent if no client certificate is provided (default = enable).
`empty-cert-action {accept | block | accept-unmanageable}`	Set the action for an empty client certificate: • `accept`: accept the SSL handshake if the client certificate is empty. • `block`: block the SSL handshake if the client certificate is empty. • `accept-unmanageable`: accept the SSL handshake only if the end point is unmanageable.

The user-agent-detect and empty-cert-action settings can only be configured in the CLI.

```
config firewall proxy-policy
    edit <id>
        set ztna-ems-tag {EMS_ALL_UNMANAGEABLE_CLIENTS | EMS_ALL_UNKNOWN_CLIENTS}
    next
end
```

ztna-ems-tag {EMS_ALL_UNMANAGEABLE_CLIENTS | EMS_ALL_UNKNOWN_CLIENTS}	Set the EMS tag names: • EMS_ALL_UNMANAGEABLE_CLIENTS: match any device that is unmanageable. • EMS_ALL_UNKNOWN_CLIENTS: match any device that is not recognized.

Consider the following use cases.

- Case 1: if a client device sends a TLS client hello in a mobile pattern, then WAD will try to match its TLS fingerprint with a WAD original library and mark it with an EMS_ALL_UNMANAGEABLE_CLIENTS tag.
- Case 2: if WAD cannot match the TLS fingerprint with an original library but user-agent-detect is enabled (under config firewall access-proxy), WAD will try to learn the device type from client request's User-Agent header. If it matches a mobile device, then it is still marked with an EMS_ALL_UNMANAGEABLE_CLIENTS tag.
- Case 3: if WAD cannot match the TLS fingerprint with an existing original or temporary library, or cannot learn it from User-Agent header, or user-agent-detect is disabled, then it will mark the device as EMS_ALL_UNKNOWN_CLIENTS.

In the access proxy settings, if empty-cert-action is set to accept-unmanageable, then only case 1 and 2 would go through the proxy policy. Case 3 would be denied, and a replacement message page would appear.

To configure ZTNA policy access control of unmanageable devices:

1. Configure the client certificate actions:

```
config firewall access-proxy
    edit "zt1"
        set vip "zt1"
        set client-cert enable
        set user-agent-detect enable
        set auth-portal disable
        set empty-cert-action accept
        set log-blocked-traffic disable
        set add-vhost/domain-to-dnsdb disable
        set decrypted-traffic-mirror ''
    next
end
```

2. Configure the proxy policy with the ZTNA EMS tag to control device access:

```
config firewall proxy-policy
    edit 1
```

```
        set access-proxy "zt1"
        set srcintf "port2" "ag2"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "EMS_ALL_UNMANAGEABLE_CLIENTS"
    next
end
```

Configuring dynamic address local tags

Like other ZTNA tags,EMS_ALL_UNMANAGEABLE_CLIENTS and EMS_ALL_UNKNOWN_CLIENTS are dynamic addresses on the FortiProxy. The following diagnostic commands can be used to view local tag information:

- `diagnose firewall dynamic address`: a list of unmanageable and unknown clients' IP addresses associated with the EMS_ALL_MANAGEABLE_CLIENTS and EMS_ALL_UNKNOWN_CLIENTS dynamic addresses, respectively, is displayed.
- `diagnose user-device-store device memory list`: when device detection is enabled on a FortiProxy interface that has a layer 2 connection to unmanageable and unknown device clients, then a client's device information is displayed.

To verify the list of dynamic firewall addresses in the CLI:

```
(vdom1) # diagnose firewall dynamic address
List all dynamic addresses:
IP dynamic addresses in VDOM vdom1(vfid: 1):
...
CMDB name: EMS_ALL_UNMANAGEABLE_CLIENTS
EMS_ALL_UNMANAGEABLE_CLIENTS: ID(101)
        ADDR(10.1.100.22)
Total IP dynamic range blocks: 1.
Total IP dynamic addresses: 1.
CMDB name: EMS_ALL_UNKNOWN_CLIENTS
EMS_ALL_UNKNOWN_CLIENTS: ID(154)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 0.
...
```

To verify the client device information in the CLI:

```
(vdom1) # diagnose user-device-store device memory list
Record #1:
         ...
        device_info
                ...
                'is_online' = 'true'
                'is_ems_registered' = 'false'
                'active_start_time' = '1668811449'
```

```
                'is_fortiguard_src' = 'false'
                'tags' = 'EMS_ALL_UNMANAGEABLE_CLIENTS'
                ...
        interface_info
        ...
```

To view the local tag information in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Tags* tab.
2. Hover over a tag to view the tooltip, which displays matched endpoints and resolved addresses.

To apply a local tag in a ZTNA rule:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Rules* tab.
2. Click *Create New*, or select and edit an existing entry.
3. In the *ZTNA Tag* field, click the *+* to add tags. The local tags appear in the *IP* section.
4. Configure the other settings as needed.
5. Click *OK*.

Local tag information is also available in the following GUI widgets and pages:

- *Dashboard* > *FortiClient* widget
- *Security Fabric* > *Asset Identity Center* page

Viewing ZTNA traffic logs

ZTNA traffic logs include the following fields related to unmanageable and unknown devices.

- Client connection status with EMS server with possible values of unknown, offline, or online:
  - CLI = `emsconnection`
  - GUI = *EMS Connection*
- Device manageability status with possible values of unknown, manageable, or unmanageable:
  - CLI = `clientdevicemanageable`
  - GUI = *Client Device Manageable*

The device manageability status can have one of the following values:

- Unknown: traffic from a client with an unknown TLS fingerprint and where the user agent information is not available for learning.
- Manageable: traffic from a non-mobile device (platform or operating system), with a known TLS fingerprint, or where the user agent information is available for learning.
- Unmanageable: traffic from a mobile device with a known mobile TLS fingerprint or user agent information is available for learning.

To view the ZTNA traffic logs in the CLI:

```
(vdom1)# execute log filter category 0
(vdom1)# execute log filter field subtype ztna
```

```
(vdom1)# execute log display

1: date=2022-11-18 time=14:23:57 eventtime=1668810238188622828 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="vdom1" srcip=10.1.100.22 srcport=41400
srcintf="port2" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.16.200.207 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=12147
service="HTTPS" proxyapptype="http" proto=6 action="accept" policyid=1 policytype="proxy-policy"
poluuid="03a79dd2-6775-51ed-19a0-444a0314f1a0" policyname="ztna_rule_mobile" duration=0
gatewayid=1 vip="ztna_server" accessproxy="ztna_server" clientdeviceid="pf-mobile;os-unknown;app-
safari" clientdevicemanageable="unmanageable" clientdevicetags="EMS_ALL_UNMANAGEABLE_CLIENTS"
emsconnection="unknown" wanin=1884 rcvdbyte=1884 wanout=833 lanin=960 sentbyte=960 lanout=3046
fctuid="pf-mobile;os-unknown;app-safari" appcat="unscanned"

3: date=2022-11-18 time=14:23:52 eventtime=1668810232937847134 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="vdom1" srcip=10.1.100.22 srcport=46392
srcintf="port2" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.16.200.209 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=12144
service="HTTPS" proxyapptype="http" proto=6 action="accept" policyid=2 policytype="proxy-policy"
poluuid="141b7db8-6785-51ed-32a5-58d696e60e2d" duration=0 gatewayid=1 vip="ztna_server2"
accessproxy="ztna_server2" clientdeviceid="pf-pc;os-unknown;app-curl"
clientdevicemanageable="manageable" clientdevicetags="EMS_ALL_UNKNOWN_CLIENTS"
emsconnection="unknown" wanin=1907 rcvdbyte=1907 wanout=699 lanin=861 sentbyte=861 lanout=3089
fctuid="pf-pc;os-unknown;app-curl" appcat="unscanned"

5: date=2022-11-18 time=14:23:42 eventtime=1668810222897968134 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="vdom1" srcip=10.1.100.22 srcport=46390
srcintf="port2" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.18.62.68 dstport=4443 dstintf="vdom1" dstintfrole="undefined" sessionid=12134
service="tcp/4443" proxyapptype="http" proto=6 action="deny" policyid=0 policytype="proxy-policy"
duration=0 vip="ztna_server2" accessproxy="ztna_server2" clientdevicemanageable="unknown"
msg="Denied: failed to match a proxy-policy" wanin=0 rcvdbyte=0 wanout=0 lanin=806 sentbyte=806
lanout=2661 appcat="unscanned" crscore=30 craction=131072 crlevel="high"
```

To view the ZTNA traffic logs in the GUI:

1. Go to *Log & Report > ZTNA Traffic*.
2. Select an entry and click *Details*.
3. Check the *Client Device Manageable* and *EMS Connection* fields.

HTTP2 connection coalescing and concurrent multiplexing for ZTNA

HTTP2 connection coalescing and concurrent multiplexing allows multiple HTTP2 requests to share the same TLS connection when the destination IP is the same, and the host names are compatible in the certificate. In ZTNA scenarios, the FortiProxy application gateway may accept multiple HTTP2 requests to the same ZTNA server destined to different virtual hosts on the same real server. These HTTP2 requests can share the same TLS connection between the FortiProxy and the real server so that the handshake does not need to be performed multiple times for multiple connections.

In order for the FortiProxy to match the SNI (Server Name Indication), this SNI value must appear under the SAN extension on the server certificate. Configuring the SNI value under the CN alone will not work.

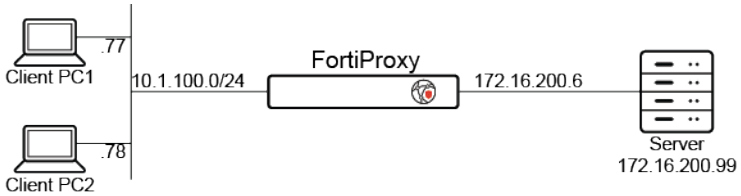
To configure the ZTNA access proxy:

```
config firewall access-proxy
    edit <name>
        set http-supported-max-version {http1 | http2}
        set svr-pool-multiplex {enable | disable}
        set svr-pool-ttl <integer>
        set svr-pool-server-max-request <integer>
    next
end
```

`http-supported-max-version {http1 | http2}`	Set the maximum supported HTTP version: • http1: support HTTP 1.1 and HTTP1. • http2: support HTTP2, HTTP 1.1, and HTTP1 (default).
`svr-pool-multiplex {enable | disable}`	Enable/disable server pool multiplexing. When enabled, share the connected server in HTTP, HTTPS, and web portal API gateway.
`svr-pool-ttl <integer>`	Set the time-to-live in the server pool for idle connections to servers (in seconds, 0 - 2147483647, default = 15).
`svr-pool-server-max-request <integer>`	Set the maximum number of requests that servers in server pool handle before disconnecting (0 - 2147483647, default = 0).

Example

In this example, multiple clients submit requests in HTTP2. The requests hit the VIP address, and then FortiProxy opens a session between itself (172.16.200.6) and the server (172.16.200.99). The coalescing occurs in this session as the multiple streams share the same TLS session to connect to the same destination server.



To configure connection coalescing and concurrent multiplexing with ZTNA:

1. Configure the VIP:

```
config firewall vip
    edit "vip-ztna"
        set type access-proxy
```

```
        set extip 10.1.100.223
        set extintf "port2"
        set server-type https
        set extport 443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure the ZTNA server and path mapping:

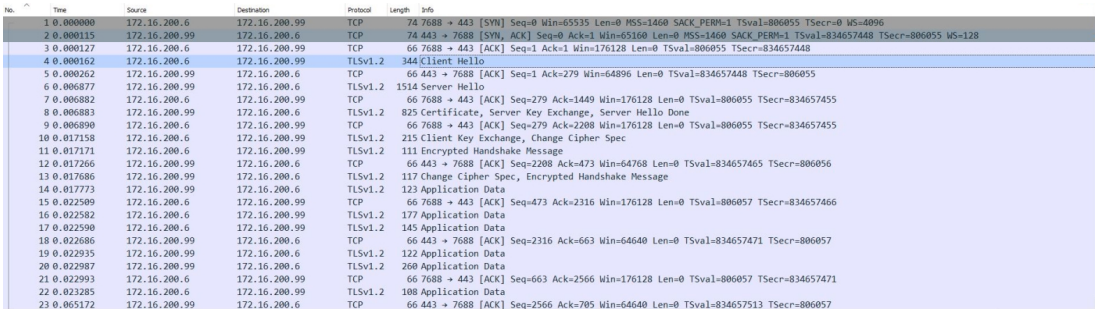
```
config firewall access-proxy
    edit "ztna"
        set vip "vip-ztna"
        set client-cert disable
        set svr-pool-multiplex enable
        set http-supported-max-version http2
        config api-gateway
            edit 1
                set url-map "/a"
                set virtual-host "a.ftnt.com"
                config realservers
                    edit 1
                        set ip 172.16.200.99
                    next
                end
            next
            edit 2
                set url-map "/b"
                set virtual-host "b.ftnt.com"
                config realservers
                    edit 1
                        set ip 172.16.200.99
                    next
                end
            next
        end
    next
end
```

3. Configure the ZTNA policy:

```
config firewall proxy-policy
    edit 3
        set proxy access-proxy
        set access-proxy "ztna"
        set srcintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set logtraffic all
        set utm-status enable
```

```
        set ssl-ssh-profile "deep-inspection-clone"
        set av-profile "av"
    next
end
```

4. Get the clients to access a.ftnt.com and b.ftnt.com. The clients share access with the same real server and certificate (CN=*.ftnt.com). The FortiProxy shares the first TLS connection with second TLS connection.
5. Verify the sniffer packet capture on the FortiProxy server side. There is one client hello.

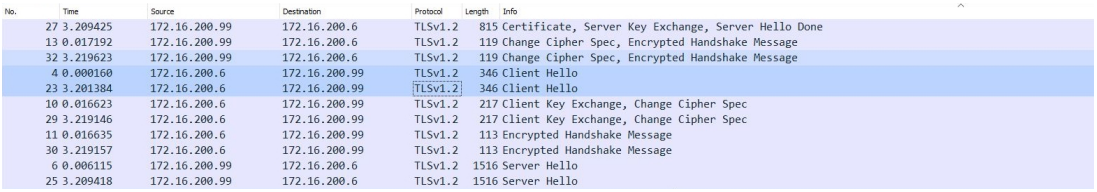


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.200.6	172.16.200.99	TCP	74	7688 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=806055 TSecr=0 WS=4096
2	0.000115	172.16.200.99	172.16.200.6	TCP	74	443 → 7688 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=834657448 TSecr=806055 WS=128
3	0.000127	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=806055 TSecr=834657448
4	0.000162	172.16.200.6	172.16.200.99	TLSv1.2	344	Client Hello
5	0.000262	172.16.200.99	172.16.200.6	TCP	66	443 → 7688 [ACK] Seq=1 Ack=279 Win=64896 Len=0 TSval=834657448 TSecr=806055
6	0.006877	172.16.200.99	172.16.200.6	TLSv1.2	1514	Server Hello
7	0.006882	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=279 Ack=1449 Win=176128 Len=0 TSval=806055 TSecr=834657455
8	0.006883	172.16.200.99	172.16.200.6	TLSv1.2	825	Certificate, Server Key Exchange, Server Hello Done
9	0.006890	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=279 Ack=2208 Win=176128 Len=0 TSval=806055 TSecr=834657455
10	0.017158	172.16.200.6	172.16.200.99	TLSv1.2	215	Client Key Exchange, Change Cipher Spec
11	0.017171	172.16.200.6	172.16.200.99	TLSv1.2	111	Encrypted Handshake Message
12	0.017266	172.16.200.99	172.16.200.6	TCP	66	443 → 7688 [ACK] Seq=2208 Ack=473 Win=64768 Len=0 TSval=834657465 TSecr=806056
13	0.017686	172.16.200.99	172.16.200.6	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
14	0.017773	172.16.200.99	172.16.200.6	TLSv1.2	123	Application Data
15	0.022509	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=473 Ack=2316 Win=176128 Len=0 TSval=806057 TSecr=834657466
16	0.022582	172.16.200.6	172.16.200.99	TLSv1.2	177	Application Data
17	0.022590	172.16.200.6	172.16.200.99	TLSv1.2	145	Application Data
18	0.022686	172.16.200.99	172.16.200.6	TCP	66	443 → 7688 [ACK] Seq=2316 Ack=663 Win=64640 Len=0 TSval=834657471 TSecr=806057
19	0.022935	172.16.200.99	172.16.200.6	TLSv1.2	122	Application Data
20	0.022987	172.16.200.99	172.16.200.6	TLSv1.2	260	Application Data
21	0.022993	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=663 Ack=2566 Win=176128 Len=0 TSval=806057 TSecr=834657471
22	0.023285	172.16.200.6	172.16.200.99	TLSv1.2	108	Application Data
23	0.065172	172.16.200.99	172.16.200.6	TCP	66	443 → 7688 [ACK] Seq=2566 Ack=705 Win=64640 Len=0 TSval=834657513 TSecr=806057

6. Disable server pool multiplexing:

```
config firewall access-proxy
    edit "ztna"
        set vip "vip-ztna"
        set svr-pool-multiplex disable
    next
end
```

7. Verify the sniffer packet capture. This time, the FortiProxy does not coalesce the TLS connection, so there are two client hellos.



No.	Time	Source	Destination	Protocol	Length	Info
27	3.209425	172.16.200.99	172.16.200.6	TLSv1.2	815	Certificate, Server Key Exchange, Server Hello Done
13	0.017192	172.16.200.99	172.16.200.6	TLSv1.2	119	Change Cipher Spec, Encrypted Handshake Message
32	3.219623	172.16.200.99	172.16.200.6	TLSv1.2	119	Change Cipher Spec, Encrypted Handshake Message
4	0.000160	172.16.200.6	172.16.200.99	TLSv1.2	346	Client Hello
23	3.201384	172.16.200.6	172.16.200.99	TLSv1.2	346	Client Hello
10	0.016623	172.16.200.6	172.16.200.99	TLSv1.2	217	Client Key Exchange, Change Cipher Spec
29	3.219146	172.16.200.6	172.16.200.99	TLSv1.2	217	Client Key Exchange, Change Cipher Spec
11	0.016635	172.16.200.6	172.16.200.99	TLSv1.2	113	Encrypted Handshake Message
30	3.219157	172.16.200.6	172.16.200.99	TLSv1.2	113	Encrypted Handshake Message
6	0.006115	172.16.200.99	172.16.200.6	TLSv1.2	1516	Server Hello
25	3.209418	172.16.200.99	172.16.200.6	TLSv1.2	1516	Server Hello

ZTNA traffic forwarding proxy

For security-sensitive network services running on a host in cloud, partner site, or internal network, the host does not have any open ports to be detected by a network scanner or DDOS attacker. Instead, the host relies on a ZTNA service connector to facilitate outbounding connection to a ZTNA access proxy and connect to the network service. Below is the process for a client to access the network service:

1. The client makes a connection to the ZTNA edge and requests to access the registered network service.
2. The ZTNA edge performs ZTNA check and enforces ZTNA policy. If the request is allowed, it signals the intention through control connection.

3. The ZTNA service connector triggers a connection to the ZTNA edge and another connection to the server.
4. The ZTNA edge forwards the request through ZTNA service connector to the server.

FortiProxy as a forward proxy

This applies when a FortiProxy is directly between a client and a server.

To configure FortiProxy as the ZTNA traffic forwarding proxy:

```
config firewall policy
       edit 15
              set type ztna-proxy
              set uuid c7207330-bc99-51ef-6ab2-be36a0752438
              set srcintf "any"
              set dstintf "any"
              set srcaddr "all"
              set dstaddr "all"
              set action accept
              set schedule "always"
              set ztna-proxy "ztfp"
              set logtraffic all
              set logtraffic-start enable
              set log-http-transaction enable
              set extended-log enable
              set ssl-ssh-profile "deep-inspection"
       next
end
config ztna traffic-forward-proxy
       edit "ztfp"
              set vip "vip1"
       next
end
config firewall vip
       edit "vip1"
              set uuid 526803fa-bca3-51ef-6362-2d8a9bb7b6e4
              set type access-proxy
              set server-type https
              set extip 10.121.1.209
              set extintf "any"
              set extport 8443
              set ssl-certificate "Fortinet_SSL"
       next
end
```

Example ZTNA log the FortiProxy:

```
date=2024-12-17 time=11:04:32 eventtime=1734462272753347831 tz="-0800" logid="0005000024"
      type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.121.1.27 srcport=55783
      srcintf="port5" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
      dstip=172.18.20.80 dstport=22 dstintf="port1" dstintfrole="undefined" sessionid=1392251262
      service="SSH" proxyapptype="http" proto=6 action="accept" policyid=15 policytype="proxy-
      policy" poluuid="c7207330-bc99-51ef-6ab2-be36a0752438" policyname="test1" clientip=10.121.1.27
      appcat="unscanned" duration=25 gatewayid=1 vip="vip1" clientdevicemanageable="unknown"
      clientcert="no" wanin=4738 rcvdbyte=4738 wanout=3540 lanin=4417 sentbyte=4417 lanout=6662
      fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794" unauthuser="guodong" unauthusersource="forticlient"
      srcremote=207.102.138.19
```

Example forward traffic log on the FortiProxy:

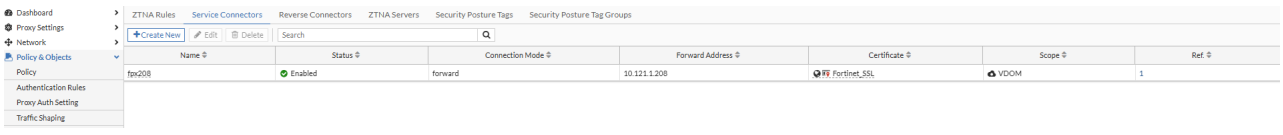
```
date=2024-12-17 time=11:04:07 eventtime=1734462247388211699 tz="-0800" logid="0000000015"
      type="traffic" subtype="forward" level="notice" vd="root" srcip=10.121.1.27 srcport=55783
      srcintf="port5" srcintfrole="undefined" dstip=172.18.20.80 clientip=10.121.1.27 dstport=22
      dstintf="port1" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
      sessionid=1392251262 proto=6 action="start" policyid=15 policytype="policy" poluuid="c7207330-
      bc99-51ef-6ab2-be36a0752438" policyname="test1" service="SSH" trandisp="noop"
      url="https://10.121.1.209/tcp?address=172.18.20.80&port=22&tls=1" agent="Forticlient"
      appcat="unscanned" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0
      fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794" unauthuser="guodong" unauthusersource="forticlient"
      srcremote=207.102.138.19
```

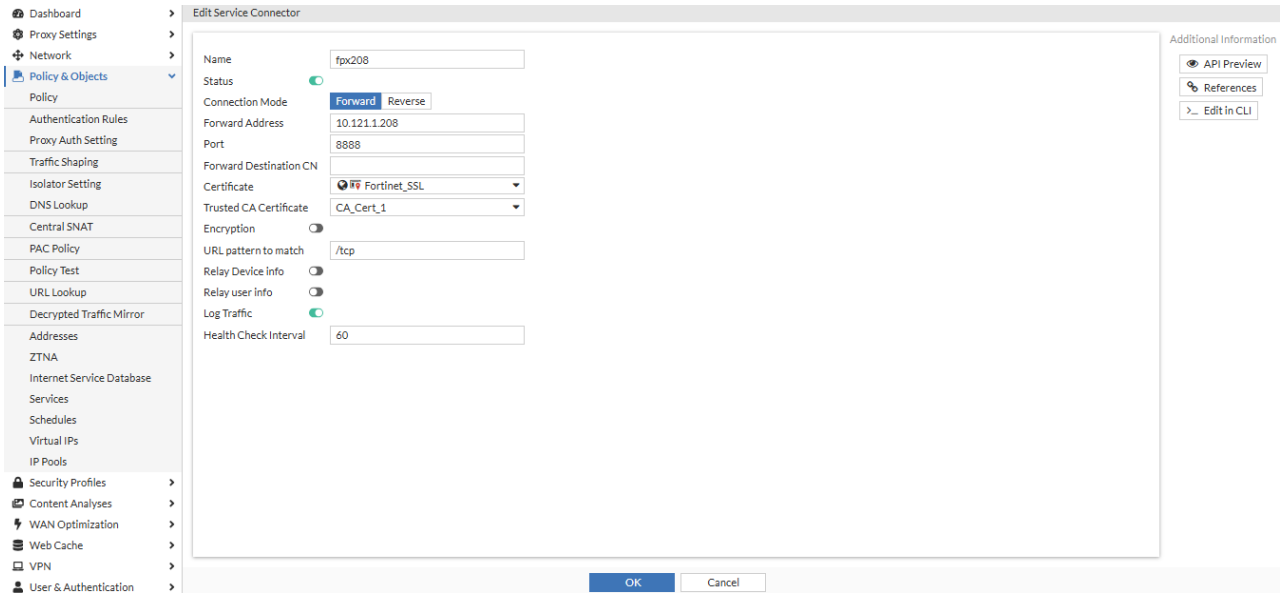
FortiProxy as proxy to a service connector

To configure FortiProxy as the proxy to a service connector:

1. Configure the first FortiProxy (209 in this example) as follows:

```
config firewall policy
       edit 15
              set type ztna-proxy
              set name "test2"
              set uuid c7207330-bc99-51ef-6ab2-be36a0752438
              set srcintf "any"
              set dstintf "any"
              set srcaddr "all"
              set dstaddr "all"
              set action accept
              set schedule "always"
              set ztna-proxy "fwdfpx208"
              set logtraffic all
              set logtraffic-start enable
              set log-http-transaction enable
              set extended-log enable
              set ssl-ssh-profile "deep-inspection"
       next
end
```






```
config ztna service-connector
       edit "fpx208"
              set connection-mode forward
              set forward-address "10.121.1.208"
              set forward-port 8888
              set certificate "Fortinet_SSL"
              set trusted-ca "CA_Cert_1"
       next
end
config ztna traffic-forward-proxy
       edit "fwdfpx208"
              config url-route
                     edit "for208"
                            set service-connector "fpx208"
                     next
                 end
              set vip "vip2"
       next
end
config firewall vip
       edit "vip2"
              set uuid 21beb26e-bca6-51ef-f49d-42e366afdab8
              set type access-proxy
              set server-type https
              set extip 10.121.1.209
              set extintf "any"
              set extport 8888
              set ssl-certificate "Fortinet_SSL"
       next
end
```

2. Configure the second FortiProxy (208 in this example) as follows:

```
config firewall policy
       edit 4
              set type ztna-proxy
              set name "test2"
              set uuid e7e77c9c-bca5-51ef-8cc3-275398e1d455
```

```
                set dstintf "any"
                set srcaddr "all"
                set dstaddr "all"
                set action accept
                set schedule "always"
                set ztna-proxy "1"
                set logtraffic all
                set logtraffic-start enable
                set log-http-transaction enable
                set extended-log enable
                set ssl-ssh-profile "deep-inspection"
        next
    end
    config ztna traffic-forward-proxy
        edit "1"
                set vip "vip208"
        next
    end
    config firewall vip
        edit "vip208"
                set uuid 869d9b74-bca5-51ef-34f6-343c7d20efe7
                set type access-proxy
                set server-type https
                set extip 10.121.1.208
                set extintf "any"
                set client-cert disable
                set extport 8888
                set ssl-certificate "208cert"
        next
    end
```

Example forward traffic log on first FortiProxy:

```
date=2024-12-19 time=09:51:00 eventtime=1734630659815265080 tz="-0800" logid="0000000015"
      type="traffic" subtype="forward" level="notice" vd="root" srcip=10.121.1.27 srcport=53062
      srcintf="port5" srcintfrole="undefined" dstip=10.121.1.208 clientip=10.121.1.27 dstport=8888
      dstintf="port5" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
      sessionid=1679660394 proto=6 action="start" policyid=15 policytype="policy" poluuid="c7207330-
      bc99-51ef-6ab2-be36a0752438" policyname="test2" service="tcp/8888" trandisp="noop"
      url="https://10.121.1.209/tcp?address=172.18.20.84&port=22&tls=1" agent="Forticlient"
      appcat="unscanned" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0
      fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794" unauthuser="guodong" unauthusersource="forticlient"
      srcremote=207.102.138.19
```

Example ZTNA log on first FortiProxy:

```
date=2024-12-19 time=09:51:06 eventtime=1734630666432308571 tz="-0800" logid="0005000024"
      type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.121.1.27 srcport=53062
      srcintf="port5" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
      dstip=10.121.1.208 dstport=8888 dstintf="port5" dstintfrole="undefined" sessionid=1679660394
      service="tcp/8888" proxyapptype="http" proto=6 action="accept" policyid=15 policytype="proxy-
      policy" poluuid="c7207330-bc99-51ef-6ab2-be36a0752438" policyname="test2" clientip=10.121.1.27
      appcat="unscanned" duration=7 gatewayid=1 vip="vip2" clientdevicemanageable="manageable"
      clientcert="yes" wanin=0 rcvdbyte=0 wanout=0 lanin=3782 sentbyte=3782 lanout=3600
      fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794" unauthuser="guodong" unauthusersource="forticlient"
      srcremote=207.102.138.19
```

Example forward traffic log on second FortiProxy:

```
date=2024-12-19 time=09:51:00 eventtime=1734630660241936738 tz="-0800" logid="0000000015"
      type="traffic" subtype="forward" level="notice" vd="root" srcip=10.121.1.209 srcport=7844
      srcintf="port3" srcintfrole="undefined" dstip=172.18.20.84 clientip=10.121.1.209 dstport=22
      dstintf="port1" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
      sessionid=582239958 proto=6 action="start" policyid=4 policytype="policy" poluuid="e7e77c9c-
      bca5-51ef-8cc3-275398e1d455" policyname="test2" service="SSH" trandisp="noop"
      url="https://10.121.1.208/tcp?address=172.18.20.84&port=22&tls=1" agent="Forticlient"
      appcat="unscanned" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0
```

Example ZTNA log on second FortiProxy:

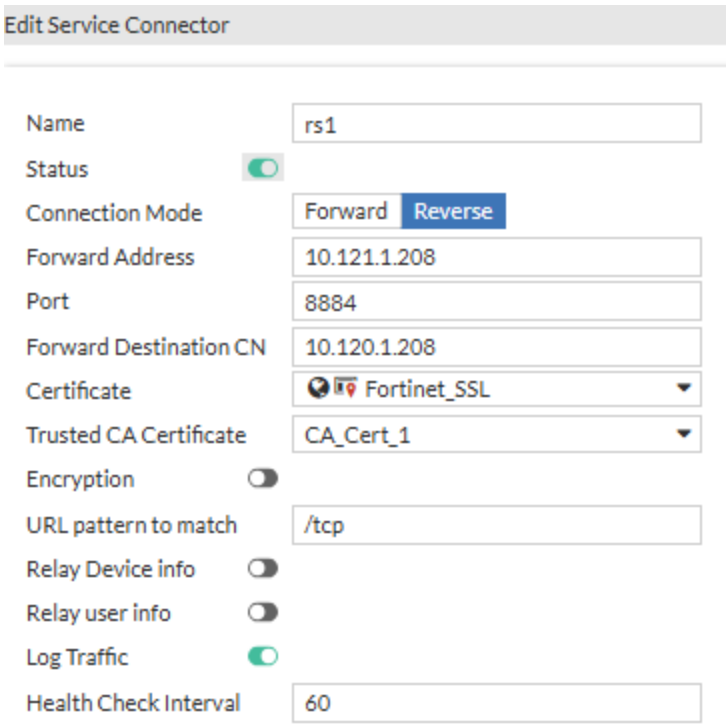
```
date=2024-12-19 time=09:51:06 eventtime=1734630666285628785 tz="-0800" logid="0005000024"
      type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.121.1.209 srcport=7844
      srcintf="port3" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
      dstip=172.18.20.84 dstport=22 dstintf="port1" dstintfrole="undefined" sessionid=582239958
      service="SSH" proxyapptype="http" proto=6 action="accept" policyid=4 policytype="proxy-policy"
      poluuid="e7e77c9c-bca5-51ef-8cc3-275398e1d455" policyname="test2" clientip=10.121.1.209
      appcat="unscanned" duration=7 gatewayid=1 vip="vip208" clientdevicemanageable="unknown"
      clientcert="no" wanin=1650 rcvdbyte=1650 wanout=1772 lanin=2570 sentbyte=2570 lanout=3062
```

FortiProxy as reverse proxy to service connector

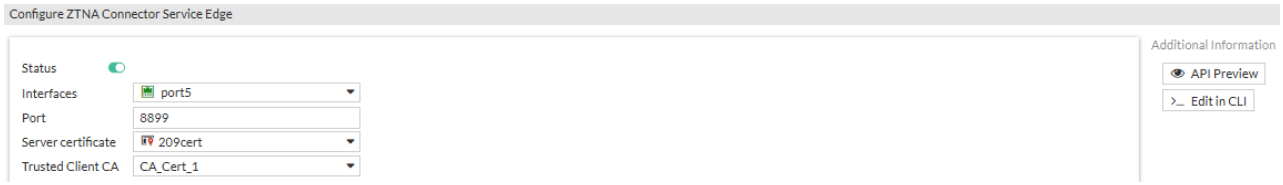
To configure FortiProxy as the reverse proxy to a service connector:

1. Configure the first FortiProxy (209 in this example) as follows:

```
config firewall policy
       edit 16
              set type ztna-proxy
              set name "test3"
              set uuid c62496ca-be36-51ef-490c-4f2ee03279a9
              set srcintf "any"
              set dstintf "any"
              set srcaddr "all"
              set dstaddr "all"
              set action accept
              set schedule "always"
              set ztna-proxy "re208"
              set logtraffic all
              set logtraffic-start enable
              set log-http-transaction enable
              set extended-log enable
       next
end
config ztna traffic-forward-proxy
       edit "re208"
              config url-route
                     edit "re208"
                            set service-connector "rs1"
                     next
              end
              set vip "vip3"
       next
end
```




```
config ztna service-connector
       edit "rs1"
              set connection-mode reverse
              set forward-address "10.121.1.208"
              set forward-port 8884
              set forward-destination-cn "10.120.1.208"
              set certificate "Fortinet_SSL"
              set trusted-ca "CA_Cert_1"
       next
end
config firewall vip
       edit "vip3"
              set uuid 022945e0-be36-51ef-6edf-96a8bfbb880c
              set type access-proxy
              set server-type https
              set extip 10.121.1.209
              set extintf "any"
              set extport 8844
              set ssl-certificate "Fortinet_SSL"
       next
end
```

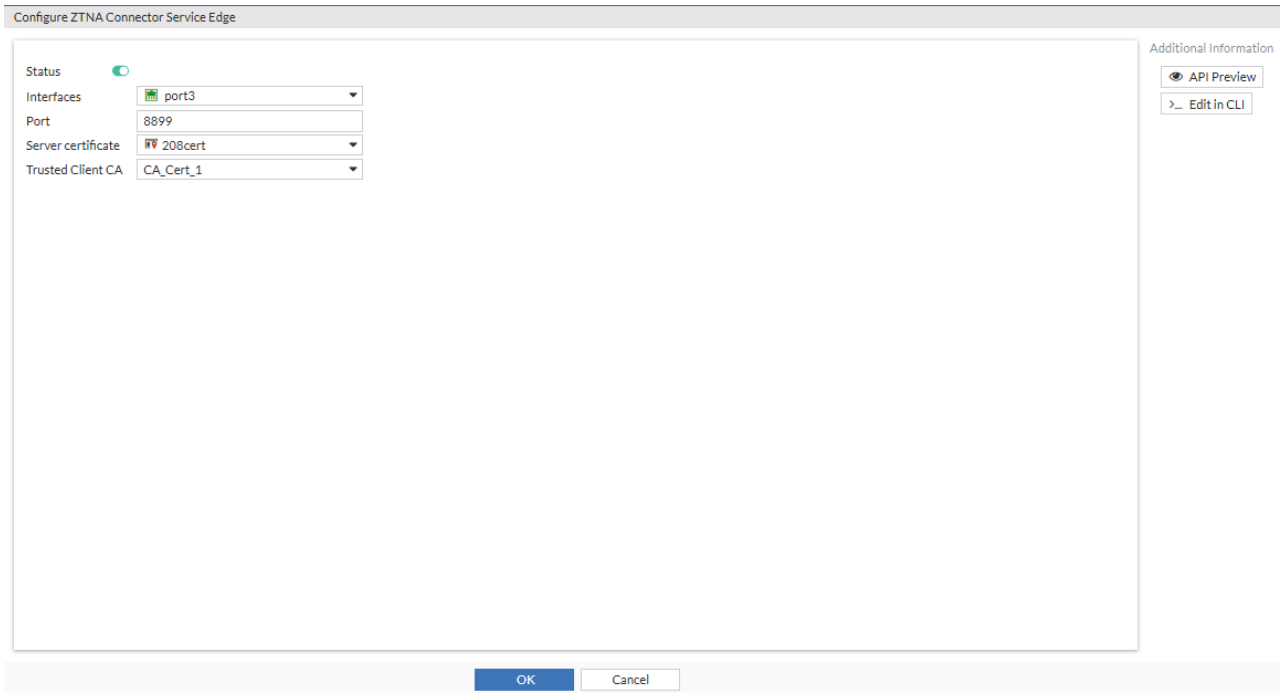



```
config ztna connector-service-edge
       set status enable
       set interface "port5"
       set port 8899
       set server-cert "209cert"
```

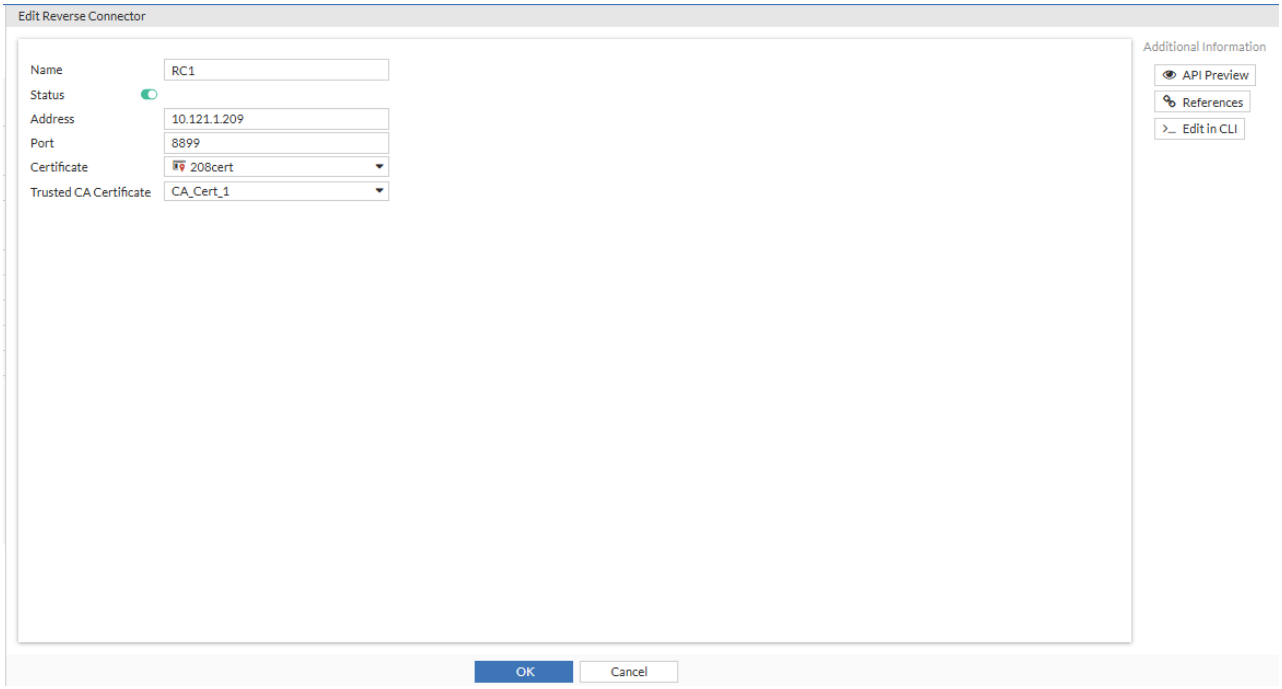
```
        set trusted-client-ca "CA_Cert_1"
    end
```

2. Configure the second FortiProxy (208 in this example) as follows:

```
    config firewall policy
        edit 5
            set type ztna-proxy
            set name "test3"
            set uuid 647928bc-be38-51ef-5ae5-b0b34c7f11df
            set srcintf "any"
            set dstintf "any"
            set srcaddr "all"
            set dstaddr "all"
            set action accept
            set schedule "always"
            set ztna-proxy "2"
            set logtraffic all
            set logtraffic-start enable
            set log-http-transaction enable
            set extended-log enable
        next
    end
    config ztna traffic-forward-proxy
        edit "2"
            set vip "vip2"
        next
    end
    config firewall vip
        edit "vip2"
            set uuid 992b5256-be38-51ef-56e6-a5c8c29c209e
            set type access-proxy
            set server-type https
            set extip 10.121.1.208
            set extintf "any"
            set client-cert disable
            set extport 8884
            set ssl-certificate "208cert"
        next
    end
```




```
config ztna connector-service-edge
       set status enable
       set interface "port3"
       set port 8899
       set server-cert "208cert"
       set trusted-client-ca "CA_Cert_1"
end
```




```
config ztna reverse-connector
       edit "RC1"
              set address "10.121.1.209"
```

```
                set port 8899
                set certificate "208cert"
                set trusted-server-ca "CA_Cert_1"
            next
    end
```

Example forward traffic log on first FortiProxy:

```
date=2024-12-19 time=13:28:01 eventtime=1734643680738100796 tz="-0800" logid="0000000015"
      type="traffic" subtype="forward" level="notice" vd="root" srcip=10.121.1.27 srcport=55399
      srcintf="port5" srcintfrole="undefined" dstip=10.121.1.208 clientip=10.121.1.27 dstport=8884
      dstintf="port5" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
      sessionid=1534640176 proto=6 action="start" policyid=16 policytype="policy" poluuid="c62496ca-
      be36-51ef-490c-4f2ee03279a9" policyname="test3" service="tcp/8884" trandisp="noop"
      url="https://10.121.1.209/tcp?address=172.18.20.83&port=22&tls=1" agent="Forticlient"
      appcat="unscanned" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0
      fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794" unauthuser="guodong" unauthusersource="forticlient"
      srcremote=207.102.138.19
```

Example ZTNA log on first FortiProxy:

```
date=2024-12-19 time=12:02:14 eventtime=1734638533879306863 tz="-0800" logid="0005000024"
      type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.121.1.27 srcport=54459
      srcintf="port5" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
      dstip=10.121.1.208 dstport=8884 dstintf="port5" dstintfrole="undefined" sessionid=1534640175
      service="tcp/8884" proxyapptype="http" proto=6 action="accept" policyid=16 policytype="proxy-
      policy" poluuid="c62496ca-be36-51ef-490c-4f2ee03279a9" policyname="test3" clientip=10.121.1.27
      appcat="unscanned" duration=121 gatewayid=1 vip="vip3" clientdevicemanageable="manageable"
      clientcert="yes" wanin=0 rcvdbyte=0 wanout=0 lanin=3782 sentbyte=3782 lanout=3514
      fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794" unauthuser="guodong" unauthusersource="forticlient"
      srcremote=207.102.138.19
```

Example forward traffic log on second FortiProxy:

```
date=2024-12-19 time=13:28:01 eventtime=1734643681000410543 tz="-0800" logid="0000000015"
      type="traffic" subtype="forward" level="notice" vd="root" srcip=10.121.1.208 srcport=38864
      srcintf="unknown-0" srcintfrole="undefined" dstip=172.18.20.83 dstport=22 dstintf="port1"
      dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=1842818121
      proto=6 action="start" policyid=5 policytype="policy" poluuid="647928bc-be38-51ef-5ae5-
      b0b34c7f11df" policyname="test3" service="SSH" trandisp="noop"
      url="https://10.121.1.208/tcp?address=172.18.20.83&port=22&tls=1" agent="Forticlient"
      appcat="unscanned" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0
```

FortiProxy as reverse proxy to service connector with relay info (authentication)

To configure FortiProxy as the reverse proxy to a service connector with authentication:

1. Configure the first FortiProxy (209 in this example) as follows:

```
config firewall policy
   edit 17
      set type ztna-proxy
      set name "test4"
      set uuid 4cb311a2-be51-51ef-2ca9-e44aa30538be
      set srcintf "any"
      set dstintf "any"
      set srcaddr "all"
      set dstaddr "all"
```

```
            set action accept
            set schedule "always"
            set ztna-proxy "re208"
            set logtraffic all
            set logtraffic-start enable
            set log-http-transaction enable
            set extended-log enable
            set groups "ldap-grp"
        next
    end
    config ztna service-connector
        edit "rs1"
            set connection-mode reverse
            set forward-address "10.121.1.208"
            set forward-port 8884
            set forward-destination-cn "10.120.1.208"
            set certificate "Fortinet_SSL"
            set trusted-ca "CA_Cert_1"
            set relay-user-info enable
            relay-user
        next
    end
    config ztna traffic-forward-proxy
        edit "re208"
            config url-route
                edit "re208"
                    set service-connector "rs1"
                next
            end
            set vip "vip3"
        next
    end
    config ztna connector-service-edge
        set status enable
        set interface "port5"
        set port 8899
        set server-cert "209cert"
        set trusted-client-ca "CA_Cert_1"
    end
    config firewall vip
        edit "vip3"
            set uuid 022945e0-be36-51ef-6edf-96a8bfbb880c
            set type access-proxy
            set server-type https
            set extip 10.121.1.209
            set extintf "any"
            set extport 8844
            set ssl-certificate "Fortinet_SSL"
        next
    end
    config authentication scheme
        edit "fac_ldap_scheme"
            set method basic
            set user-database "ldap"
        next
    end
    config authentication rule
```

```
    edit "ru-basic"
       set srcintf "any"
       set srcaddr "all"
       set dstaddr "all"
       set active-auth-method " fac_ldap_scheme"
    next
end
```

2. Configure the second FortiProxy (208 in this example) as follows:

```
config firewall policy
    edit 6
       set type ztna-proxy
       set name "test4"
       set uuid 765dbc14-be51-51ef-c1d3-a20777201165
       set srcintf "any"
       set dstintf "any"
       set srcaddr "all"
       set dstaddr "all"
       set action accept
       set schedule "always"
       set ztna-proxy "2"
       set logtraffic all
       set logtraffic-start enable
       set log-http-transaction enable
       set extended-log enable
       set groups "ldap-grp"
    next
end
config ztna reverse-connector
    edit "RC1"
       set address "10.121.1.209"
       set port 8899
       set certificate "208cert"
       set trusted-server-ca "CA_Cert_1"
    next
end
config ztna traffic-forward-proxy
    edit "2"
       set vip "vip2"
    next
end
config firewall vip
    edit "vip2"
       set uuid 992b5256-be38-51ef-56e6-a5c8c29c209e
       set type access-proxy
       set server-type https
       set extip 10.121.1.208
       set extintf "any"
       set client-cert disable
       set extport 8884
       set ssl-certificate "208cert"
    next
end
config authentication scheme
    edit "ztna"
       set method ztna-relay
       set user-database "ldap"
```

```
      next
   end
   config authentication rule
      edit "rule-relay"
         set srcintf "any"
         set srcaddr "all"
         set dstaddr "all"
         set sso-auth-method "ztna"
      next
   end
```

Example forward traffic log on first FortiProxy:

```
date=2025-02-12 time=14:48:02 eventtime=1739400481939063719 tz="-0800" logid="0000000015"
      type="traffic" subtype="forward" level="notice" vd="root" srcip=10.121.1.27 srcport=49436
      srcintf="port5" srcintfrole="undefined" dstip=10.121.1.208 clientip=10.121.1.27 dstport=8884
      dstintf="port5" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
      sessionid=1368748332 proto=6 action="start" policyid=17 policytype="policy" poluuid="4cb311a2-
      be51-51ef-2ca9-e44aa30538be" policyname="test4" user="usera@qa.domaintest.com" group="ldap-
      grp" service="tcp/8884" trandisp="noop"
      url="https://10.121.1.209/tcp?address=172.18.20.83&port=22&tls=1" agent="Forticlient"
      appcat="unscanned" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0
      fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794" unauthuser="guodong" unauthusersource="forticlient"
      srcremote=207.102.138.19
```

Example ZTNA log on first FortiProxy:

```
date=2025-02-12 time=14:49:56 eventtime=1739400596457255371 tz="-0800" logid="0005000024"
      type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.121.1.27 srcport=49436
      srcintf="port5" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
      dstip=10.121.1.208 dstport=8884 dstintf="port5" dstintfrole="undefined" sessionid=1368748332
      service="tcp/8884" proxyapptype="http" proto=6 action="accept" policyid=17 policytype="proxy-
      policy" poluuid="4cb311a2-be51-51ef-2ca9-e44aa30538be" policyname="test4" clientip=10.121.1.27
      appcat="unscanned" duration=115 user="usera@qa.domaintest.com" group="ldap-grp" gatewayid=1
      vip="vip3" clientdevicemanageable="manageable" clientcert="yes" wanin=0 rcvdbyte=0 wanout=0
      lanin=5249 sentbyte=5249 lanout=5552 fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794"
      unauthuser="guodong" unauthusersource="forticlient" srcremote=207.102.138.19
```

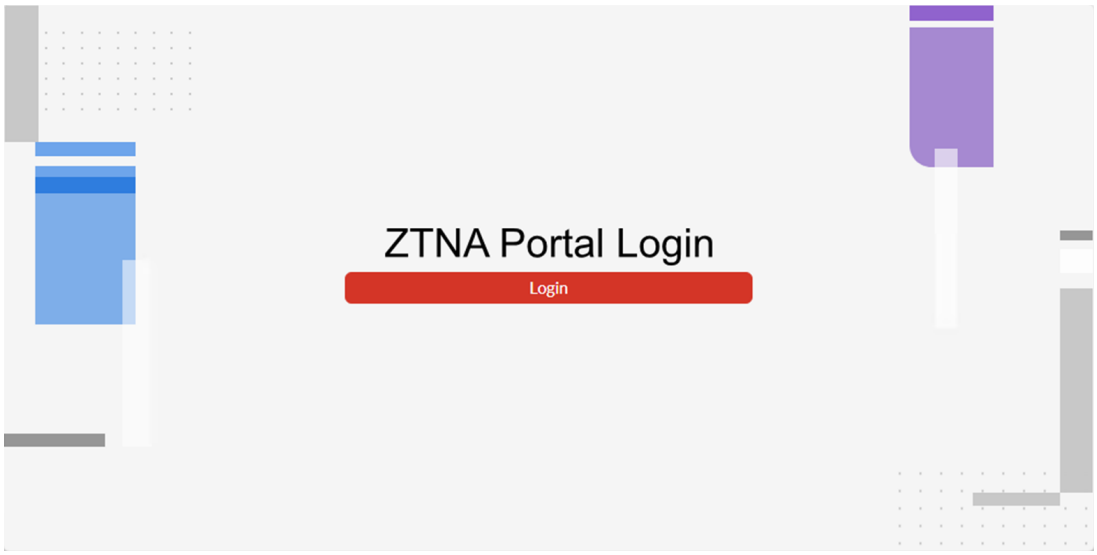
Example forward traffic log on second FortiProxy:

```
date=2025-02-12 time=14:49:57 eventtime=1739400596385868699 tz="-0800" logid="0005000024"
      type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.121.1.208 srcport=12170
      srcintf="unknown-0" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
      dstip=172.18.20.83 dstport=22 dstintf="port1" dstintfrole="undefined" sessionid=2131368715
      service="SSH" proxyapptype="http" proto=6 action="accept" policyid=6 policytype="proxy-policy"
      poluuid="765dbc14-be51-51ef-c1d3-a20777201165" policyname="test4" appcat="unscanned"
      duration=114 user="usera@qa.domaintest.com" group="ldap-grp" gatewayid=1 vip="vip2"
      clientdevicemanageable="unknown" clientcert="no" wanin=3341 rcvdbyte=3341 wanout=3036 lanin=0
      sentbyte=0 lanout=0
```

ZTNA agentless web-based application access

A ZTNA web portal is an agentless ZTNA solution that provide end-user access to applications without FortiClient or client certificate checks. The ZTNA portal handles authentication and authorization of traffic destined for the protected resources. It is implemented entirely in WAD (Web Application and Database) and provides a convenient way for users to access internal resources securely.

When end-users connect to the ZTNA web portal, they are directed to a login page:

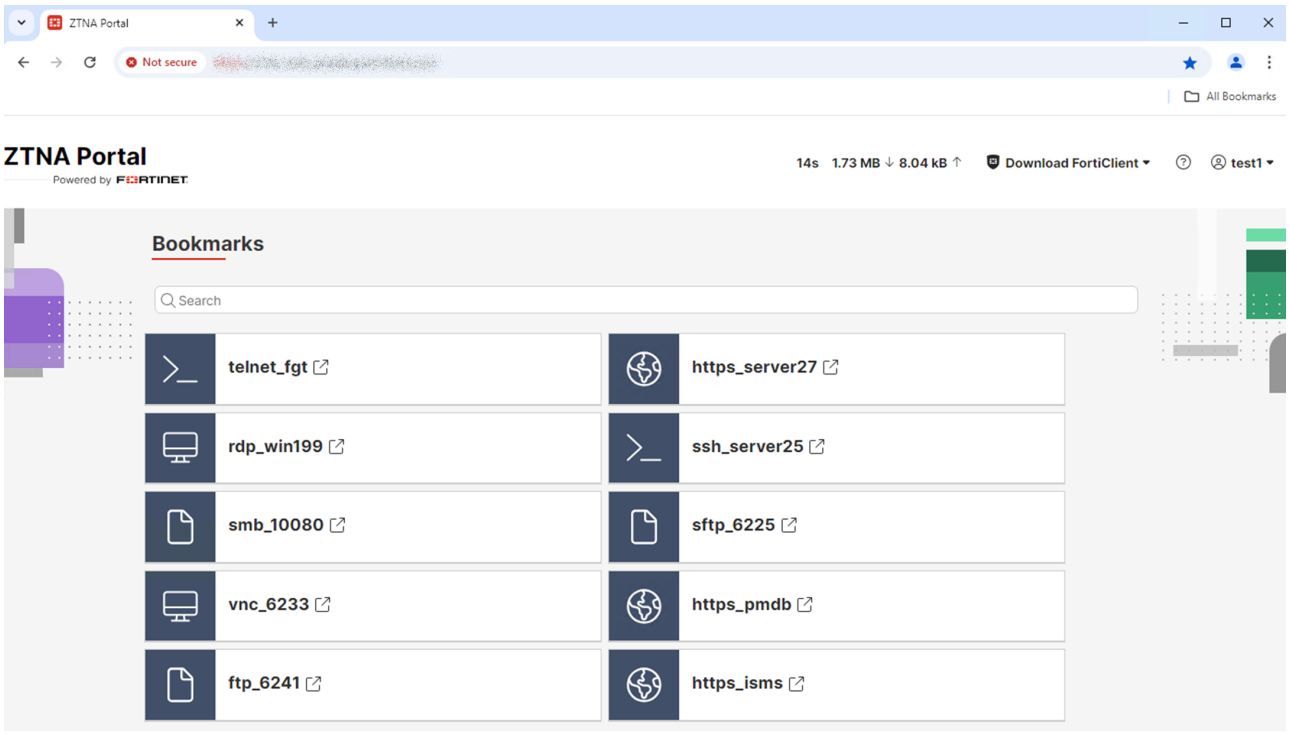


Once logged in, end-users can access bookmarks defined by the administrator:

Dynamic bookmarks can be defined using an LDAP or SAML attribute within the user's LDAP or SAML account so that bookmarks are auto-populated with the values defined in that attribute instead of static pre-defined IP or hostnames.

Dynamic bookmarks are useful in the following cases:

- Department-specific application access to ensure users only see applications relevant to their role.
- Regional server access by using the location attributes to connect users to the geographically closest servers automatically.
- Role-based permission control by referencing role attributes to provide appropriate access levels for different user roles.



Prerequisites

Before configuring the ZTNA web portal, ensure the following:

- Network connectivity between the following:
  - Client devices and the FortiProxy external interface
  - FortiProxy and the internal protected resources
- For web applications, the client must resolve the FQDN to the ZTNA portal VIP.
- SSL certificate for the ZTNA web portal—When accessing the web application, end users are presented with the certificate configured on the ZTNA portal VIP instead of the certificate on the end web server. Hence, the certificate requires the correct Subject Alternate Name(s) to avoid browser certificate errors. You must also ensure the certificate includes the web portal FQDN as well as any application FQDNs to avoid browser certificate errors.

CLI syntax

Configure an access-proxy type of VIP. Disable `client-cert` so that it is not checked when an agentless client connects.

```
config firewall vip
    edit <name>
        set type access-proxy
        set server-type https
        set extip <ip address>
        set extintf <interface>
```

```
        set client-cert disable
        set extport <port>
        set ssl-certificate <certificate>
    next
end
```

Configure an access-proxy virtual host. End-users will connect to this destination to access the ZTNA web portal. Disable `client-cert` for this virtual host.

```
config firewall access-proxy-virtual-host
    edit "ztna-web-portal-fqdn"
        set host < web portal host name or ip >
        set client-cert disable
    next
end
```

Configure an authentication scheme. Then configure an authentication rule with the new protocol `ztna-portal`.

```
config authentication rule
    edit <rule>
        set protocol ztna-portal
        set active-auth-method < auth scheme >
    next
end
```

New syntax for configuring the ZTNA web portal:

```
config ztna web-portal
    edit <name>
       set vip <vip name>
        set host <virtual host name>
        set auth-portal {enable | disable}
        set vip6 <virtual IPv6 name>
        set auth-rule <rule>
    next
end
```

`set vip <vip name>`	The access-proxy VIP associated with this portal.
`set host <virtual host name>`	The access-proxy virtual host object and FQDN defined for accessing this portal. This setting must be configured.
`set auth-portal {enable | disable}`	Enable/disable the authentication portal.
`set vip6 <virtual IPv6 name>`	The access-proxy VIP6 associated with the ZTNA server and applications that this portal is allowing.

New syntax for creating the web portal bookmarks:

```
config ztna web-portal-bookmark
    edit <name>
     set type {user|ldap-dynamic|saml-dynamic}
```

```
     config bookmarks
       edit <name>
        set apptype {ftp | rdp | sftp | smb | ssh | telnet | vnc | web}
        set folder "10.100.1.111"
        set url <string>
        set host <name or IP>
        set description <description>
        set port <remote port>
        set sso {enable | disable}
    next
end
```

`set type`	Bookmark type. You can use static bookmarks for users/groups or dynamic bookmarks using LDAP or SAML attributes.
`set apptype {ftp | rdp | sftp | smb | ssh | telnet | vnc | web}`	Supported types of bookmarks: ftp, rdp, sftp, smb, ssh, telnet, vnc, web (default).
`set folder <ip>`	The IP for the destination folder.
`set url <url>`	For different types of applications, the URL used to define the destination.
`set host <name or ip>`	For different types of applications, the host name or IP used to define the destination.
`set port <remote port>`	Where applicable, define the port for the service.
`set sso {enable | disable}`	Enable/disable the SSO user login and credentials to connect to the application, where applicable.



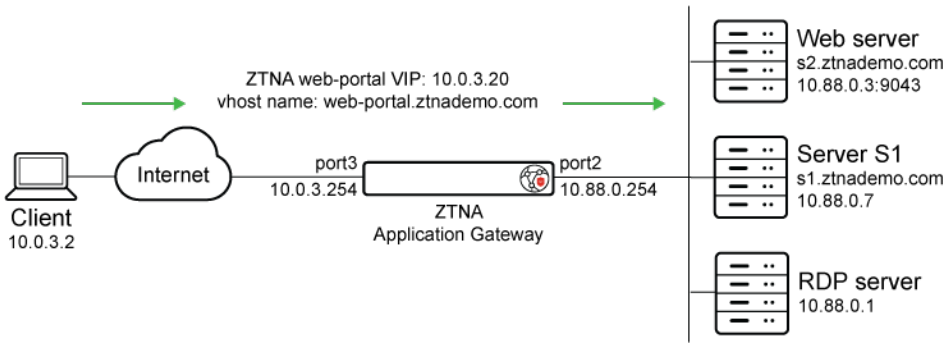
Not all options are listed. Some options are available only for certain types of applications.

Within the proxy-policy (full ZTNA policy), a new proxy type is added called `ztna-proxy`. Configure your proxy-policy to map to your web-portal.

```
config firewall policy
    edit <id>
        set type ztna-proxy
        set active-auth-method <authentication rule>
        set ztna-proxy <web-portal>
        …
    next
end
```

Example

This example demonstrates connecting to a ZTNA web portal to gain access to protected resources. Authentication is performed with LDAP.



Prerequisites:

- The Client can resolve:
  - The hostname web-portal.ztnademo.com to the VIP address 10.0.3.20
  - The server s1.ztnademo.com to the VIP address 10.0.3.20
  - The server s2.ztnademo.com to the VIP address 10.0.3.20
- The FortiProxy resolves:
  - s1.ztnademo.com to the real server IP of 10.88.0.7
  - s2.ztnademo.com to the real server IP of 10.88.0.3
- The FortiProxy has an LDAP connection and user group already created.

To configure from the CLI:

1. Configure a firewall VIP with external IP 10.0.3.20:

```
config firewall vip
    edit "ZTNA-web-proxy"
        set type access-proxy
        set server-type https
        set extip 10.0.3.20
        set extintf "port3"
        set client-cert disable
        set extport 443
        set ssl-certificate "ztna-wildcard"
    next
end
```

2. Configure an access-proxy virtual host:

   The configuration here defines the virtual host used to access the ZTNA web portal, as well as the server certificate for the portal. It overrides the settings in the VIP. Ensure that `client-cert` is disabled.

```
config firewall access-proxy-virtual-host
    edit "ztna-web-portal-fqdn"
        set host "web-portal.ztnademo.com"
        set client-cert disable
    next
end
```

3. Configure the authentication scheme and rule:

```
config authentication scheme
    edit "ztna-web-portal-ldap"
        set method basic
        set user-database "LDAP-fortiad"
    next
end
config authentication rule
    edit "ztna-web-portal-rule"
        set protocol ztna-portal
        set ip-based disable
        set active-auth-method "ztna-web-portal-ldap"
        set web-auth-cookie enable
    next
end
```

4. Configure the ZTNA web-portal:
   Map the portal to the VIP, virtual host, and authentication rule that were previously created.

```
config ztna web-portal
    edit "ztna-web-portal-ldap"
        set vip "ZTNA-web-proxy"
        set host "ztna-web-portal-fqdn"
        set auth-rule "ztna-web-portal-rule"
    next
end
```

5. Create web-portal bookmarks that will point to your internal resources:

```
config ztna web-portal-bookmark
    edit "bookmark"
        config bookmarks
            edit "Webserver"
                set url "https://s2.ztnademo.com:9043"
            next
            edit "Server-S1-Web"
                set sso enable
                set url "https://s1.ztnademo.com"
            next
            edit "Server-S1-SSh"
                set apptype ssh
                set sso enabled
                set host "10.88.0.7"
                set logon-user "admin"
                set logon-password <password>
            next
            edit "FortiProxy-Internal-SSH"
                set apptype ssh
                set host "10.88.0.254"
            next
            edit "RDP"
```

```
                set apptype rdp
                set host "10.88.0.1"
                set port 3389
            next
        end
    next
end
```

Alternatively, you can define dynamic bookmarks using an LDAP or SAML attribute within the user's LDAP or SAML account to generate personalized application shortcuts:

- For LDAP users, the attributes can be built-in or user-defined attributes stored in the LDAP directory.
- NEW For SAML users, the attributes are received in SAML assertions during authentication.

See configuration examples below:

LDAP:

```
config ztna web-portal-bookmark
   edit "bookmark"
      set type ldap-dynamic
         config bookmarks
         edit "ssh"
         set apptype ssh
         set host "|remoteHost|"
      next
         edit "ftp"
            set apptype ftp
            set folder "|remoteHost|"
         next
      end
   next
end
```

SAML NEW:

```
config ztna web-portal-bookmark
   edit "bookmark"
      set type saml-dynamic
      config bookmarks
         edit "ssh"
            set apptype ssh
            set host "|remoteHost|"
         next
         edit "tel78"
            set apptype telnet
            set host "|remoteHost|"
         next
      end
   next
end
```

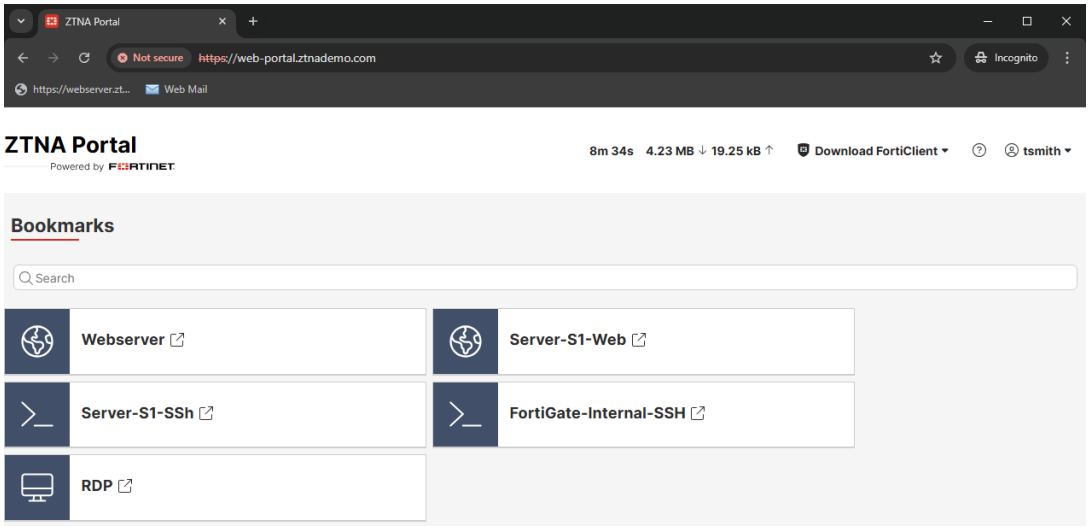
6. Create a full ZTNA policy to allow access to the new VIP:

```
config firewall policy
    edit 13
        set type ztna-proxy
        set name "ZTNA-web-portal"
```

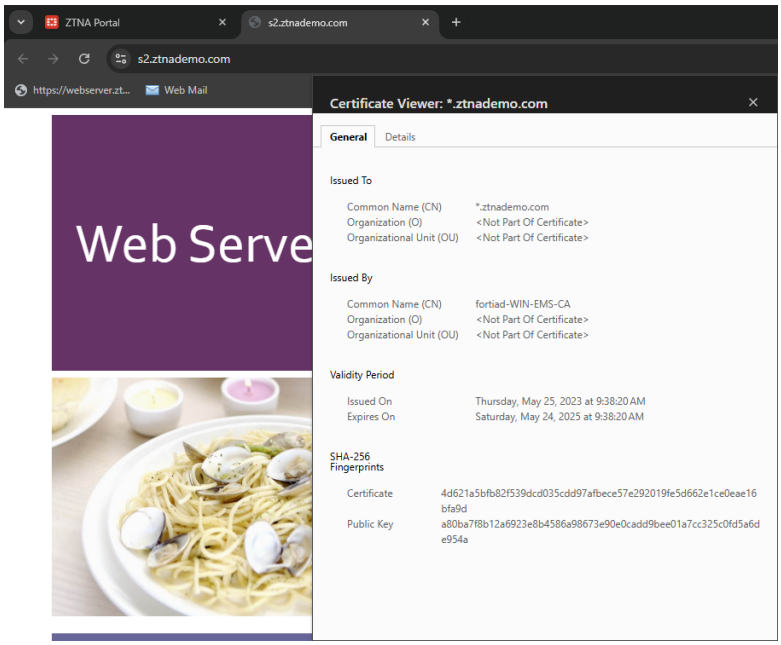
```
        set uuid fe696a38-a851-51ef-dc62-9d7c7f91352a
        set srcintf "any"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set ztna-proxy "ztna-web-portal-ldap"
        set logtraffic all
        set comments " (Copy of 9) (Copy of )"
        set ssl-ssh-profile "deep-inspection"
    next
end
```

Verification:

1. On the Client 10.0.3.2, access the portal on https://web-portal.ztnademo.com.
2. When prompted, enter the LDAP user credentials.
3. Once logged into the ZTNA Portal, choose the application bookmark to connect to.



4. Click *Webserver* to access *s2.ztnademo.com*. A new tab opens up to the web page.
5. Check the certificate to confirm it is signed by the CA certificate used in the VIP configurations.



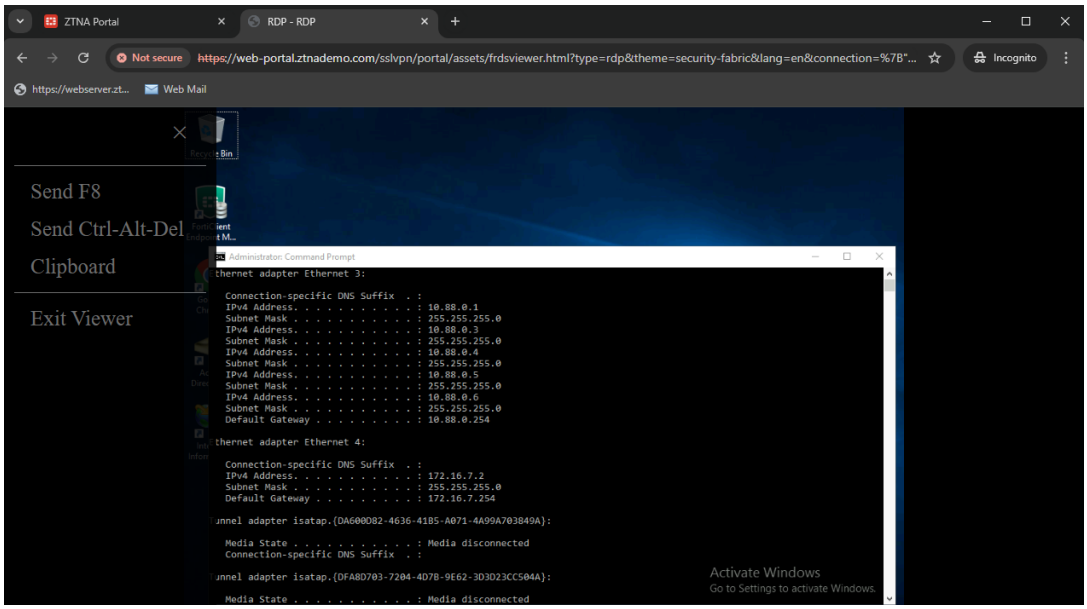
6. On the FortiProxy, go to *Log & Report > ZTNA Traffic* to view the latest traffic log. Alternatively, use these commands to view the logs from CLI:

```
# execute log filter field subtype ztna

# execute log display
32 logs found.
10 logs returned.

1: 1: date=2025-01-21 time=12:24:56 eventtime=1737491095186981906 tz="-0800"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2
srcport=1629 srcintf="port3" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved"
dstip=10.0.3.20 dstport=443 dstintf="port2" dstintfrole="dmz" sessionid=6761 service="HTTPS"
proxyapptype="http" proto=6 action="accept" policyid=2 policytype="proxy-policy"
poluuid="fe696a38-a851-51ef-dc62-9d7c7f91352a" policyname="ZTNA-web-portal" trandisp="snat"
transip=10.88.0.3 transport=9043 clientip=10.120.1.41 appcat="unscanned" duration=159
gatewayid=1 vip="ZTNA-web-proxy" clientdevicemanageable="unknown" clientcert="no" wanin=303011
rcvdbyte=303011 wanout=5460 lanin=3202 sentbyte=3202 lanout=306669
fctuid="6F6248B158C74FF98905ADCE528DB1E7" unauthuser="userb" unauthusersource="forticlient"
srcremote=207.102.138.19 utmaction="allow"
```

7. On the ZTNA Portal, connect to RDP. When prompted enter the credentials.
8. Once successfully connected, users can press F8 for additional controls.



9. Review the logs:

```
# execute log filter field subtype ztna

# execute log display
35 logs found.
10 logs returned.
9: date=2025-01-20 time=15:29:54 eventtime=1737415793573037679 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2 srcport=2540
srcintf="port3" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved" dstip=10.0.3.20
dstport=443 dstintf="port2" dstintfrole="dmz" sessionid=8146 service="HTTPS"
proxyapptype="ztna-proxy" proto=6 action="accept" policyid=2 policytype="proxy-policy"
poluuid="fe696a38-a851-51ef-dc62-9d7c7f91352a" policyname="ZTNA-web-portal" trandisp="snat"
tranip=10.88.0.1 tranport=3389 clientip=10.120.1.41 appcat="unscanned" duration=0 gatewayid=1
vip="ZTNA-web-proxy" clientdevicemanageable="unknown" clientcert="no" wanin=0 rcvdbyte=0
wanout=0 lanin=3242 sentbyte=3242 lanout=1726 fctuid="6F6248B158C74FF98905ADCE528DB1E7"
unauthuser="userb" unauthusersource="forticlient" srcremote=207.102.138.19
```

Additional troubleshooting and debugs:

If an issue occurs, you can troubleshoot by running these commands:

```
# diagnose wad debug enable category all
# diagnose wad debug enable level verbose
# diagnose debug enable
```

A working connection will output the debugs indicating the web-portal matched the proper gateway. Then accessing the bookmark will output debugs for matching the bookmark.

```
GET /XX/YY/ZZ/webservice?bmgroup=hidden_bookmarks_for_
lu1&bmname=url78&cookie=5572CCD473670123931EC262F4AF1C8A HTTP/1.1
Host: s2.ztnademo.com
```

```
user-agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:133.0) Gecko/20100101 Firefox/133.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-language: en-CA,en-US;q=0.7,en;q=0.3
accept-encoding: gzip, deflate, br, zstd
referer: https://10.20.20.220.devqa.wang/
dnt: 1
sec-gpc: 1
cookie: ZTNAWebPortal=5572CCD673670123931EC262F4AF1C8A
cookie: ZTNAWEB=bmgroup=hidden_bookmarks_for_lu1&bmname=url78
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: cross-site
sec-fetch-user: ?1
priority: u=0, i
te: trailers

[V][p:1238][s:1432116668][r:120] wad_http_marker_uri               :1269
path=/XX/YY/ZZ/webservice len=20
[V][p:1238][s:1432116668][r:120] wad_http_parse_host               :1660  host_len=16
[I][p:1238][s:1432116668][r:120] wad_http_parse_host               :1692  host=[16]s2.ztnademo.com
[I][p:1238][s:1432116668][r:120] wad_http_str_canonicalize         :2211  enc=0
path=/XX/YY/ZZ/webservice len=20 changes=0
[I][p:1238][s:1432116668][r:120] wad_http_str_canonicalize         :2213  end=5
path=bmgroup=hidden_bookmarks_for_lu1&bmname=url78&cookie=5572CCD473670123931EC262F4AF1C8A len=85
changes=0
[V][p:1238][s:1432116668][r:120] wad_http_normalize_uri            :2652  host_len=16 path_len=20
query_len=85
[I][p:1238][s:1432116668][r:120] wad_vs_proxy_match_gwy            :4631  16339:ztna_portal_fqdn:
matching gwy with vhost(_def_virtual_host_)
[V][p:1238][s:1432116668][r:120] wad_vs_proxy_match_vhost          :4750  16339:ztna_portal_fqdn:
matching vhost by: s2.ztnademo.com
[V][p:1238][s:1432116668][r:120] wad_vs_proxy_match_vhost          :4753  16339:ztna_portal_fqdn:
no host matched.
[V][p:1238][s:1432116668][r:120] wad_vs_web_portal_cookie_lookup   :9136  decode cookie_
str=5572CCD473670123931EC262F4AF1C8A as cookie_val=1325877068, vd_id=0, vs_id=16339, gwy_id=1
[I][p:1238][s:1432116668][r:120] wad_vs_proxy_match_gwy            :4675  16339:ztna_portal_fqdn:
Matched gwy(1) type(ztna-portal) via cookie in query 0x7f0dec4b9f48.
[I][p:1238][s:1432116668][r:120] wad_vs_gwy_ztna_portal_get_wp     :4350  16339:ztna_portal_
fqdn:1: trace
[I][p:1238][s:1432116668][r:120] wad_http_str_canonicalize         :2211  enc=3
path=/XX/YY/ZZ/webservice len=20 changes=0
[I][p:1238][s:1432116668][r:120] wad_http_str_canonicalize         :2213  end=4
path=bmgroup=hidden_bookmarks_for_lu1&bmname=url78&cookie=5572CCD473670123931EC262F4AF1C8A len=85
changes=0
[V][p:1238][s:1432116668][r:120] __wad_http_build_redir_resp2      :1281  Recieved req method=0,
exp_get=1
[I][p:1238][s:1432116668][r:120] wad_vs_gwy_ztna_portal_get_wp     :4350  16339:ztna_portal_
fqdn:1: trace
[I][p:1238][s:1432116668][r:120] wad_vs_gwy_get_wp_nop             :2877  16339:ztna_portal_
fqdn:1: trace
[V][p:1238][s:1432116668][r:120] __wad_vs_web_portal_cookie_hdr_make:9189  cookie_val=1325877071,
```

```
vd_id=0, vs_id=16339, gwy_id=1, cookie=ZTNAWebPortal=5572CCD773670123931EC262F4AF1C8A; Max-
Age=3600; Path=/; HTTPOnly; Secure
[V][p:1238][s:1432116668][r:120] wad_http_req_exec_act             :14274 response is ready!
[V][p:1238][s:1432116668][r:120] wad_http_msg_start_setup_proc     :2298  msg(0x7f0dea5f1890)
proc-setup started from: req_resp_ready.
[V][p:1238][s:1432116668][r:120] wad_http_def_proc_msg_plan        :2260  msg(0x7f0dea5f1890)
setting up processor(req_resp_ready)
[V][p:1238][s:1432116668][r:120] wad_http_msg_start_setup_proc     :2298  msg(0x7f0deb9fdb20)
proc-setup started from: resp_forward.
[V][p:1238][s:1432116668][r:120] wad_http_def_proc_msg_plan        :2260  msg(0x7f0deb9fdb20)
setting up processor(resp_forward)
[I][p:1238][s:1432116668][r:120] wad_dump_fwd_http_resp            :3086  hreq=0x7f0dea5f1890
Forward response from Internal:

HTTP/1.1 303 See Other
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000
Content-Security-Policy: frame-ancestors 'self'; object-src 'self'; script-src 'self' https:
'unsafe-eval' 'unsafe-inline' blob:;
Connection: close
Content-Type: text/html
Cache-Control: no-cache
Location: https://s2.ztnademo.com:443
Content-Length: 134
Set-Cookie: ZTNAWebPortal=5572CCD773670123931EC262F4AF1C8A; Max-Age=3600; Path=/; HTTPOnly; Secure
Set-Cookie: ZTNAWEB=bmgroup=hidden_bookmarks_for_lu1&bmname=url78; Path=/; HTTPOnly; Secure
```

ZTNA configuration examples

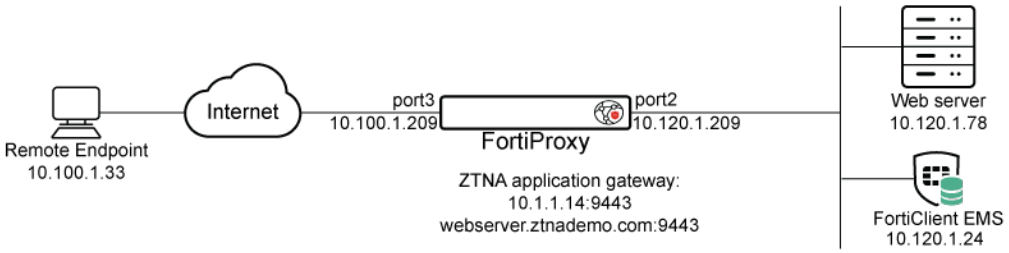
This section includes the following ZTNA configuration examples:

- ZTNA HTTPS access proxy example on page 292
- ZTNA HTTPS access proxy with basic authentication example on page 302
- ZTNA TCP forwarding access proxy example on page 311
- ZTNA SSH access proxy example on page 318
- ZTNA application gateway with SAML authentication example on page 326
- Secure LDAP connection from FortiAuthenticator with zero trust tunnel example on page 331
- Access control between on-net devices and internal web server using security posture tags on page 332
- UTM scanning on TCP forwarding access proxy traffic on page 339
- ZTNA Zero Trust application gateway example on page 342
- ZTNA inline CASB for SaaS application access control on page 343
- ZTNA application gateway with KDC to access shared drives on page 348
- Custom replacement message for ZTNA virtual hosts on page 353

- ZTNA for UDP traffic on page 357

ZTNA HTTPS access proxy example

In this example, an HTTPS access proxy is configured to demonstrate its function as a reverse proxy on behalf of the web server it is protecting. It verifies user identity, device identity, and trust context, before granting access to the protected source.

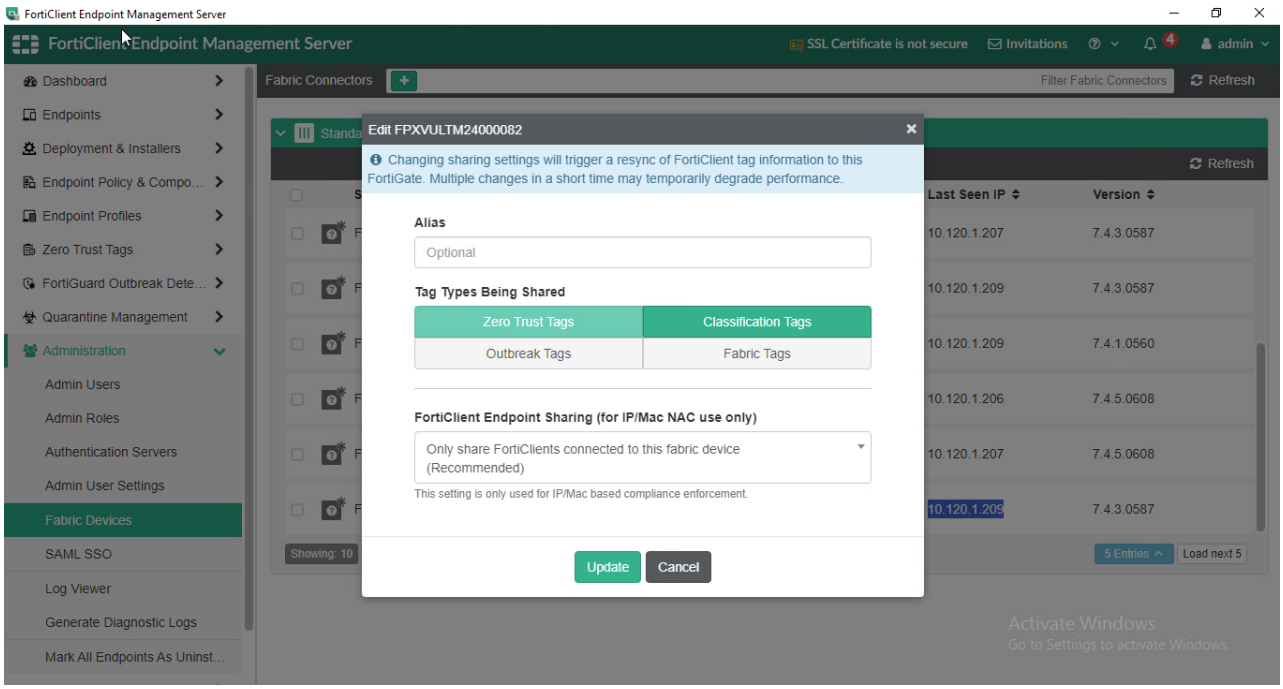


This example shows access control that allows traffic when the FortiClient endpoint is tagged as *Low Importance* using Classification tags. This example assumes that the FortiProxy EMS fabric connector is already successfully connected.

To configure ZTNA in the GUI, go to *System* > *Feature Visibility* and enable *Zero Trust Network Access*.

To configure FortiClient EMS to share classification tags:

1. Go to *Administration* > *Fabric Devices*.
2. Select the FortiProxy device.
3. Click *Edit*.
4. Under *Tag Types Being Shared*, add *Classification Tags*.



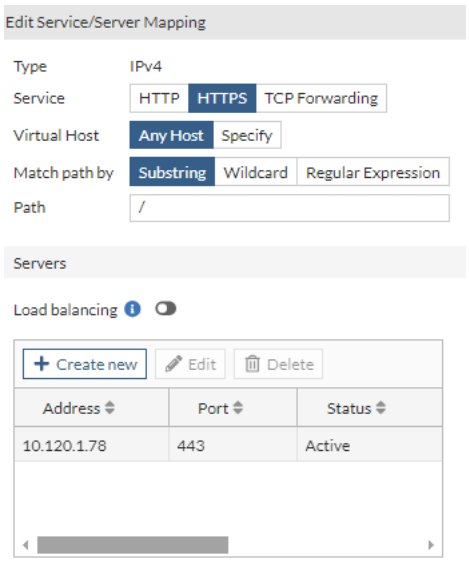
5. Click *Save*.

To configure a ZTNA server for HTTPS access proxy in the GUI:

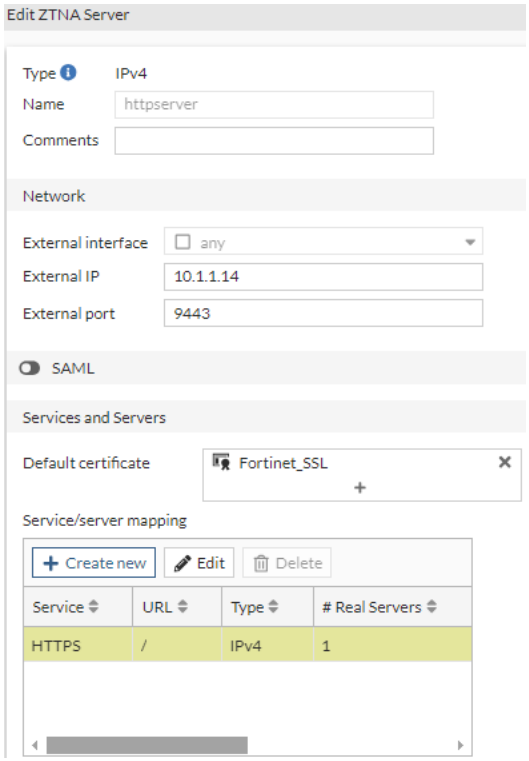
1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Servers* tab.
2. Click *Create New*.
3. Set *Name* to *ZTNA-webserver*.
4. Set *Interface* to *port3*. The *IP address* and *Port* fields are automatically set to the IP of the selected interface and the default port of 443.
   a. Set *External IP* to *10.1.1.14*.
   b. Set *External port* to *9443*.

   Verify that the IP address and port do not conflict with management access to the interface. Otherwise, change the IP address to another address on that subnet.

5. Select the *Default certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.
6. Add server mapping:
   a. In the *Service/server mapping* table, click *Create New*.
   b. Set *Service* to *HTTPS*.
   c. Set *Virtual Host* to *Any Host*.
   d. Configure the path as needed. For example, to map to *webserver.ztnademo.com/fortiproxy*, enter */fortiproxy*.
   e. In the *Server* section, set *Address type* to *IP*.
   f. Set *IP address* to *10.120.1.78*.
   g. Set *Port* to *443*.



h. Click *OK*. The server mapping is displayed.

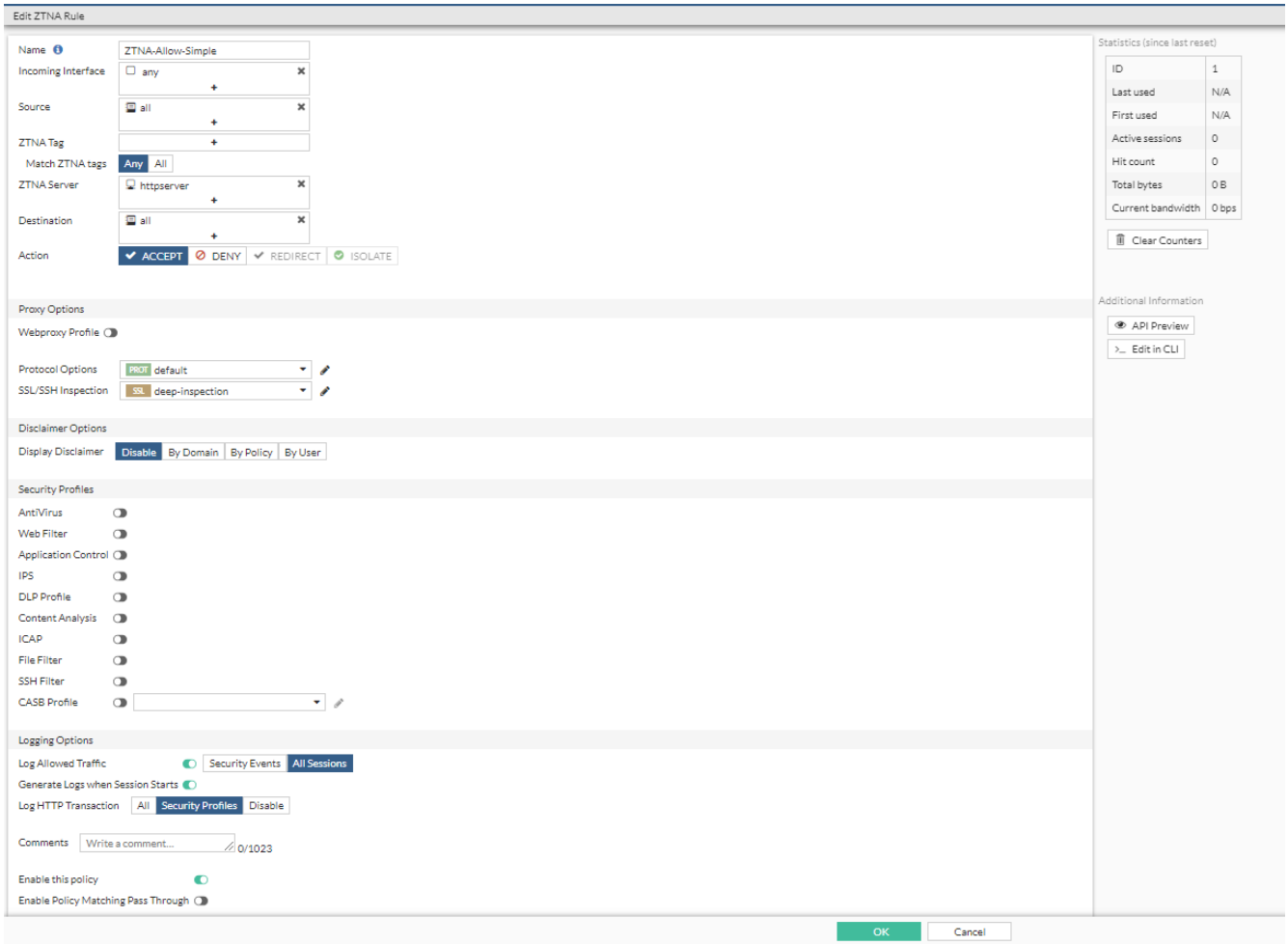


7. Click *OK*.

To configure ZTNA rules to allow traffic based on security posture tags in the GUI:

1. Go to *Policy & Objects* > *ZTNA*.
2. Create a ZTNA rule to allow traffic:
   a. Click *Create New*.
   b. Set *Name* to *ZTNA-Allow-Simple*.
   c. Set *Incoming Interface* to *port3*.

d. Set *Source* to *all*. This can also be set to specific IP addresses to only allow those addresses to connect to this HTTPS access proxy.
e. Add the ZTNA (posture) tag *Low*.
f. Select the ZTNA server *ZTNA-webserver*.
g. Configure the remaining options as needed.
h. Click *OK*.



To configure HTTPS access in the CLI:

1. Configure the access proxy VIP:

```
config firewall vip
    edit "httpsvip"
        set type access-proxy
        set extip 10.1.1.14
        set extintf "any"
        set server-type https
        set extport 9443
        set ssl-certificate "Fortinet_SSL"
```

```
    next
end
```

2. Configure the server and path mapping:

```
config firewall access-proxy
    edit "httpserver"
        set vip "httpsvip"
        config api-gateway
            edit 1
                config realservers
                    edit 1
                        set ip 10.120.1.78
                    next
                end
            next
        end
    next
end
```

3. Configure a ZTNA rule:

```
config firewall policy
     edit 1
        set type access-proxy
        set uuid 286706fa-55b5-51ef-1b9a-e4ea291bae6a
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set access-proxy "httpserver"
        set logtraffic all
        set logtraffic-start enable
        set extended-log enable
        set ssl-ssh-profile "deep-inspection"
    next
end
```

Testing the remote access to the HTTPS access proxy

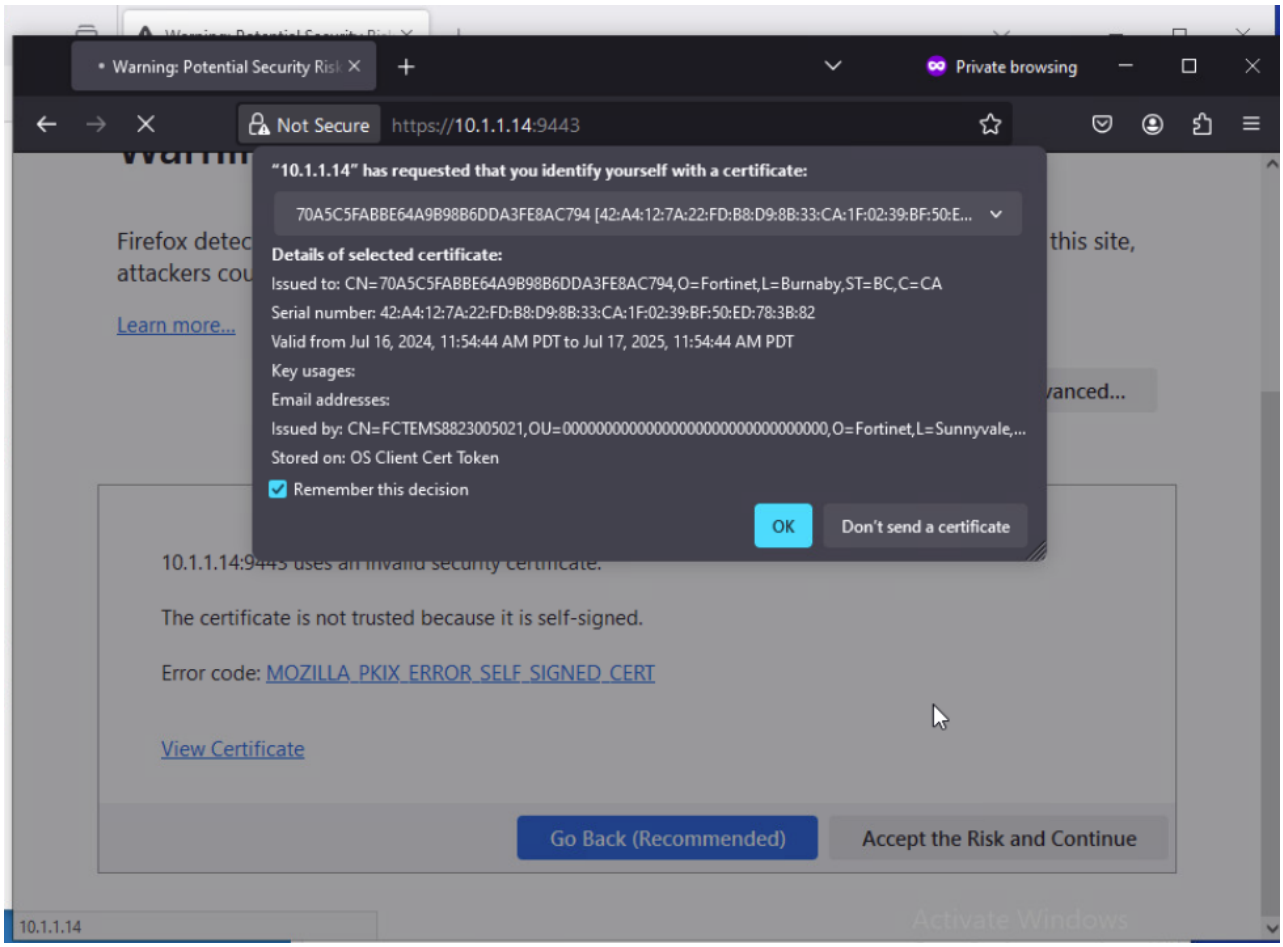
After FortiClient EMS and FortiProxy are configured, the HTTPS access proxy remote connection can be tested.

1. On the remote Windows PC, open FortiClient.
2. On the *Zero Trust Telemetry* tab, make sure that you are connected to the EMS server.

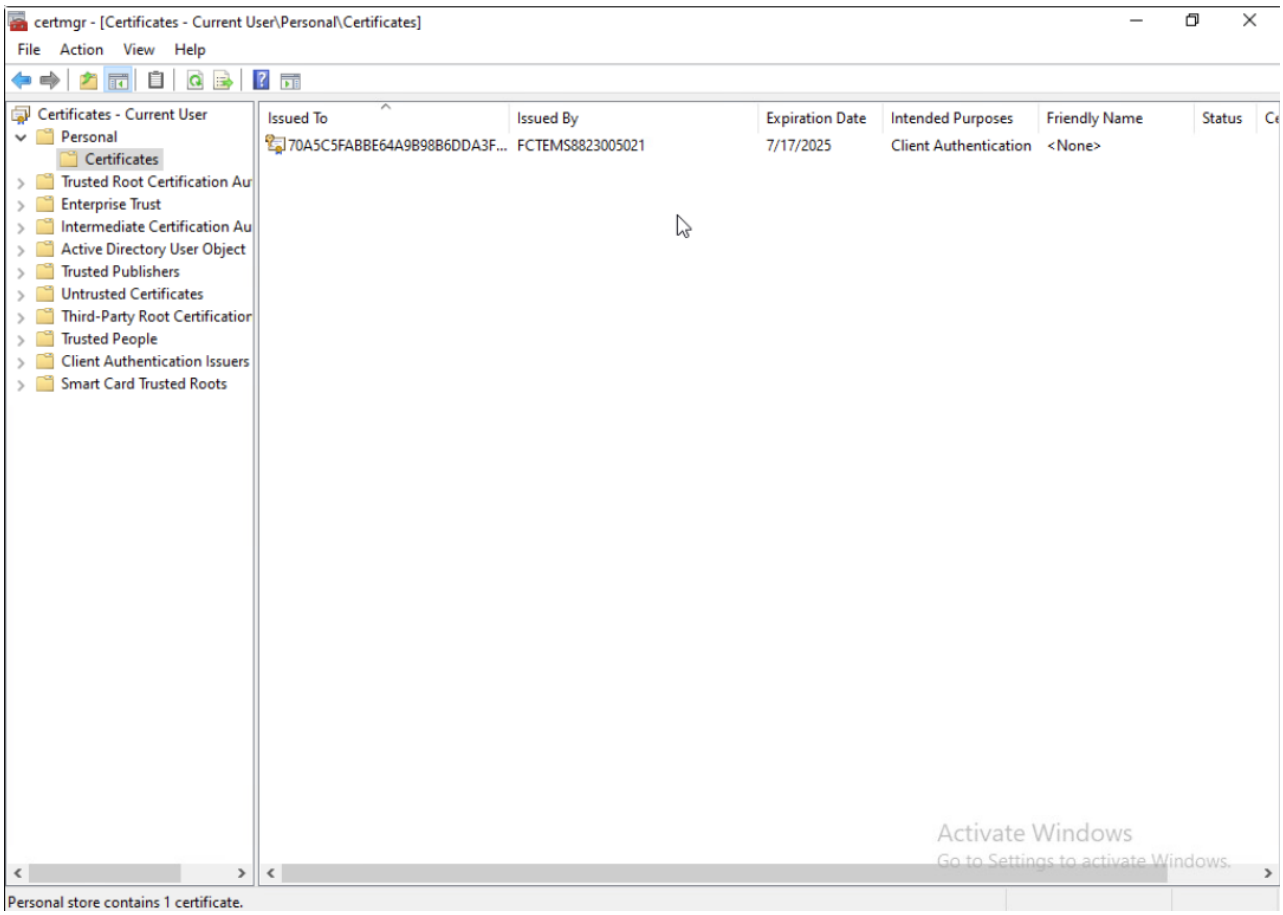


It is not necessary to configure a *ZTNA Destination* on FortiClient for the HTTPS access proxy use case. In fact, configuring a *ZTNA Destination* rule for the website may interfere with its operation.

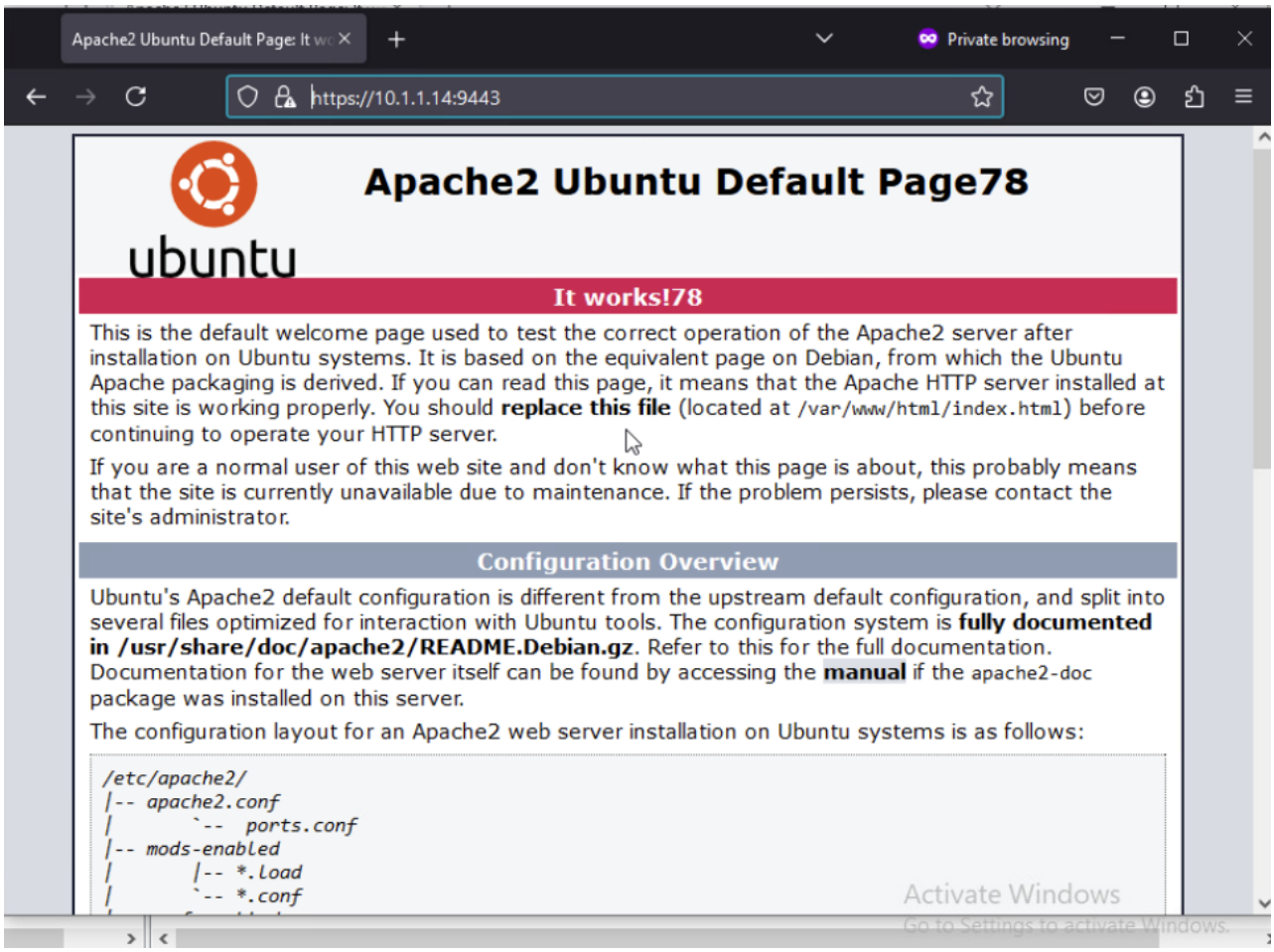
3. Open a browser and enter the address of the server and the access port. When entering the FQDN, make sure that the DNS can resolve the address to the IP address of the FortiProxy. In this example, webserver.ztnademo.com resolves to 10.1.1.14.
4. The browser prompts for the client certificate to use. Select the EMS signed certificate, then click *OK*.



The certificate is in the *User Configuration* store, under *Personal* > *Certificates*. The details show the SN of the certificate, which matches the record on the FortiClient EMS and the FortiProxy.



5. The client is verified by the FortiProxy to authenticate your identity.
6. The FortiProxy matches your security posture by verifying your security posture tag and matching the corresponding ZTNA rule, and you are allowed access to the web server.



Logs and debugs

```
# diagnose endpoint record list
Record #1:
                IP Address = 10.100.1.33
                MAC Address = 00:0c:29:71:39:17
                MAC list =
                VDOM = root (0)
                EMS serial number: FCTEMS8823005021
                EMS tenant id: 00000000000000000000000000000000
                Client cert SN: 42A4127A22FDB8D98B33CA1F0239BF50ED783B82
                Public IP address: 207.102.138.19
                Quarantined: no
                Online status: online
                Registration status: registered
                On-net status: on-net
                Gateway Interface: port1
                FortiClient version: 7.4.0
                AVDB version: 1.0
                FortiClient app signature version: 28.831
                FortiClient vulnerability scan engine version: 3.2
```

```
                FortiClient UID: 70A5C5FABBE64A9B98B6DDA3FE8AC794
                Host Name: DESKTOP-SNBQJ04
                OS Type: WIN64
                OS Version: Microsoft Windows 10 Professional Edition, 64-bit (build 19045)
                Host Description:
                Domain:
                Last Login User: guodong
                Owner:
                Host Model: VMware7,1
                Host Manufacturer: VMware, Inc.
                CPU Model: Intel(R) Xeon(R) CPU E5-2630 v2 @ 2.60GHz
                Memory Size: 8190
                AV Feature: 1
                FW Feature: 1
                WF Feature: 1
                AS Feature: 0
                VS Feature: 1
                VN Feature: 1
                Last vul message received time: N/A
                Last vul scanned time: N/A
                Last vul statistic: critical=0, high=0, medium=0, low=0, info=0
                Avatar fingerprint: 05b9940c015425a375caafa28096d695be6e9ad2
                Avatar source username:
                Avatar source email:
                Avatar source: OS
                Phone number:
                Number of Routes: (1)
                        Gateway Route #0:
                                - IP:10.100.1.33, MAC: 00:0c:29:71:39:17, VPN: no
                                - Interface:port1, VFID:0, SN: FPXVULTM24000082
online records: 1; offline records: 0; quarantined records: 0; out-of-sync records: 0

FPXVULTM24000082 # diagnose test application fcnacd 7

ZTNA Cache V2:
Entry #1:

 - UID: 70A5C5FABBE64A9B98B6DDA3FE8AC794
 - EMS Fabric ID: FCTEMS8823005021:00000000000000000000000000000000
 - Domain:
 - User: guodong
 - Owner:
 - Certificate SN: 42A4127A22FDB8D98B33CA1F0239BF50ED783B82
 - online: true
 - Routes (1):
  -- Route #0: IP=10.100.1.33, vfid=0
 - FWAddrNames (10):
  -- Name (#0): EMS1_ZTNA_disk-en
  -- Name (#1): MAC_EMS1_ZTNA_disk-en
  -- Name (#2): EMS1_ZTNA_Malicious-File-Detected
  -- Name (#3): MAC_EMS1_ZTNA_Malicious-File-Detected
  -- Name (#4): EMS1_CLASS_Low
```

```
  -- Name (#5): MAC_EMS1_CLASS_Low
  -- Name (#6): EMS1_ZTNA_all_registered_clients
  -- Name (#7): MAC_EMS1_ZTNA_all_registered_clients
  -- Name (#8): EMS1_ZTNA_anti-virus-ok
  -- Name (#9): MAC_EMS1_ZTNA_anti-virus-ok
lls_idx_mask = 0x00000001,

FPXVULTM24000082 # diagnose wad dev query-by uid 70A5C5FABBE64A9B98B6DDA3FE8AC794 FCTEMS8823005021
00000000000000000000000000000000
Attr of type=0, length=83, value(ascii)=70A5C5FABBE64A9B98B6DDA3FE8AC794
Attr of type=4, length=0, value(ascii)=
Attr of type=6, length=1, value(ascii)=true
Attr of type=5, length=40, value(ascii)=42A4127A22FDB8D98B33CA1F0239BF50ED783B82
Attr of type=3, length=17, value(ascii)=EMS1_ZTNA_disk-en
Attr of type=3, length=21, value(ascii)=MAC_EMS1_ZTNA_disk-en
Attr of type=3, length=33, value(ascii)=EMS1_ZTNA_Malicious-File-Detected
Attr of type=3, length=37, value(ascii)=MAC_EMS1_ZTNA_Malicious-File-Detected
Attr of type=3, length=14, value(ascii)=EMS1_CLASS_Low
Attr of type=3, length=18, value(ascii)=MAC_EMS1_CLASS_Low
Attr of type=3, length=32, value(ascii)=EMS1_ZTNA_all_registered_clients
Attr of type=3, length=36, value(ascii)=MAC_EMS1_ZTNA_all_registered_clients
Attr of type=3, length=23, value(ascii)=EMS1_ZTNA_anti-virus-ok
Attr of type=3, length=27, value(ascii)=MAC_EMS1_ZTNA_anti-virus-ok
Response termination due to no more data

FPXVULTM24000082 # execute log filter category 0

FPXVULTM24000082 # execute log filter field subtype ztna

FPXVULTM24000082 # execute log display
2 logs found.
2 logs returned.

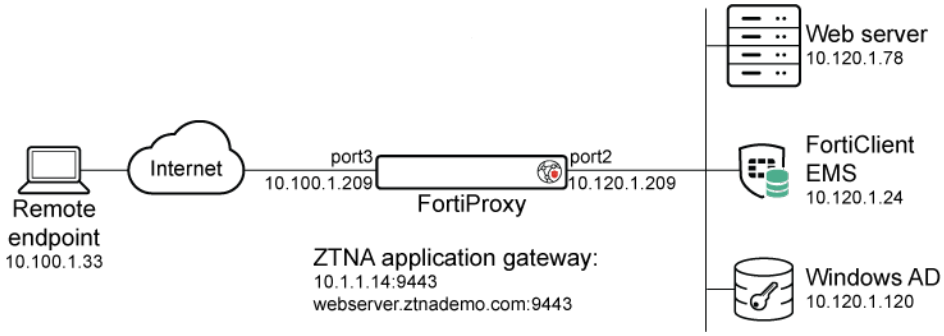
1: date=2024-08-08 time=15:02:00 eventtime=1723154519994707696 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.100.1.33 srcport=49397
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.120.1.78 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=2061742751
service="HTTPS" proxyapptype="http" proto=6 action="accept" policyid=1 policytype="proxy-policy"
poluuid="286706fa-55b5-51ef-1b9a-e4ea291bae6a" trandisp="snat" transip=10.120.1.209
transport=25370 clientip=10.100.1.33 duration=172200 gatewayid=1 vip="httpsvip"
accessproxy="httpserver" clientdevicemanageable="manageable" wanin=9606 rcvdbyte=9606 wanout=2047
lanin=2919 sentbyte=2919 lanout=9776 appcat="unscanned" utmaction="allow"

2: date=2024-08-08 time=14:59:04 eventtime=1723154343928534388 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.100.1.33 srcport=49394
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.120.1.78 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=2061742750
service="HTTPS" proxyapptype="http" proto=6 action="accept" policyid=1 policytype="proxy-policy"
poluuid="286706fa-55b5-51ef-1b9a-e4ea291bae6a" trandisp="snat" transip=10.120.1.209
transport=15780 clientip=10.100.1.33 duration=91259 gatewayid=1 vip="httpsvip"
accessproxy="httpserver" clientdevicemanageable="manageable" wanin=9609 rcvdbyte=9609 wanout=2047
lanin=2880 sentbyte=2880 lanout=9740 appcat="unscanned" utmaction="allow"
```

ZTNA HTTPS access proxy with basic authentication example

This example expands on the previous example (ZTNA HTTPS access proxy example on page 292), adding LDAP authentication to the ZTNA rule. Users are allowed based on passing the client certificate authentication check, user authentication, and security posture check.

Users that are in the AD security group *ALLOWED-VPN* are allowed access to the access proxy. Users that are not part of this security group are not allowed access.



This example assumes that the FortiProxy EMS fabric connector is already successfully connected.

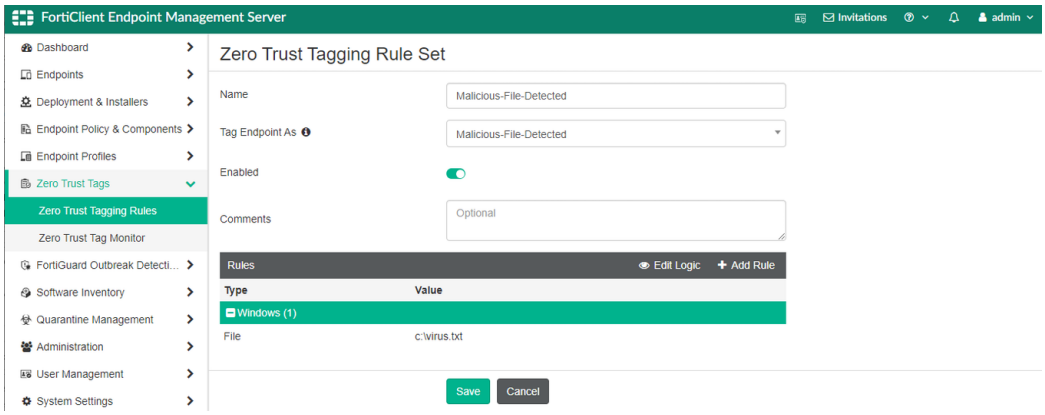
LDAP/Active Directory Users and Groups:

- Domain:qa.domaintest.local
- Users (Groups):
  - userb (Domain Users, Remote-Allowed)
  - userc (Domain Users)

This example uses two Zero Trust tags: one is the built-in *Low* tag used in ZTNA HTTPS access proxy example on page 292 and the other is the *Malicious-File-Detected* tag which you will create below.

To configure the *Malicious-File-Detected* tag on the FortiClient EMS:

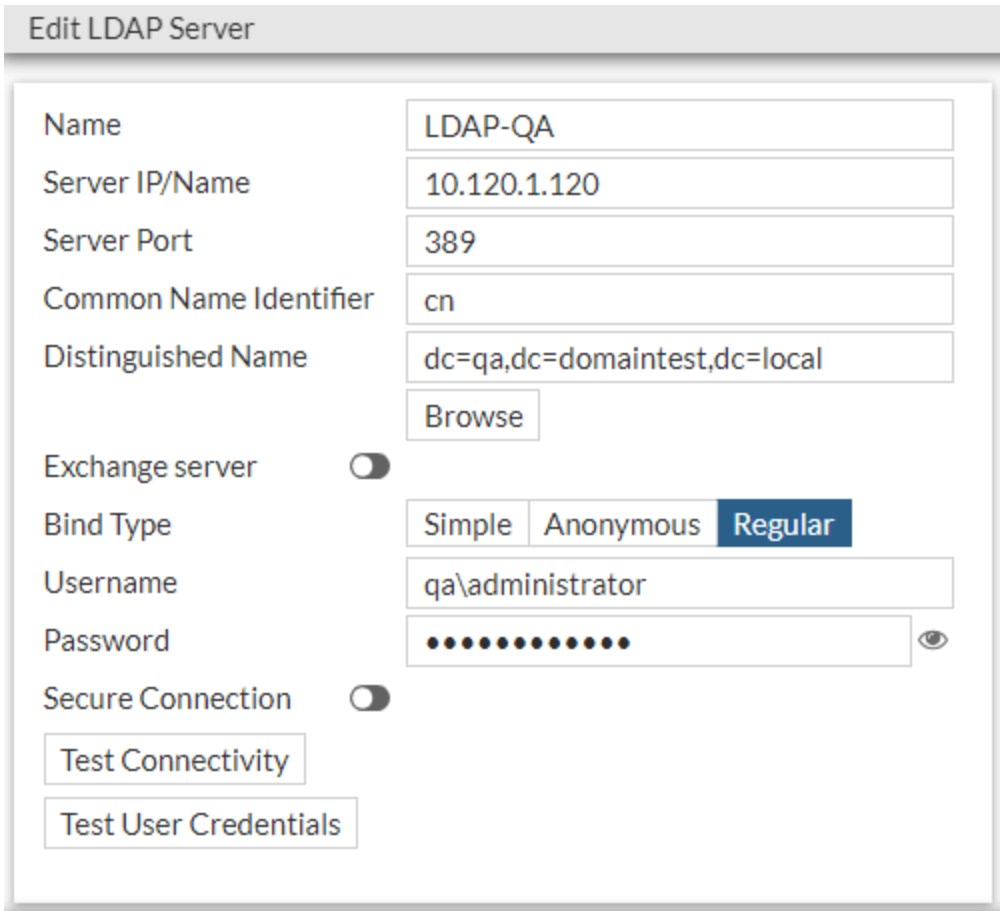
1. Log in to the FortiClient EMS.
2. Go to *Zero Trust Tags* > *Zero Trust Tagging Rules*, and click *Add*.
3. In the *Name* field, enter *Malicious-File-Detected*.
4. In the *Tag Endpoint As* dropdown list, select *Malicious-File-Detected*.
   EMS uses this tag to dynamically group together endpoints that satisfy the rule, as well as any other rules that are configured to use this tag.
5. Click *Add Rule* then configure the rule:
   a. For *OS*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *File* and click the + button.
   c. Enter a file name, such as *C:\virus.txt*.
   d. Click *Save*.



To configure a secure connection to the LDAP server in the GUI:

1. Go to *User & Authentication* > *LDAP Servers* and click *Create New*.
2. Configure the following settings:

Name	LDAP-QA
Server IP/Name	10.120.1.120
Server Port	389
Common Name Identifier	cn
Distinguished Name	dc=qa,dc=domaintest,dc=local
Exchange server	Disabled
Bind Type	Regular Enter the *Username* and *Password* for LDAP binding and lookup.
Secure Connection	Disabled



3. Click *Test Connectivity* to verify the connection to the server.
4. Click *OK*.

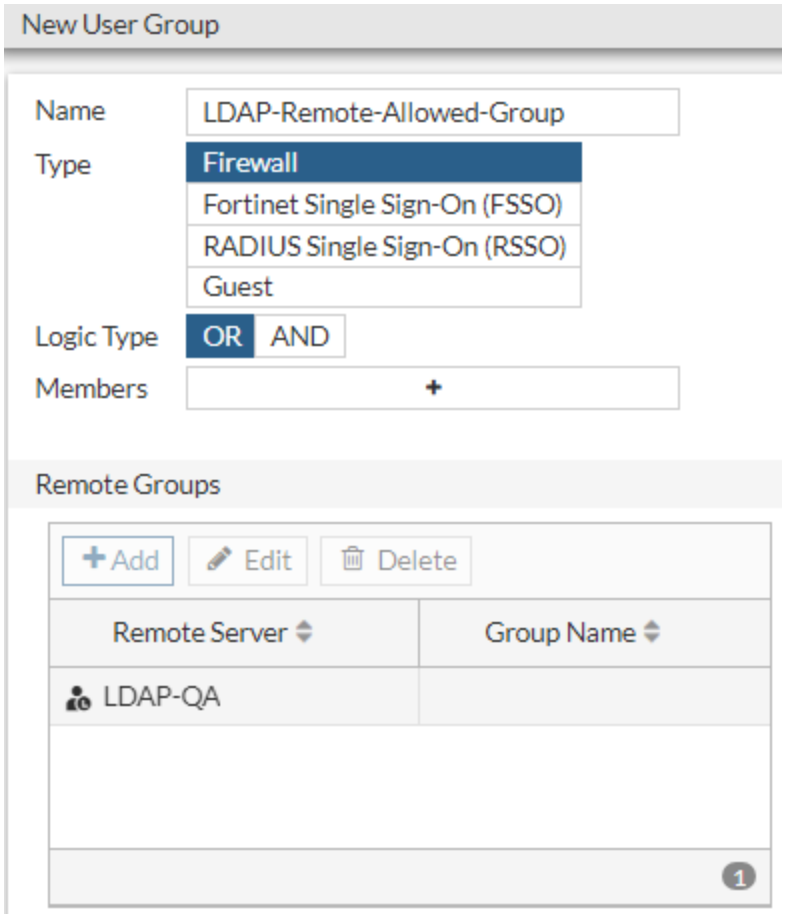
To configure a secure connection to the LDAP server in the CLI:

```
config user ldap
    edit "ldap-qa"
        set server "10.120.1.120"
        set cnid "cn"
        set dn "dc=qa,dc=domaintest,dc=local"
        set type regular
        set username <username>
        set password <password>
    next
end
```

To configure a remote user group from the LDAP server in the GUI:

1. Go to *User & Authentication* > *User Groups* and click *Create New*.
2. Set the name to *LDAP-Remote-Allowed-Group*.
3. Set *Type* to *Firewall*.
4. In the *Remote Groups* table click *Add*:

a. Set *Remote Server* to *LDAP-QA*.
b. Locate the *Remote-Allowed* group, right-click on it, and click *Add Selected*.
c. Click *OK*.



5. Click *OK*.

To configure a remote user group from the LDAP server in the CLI:

```
config user group
    edit "LDAP-Remote-Allowed-Group"
        set member "LDAP-QA"
        config match
            edit 1
                set server-name "LDAP-QA"
                set group-name "CN=usergrp1,CN=Users,DC=qa,DC=domaintest,DC=local"
            next
        end
    next
end
```

Authentication scheme and rules

After the LDAP server and user group have been configured, an authentication scheme and rule must be configured.

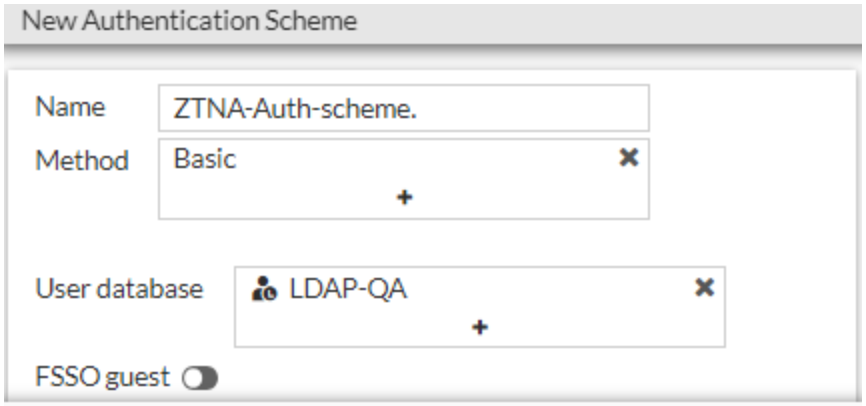
To configure authentication schemes and rules in the GUI, go to *System > Feature Visibility* and enable *Explicit Proxy*.

Authentication scheme

The authentication scheme defines the method of authentication that is applied. In this example, basic HTTP authentication is used so that users are prompted for a username and password the first time that they connect to a website through the HTTPS access proxy.

To configure an authentication scheme in the GUI:

1. Go to *Policy & Objects > Authentication Rules* and click *Create New > Authentication Scheme*.
2. Set the name to *ZTNA-Auth-scheme*.
3. Set *Method* to *Basic*.
4. Set *User database LDAP-QA* as the LDAP server.



5. Click *OK*.

To configure an authentication scheme in the CLI:

```
config authentication scheme
    edit "ZTNA-Auth-scheme"
        set method basic
        set user-database "LDAP-QA"
    next
end
```

Authentication rule

The authentication rule defines the proxy sources and destination that require authentication, and what authentication scheme is applied. In this example, active authentication through the basic HTTP prompt is used and applied to all sources.

To configure an authentication rule in the GUI:

1. Go to *Policy & Objects* > *Authentication Rules* and click *Create New* > *Authentication Rule*.
2. Set the name to *ZTNA-Auth-rule*.
3. Set *Source Address* to *all*.
4. Set *Protocol* to *HTTP*.
5. Enable *Authentication Scheme* and select *ZTNA-Auth-scheme*.
6. Click *OK*.

To configure an authentication rule in the CLI:

```
config authentication rule
    edit "ZTNA-Auth-rule"
        set srcaddr "all"
        set dstaddr "all"
        set active-auth-method "ZTNA-Auth-scheme"
    next
end
```

Applying the user group to a ZTNA rule

A user or user group must be applied to the ZTNA rule that you need to control user access to. The authenticated user from the authentication scheme and rule must match the user or user group in the ZTNA rule.

In this example, the user group is applied to the two ZTNA rules: one is the *ZTNA-Allow-Simple* rule configured in ZTNA HTTPS access proxy example on page 292 and the other is the *ZTNA-Deny-malicious* rule which you will create below.

To configure ZTNA rules to deny traffic based on user groups in the GUI:

1. Go to *Policy & Objects* > *ZTNA*.
2. Create the *ZTNA-Deny-malicious* rule to deny traffic based on user groups:
   a. Click *Create New*.
   b. Set *Name* to *ZTNA-Deny-malicious*.
   c. Set *Incoming Interface* to *port3*.
   d. Click in the *Source* field, select the *User* tab, select the *LDAP-Remote-Denied-Group* group, then click *Close*.
   e. Add the ZTNA (posture) tag *Malicious-File-Detected*.
      This tag is dynamically retrieved from EMS when you first created the Zero Trust Tagging Rule.

   f. Select the ZTNA server *ZTNA-webserver*.
   g. Configure the remaining options as needed.
   h. Click *OK*.
3. Edit the *ZTNA-Allow-Simple* rule to allow traffic based on user groups:
   a. Edit the *ZTNA-Allow-Simple* rule.
   b. Click in the *Source* field, select the *User* tab, select the *LDAP-Remote-ALlowed-Group* group, then click *Close*.
   c. Click *OK*.

To apply a user group to the ZTNA rules in the CLI:

```
config firewall policy
     edit 0
        set type access-proxy
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set access-proxy "httpserver"
        set ztna-ems-tag "Malicious-File-Detected"
        set logtraffic all
        set logtraffic-start enable
        set log-http-transaction all
        set extended-log enable
        set groups "LDAP-Remote-Denied-Group"
        set ssl-ssh-profile "deep-inspection"

    next
    edit 1
        set type access-proxy
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set access-proxy "httpserver"
        set ztna-ems-tag "EMS1_CLASS_Low"
        set logtraffic all
        set logtraffic-start enable
        set log-http-transaction all
        set extended-log enable
        set groups "LDAP-Remote-Allowed-Group"
        set ssl-ssh-profile "deep-inspection"
    next
end
```

For configuration examples of ZTNA rules, see Configure a ZTNA rule on page 254.

Testing remote access to the HTTPS access proxy with user authentication

Scenario 1: access allowed - userb

1. On a remote Windows PC, open the FortiClient app, select the *Zero Trust Telemetry* tab, and confirm that you are connected to the EMS server.

   It is not necessary to configure a *ZTNA Destination* on the FortiClient for the HTTPS access proxy use case. In fact, configuring a *ZTNA Destination* rule for the website may interfere with its operation.

2. In a browser, enter the address of the server and the access port.
3. When the browser asks for the client certificate to use, select the EMS signed certificate, then click *OK*.

   The client certificate is verified by the FortiProxy to authenticate your identity.
4. When prompted, enter the username *userb* and the password, and click *Sign in*.

   As *userb* is a member of the *Remote-Allowed-Group* group in Active Directory, it will match the *LDAP-Remote-Allowed-Group* user group. After the user authentication passes, the FortiProxy performs a posture check on the ZTNA group. When that passes, you are allowed access to the website.

Verifying the results

```
# diagnose firewall auth list

10.100.1.33, userb@qa.domaintest.local
        type: fw, id: 0, duration: 143, idled: 143
        expire: 457, allow-idle: 600
        packets: in 0 out 0, bytes: in 0 out 0
        group_id: 2
        group_name: LDAP-Remote-Allowed-Group

FPXVULTM24000082 # diagnose test app fcnacd 7

ZTNA Cache V2:
Entry #1:

 - UID: 70A5C5FABBE64A9B98B6DDA3FE8AC794
 - EMS Fabric ID: FCTEMS8823005021:00000000000000000000000000000000
 - Domain:
 - User: guodong
 - Owner:
 - Certificate SN: 42A4127A22FDB8D98B33CA1F0239BF50ED783B82
 - online: true
 - Routes (1):
  -- Route #0: IP=10.100.1.33, vfid=0
 - FWAddrNames (10):
  -- Name (#0): EMS1_ZTNA_disk-en
```

```
  -- Name (#1): MAC_EMS1_ZTNA_disk-en
  -- Name (#2): EMS1_ZTNA_Malicious-File-Detected
  -- Name (#3): MAC_EMS1_ZTNA_Malicious-File-Detected
  -- Name (#4): EMS1_CLASS_Low
  -- Name (#5): MAC_EMS1_CLASS_Low
  -- Name (#6): EMS1_ZTNA_all_registered_clients
```



The user_name is the windows log in username learned by FortiClient. It might not match the username used in firewall user authentication.

```
  -- Name (#7): MAC_EMS1_ZTNA_all_registered_clients
  -- Name (#8): EMS1_ZTNA_anti-virus-ok
  -- Name (#9): MAC_EMS1_ZTNA_anti-virus-ok
lls_idx_mask = 0x00000001,

FPXVULTM24000082 # execute log filter category 0
FPXVULTM24000082 # execute log filter field subtype ztna
FPXVULTM24000082 # execute log display

1: date=2024-08-13 time=11:07:54 eventtime=1723572473800477245 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.100.1.33 srcport=56417
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.120.1.78 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=2061742765
service="HTTPS" proxyapptype="http" proto=6 action="accept" policyid=1 policytype="proxy-policy"
poluuid="286706fa-55b5-51ef-1b9a-e4ea291bae6a" trandisp="snat" transip=10.120.1.209
transport=26202 clientip=10.100.1.33 duration=176645 user="userb@qa.domaintest.local" group="LDAP-
Remote-Allowed-Group" gatewayid=1 vip="httpsvip" accessproxy="httpserver"
clientdeviceid="70A5C5FABBE64A9B98B6DDA3FE8AC794" clientdevicemanageable="manageable"
clientdevicetags="MAC_EMS1_ZTNA_anti-virus-ok/EMS1_ZTNA_anti-virus-ok/MAC_EMS1_ZTNA_all_
registered_clients/EMS1_ZTNA_all_registered_clients" emsconnection="online" wanin=9606
rcvdbyte=9606 wanout=2176 lanin=3059 sentbyte=3059 lanout=39375
fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794" appcat="unscanned" utmaction="allow"
```

Scenario 2: access denied – userc

1. If scenario 1 has just been tested, log in to the FortiProxy and deauthenticate the user:
   a. Go to *Dashboard > Users & Devices* and click the *User Monitor* widget to expand it.
   b. Select *userb* and click *Deauthenticate*.
2. On a remote Windows PC, open the FortiClient app, select the *Zero Trust Telemetry* tab, and confirm that you are connected to the EMS server.
3. In a browser, enter the address *webserver.ztnademo.com*.
4. When the browser asks for the client certificate to use, select the EMS signed certificate, then click *OK*. This option might not appear if you have already selected the certificate when testing scenario 1.

   The client certificate is verified by the FortiProxy to authenticate your identity.
5. When prompted, enter the username *userc* and the password, and click *Sign in*.

As *userc* is not a member of the *Remote-Allowed* group in Active Directory, it will not match the *LDAP-Remote-Allowed-Group* user group. Because no other rules are matched, this user is implicitly denied

Verifying the results

Go to *Dashboard > Users & Devices*, click the *User Monitor* widget to expand it and confirm that *userc* is listed but no applicable user group is returned.

```
# execute log display

1: date=2024-08-13 time=11:12:11 eventtime=1723572731860519937 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.100.1.33 srcport=56425
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.1.1.14 dstport=9443 dstintf="port1" dstintfrole="undefined" sessionid=2061742766
service="tcp/9443" proxyapptype="http" proto=6 action="deny" policyid=0 policytype="proxy-policy"
trandisp="snat" transip=10.120.1.209 transport=0 clientip=10.100.1.33 duration=6269
user="userc@qa.domaintest.local" vip="httpsvip" accessproxy="httpserver"
clientdeviceid="70A5C5FABBE64A9B98B6DDA3FE8AC794" clientdevicemanageable="manageable"
clientdevicetags="MAC_EMS1_ZTNA_anti-virus-ok/EMS1_ZTNA_anti-virus-ok/MAC_EMS1_ZTNA_all_
registered_clients/EMS1_ZTNA_all_registered_clients" emsconnection="online" msg="Traffic denied
because of failed to match a proxy-policy" wanin=0 rcvdbyte=0 wanout=0 lanin=2805 sentbyte=2805
lanout=61620 fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794" appcat="unscanned" crscore=30
craction=131072 crlevel="high"
```

ZTNA TCP forwarding access proxy example

In this example, a TCP forwarding access proxy (TFAP) is configured to demonstrate an HTTPS reverse proxy that forwards TCP traffic to the designated resource. The access proxy tunnels TCP traffic between the client and the FortiProxy over HTTPS, and forwards the TCP traffic to the protected resource. It verifies user identity, device identity, and trust context, before granting access to the protected source.

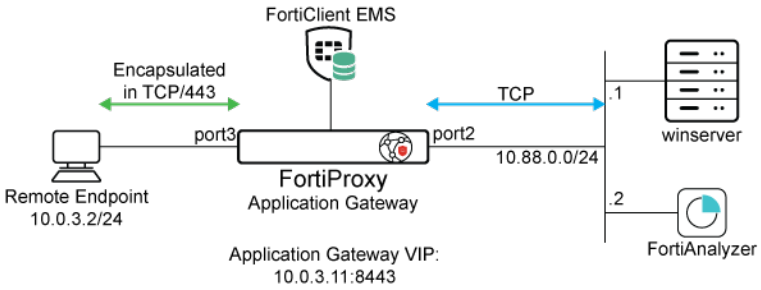
TCP forwarding access proxy supports communication between the client and the access proxy without SSL/TLS encryption. The connection still begins with a TLS handshake. The client uses the HTTP 101 response to switch protocols and remove the HTTPS stack. Further end to end communication between the client and server are encapsulated in the specified TCP port, but not encrypted by the access proxy. This improves performance by reducing the overhead of encrypting an already secured underlying protocol, such as RDP, SSH, or FTPS. Users should still enable the encryption option for end to end protocols that are insecure.

In this example, RDP (Remote Desktop Protocol) and SMB (Server Message Block) protocol access are configured to one server, and SSH access to the other server. Encryption is disabled for RDP and SSH, and enabled for SMB.



FortiClient (Windows) must be running 7.0.3 or later to detect SMB.

You cannot use ZTNA connection rules and TCP forwarding on a Windows 7 endpoint.



This example assumes that the FortiProxy EMS fabric connector is already successfully connected.

To configure the ZTNA server for TCP access proxy in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Servers* tab.
2. Click *Create New*.
3. Set *Name* to *ZTNA-tcp-server*.
4. Set *Interface* to *port3*. The *IP address* and *Port* fields are automatically set to the IP address of the selected interface and the default port 443.
   a. Set *External IP* to *10.0.3.11*.
   b. Set *External port* to *8443*.

   Verify that the IP address and port do not conflict with management access to the interface. Otherwise, change the IP address to another address on that subnet.
5. Select the *Default certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.
6. Add server mapping:
   a. In the *Service/server mapping* table, click *Create New*.
   b. Set *Service* to *TCP Forwarding*.
   c. In the *Server* section, click *Address* and create a new address for the FortiAnalyzer server at 10.88.0.2.
   d. Set *Port* to *22*.
   e. Click *OK*.
7. Click *OK*.
8. Use the CLI to add another server for the winserver server at 10.88.0.1 with ports 445 and 3389 to correspond to SMB and RDP:

```
config firewall access-proxy
    edit "ZTNA-tcp-server"
        config api-gateway
            edit 1
```

```
                config realservers
                    edit 0
            set address "winserver"
            set mappedport 445 3389
                    next
                end
             next
        end
    next
end
```

9. In the GUI, edit the ZTNA server named *ZTNA-tcp-server*, and verify the server mapping for winserver.

To configure a simple ZTNA policy to allow traffic to the TCP access proxy in the GUI:

1. Go to *Policy & Objects* > *Policy*, and click *Create New*.
2. Set *Name* to *ZTNA_remote*.
3. Set *Type* to *ZTNA*.
4. Set *Incoming Interface* to *port3*.
5. Set *Source* to *all*.
6. Select the ZTNA server *ZTNA-tcp-server*.
7. Configure the remaining options as needed.
8. Click *OK*.

To configure the access proxy VIP in the CLI:

```
config firewall vip
    edit "ZTNA-tcp-server"
        set type access-proxy
        set extip 10.0.3.11
        set extintf "port3"
        set server-type https
        set extport 8443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

To configure the server addresses in the CLI:

```
config firewall address
    edit "FAZ"
        set subnet 10.88.0.2 255.255.255.255
    next
    edit "winserver"
        set subnet 10.88.0.1 255.255.255.255
    next
end
```

To configure access proxy server mappings in the CLI:

```
config firewall access-proxy
    edit "ZTNA-tcp-server"
        set vip "ZTNA-tcp-server"
        config api-gateway
            edit 1
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "FAZ"
                        set mappedport 22
                    next
                    edit 2
                        set address "winserver"
                        set mappedport 445 3389
                    next
                end
            next
        end
    next
end
```

The mapped port (`mappedport`) restricts the mapping to the specified port or port range. If `mappedport` is not specified, then any port will be matched.

To configure a ZTNA rule (policy) in the CLI:

```
config firewall policy
    edit 11
        set name "ZTNA_remote"
        set srcintf "port3"
        set dstintf "any"
        set action accept
        set srcaddr "all"
        set dstaddr "ZTNA-tcp-server"
        set schedule "always"
        set logtraffic all
        set nat enable
    next
end
```

For configuration examples using full ZTNA policy, see Configure a ZTNA rule on page 254.

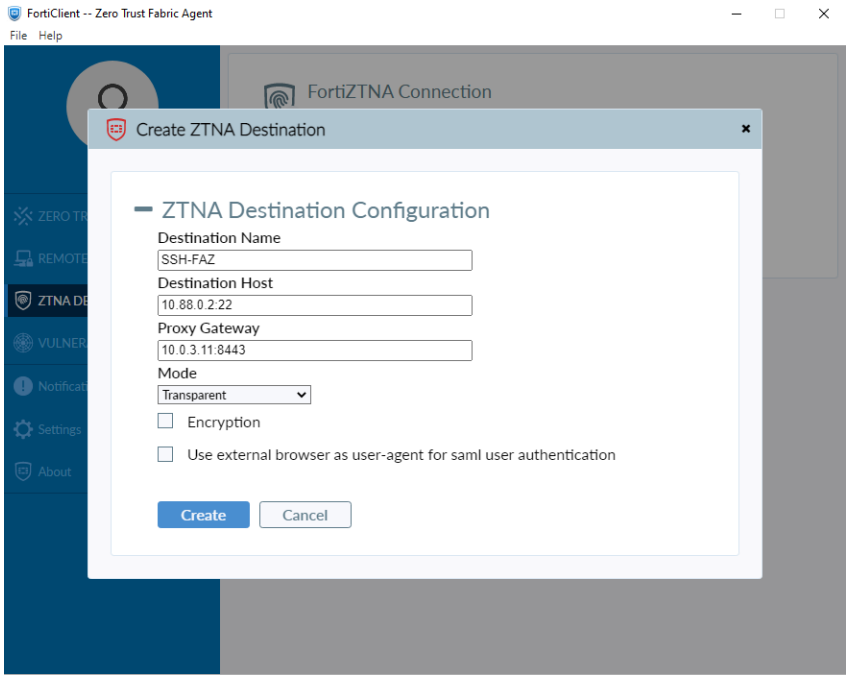
Test the connection to the access proxy

Before connecting, users must have a ZTNA connection rule in FortiClient.

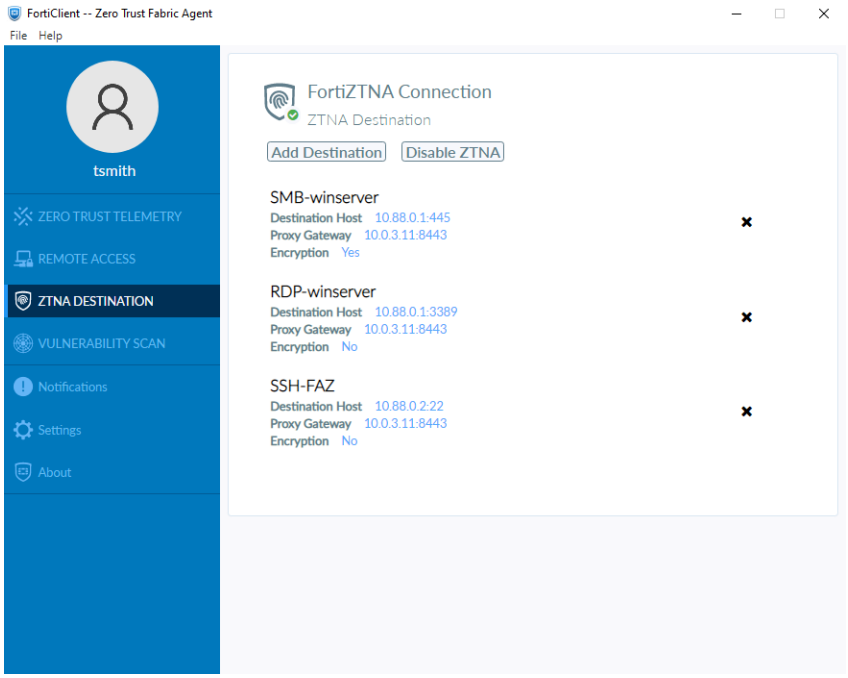
ZTNA TCP forwarding rules can be provisioned from the EMS server.

To create a ZTNA Destination in FortiClient:

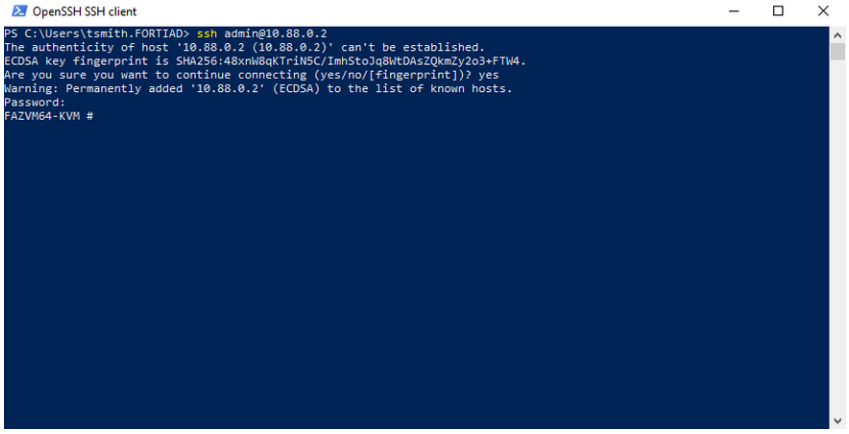
1. On the *ZTNA Destination* tab, click *Add Destination*.
2. Set *Destination Name* to *SSH-FAZ*.
3. Set *Destination Host* to *10.88.0.2:22*. This is the real IP address and port of the server.
4. Set *Proxy Gateway* to *10.0.3.11:8443*. This is the access proxy address and port that are configured on the FortiProxy.
5. Leave *Encryption* disabled. This option determines whether or not the Client to FortiProxy access proxy connection is encrypted in HTTPS.

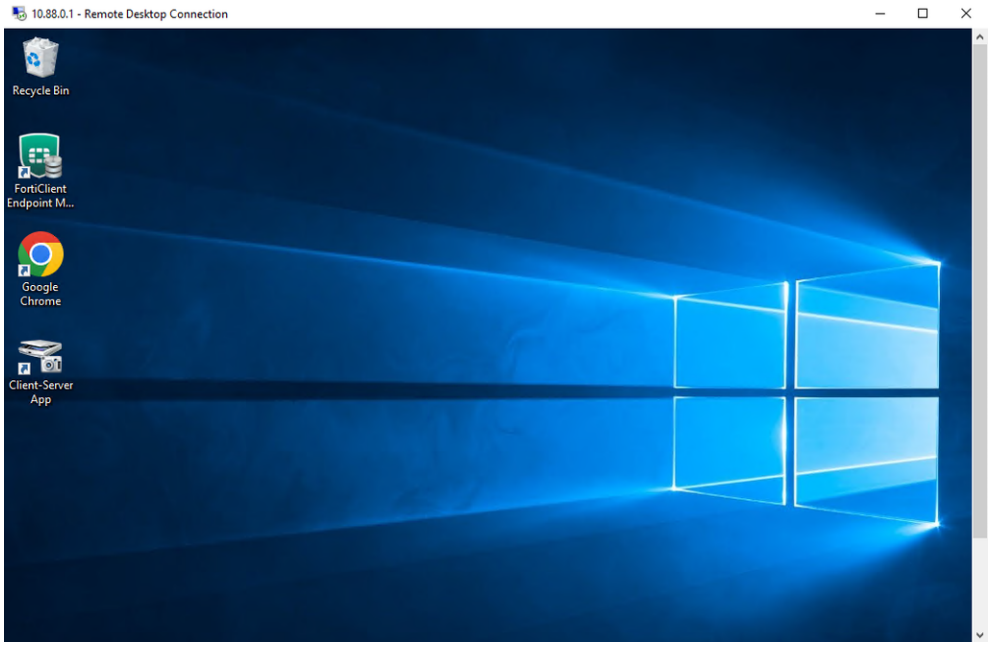


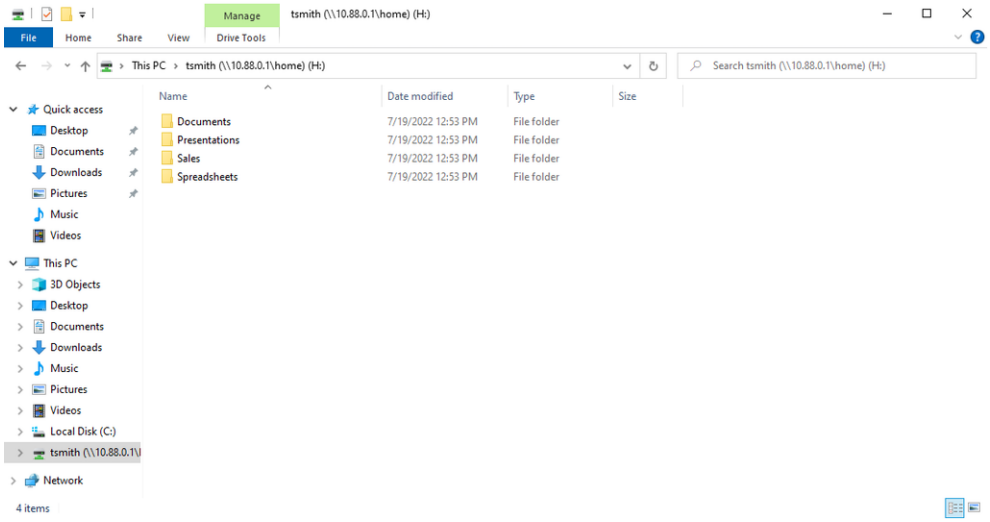
6. Click *Create*.
7. Create a second rule with the following settings:
   - *Rule Name*: *RDP-winserver*
   - *Destination Host*: *10.88.0.1:3389*
   - *Proxy Gateway*: *10.0.3.11:8443*
   - *Encryption*: Disabled
8. Create a third rule with the following settings:
   - *Rule Name*: *SMB-winserver*
   - *Destination Host*: *10.88.0.1:445*
   - *Proxy Gateway*: *10.0.3.11:8443*
   - *Encryption*: Enabled



After creating the ZTNA connection rules, you can SSH, RDP, and SMB directly to the server IP address and port.







Logs

```
# execute log filter category 0
# execute log filter field subtype ztna
# execute log display
```

SSH:

```
1: date=2023-05-04 time=11:56:35 eventtime=1683226594376318600 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2 srcport=62958
srcintf="port3" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved" dstip=10.88.0.2
dstport=22 dstintf="port2" dstintfrole="dmz" sessionid=31382 srcuuid="b458a65a-f759-51ea-d7df-
```

```
ef2e750026d1" service="SSH" proxyapptype="http" proto=6 action="accept" policyid=11
policytype="policy" poluuid="a63a424a-eaa9-51ed-cf84-b36eec5d2195" policyname="ZTNA_remote"
duration=178 gatewayid=1 vip="ZTNA-tcp-server" accessproxy="ZTNA-tcp-server"
clientdevicemanageable="manageable" wanin=2821 rcvdbyte=2821 wanout=2705 lanin=4556 sentbyte=4556
lanout=5087 appcat="unscanned"
```

RDP:

```
1: date=2023-05-04 time=11:59:14 eventtime=1683226753600713941 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2 srcport=63053
srcintf="port3" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved" dstip=10.88.0.1
dstport=3389 dstintf="port2" dstintfrole="dmz" sessionid=31513 srcuuid="b458a65a-f759-51ea-d7df-
ef2e750026d1" service="RDP" proxyapptype="http" proto=6 action="accept" policyid=11
policytype="policy" poluuid="a63a424a-eaa9-51ed-cf84-b36eec5d2195" policyname="ZTNA_remote"
duration=13 gatewayid=1 vip="ZTNA-tcp-server" accessproxy="ZTNA-tcp-server"
clientdevicemanageable="manageable" wanin=1588 rcvdbyte=1588 wanout=1040 lanin=2893 sentbyte=2893
lanout=3854 appcat="unscanned"
```

SMB:

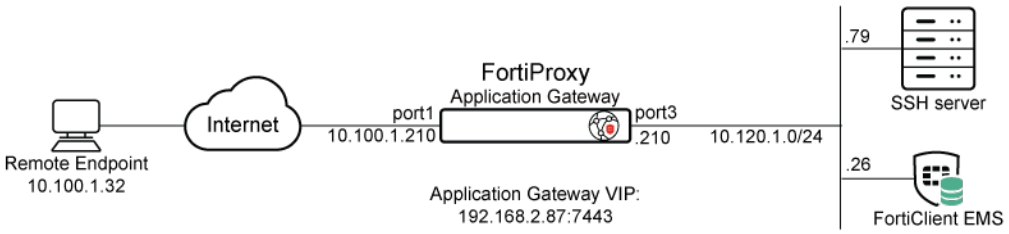
```
1: date=2023-05-04 time=12:15:07 eventtime=1683227707205696615 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2 srcport=63113
srcintf="port3" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved" dstip=10.88.0.1
dstport=445 dstintf="port2" dstintfrole="dmz" sessionid=31635 srcuuid="b458a65a-f759-51ea-d7df-
ef2e750026d1" service="SMB" proxyapptype="http" proto=6 action="accept" policyid=11
policytype="policy" poluuid="a63a424a-eaa9-51ed-cf84-b36eec5d2195" policyname="ZTNA_remote"
duration=801 gatewayid=1 vip="ZTNA-tcp-server" accessproxy="ZTNA-tcp-server"
clientdevicemanageable="manageable" wanin=37670 rcvdbyte=37670 wanout=27153 lanin=33484
sentbyte=33484 lanout=44429 appcat="unscanned"
```

ZTNA SSH access proxy example

ZTNA can be configured with SSH access proxy to provide a seamless SSH connection to the server.

Advantages of using an SSH access proxy instead of a TCP forwarding access proxy include:

- Establishing device trust context with user identity and device identity checks.
- Applying SSH deep inspection to the traffic through the SSH related profile.
- Performing optional SSH host-key validation of the server.
- Using one-time user authentication to authenticate the ZTNA SSH access proxy connection and the SSH server connection.

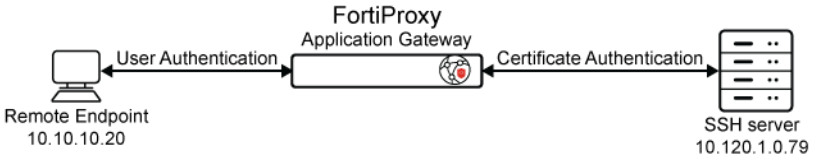


Perform SSH host-key validation of the server

To act as a reverse proxy for the SSH server, the FortiProxy must perform SSH host-key validation to verify the identity of the SSH server. The FortiProxy does this by storing the public key of the SSH server in its SSH host-key configurations. When a connection is made to the SSH server, if the public key matches one that is used by the server, then the connection is established. If there is no match, then the connection fails.

One-time user authentication

SSH access proxy allows user authentication to occur between the client and the access proxy, while using the same user credentials to authenticate with the SSH server. The following illustrates how this works:



1. The remote endpoint registers to FortiClient EMS and receives the client certificate.
2. The remote endpoint tries to connect to the SSH access proxy. It must use the same username that is later used for access proxy authentication.
3. The FortiProxy challenges the endpoint with device identity validation.
4. The remote endpoint provides the EMS issued certificate for device identification.
5. The FortiProxy challenges the endpoint with user authentication. For example, this could be done with basic or SAML authentication.
6. The users enters their credentials on the remote endpoint.
7. The FortiProxy authenticates the user and collects the username.
8. Using the FortiProxy's CA or the customer's CA certificate, the FortiProxy signs an SSH certificate and embeds the username in its principal.
9. The FortiProxy attempts to connect to the SSH server using the certificate authentication.
10. The SSH server verifies the authenticity of the certificate, and matches the username principal against its authorized_keys file.
11. If the username matches a record in the file, then the SSH connection is established. If no match is found, then the SSH connection fails.

Example

In this example, an SSH connection is established using SSH access proxy with host-key validation and one-time authentication.

- The SSH server is a Linux based server that uses sshd to provide remote access
- For SSH host-key validation, the public key of the SSH server has been imported into the FortiProxy.
- For one-time authentication using certificate authentication:
  - The SSH server must allow certificate authentication.
  - The SSH server must have the proper entry in its authorized_keys file that contains the user principal and the FortiProxy CA's public key.
  - The entry is present in the user directory corresponding to the user that is trying to log in.

To pre-configure the Linux SSH server:

1. Retrieve the public key used for host-key validation:
   a. Locate the public key files in the SSH server:

```
$ ls -la /etc/ssh/*.pub
-rw-r--r-- 1 root root 186 Mar 29  2020 /etc/ssh/ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root 106 Mar 29  2020 /etc/ssh/ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 406 Mar 29  2020 /etc/ssh/ssh_host_rsa_key.pub2
```

   b. Choose the public key file based on the hash type (in this case, ECDSA), and show it's content:

```
$ cat /etc/ssh/ssh_host_ecdsa_key.pub
ecdsa-sha2-nistp256 AAAAE2*********IpEik=
```

   This key will be used when configuring the FortiProxy.
2. Retrieve the FortiProxy CA’s public key from the FortiProxy:

```
# show full firewall ssh local-ca Fortinet_SSH_CA
config firewall ssh local-ca
    edit "Fortinet_SSH_CA"
        set password ENC <hidden password>
        set private-key "-----BEGIN OPENSSH PRIVATE KEY-----
<hidden private key>
-----END OPENSSH PRIVATE KEY-----"
        set public-key "ssh-rsa AAAAB3**********JLXlxj3”
        set source built-in
    next
end
```

3. On the Linux server, enable the SSH service to use the authorized_keys file:
   a. Locate and edit the */etc/ssh/sshd_config* file.
   b. Ensure that the *AuthorizedKeysFile* line is uncommented, for example:

```
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
```

4. Allow remote SSH log in with certificate authentication and principal name:
   a. Log in to the SSH server using the account that will be granted remote SSH access (in this example: *sshtest*):
   b. Locate the account's authorized_keys file in the *~/.ssh* directory:

```
$ ls -la ~/.ssh
total 12
drwxrwxr-x 2 sshtest sshtest 4096 Aug 10 19:14 .
drwxr-xr-x 5 sshtest sshtest 4096 Aug 10 19:13 ..
-rw-rw-r-- 1 sshtest sshtest  419 Aug 10 19:14 authorized_keys
```

   c. If the directory and file do not exist, create the directory:

```
$ mkdir ~/.ssh
```

   d. Create an entry containing the following keywords and add them to the authorized_keys file:

```
echo 'cert-authority,principals="sshtest" ssh-rsa AAAAB3**********JLXlxj3' >> authorized_
keys
```

   Where:
   - `cert-authority` - indicates that this entry is used in certificate authentication by validating the certificate using the public key provided in this entry.
   - `principals="sshtest"` - indicates the user that must match with the username embedded in the SSH certificate.
   - `ssh-rsa AAAAB3**********JLXlxj3` - indicates the FortiProxy CA's public key that is used to validate the SSH certificate.
5. Restart the sshd service:

```
$ sudo systemctl stop sshd
$ sudo systemctl start sshd
```

The SSH server can now accept SSH connection from *sshtest@<server IP>*, where the SSH certificate used by the FortiProxy to log in contains sshtest embedded as a principal.



When a user connects from a SSH client using *<username>@<server IP>*, sshd will locate the authorized_keys file in the directory */home/<username>/.ssh/authorized_keys*. If the authorized_keys is not in that directory, authentication will fail on the SSH server side.

If you suspect that authentication is failing on the SSH server, use the following commands to manually start sshd in debug mode to troubleshoot:

```
$ sudo systemctl stop sshd

$ /usr/sbin/sshd -ddd -p 22
```

To configure the FortiProxy :

1. Configure a new VIP to allow access to the SSH access proxy over 192.168.2.87:443:

```
config firewall vip
    edit "ZTNA_SSH"
        set type access-proxy
        set extip 10.1.1.13
        set extintf "any"
        set server-type https
        set extport 7443
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure the address object for the SSH server:

```
config firewall address
    edit "SSH_server"
        set subnet 10.120.1.79 255.255.255.255
    next
end
```

3. Configure the host-key that will be used to authenticate the SSH server. The public-key was retrieved when pre-configure the Linux SSH server (step 1b).

```
config firewall ssh host-key
    edit "ed25519"
        set type ECDSA
        set usage access-proxy
        set public-key "AAAAE2**********IpEik="
    next
end
```

4. Configure the access proxy SSH client certificate:

   A CA certificate is assigned to sign the SSH certificate that will be used in the SSH authentication. The SSH certificate will have the username embedded in the certificate principal.

```
config firewall access-proxy-ssh-client-cert
    edit "ssh-access-proxy"
        set source-address enable
        set auth-ca "Fortinet_SSH_CA"
    next
end
```

5. Configure the access-proxy server setting:

```
config firewall access-proxy
    edit "ZTNA_SSH"
        set vip "ZTNA_SSH"
        set client-cert enable
        config api-gateway
            edit 1
```

```
                set url-map "tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "SSH_server"
                        set type ssh
                        set ssh-client-cert "ssh-access-proxy"
                        set ssh-host-key-validation enable
                        set ssh-host-key "ed25519"
                    next
                end
            next
        end
    next
end
```

6. Configure the user setting, and user group to apply user authentication to the access proxy connection using local-user-db:

```
config user local
    edit ""sshtest"
        set type password
        set passwd-time 2024-09-11 13:05:32
        set passwd **********
    next
end
config user group
        edit "test-grp"
        set member "sshtest"
    next
end
```

7. Create the authentication scheme and rule to perform the authentication:

```
config authentication scheme
    edit "scheme-basic"
        set method basic
        set user-database "local-user-db"
    next
end
config authentication rule
    edit "rule-basic"
       set srcintf "any"
       set srcaddr "all"
       set dstaddr "all"
       set active-auth-method "scheme-basic"
    next
end
```

8. Configure the full ZTNA policy to allow traffic to the SSH server, and apply user authentication, posture check, and a security profile where necessary:

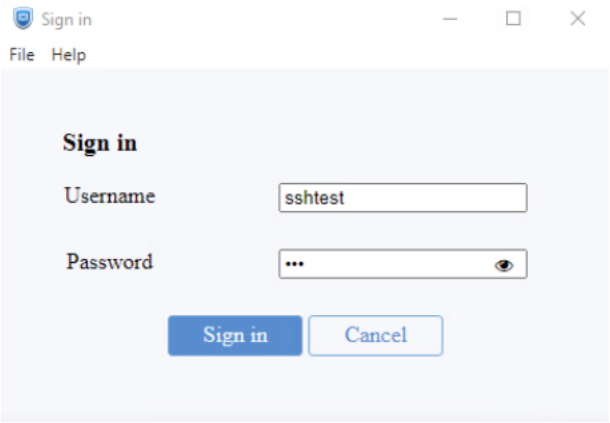
```
config firewall policy
    edit 3
       set type access-proxy
       set name "SSH-proxy"
       set uuid ba5687be-6fa2-51ef-a6be-59326c02ad24
       set srcintf "any"
       set srcaddr "all"
       set dstaddr "all"
       set action accept
       set schedule "always"
       set access-proxy "ZTNA_SSH"
       set ztna-ems-tag "EMS1_ZTNA_win10"
       set logtraffic all
       set log-http-transaction enable
       set extended-log enable
       set groups "test-grp"
    next
end
```

To check the results:

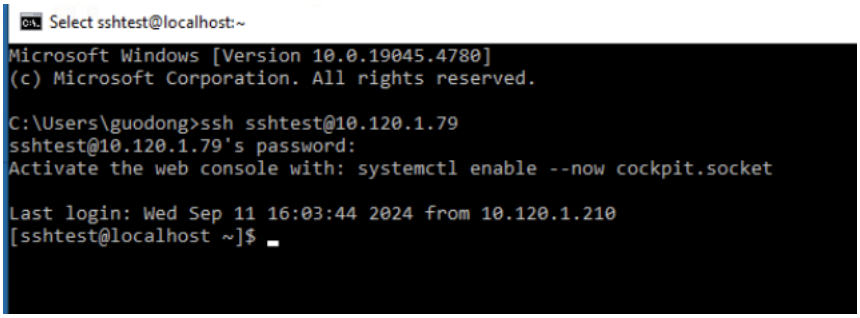
1. On the remote client, open FortiClient, go to the *Zero Trust Telemetry* tab, and make sure that it is connected to the EMS server.
2. Go to the *ZTNA Destination* tab and click *Add Destination*.
3. Configure the Destination, then click *Create*:

Rule Name	SSH-Linux
Destination Host	10.120.1.79:22
Proxy Gateway	10.1.1.13:7443
Mode	Transparent
Encryption	Disabled (recommended)

   When Encryption is disabled, the connection between the client and FortiProxy application gateway is not encapsulated in HTTPS after the client and FortiProxy connection is established. This allows for less overhead, because SSH is already a secure connection.
4. Open an SSH client, such as PuTTy, and make an SSH connection to *sshtest@10.120.1.79* on port *22*.
5. After device authentication is performed and passes in the background, FortiClient prompts the user to sign in. Enter the username, *sshtest*, and password, then click *Sign in*.



After successful user authentication, the SSH connection is established without an additional log in.



6. On the FortiProxy, check the logged in user:
   a. Go to *Dashboard > > User & Devices > User Monitor*.
   b. Check the WAD proxy user list:

```
# diagnose wad user list
ID: 22, VDOM: root, IPv4: 10.100.1.32
  user name    : sshtest
  worker       : 0
  duration     : 824 seconds
  auth_type    : IP
  auth_method  : Basic
  pol_id       : 3
  g_id         : 2
  user_based   : 0
  expire       : N/A (in use)
  LAN:
    bytes_in=5711 bytes_out=35720
  WAN:
    bytes_in=2617 bytes_out=3377
```

7. The successful connection is logged in the forward traffic logs after the SSH connection has disconnected:

```
# execute log display
25 logs found.
10 logs returned.
```

```
date=2024-09-11 time=13:13:12 eventtime=1726085591891200442 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.100.1.32 srcport=53562
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.120.1.79 dstport=22 dstintf="port1" dstintfrole="undefined" sessionid=598330087
service="SSH" proxyapptype="http" proto=6 action="accept" policyid=3 policytype="proxy-policy"
poluuid="ba5687be-6fa2-51ef-a6be-59326c02ad24" policyname="SSH-proxy" clientip=10.100.1.32
duration=564 user="sshtest" group="test-grp" gatewayid=1 vip="ZTNA_SSH" accessproxy="ZTNA_SSH"
clientdeviceid="F0D60B28FCAB464E81C725270B62BEC0" clientdevicemanageable="manageable"
clientdevicetags="MAC_EMS1_ZTNA_win10/MAC_EMS1_ZTNA_Anti_Virus/EMS1_ZTNA_Anti_Virus/MAC_EMS1_
ZTNA_all_registered_clients" emsconnection="online" wanin=0 rcvdbyte=0 wanout=0 lanin=1890
sentbyte=1890 lanout=1865 fctuid="F0D60B28FCAB464E81C725270B62BEC0" unauthuser="userb"
unauthusersource="forticlient" srcremote=207.102.138.19 appcat="unscanned"
```

ZTNA application gateway with SAML authentication example

SAML can be used with ZTNA as an authentication method. This allows user credentials to be stored remotely on an Identity Provider (IdP), with the FortiProxy acting as the Service Provider (SP) to redirect users to the IdP for authentication. Once authenticated, the FortiProxy as the trust broker can perform policy enforcement and authorization based on the SAML assertion that is returned.

For a basic configuration:

1. Configure a SAML SSO object on the FortiProxy.
2. Apply the SAML SSO object to an authentication scheme.
3. Apply SAML to the ZTNA server object.
4. Create a user group that uses the SAML SSO object as its remote authentication server.
5. Apply the user group to a ZTNA policy.

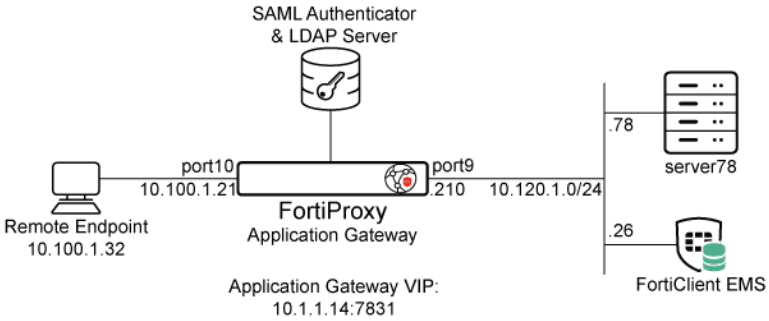
For a more advanced configuration, the group attribute returned from the SAML assertion from the IdP can be ignored and instead, the authenticated user can be queried using a different method, such as LDAP, to acquire its user group. The returned user group is then used for authorization on the ZTNA policy.

In this example, the configuration steps are:

1. Configure a SAML SSO object on the FortiProxy.
2. Configure an LDAP server object on the FortiProxy.
3. Apply the SAML SSO object to an authentication scheme, with the user-database configured to the LDAP server object.
4. Apply SAML to the ZTNA server object.
5. Create a user group that uses the LDAP server object as its remote authentication server.
6. Apply the user group to a ZTNA policy.

Example

In this example, an HTTPS access proxy is configured, and SAML authentication is applied to authenticate the client. The FortiProxy acts as the SAML SP and a SAML authenticator serves as the IdP. In addition to verifying the user and device identity with the client certificate, the user is also authorized based on user credentials to establish a trust context before granting access to the protected resource. The user group returned from the SAML assertion is overridden by the group returned from querying the LDAP server directly.



This example assumes that the FortiProxy EMS fabric connector is already successfully connected.

To configure the access proxy VIP:

```
config firewall vip
    edit "ZTNA_server01"
        set uuid 42123240-7087-51ef-0bc6-27c2c7abb7f8
        set type access-proxy
        set extip 10.1.1.14
        set extintf "any"
        set server-type https
        set extport 7831
        set ssl-certificate "Fortinet_SSL"
    next
end
```

To configure access proxy server mappings:

```
config firewall access-proxy
    edit "ZTNA_server01"
        set vip "ZTNA_server01"
        config api-gateway
            edit 1
                config realservers
                    edit 1
                        set ip 10.120.1.78
                    next
                end
            next
        end
```

```
   next
end
```

To configure a SAML server:

```
config user saml
    edit "fac_saml"
        set cert "Fortinet_SSL"
        set entity-id "https://10.120.1.210:7831/XX/YY/ZZ/saml/metadata/"
        set single-sign-on-url "https://10.120.1.210:7831/XX/YY/ZZ/saml/login/"
        set single-logout-url "https://10.120.1.210:7831/XX/YY/ZZ/saml/logout/"
        set idp-entity-id "http://10.120.1.206/saml-idp/z1l7z7jw5kt5tidy/metadata/"
        set idp-single-sign-on-url "https://10.120.1.206/saml-idp/z1l7z7jw5kt5tidy/login/"
        set idp-single-logout-url "https://10.120.1.206/saml-idp/z1l7z7jw5kt5tidy/logout/"
        set idp-cert "REMOTE_Cert_1"
        set user-name "username
        set group-name "groupname"
        set digest-method sha1
    next
end
```

To map the SAML server into an access proxy configuration:

```
config firewall access-proxy
    edit "ZTNA_server01"
        set vip "ZTNA_server01"
        config api-gateway
             edit 3
                set service samlsp
                set saml-server "fac_saml"
            next
        end
    next
end
```

To configure an LDAP server and an LDAP server group to verify user groups:

```
config user ldap
    edit "ldap"
        set server "10.120.1.120"
        set cnid "cn"
        set dn "dc=qa,dc=domaintest,dc=com"
        set type regular
        set username ""qa\\administrator"
        set password **********
    next
end
```

```
config user group
    edit "ldap-group-saml"
```

```
        set member "ldap"
        config match
          edit 1
               set server-name "ldap"
               set group-name "CN=usergrp1,CN=Users,DC=qa,DC=domaintest,DC=com"
    next
end
```

To configure the authentication rule and scheme to match the new SAML server:

```
config authentication rule
    edit "fac_saml_rule"
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set ip-based disable
        set active-auth-method "fac_saml_scheme"
        set web-auth-cookie enable
    next
end
```

```
config authentication scheme
    edit "fac_saml_scheme"
        set method saml
        set saml-server "fac_saml"
        set saml-timeout 120
        set user-database "ldap"
    next
end
```

To enable user group authentication in a policy:

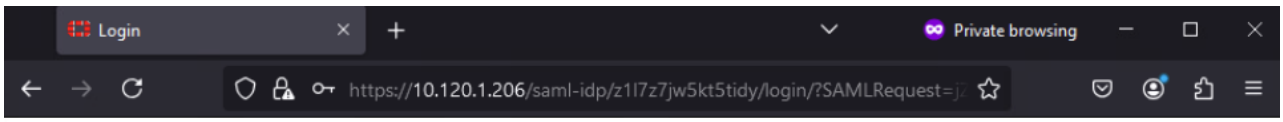
```
config firewall policy
    edit 5
       set type access-proxy
       set name "ZTNA_remote"
       set uuid 7dd3f902-7088-51ef-1c79-61ffa38b91b2
       set srcintf "any"
       set srcaddr "all"
       set dstaddr "all"
       set action accept
       set schedule "always"
       set access-proxy "ZTNA_server01"
       set logtraffic all
       set log-http-transaction enable
       set extended-log enable
       set groups "ldap-group-saml"
       set ssl-ssh-profile "certificate-inspection"
    next
end
```

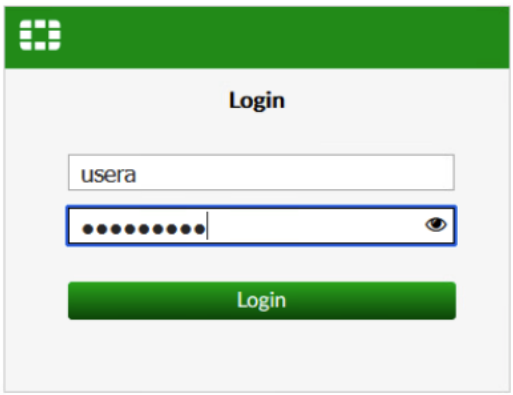
Testing the connection

To test the connection:

It is not necessary to configure a *ZTNA Destination* on the FortiClient for the HTTPS access proxy use case. In fact, configuring a *ZTNA Destination* rule for the website may interfere with its operation.

1. On a client PC, try to access the webpage through the HTTPS access proxy. For example, go to http://10.1.1.14:7831 in a browser.
2. The client PC is prompted for a client certificate. After the certificate is validated, you are redirected to a SAML log in portal.





3. Enter your user credentials. The SAML server authenticates and sends a SAML assertion response message to the FortiProxy.
4. The FortiProxy queries the LDAP server for the user group, and then verifies the user group against the groups or groups defined in the proxy policy.
5. The user is proxied to the webpage on the real web server.

Logs and debugs

Use the following command to check the user information after the user has been authenticated:

```
# diagnose wad user list
ID: 13, VDOM: root, IPv4: 10.100.1.32
  user name    : usera@qa.domaintest.com
  worker       : 0
  duration     : 14 seconds
  auth_type    : Session
  auth_method  : SAML
  pol_id       : 5
  g_id         : 4
  user_based   : 0
  expire       : N/A (in use)
  LAN:
    bytes_in=404 bytes_out=8369
  WAN:
    bytes_in=0 bytes_out=0
```

Event log:

```
date=2024-09-11 time=15:25:15 eventtime=1726093514754345944 tz="-0700" logid="0102043025"
type="event" subtype="user" level="notice" vd="root" logdesc="Explicit proxy authentication
successful" srcip=10.100.1.32 dstip=10.120.1.210 authid="fac_saml_rule"
user="usera@qa.domaintest.com" authproto="HTTP(10.100.1.32)" action="authentication"
status="success" reason="Authentication succeeded" msg="User usera@qa.domaintest.com succeeded in
authentication
```

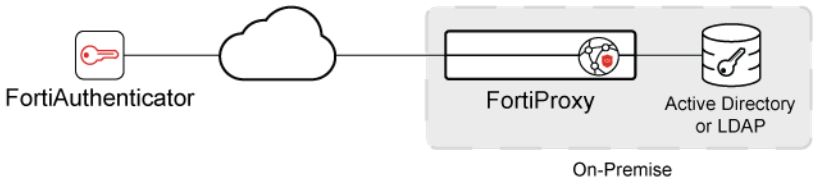
Traffic log:

```
date=2024-09-11 time=15:28:06 eventtime=1726093685808900790 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.100.1.32 srcport=53762
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.120.1.78 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=1148927321
service="HTTPS" proxyapptype="http" proto=6 action="accept" policyid=5 policytype="proxy-policy"
poluuid="7dd3f902-7088-51ef-1c79-61ffa38b91b2" policyname="ZTNA_remote" clientip=10.100.1.32
duration=188580 user="usera@qa.domaintest.com" group="ldap-group-saml" gatewayid=1 vip="ZTNA_
server01" accessproxy="ZTNA_server01" clientdevicemanageable="manageable" wanin=9606 rcvdbyte=9606
wanout=2065 lanin=3516 sentbyte=3516 lanout=11202 fctuid="F0D60B28FCAB464E81C725270B62BEC0"
unauthuser="userb" unauthusersource="forticlient" srcremote=207.102.138.19 appcat="unscanned"
utmaction="allow"
```

Secure LDAP connection from FortiAuthenticator with zero trust tunnel example

When an on-premise Active Directory or LDAP server must be accessed remotely, a secure connection is important. LDAP without security should not be exposed on the internet, as user information and passwords are transferred in plain text.

This example describes how to configure a secure LDAP connection from a remote FortiAuthenticator to an on-premise AD server.

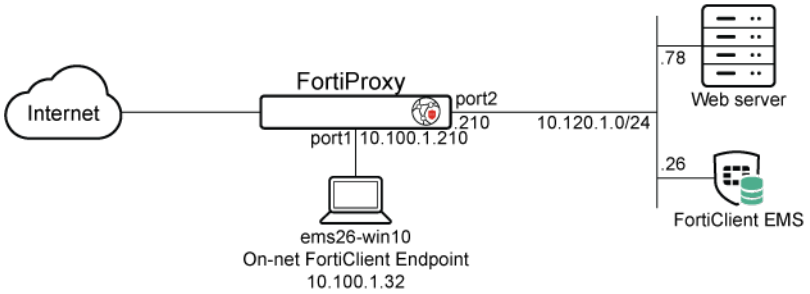


The on-premise FortiProxy acts as a ZTNA application gateway to allow the FortiAuthenticator access to the AD using a TCP forwarding access proxy. Traditionally, this requires endpoints to have FortiClient installed with ZTNA destinations configured in order to connect and authenticate with a client certificate. In this scenario, the FortiAuthenticator will operate a local certificate authority, which generates a client certificate for the connection. The local root CA certificate is exported and installed on the FortiProxy in order to authenticate and trust the client connection. This replaces the need for a FortiClient EMS server to manage the client certificate and act as the certificate authority.

For detailed configuration steps, see Setting up a zero trust tunnel on the FortiAuthenticator page.

Access control between on-net devices and internal web server using security posture tags

In this example, policies are configured that use security posture tags to control access between on-net devices and an internal web server. This mode does not require the use of the access proxy, and only uses security posture tags for access control. Traffic is passed when the FortiClient endpoint is tagged with the customized security posture tag, identifying the device as logged on. Traffic is denied when the FortiClient endpoint is tagged with *Malicious-File-Detected*.



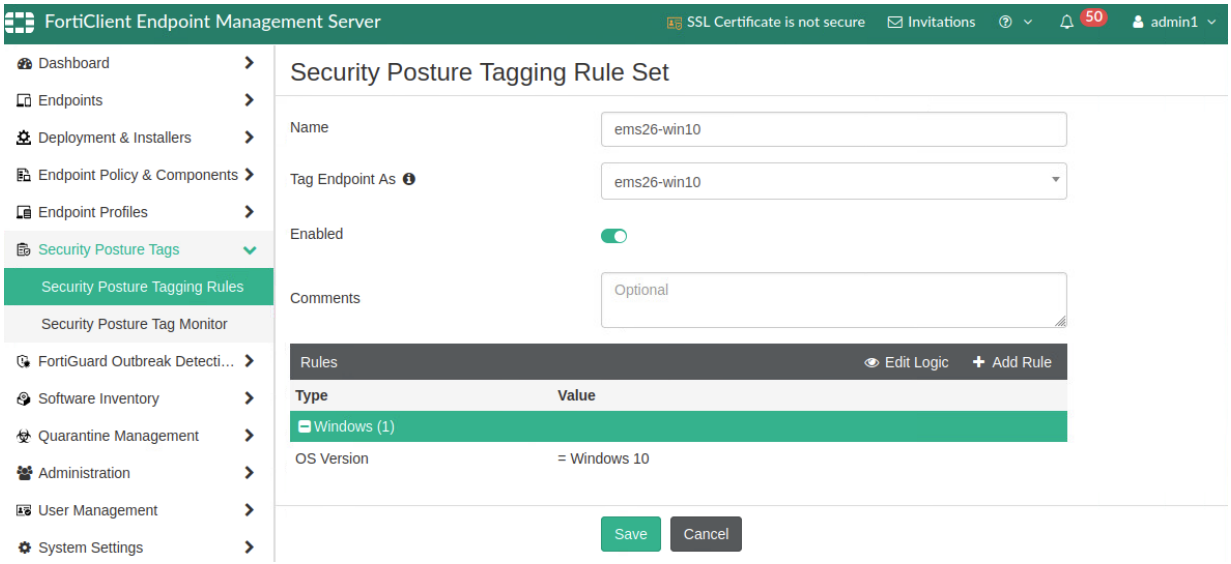
This example assumes that the FortiProxy EMS fabric connector is already successfully connected.

To configure ZTNA in the GUI, go to *System* > *Feature Visibility* and enable *Zero Trust Network Access*.

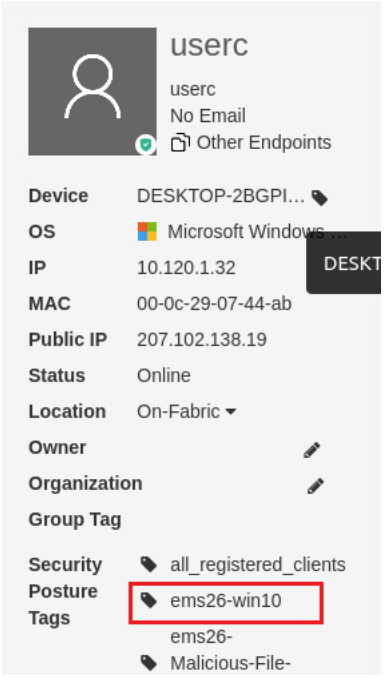
To configure a security posture tag on the FortiClient EMS:

1. Log in to the FortiClient EMS.
2. Go to *Security posture tags* > *Security posture tagging rules*, and click *Add*.
3. In the *Name* field, enter *ems26-win10*.
4. In the *Tag Endpoint As* dropdown list, select the custom tag.
5. Click *Add Rule* and configure the rule so that the client computer can fulfill this rule:

a. For *OS*, select *Windows*.
b. From the *Rule Type* dropdown list, select *File* and click the + button.
c. Enter a file name, such as *C:\virus.txt*.
d. Click *Save*.



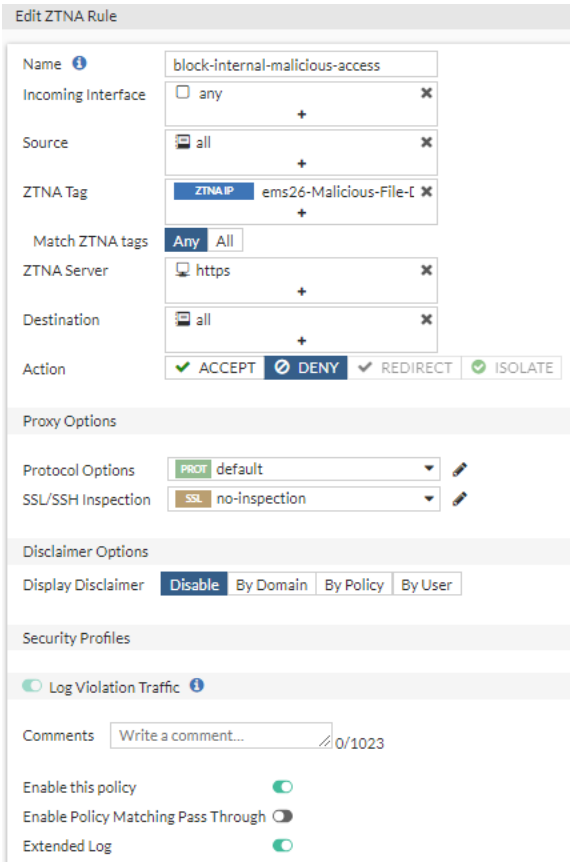
6. Go to *Endpoint > All Endpoints*.
7. Select the computer that will be granted access. This computer should be already registered to FortiClient EMS.
8. Ensure that the computer fulfills the custom tag you defined earlier.



9. Click *Save*.

To configure a ZTNA rule to deny traffic in the GUI:

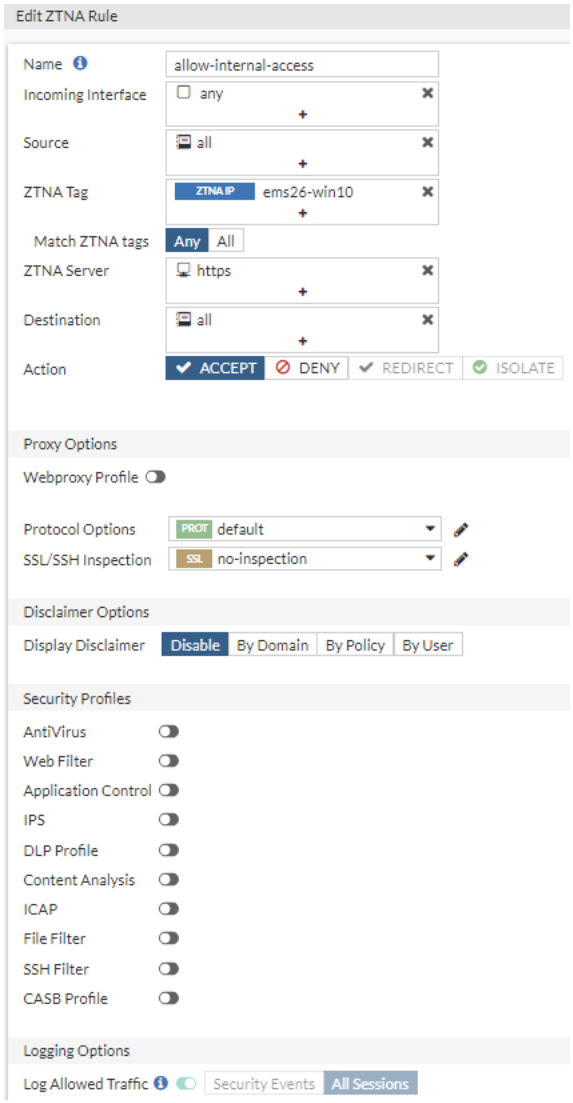
1. Go to *Policy & Objects > ZTNA* and click *Create New* on the *ZTNA Rules* tab.
2. Set *Name* to *block-internal-malicious-access*.
3. Set *Action* to *DENY*.
4. Set *Incoming Interface* to *any*.
5. Set *Source* to *all*.
6. Set *ZTNA Tag* to *EMS1_ZTNA_Malicious-File-Detected*.
7. Set *Destination* to the address of the Web server.
8. Enable *Log Violation Traffic*.
9. Configure the remaining settings as needed.
10. Click *OK*.



To configure a ZTNA rule to allow access in the GUI:

1. Go to *Policy & Objects > ZTNA* and click *Create New* on the *ZTNA Rules* tab.
2. Set *Name* to *allow-internal-access*.
3. Set *Action* to *ACCEPT*.
4. Set *Incoming interface* to *any*.
5. Set *Source* to *all*.
6. Set *Destination* to the address of the Web server.
7. Enable *Log allowed traffic* and set it to *All Sessions*.

8. Configure the remaining settings as needed.
9. Click *OK*.



To configure policies to block and allow access in the CLI:

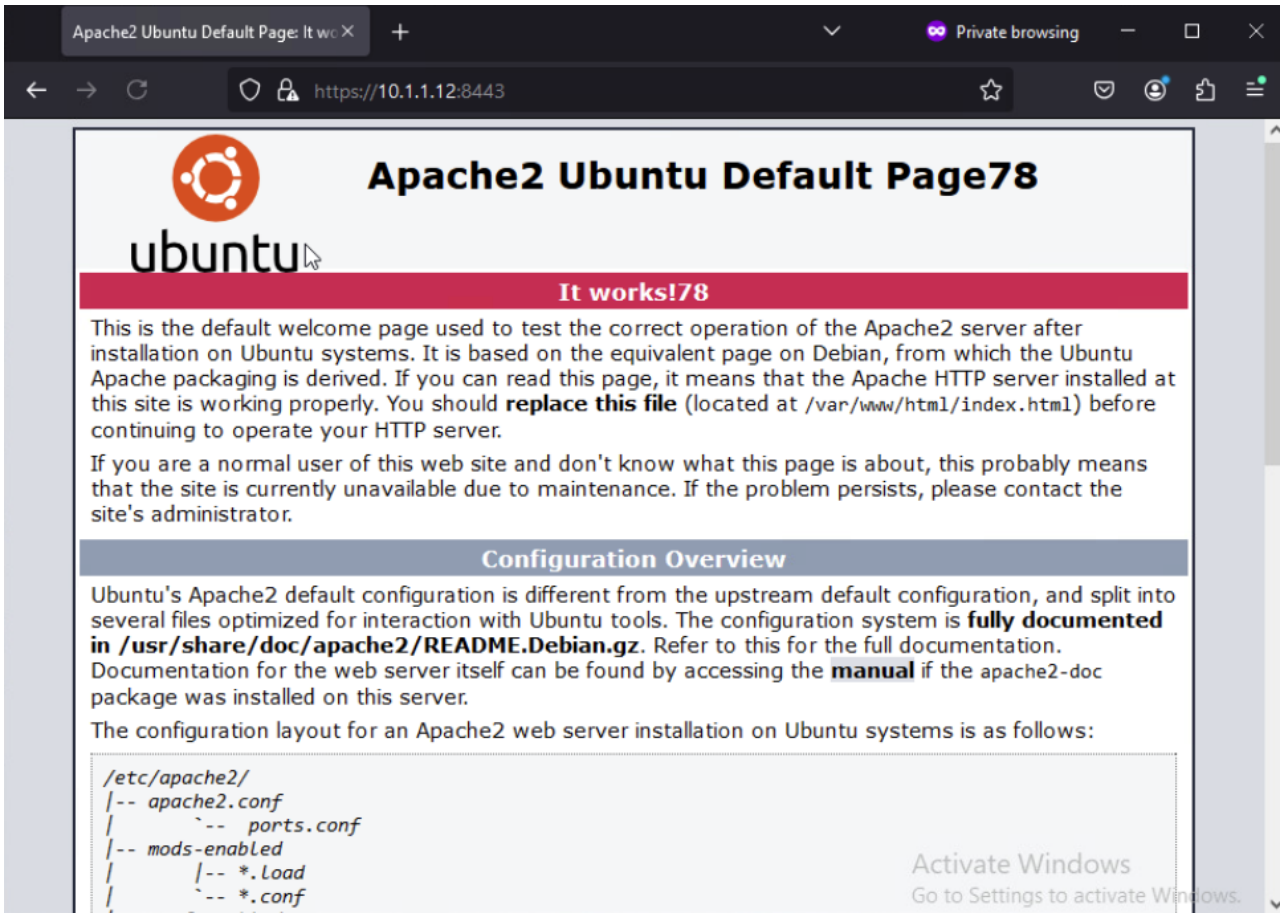
```
config firewall policy
    edit 6
        set type access-proxy
        set name "block-internal-malicious-access"
        set uuid 13ece116-7218-51ef-626c-66ba0f7c3dbd
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set access-proxy "https"
        set ztna-ems-tag "EMS1_ZTNA_ems26-Malicious-File-Detected"
        set logtraffic all
```

```
        set log-http-transaction enable
        set extended-log enable
    next
    edit 7
        set type access-proxy
        set name "allow-internal-access"
        set uuid 36296498-7218-51ef-5625-d2e3c7b5e6a2
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set access-proxy "https"
        set ztna-ems-tag "EMS1_ZTNA_ems26-win10"
        set logtraffic all
        set log-http-transaction enable
        set extended-log enable
    next
end
```

Testing the access to the web server from the on-net client endpoint

Access allowed:

1. On the client computer, open FortiClient.
2. On the *Zero Trust Telemetry* tab, make sure that you are connected to the EMS server.
3. Open a browser and enter the address of the server.
4. The FortiProxy matches your security posture by verifying your security posture tags and matching the corresponding `allow-internal-access` policy, and you are allowed access to the web server.



Logs and debugs

Access allowed:

```
# diagnose endpoint record list
Record #2:
                IP Address = 10.120.1.32
                MAC Address = 00:0c:29:07:44:ab
                MAC list =
                VDOM = root (0)
                EMS serial number: FCTEMS8824006853
                EMS tenant id: 00000000000000000000000000000000
                Client cert SN: 97B05CC32B3C2BC73DE7D7C09AE6A867DAA0BD8C
                Public IP address: 207.102.138.19
                Quarantined: no
                Online status: online
                Registration status: registered
                On-net status: on-net
                Gateway Interface: port1
                FortiClient version: 7.4.0
                …
                Number of Routes: (1)
```

```
                        Gateway Route #0:
                                - IP:10.120.1.32, MAC: 00:0c:29:07:44:ab, VPN: no
                                - Interface:port1, VFID:0, SN: FPXVULTM24000083
```

```
# diagnose wad dev query-by uid F0D60B28FCAB464E81C725270B62BEC0 FCTEMS8824006853
00000000000000000000000000000000
Attr of type=0, length=83, value(ascii)=F0D60B28FCAB464E81C725270B62BEC0
Attr of type=4, length=0, value(ascii)=
Attr of type=6, length=1, value(ascii)=true
Attr of type=5, length=40, value(ascii)=97B05CC32B3C2BC73DE7D7C09AE6A867DAA0BD8C
Attr of type=3, length=39, value(ascii)=EMS1_ZTNA_ems26-Malicious-File-Detected
Attr of type=3, length=43, value(ascii)=MAC_EMS1_ZTNA_ems26-Malicious-File-Detected
Attr of type=3, length=21, value(ascii)=EMS1_ZTNA_ems26-win10
Attr of type=3, length=25, value(ascii)=MAC_EMS1_ZTNA_ems26-win10
Attr of type=3, length=26, value(ascii)=EMS1_ZTNA_ems26_Anti_Virus
Attr of type=3, length=30, value(ascii)=MAC_EMS1_ZTNA_ems26_Anti_Virus
Attr of type=3, length=32, value(ascii)=EMS1_ZTNA_all_registered_clients
Attr of type=3, length=36, value(ascii)=MAC_EMS1_ZTNA_all_registered_clients
Attr of type=3, length=15, value(ascii)=EMS1_CLASS_High
Attr of type=3, length=19, value(ascii)=MAC_EMS1_CLASS_High
Response termination due to no more data
```

```
# diagnose firewall dynamic list
List all dynamic addresses:
IP dynamic addresses in VDOM root(vfid: 0):
…
CMDB name: EMS1_ZTNA_ems26-Malicious-File-Detected
TAG name: ems26-Malicious-File-Detected
EMS1_ZTNA_ems26-Malicious-File-Detected: ID(22)
        ADDR(10.120.1.32)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 1.

...
CMDB name: EMS1_ZTNA_ems26-win10
TAG name: ems26-win10
EMS1_ZTNA_ems26-win10: ID(131)
        ADDR(10.120.1.12)
        ADDR(10.120.1.32)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 2.

...
```

```
# diagnose test application fcnacd 7
Entry #1:
 - UID: F0D60B28FCAB464E81C725270B62BEC0
 - EMS Fabric ID: FCTEMS8824006853:00000000000000000000000000000000
 - Domain:
 - User: userc
```

```
 - Owner:
 - Certificate SN: 97B05CC32B3C2BC73DE7D7C09AE6A867DAA0BD8C
 - online: true
 - Routes (1):
  -- Route #0: IP=10.120.1.32, vfid=0
 - FWAddrNames (10):
  -- Name (#0): EMS1_ZTNA_ems26-Malicious-File-Detected
  -- Name (#1): MAC_EMS1_ZTNA_ems26-Malicious-File-Detected
  -- Name (#2): EMS1_ZTNA_ems26-win10
  -- Name (#3): MAC_EMS1_ZTNA_ems26-win10
  -- Name (#4): EMS1_ZTNA_ems26_Anti_Virus
  -- Name (#5): MAC_EMS1_ZTNA_ems26_Anti_Virus
  -- Name (#6): EMS1_ZTNA_all_registered_clients
  -- Name (#7): MAC_EMS1_ZTNA_all_registered_clients
  -- Name (#8): EMS1_CLASS_High
  -- Name (#9): MAC_EMS1_CLASS_High
lls_idx_mask = 0x00000001,
```

```
date=2024-09-18 time=15:01:13 eventtime=1726696873510296962 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.32 srcport=57720
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.100.1.78 dstport=443 dstintf="port2" dstintfrole="undefined" sessionid=49073183
service="HTTPS" proxyapptype="http" proto=6 action="accept" policyid=7 policytype="proxy-policy"
poluuid="36296498-7218-51ef-5625-d2e3c7b5e6a2" policyname="allow-internal-access"
clientip=10.120.1.32 duration=176570 gatewayid=1 vip="https" accessproxy="https"
clientdeviceid="F0D60B28FCAB464E81C725270B62BEC0" clientdevicemanageable="manageable"
clientdevicetags="MAC_EMS1_CLASS_High/EMS1_CLASS_High/MAC_EMS1_ZTNA_all_registered_clients/EMS1_
ZTNA_all_registered_clients" emsconnection="online" wanin=9606 rcvdbyte=9606 wanout=2047
lanin=2920 sentbyte=2920 lanout=9776 fctuid="F0D60B28FCAB464E81C725270B62BEC0" unauthuser="userc"
unauthusersource="forticlient" srcremote=207.102.138.19 appcat="unscanned" utmaction="allow"
```

UTM scanning on TCP forwarding access proxy traffic

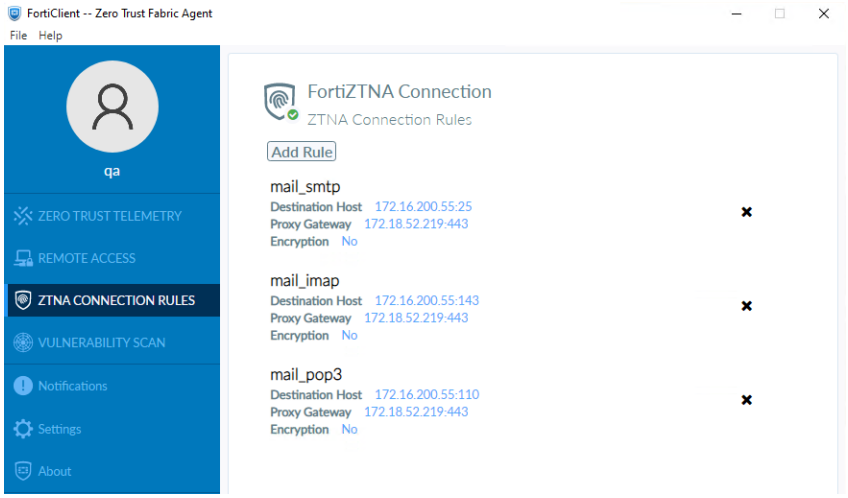
UTM scanning and deep inspection is supported for multiple protocols in a ZTNA TCP forwarding access proxy. In addition to HTTP and HTTPS, the mail protocols (SMTP, IMAP, and POP3) and file sharing protocols (SMB and CIFS) are supported.

Examples

AV scanning for normal POP3, IMAP, and SMTP traffic

To configure AV scanning for normal POP3, IMAP, and SMTP traffic:

1. In FortiClient, add ZTNA connection rules for the email server IP and POP3, IMAP, and SMTP ports.

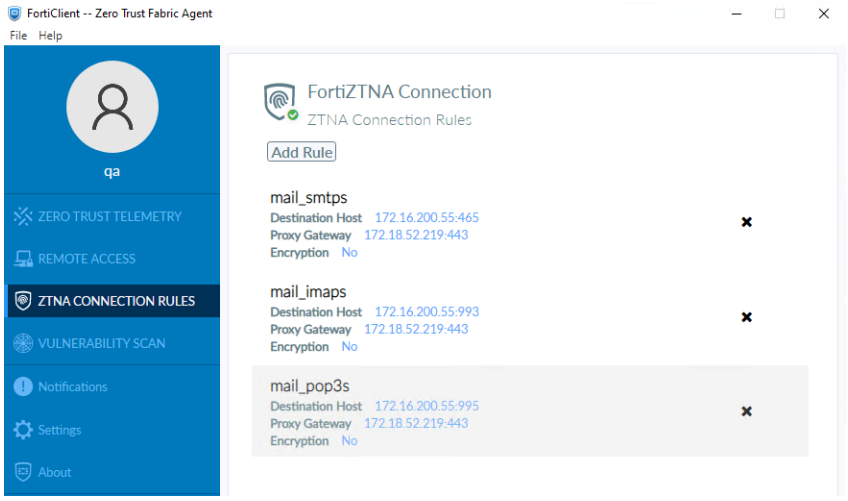


2. On the FortiProxy, configure the ZTNA TCP forwarding server to add the email server address and enable AV profile scanning in the ZTNA rules.
3. On the client PC, open Outlook app and send emails with attachments containing virus affected files.
4. The ZTNA rule on the FortiProxy blocks the email send/receive traffic and generates AV logs.

AV deep scanning for SSL encrypted POP3S, IMAPS, and SMTPS traffic

To configure AV deep scanning for SSL encrypted POP3S, IMAPS, and SMTPS traffic:

1. In FortiClient, add ZTNA connection rules for the email server IP and POP3S, IMAPS, and SMTPS ports.

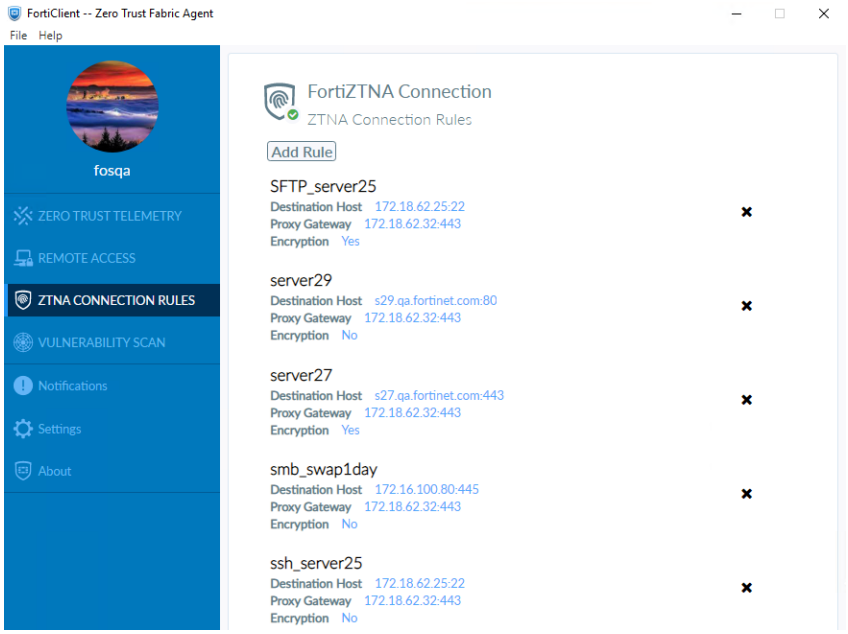


2. On the FortiProxy, configure the ZTNA TCP forwarding server to add the email server address and enable AV profile scanning in the ZTNA rules.
3. On the client PC, open Outlook app and send emails with attachments containing virus affected files.
4. The ZTNA rule on the FortiProxy blocks the email send/receive traffic and generates AV logs.

AV scanning for SMB service traffic

To configure AV scanning for SMB service traffic:

1. In FortiClient, add ZTNA connection rules for the SMB file sharing server IP and ports.



2. On the FortiProxy, configure the ZTNA TCP forwarding server to add the SMB server address and enable AV profile scanning in the ZTNA rules.
3. On the client PC, upload and download virus affected files to and from the SMB server.
4. The ZTNA rule on the FortiProxy blocks the email send/receive traffic and generates AV logs.

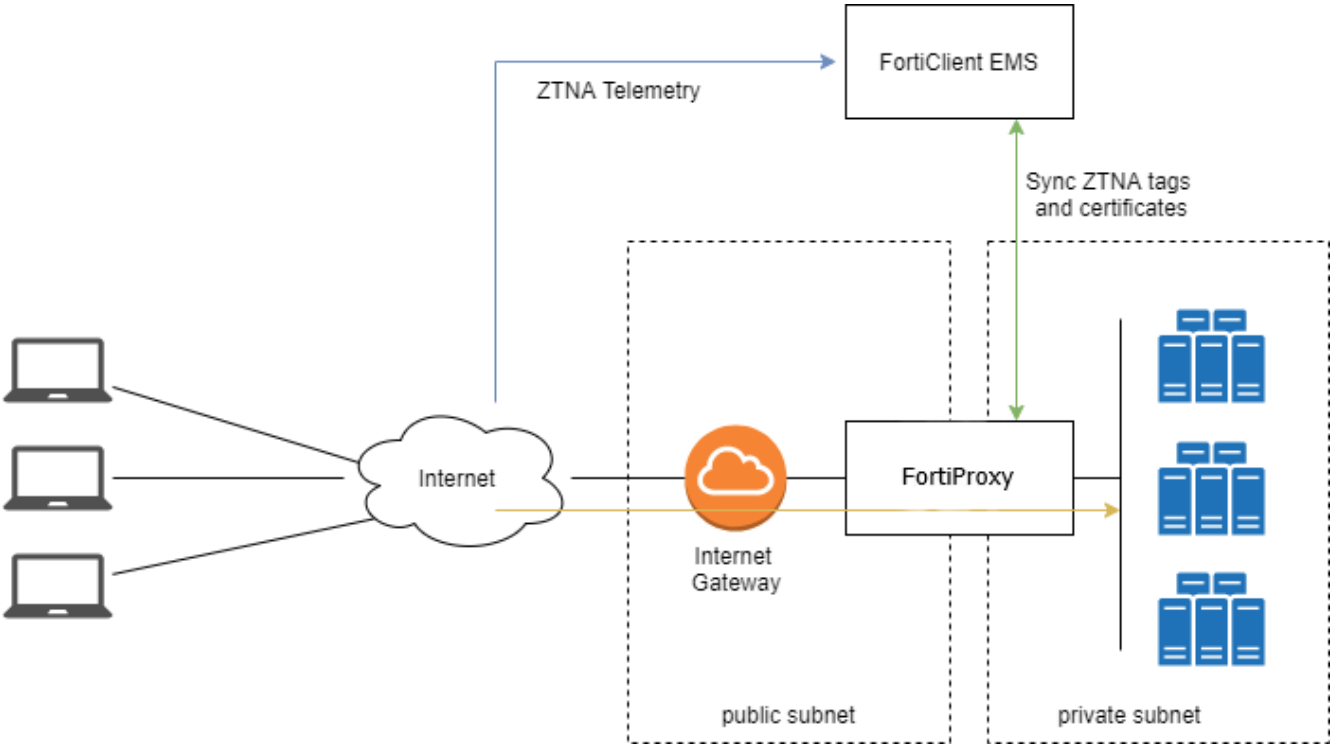
File filter scanning for CIFS service traffic

To configure file filter scanning for CIFS service traffic:

1. In FortiClient, add ZTNA connection rules for the CIFS server IP and port.
2. On the FortiProxy, configure the ZTNA TCP forwarding server to add the CIFA server address and enable file filter profile scanning in the ZTNA rules.
3. On the client PC, upload and download predefined file types (such as .EXE) to and from the CIFS server.
4. The ZTNA rule on the FortiProxy blocks the email send/receive traffic and generates AV logs.

ZTNA Zero Trust application gateway example

The Zero Trust application gateway (ZTAG) for SaaS applications delivers Zero Trust Network Access (ZTNA) to companies that deploy SaaS applications and services in the cloud. A Zero Trust application gateway is deployed in the cloud, protecting resources on the private subnets by enforcing security and access control.



A Zero Trust application gateway can be deployed directly on AWS, Azure, and VMware. The deployment template can configure the necessary ZTNA settings to get the ZTNA configurations started.

ZTNA inline CASB for SaaS application access control

The FortiProxy ZTNA application gateway can be configured to act as an inline cloud access security broker (CASB) by providing access control to software-as-a-service (SaaS) traffic using ZTNA access control rules. A CASB sits between users and their cloud service to enforce security policies as they access cloud-based resources.

The following components are required to use the ZTNA inline CASB feature:

- The FortiGuard Inline CASB Database (ICDB) used by the FortiProxy and FortiClient EMS.
  This database includes all FQDNs related to specific SaaS applications and corresponding FortiGuard packages for FortiProxy and FortiClient.
- A FortiProxy ZTNA TCP forwarding access proxy configuration that specifies SaaS application destinations using application names defined in the ICDB.
- ZTNA connection rules for SaaS traffic that are provisioned using FortiClient EMS (version 7.2.2 and later).
- FortiClient (version 7.2.0 and later) installed on the user's machine to receive the ZTNA connection rules for SaaS traffic from FortiClient EMS.

Syntax

Users can configure the ZTNA application gateway with a new SaaS proxy access type and conveniently specify SaaS application destinations by application name or by application group name without needing to manually search for and enter FQDNs specific to each SaaS application. This can only be configured in the CLI.

To configure a ZTNA application gateway to use SaaS from the CLI:

```
config firewall access-proxy
    edit <name>
        config api-gateway
            edit <ID>
                set url-map "/saas"
                set service saas
                set application <app 1> [app 2] ...
            next
        end
    next
end
```

To configure the SaaS application destination from the CLI:

```
config firewall proxy-address
    edit <name>
        set type saas
        set application <app 1> [app 2] ...
    next
end
```

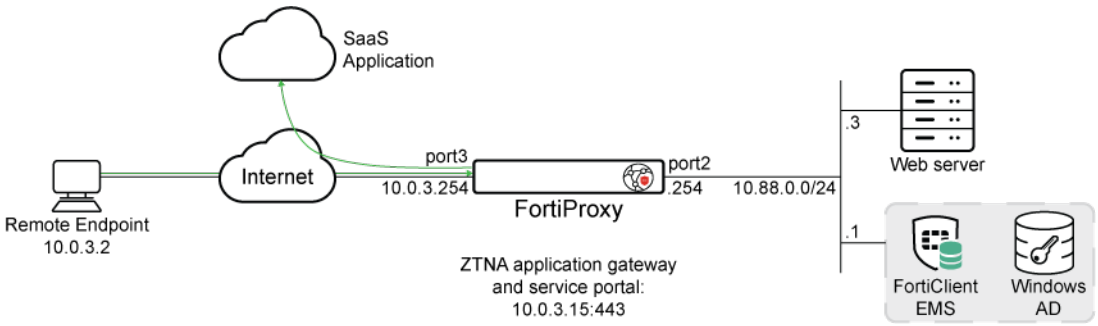
To configure a ZTNA rule (policy) to use the SaaS destination from the CLI:

```
config firewall policy
    edit <ID>
        set dstaddr <proxy-address>
    next
end
```

The FortiProxy traffic log includes a `saasname` field when traffic is controlled by inline CASB for logging SaaS traffic on the FortiProxy and FortiAnalyzer.

Example

In this example, the FortiProxy is configured as a ZTNA application gateway with a VIP of 10.0.3.15 and uses the SaaS access proxy type. SaaS application Gmail is allowed, but the action of getting an attachment on Gmail is blocked.



To configure the FortiProxy:

1. Configure the access proxy VIP for ZTNA:

```
config firewall vip
    edit "ZTNA-SaaS-Access"
        set type access-proxy
        set extip 10.0.3.15
        set extintf "any"
        set server-type https
        set extport 443
        set ssl-certificate “ztna-wildcard”
    next
end
```

2. Configure the firewall access proxy using the SaaS proxy access type and specify the SaaS application destinations:

```
config firewall access-proxy
    edit "ZTNA-SaaS-Access-Proxy"
        set vip "ZTNA-SaaS-Access"
        config api-gateway
            edit 1
```

```
                set service saas
                set url-map "/saas"
                set application "gmail"
            next
        end
    next
end
```

3. Configure the SaaS proxy address, which can be applied in a ZTNA proxy policy to allow Gmail:

```
config firewall proxy-address
    edit "ztna-saas-gmail"
        set type saas
        set application "gmail"
    next
end
```

4. Configure the SaaS proxy address, which can be applied in a ZTNA proxy policy to deny Gmail attachments:

```
config firewall proxy-address
    edit "ztna-saas-gmail-attach"
        set type saas
        set application "gmail-getAttach"
    next
end
```

5. Configure a ZTNA rule using the SaaS proxy address as the destination to deny Gmail attachments:

```
config firewall policy
    edit 2
        set name "ZTNA-SaaS-Deny-Access"
        set access-proxy "ZTNA-SaaS-Access-Proxy"
        set srcintf "port3"
        set srcaddr "all"
        set dstaddr "ztna-saas-gmail-attach"
        set schedule "always"
        set logtraffic all
    next
end
```

6. Configure a ZTNA rule using the SaaS proxy address as the destination to allow Gmail:

```
config firewall policy
    edit 3
        set name "ZTNA-SaaS-Access"
        set access-proxy "ZTNA-SaaS-Access-Proxy"
        set srcintf "port3"
        set srcaddr "all"
        set dstaddr "ztna-saas-gmail"
        set action accept
```

```
        set schedule "always"
        set logtraffic all
    next
end
```

7. Optionally, if user authentication is configured, the ZTNA rule (`set users` or `set groups`), configure the authentication scheme and rule.

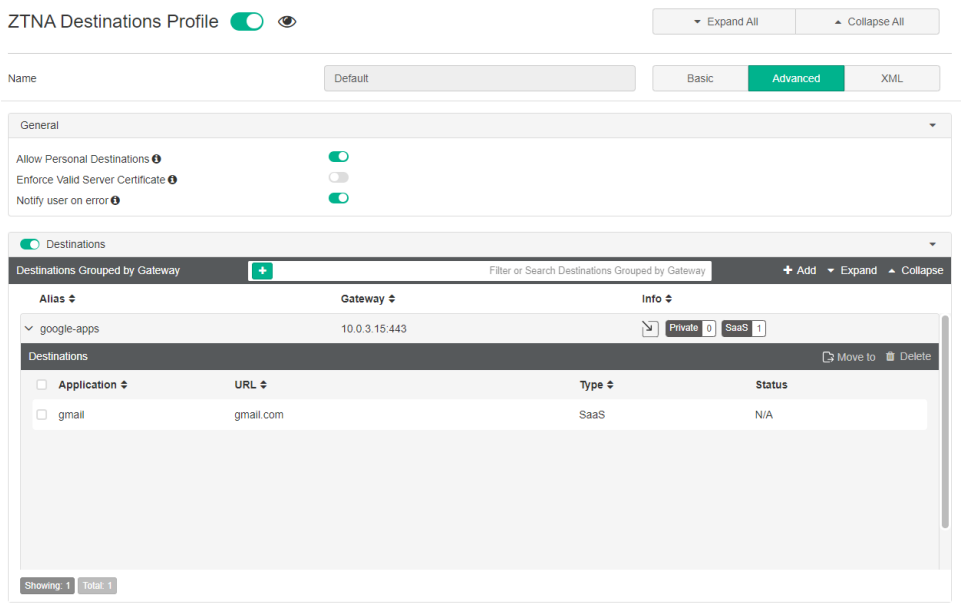
Before connecting, the users must have corresponding ZTNA Destinations in FortiClient. In FortiClient EMS, configure SaaS applications in *Endpoint Profiles > ZTNA Destinations* and push application destinations to FortiClient.

To configure the FortiClient EMS:

1. On FortiClient EMS, go to *Endpoint Profiles > ZTNA Destinations*.
2. Edit the *Default* profile.
3. Besides *Name*, click *Advanced*.
4. Click the eye icon beside *ZTNA Destination Profile* to enable this profile to be viewed on the FortiClient.
5. Under *Destinations*, click *Add* . The *Add New Gateway* dialog is displayed.
6. In *Proxy Gateway*, enter the following:

Enter the gateway proxy address	10.0.3.15:443
Select browser user-agent for SAML login	Use FortiClient embedded browser
Alias	google-apps

7. Click *Next*.
8. In *Private Applications*, click *Next*.
9. In *SaaS Applications*, expand *Google* and then select *gmail*.



10. Click *Finish*.
11. Click *Save*.
    The FortiClient endpoints will synchronize the destination from EMS.

Testing and results

Once connected, the FortiClient retrieves the list of hosted ZTNA services, including the SaaS service, and adds corresponding ZTNA connection rules for the configured SaaS applications.

Connect to Gmail from a browser. The traffic is allowed.

After closing the session, the corresponding traffic logs can be viewed from the FortiProxy GUI or from the CLI.

```
# execute log filter field subtype ztna
# execute log display
365 logs found.
10 logs returned.
2.0% of logs has been searched.

1: date=2023-11-06 time=17:55:22 eventtime=1699322121300602688 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2 srcport=37060
srcintf="port3" srcintfrole="wan" dstcountry="United States" srccountry="Reserved"
dstip=142.251.16.138 dstport=443 dstintf="port3" dstintfrole="wan" sessionid=90509
srcuuid="b458a65a-f759-51ea-d7df-ef2e750026d1" service="HTTPS" proxyapptype="http" proto=6
action="accept" policyid=3 policytype="proxy-policy" poluuid="f7739b50-7854-51ee-749a-
a792f95fb219" policyname="ZTNA-SaaS-Access" duration=50 gatewayid=1 vip="ZTNA-SaaS-Access"
accessproxy="ZTNA-SaaS-Access-Proxy" clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA"
clientdevicemanageable="manageable" saasname="gmail" clientdevicetags="EMS1_ZTNA_Domain-
Users/EMS1_ZTNA_all_registered_clients" emsconnection="online" wanin=30028 rcvdbyte=30028
wanout=2173 lanin=4206 sentbyte=4206 lanout=33385 fctuid="9A016B5A6E914B42AD4168C066EB04CA"
appcat="unscanned"
```

Connect to Gmail from a browser again. This time, open an email and download an attachment. The action will be blocked.

After closing the session, the corresponding traffic logs can be viewed from the FortiProxy GUI or from the CLI.

```
# execute log filter field subtype ztna
# execute log display

32: date=2023-11-06 time=18:09:26 eventtime=1699322965907196540 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2 srcport=37402
srcintf="port3" srcintfrole="wan" dstcountry="Reserved" srccountry="Reserved" dstip=10.0.3.15
dstport=443 dstintf="root" dstintfrole="undefined" sessionid=90864 srcuuid="95f96508-7854-51ee-
dc89-95da637bf0cf" dstuuid="2dcbb08e-7a8a-51ee-d38f-77193e22942b" service="HTTPS"
proxyapptype="http" proto=6 action="deny" policyid=2 policytype="proxy-policy" poluuid="8d1fee22-
7a82-51ee-92cf-ca1b22eacca3" policyname="ZTNA-SaaS-Deny-Access" duration=0 vip="ZTNA-SaaS-Access"
accessproxy="ZTNA-SaaS-Access-Proxy" clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA"
clientdevicemanageable="manageable" saasname="gmail" clientdevicetags="EMS1_ZTNA_Domain-
Users/EMS1_ZTNA_all_registered_clients" emsconnection="online" msg="Traffic denied because proxy-
policy action is deny. Matched tag: EMS1_ZTNA_all_registered_clients" wanin=0 rcvdbyte=0 wanout=0
lanin=1881 sentbyte=1881 lanout=3010 fctuid="9A016B5A6E914B42AD4168C066EB04CA" appcat="unscanned"
crscore=30 craction=131072 crlevel="high"
```

ZTNA application gateway with KDC to access shared drives



Fortinet technical support cannot troubleshoot third-party applications involved in this solution.

Kerberos Key Distribution Center (KDC) proxy protocol can be used to remotely authenticate domain users and issue Kerberos tickets. A remote user can use the same Kerberos ticket to authenticate when remotely accessing shared drives through ZTNA application gateway.

The following options are available when setting up ZTNA application gateway on TCP 445 for remote access to mapped drives:

- Create the mapped drive using the server's IP address, which uses Windows NT LAN Manager (NTLM) to authenticate users.
- Create the mapped drive using the server's FQDN (or DNS name), which requires Kerberos authentication.

The preferred way to create mapped drives is using the server's DNS name. KDC proxy protocol can be a reliable way to initiate Kerberos authentication for remote users to seamlessly access mapped drives and requires the following steps:

1. Set up the KDC proxy service on a server.
2. Set up the ZTNA application gateway for mapped drives.



The KDC Proxy only works for domain-joined workstations.

Setting up the KDC proxy service

The following steps are required to set up the KDC proxy service on a server:

1. Deploy a server that is joined to the domain and create a trusted certificate.
2. Configure the KDC proxy service on the server.
3. Configure clients to use the KDC proxy.
4. If client machines cannot retrieve group policy updates, configure registry keys on the clients.

Deploying a server and creating a certificate

Deploy a server that is joined to the domain. At a minimum, the server must have a public network interface with a domain name pointed to it. Clients will connect to the server over the internet. For networking, you can forward port 443 if necessary.

Create a trusted certificate for the public domain name of the proxy endpoint:

- Domain: fortitest.net
- KDC proxy: kdcproxy.fortitest.net

The KDC proxy service is present on the server, but not configured.

Configuring the KDC proxy service on the server

The KDC proxy service must be configured before it can be started.

To configure the server:

1. Start an elevated command prompt, and configure a URL ACL for the endpoint:

   ```
   netsh http add urlacl url=https://+:443/KdcProxy user="NT authority\Network Service"
   ```

2. Associate the certificate created previously with the endpoint:

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=<thumbprint of your certificate> appid=
   {generated Guid}
   ```

   This association instructs `HTTP.SYS` to use the certificate when connections occur over HTTPS.

   For example: `netsh http add sslcert ipport=0.0.0.0:443 certhash=aaaabbbbccccddddeeeeffff0000111122223333 appid={aaaaaaaa-bbbb-cccc-dddd-aaaabbbbcccc}`



For appid you should generate a random GUID here. From PowerShell try [Guid]::NewGuid(). The certhash is the thumbprint of your certificate.

If the certificate contains extensions for CRL or AIA, those URLs should be reachable from the remote client.

3. If not using smart card certificates (or Windows Hello) for authentication, disable the certificate authentication requirement:

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\KPSSVC\Settings" /v HttpsClientAuth /t REG_
DWORD /d 0x0 /f
```

4. Additionally if not using certificates, enable password authentication:

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\KPSSVC\Settings" /v
DisallowUnprotectedPasswordAuth /t REG_DWORD /d 0x0 /f
```

5. Configure the KDC Proxy Service (KPSSVC) to start automatically:

```
sc config kpssvc start=auto
```

6. Start the service:

```
net start kpssvc
```

Configuring clients to use a KDC proxy

Clients must be configured to use a KDC proxy. This can be done through GPO or through modifying the registry directly. The GPO path is:

```
Computer Configuration\Policies\Administrative Templates\System\Kerberos\Specify KDC proxy servers
for Kerberos clients
```

Enabling this policy requires setting a realm-to-value mapping. The realm is your domain name, starting with a period (for example ".fortitest.net"), or a "*" to include all domains in a wildcard format. The value is specially crafted:

```
<https kdcproxy.fortitest.net:kdcproxy />
```

Deploy the policy, and reboot the client. Wait a while for caching to complete, and then log in. You should find users are now authenticating over the KDC proxy endpoint.

To verify from a logged in session, launch a command prompt and try the following command:

```
klist get krbtgt
```

Configuring registry keys on clients

If you are trying to deploy these settings on a client machine that cannot retrieve group policy updates, manually configure the registry keys for the client:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos]
"KdcProxyServer_Enabled"=dword:00000001
```

```
[HKEY_LOCAL_
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\KdcProxy\ProxyServers]
"*"="<https kdcproxy.fortitest.net />" or ".fortitest.net"="<https kdcproxy.fortitest.net />"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters]
"NoRevocationCheck"=dword:00000000
```

Setting up the ZTNA application gateway for mapped drives

The following steps are required to set up ZTNA application gateway for mapped drives on the FortiProxy:

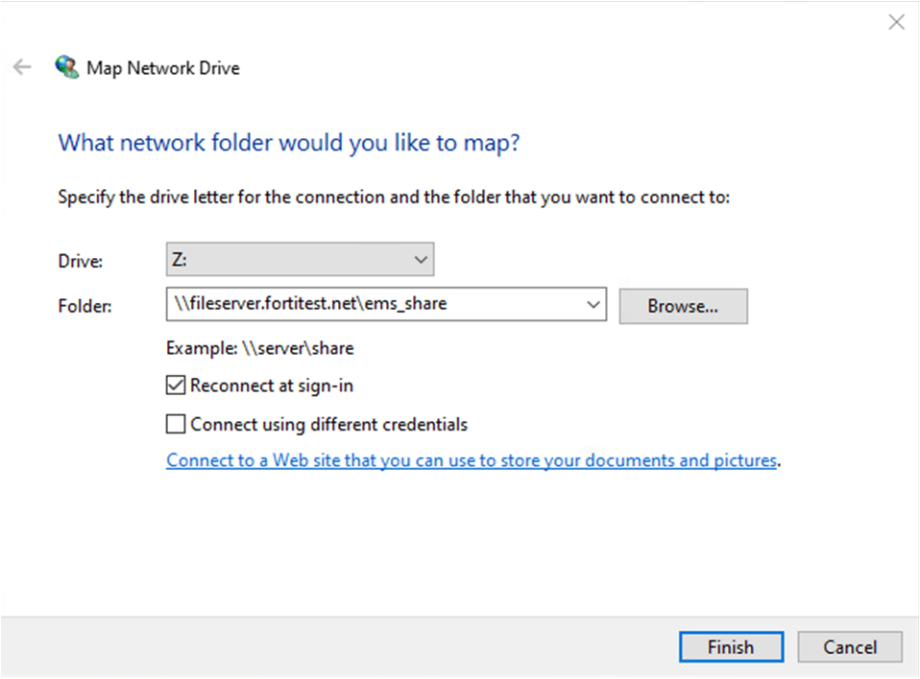
1. Configure FortiClient to have the ZTNA destination rule.
2. Configure a ZTNA server and proxy policy on FortiProxy.

Configuring a ZTNA destination rule on FortiClient

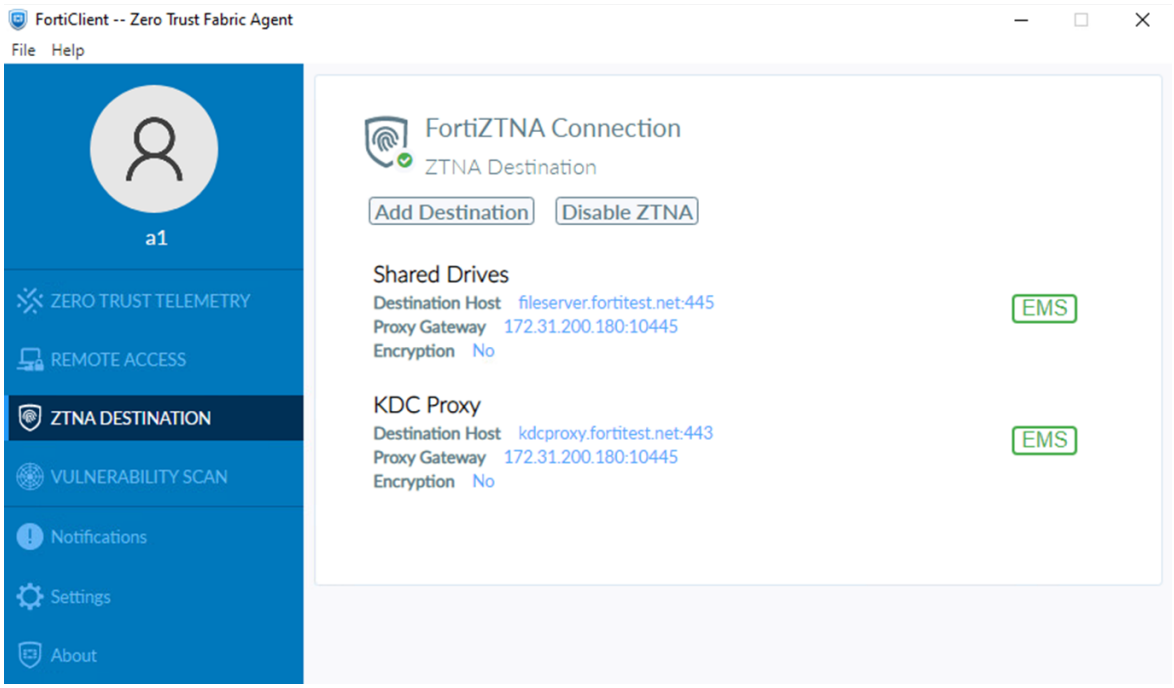
The ZTNA destination rule can be configured by using FortiClient EMS or by manually configuring FortiClient. The destination host matches the server's FQDN on port 445, and the proxy gateway should be the FortiProxy WAN port on the chosen external port.

Another rule is required for the KDC proxy communication with the destination host defined as the FQDN of the KDC proxy server and port 443.

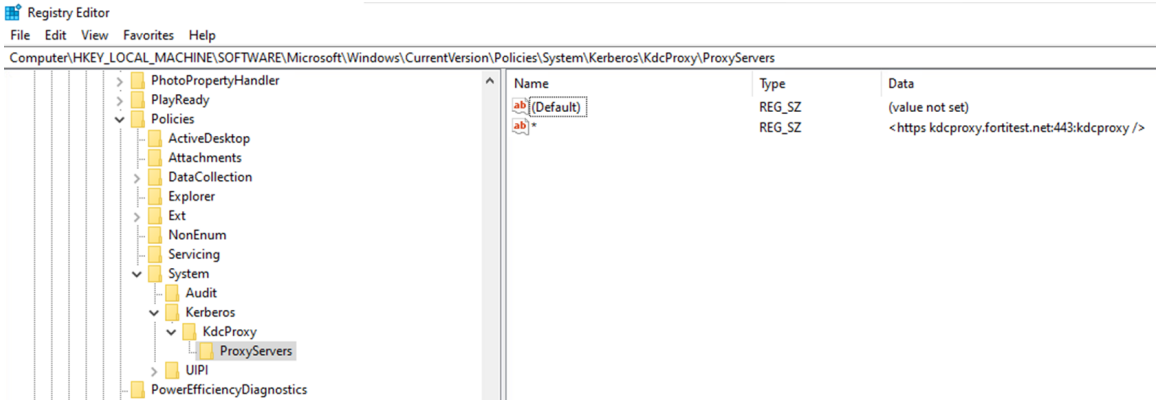
The map network drive configuration should be the last step after configuring the FortiProxy. The following example shows the mapped drive:



The following example shows a ZTNA destination configured in FortiClient with the *Proxy Gateway*:



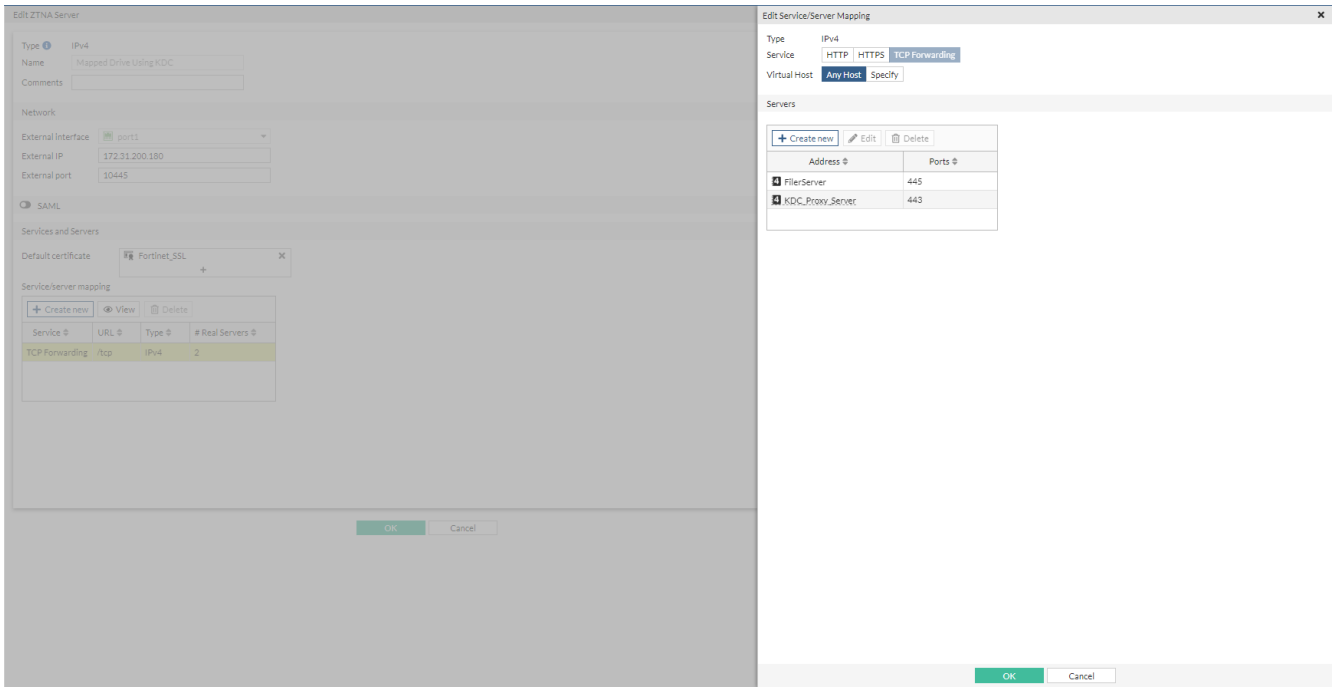
The following example shows the registry settings:



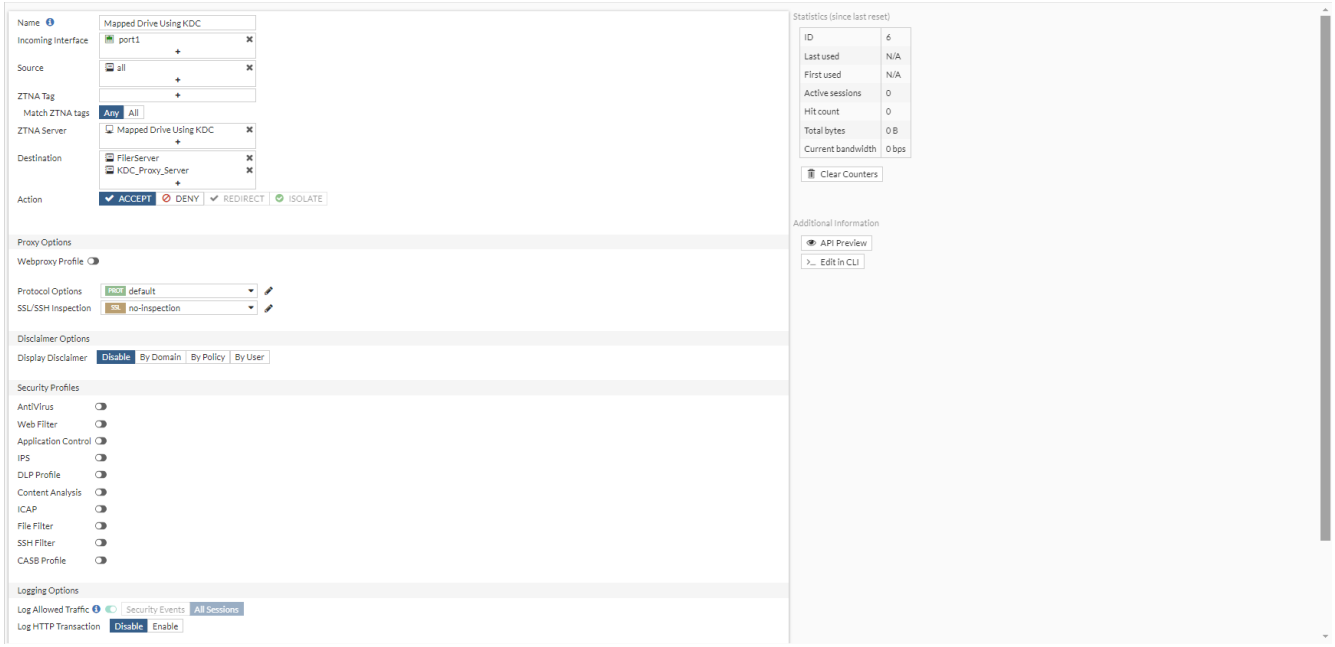
Configuring FortiProxy

A ZTNA server and a proxy policy are required to verify and forward the incoming requests on port 10445 to the file server on port 445 as well as to the KDC proxy server on port 443.

The following example shows the ZTNA server:



The following example shows the proxy policy:



Custom replacement message for ZTNA virtual hosts

Each ZTNA virtual host can be configured to display messages from a custom replacement message group.

First create a replacement message group, and customize one ore more messages in the group. Then configure one or more ZTNA virtual hosts to use the replacement message group.

```
config firewall access-proxy-virtual-host
    edit <host name>
        set replacemsg-group <replacemsg group>
    next
end
```

When a client fails a ZTNA check with the virtual host, the replacement message is displayed.

Example

In this example, a ZTNA virtual host named *10.1.1.12* is mapped to a replacement message group named *test-vhost*, and the group includes a customized *ZTNA Empty Certificate Error Page* message. The message is customized with a Company Y logo.

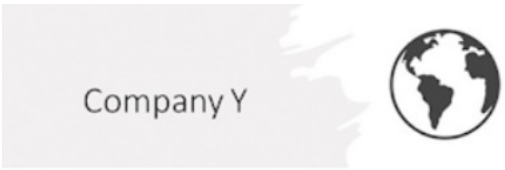
When clients fail a ZTNA check with the ZTNA virtual host (10.1.1.12) because of an empty certificate, the custom replacement message is displayed.



Go to *System* > *Feature Visibility* and enable *Replacement Message Groups*. See Feature Visibility on page 970 for more information.

To customize replacement messages for ZTNA virtual hosts:

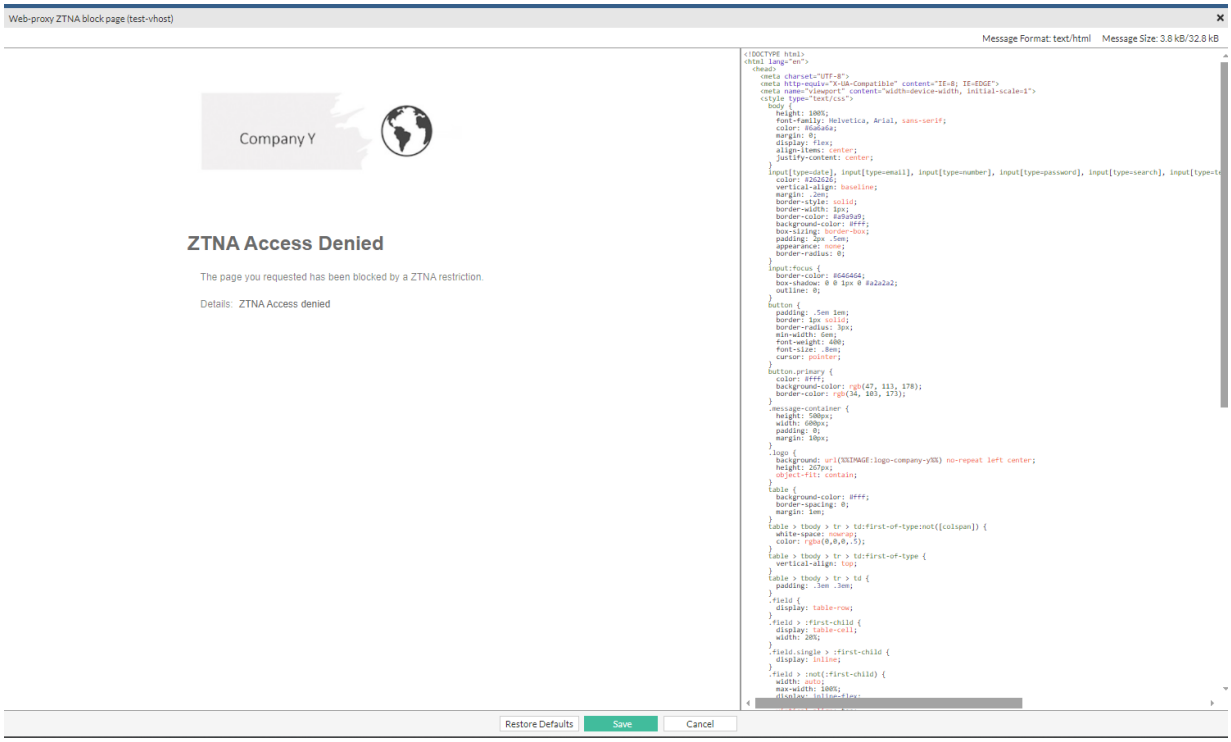
1. Upload a logo to the FortiProxy to use in replacement messages:
   a. Go to *System* > *Replacement Messages* and click *Manage Images*.
   b. Click *Create New*.
   c. Name and upload an image file.
   d. Click *OK*. The logo is uploaded to the FortiProxy.



2. Create a replacement message group named, for example, *test-vhost*:
   a. Go to *System* > *Replacement Message Groups* and click *Create New*.
   b. Specify a name for the group, such as *test-vhost*.
   c. Set *Group Type* to *Security*.
   d. Click *OK*.
3. Customize one or more messages in the *test-vhost* group:
   In this example, the *ZTNA Empty Certificate Error Page* message is edited to add a custom logo.
   a. Double-click the *test-vhost* replacement message group to open it for editing.
   b. Select the *ZTNA Empty Certificate Error Page* message and click *Edit*.

c. In the right pane, edit the URL for the `.logo` section by typing the logo name to select the uploaded logo, for example, *logo-company-y*.

```
...
}
.logo {
  background: url(%%IMAGE:logo-company-y%%) no-repeat left center;
  height: 267px;
  object-fit: contain;
}
...
```



d. Click *Save*. A green checkmark is displayed in the *Modified* column to indicate a customized message.

4. Configure a ZTNA server with a ZTNA virtual host named *10.1.1.12*. See Configure a ZTNA server on page 250.

In the *Service/server* mapping, be sure to set *Virtual Host* to *Specify*, and enter the name or IP address of the host that the request must match. For example, if 10.1.1.12 is entered as the host, then only requests to 10.1.1.12 will match.

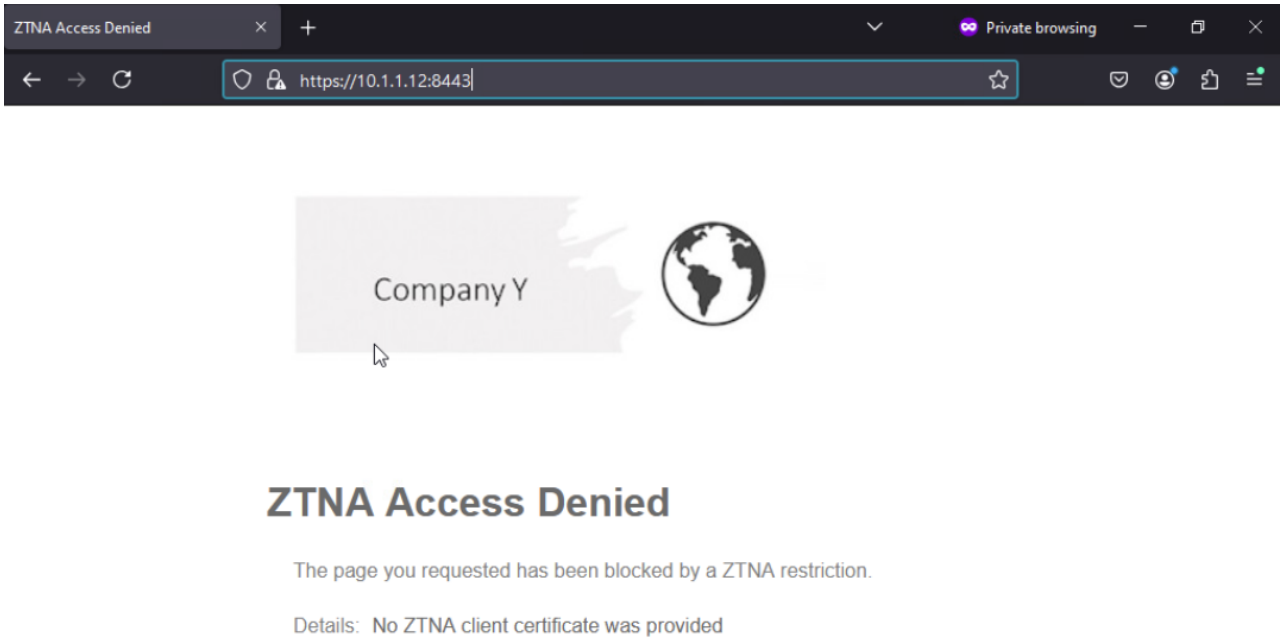
```
FPXVULTM24000083 (https) # show
config firewall access-proxy
    edit "https"
        set vip "https"
        config api-gateway
            edit 1
                set virtual-host "auto-https-0"
                config realservers
                    edit 1
                        set ip 10.100.1.78
                    next
                end
            next
        end
    next
end
```

5. Map the ZTNA virtual host to the replacement message group in the CLI.

   In this example, the ZTNA virtual host named `10.1.1.12` is configured to use the `test-vhost` replacement message group.

```
FPXVULTM24000083 (auto-https-0) # sh
config firewall access-proxy-virtual-host
    edit "auto-https-0"
        set ssl-certificate "Fortinet_SSL"
        set host "10.1.1.12"
        set replacemsg-group "test-vhost"
    next
end
```

6. Create a ZTNA rule to allow traffic to the ZTNA server. See Configure a ZTNA rule on page 254.
7. When a client fails to access the ZTNA virtual host named *10.1.1.12* because of an empty certificate error, the following custom replacement message with the Company Y logo is displayed.



ZTNA for UDP traffic

ZTNA supports UDP traffic from FortiClient 7.4.1 and later endpoints. When UDP traffic to a destination is detected, FortiClient forms a UDP connection over QUIC to the FortiProxy ZTNA gateway. After authentication, security posture check, and authorization, FortiProxy forms a connection with the destination and the end-to-end UDP traffic passes through.

Scope and limitations

- FortiClient endpoint must be running 7.4.1 or later.
- FortiClient EMS 7.4.1 and later supports the option to enable UDP on a ZTNA application.

CLI syntax

In order to support UDP traffic forwarding, the FortiProxy VIP associated with the ZTNA server configurations must have `h3-support` enabled.

```
config firewall vip
  edit <ZTNA VIP>
    set type access-proxy
    set h3-support {enable | disable}
  next
end
```

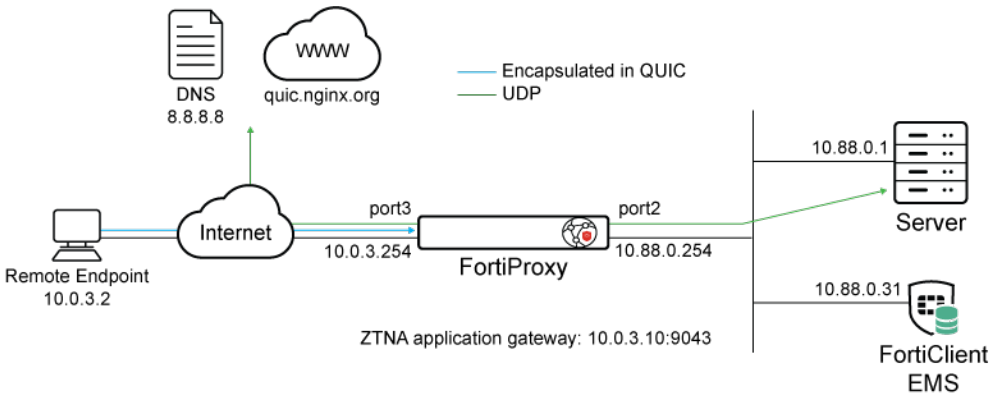
The remaining UDP applications can be configured under the `firewall access-proxy` configuration:

```
config firewall access-proxy
    edit <name>
        set vip <ZTNA VIP>
        config api-gateway
            edit 1
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address <UDP application address>
                        set mappedport <UDP application port(s)>
                    next
               end
            next
        end
    next
end
```

FortiClient EMS configuration

From the FortiClient EMS server, you must change the ZTNA applications to enable UDP.

Example



When an application on an endpoint initializes UDP traffic, FortiClient forms a UDP connection over QUIC to the FortiProxy ZTNA gateway (10.0.3.10:9043). After authentication, security posture check, and authorization, FortiProxy forms a UDP connection with the destination (quic.nginx.org), and the end-to-end UDP traffic passes through, allowing the endpoint to reach three different destinations through UDP.

To configure FortiProxy:

```
config firewall vip
    edit "ztna_vip"
        set uuid 0c0e724e-a60b-51ef-db23-26940edc4402
        set type access-proxy
        set server-type https
        set extip 10.1.20.1
        set h3-support enable
        set extintf "any"
        set extport 8888
        set ssl-certificate "Fortinet_SSL"
    next
    edit "doq_cert"
        set uuid 947371a4-a6ae-51ef-fec3-6b7f0b14c59f
        set type access-proxy
        set server-type https
        set extip 10.1.20.5
        set h3-support enable
        set extintf "any"
        set extport 8888
        set ssl-certificate "Fortinet_SSL"
    next
  edit "dns_vip"
        set uuid 1c8a8cca-a6c4-51ef-80d6-b867b9235367
        set type access-proxy
        set server-type https
        set extip 10.1.20.9
        set h3-support enable
        set extintf "any"
```

```
        set extport 8888
        set ssl-certificate "Fortinet_SSL"
    next
end


config firewall address
    edit "server_33"
        set uuid 3a3123d8-a60b-51ef-c7d6-94bf48dcd7e8
        set subnet 172.18.76.33 255.255.255.255
next
edit "server94.140.14.14"
        set uuid 6d936346-a6ae-51ef-886a-bdead78dfa81
        set subnet 94.140.14.14 255.255.255.255
    next
end


config firewall access-proxy
    edit "access-proxy"
        set vip "ztna_vip"
        config api-gateway
            edit 5
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "server_33"
                        set mappedport 443
                    next
                end
            next
        end
    next
    edit "doq_cert"
        set vip "doq_cert"
        config api-gateway
            edit 1
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "server94.140.14.14"
                        set mappedport 853
                    next
                end
            next
        end
    next
    edit "access-proxy1"
        set vip "dns_vip"
        config api-gateway
```

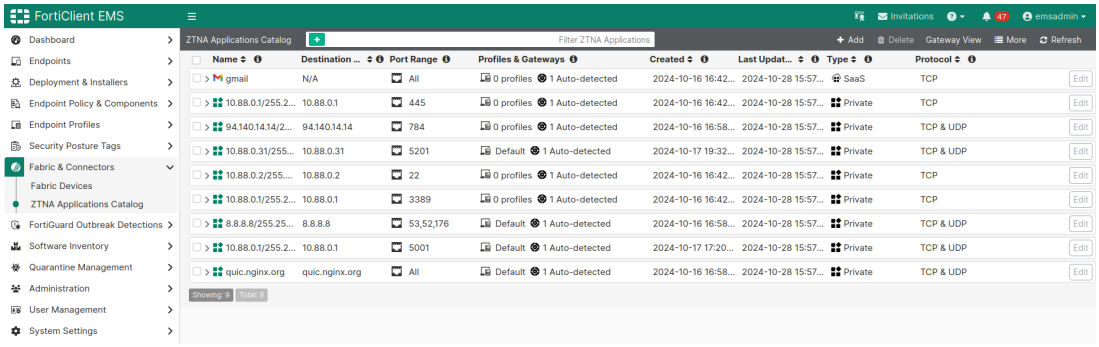
```
            edit 1
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "1.0.0.1"
                        set mappedport 53
                    next
                end
            next
        end
    next
end

config firewall policy
edit 4
        set type access-proxy
        set status disable
        set name "tc1"
        set uuid 37bb5da4-a6b4-51ef-de42-7f4108602748
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set access-proxy "doq_cert"
        set logtraffic all
        set logtraffic-start enable
        set log-http-transaction enable
        set extended-log enable
        set ssl-ssh-profile "certificate-inspection"
    next
    edit 6
        set type access-proxy
        set status disable
        set name "tc2"
        set uuid 245671fc-a6c5-51ef-0310-b41eac08fd57
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set access-proxy "access-proxy1"
        set logtraffic all
        set logtraffic-start enable
        set log-http-transaction enable
        set extended-log enable
        set ssl-ssh-profile "certificate-inspection"
    next
    edit 7
        set type access-proxy
        set name "tc3"
```

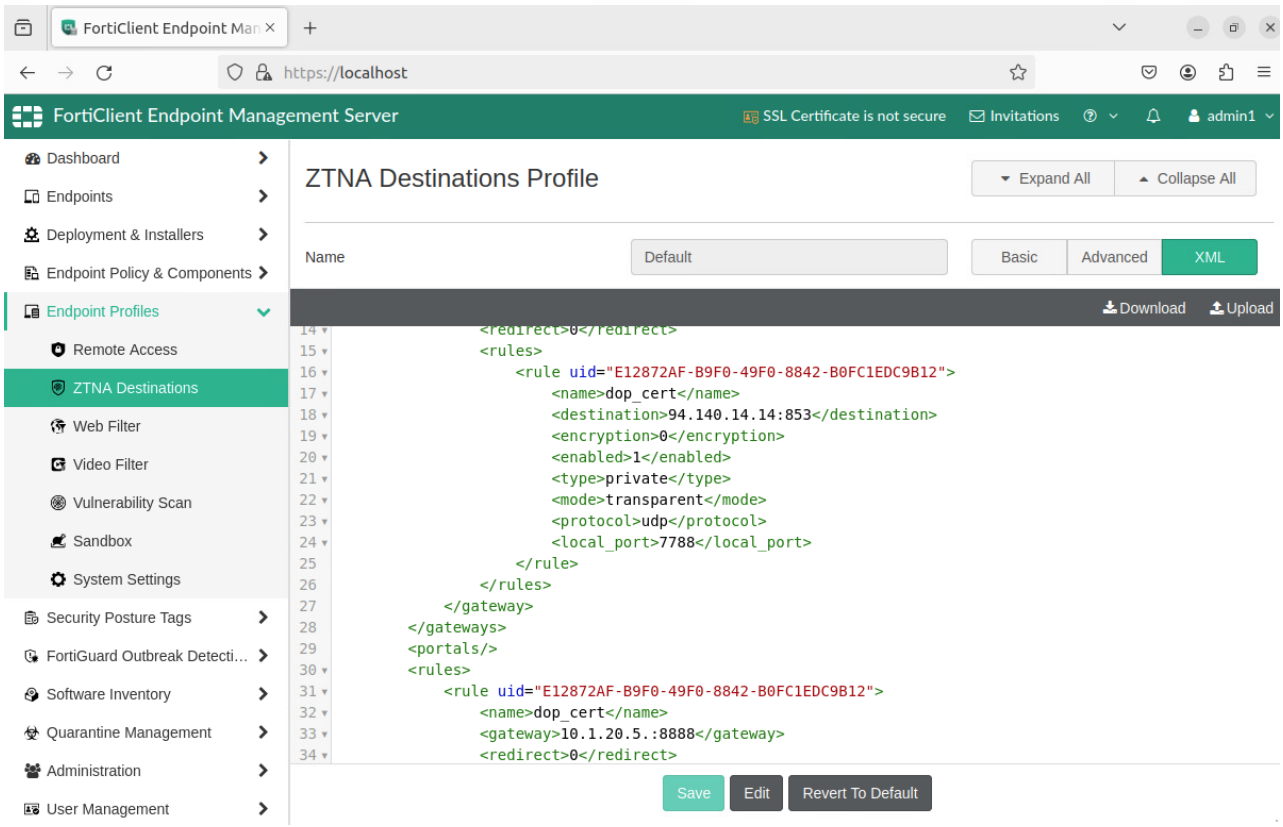
```
        set uuid ecb22964-a6c7-51ef-3b66-9aed56737e89
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set access-proxy "access-proxy"
        set logtraffic all
        set logtraffic-start enable
        set log-http-transaction enable
        set extended-log enable
        set ssl-ssh-profile "certificate-inspection"
next
end
```

To configure FortiClient EMS:

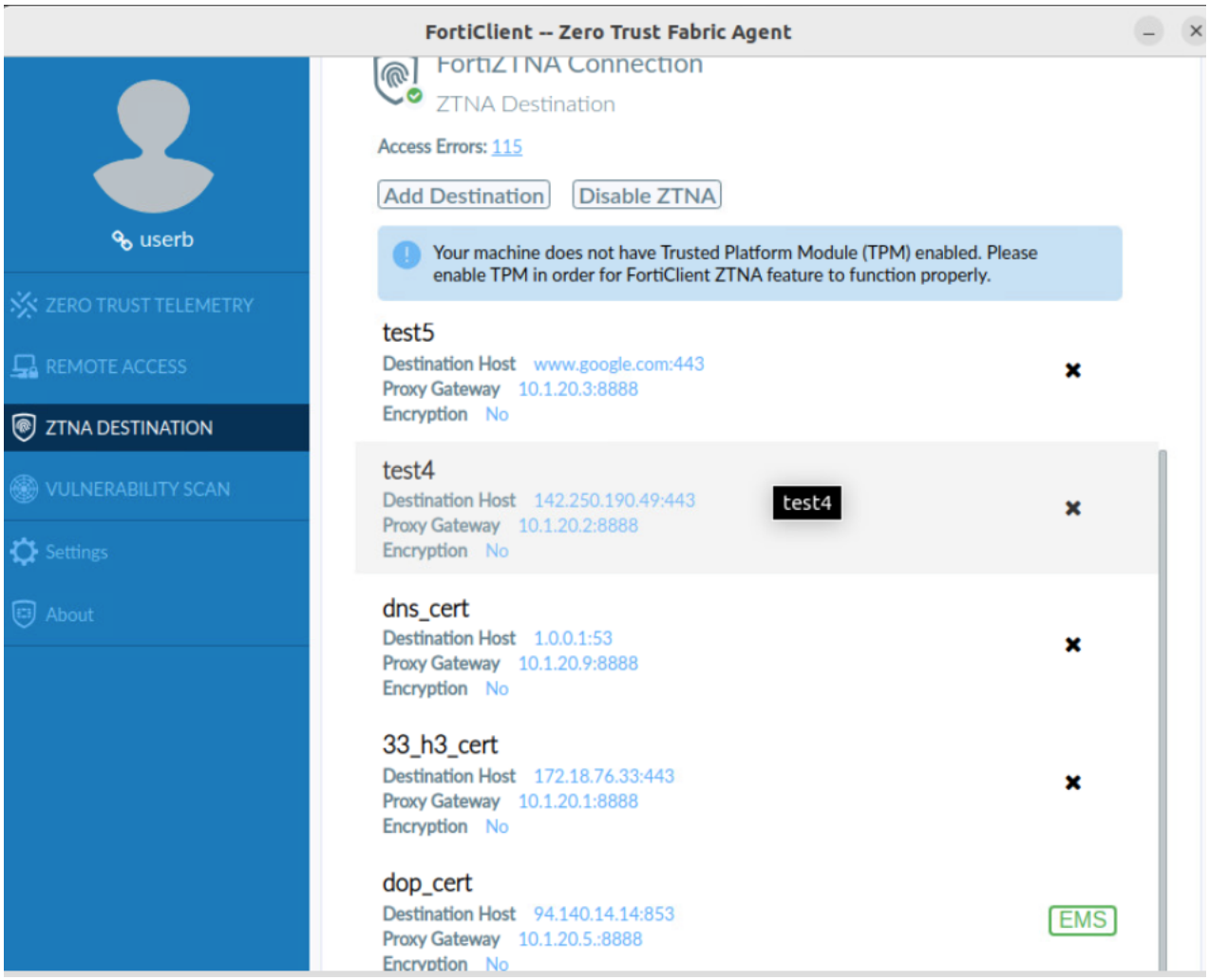
1. From *Fabric & Connectors > ZTNA Application Catalog*, locate each application retrieved from the FortiProxy.
2. Edit each application, and select *Enable UDP*.



3. Go to *Endpoint Profiles > ZTNA Destinations*, and edit the *Default* profile.
4. Under *Rules*, click *+Add*. Select the applications learned from the FortiProxy, and then click *Finish*.



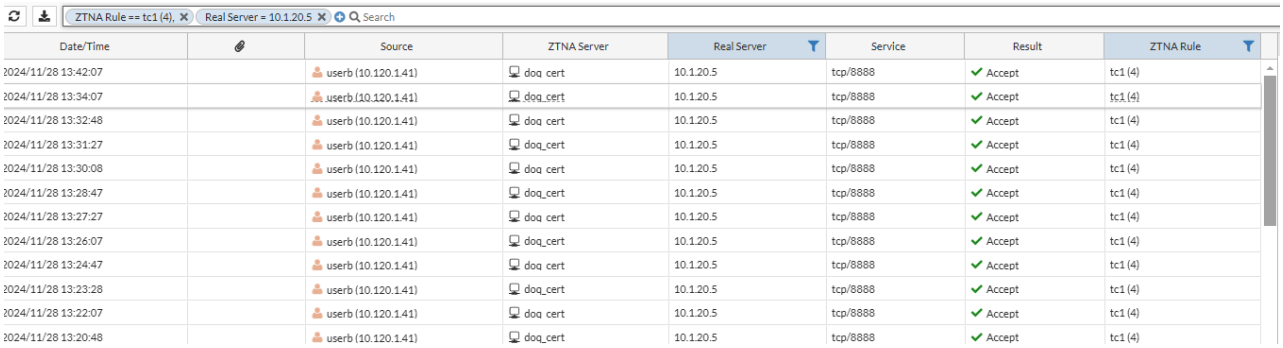
5. Click *Save* to save this profile, and push changes to managed FortiClients.



To verify:

1. Verify DNS over QUIC by running `doq script` from Linux terminal and checking the logs in FortiProxy:

```
guodong@guodong-vm:~/Downloads$ python3 doq_test.py
sending in class
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 0
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.ubc.ca.                    IN      A
;; ANSWER SECTION:
www.ubc.ca.             300     IN      CNAME   d3tie7xuvq1kvm.cloudfront.net.
d3tie7xuvq1kvm.cloudfront.net. 60       IN      A       13.33.165.97
d3tie7xuvq1kvm.cloudfront.net. 60       IN      A       13.33.165.86
d3tie7xuvq1kvm.cloudfront.net. 60       IN      A       13.33.165.35
d3tie7xuvq1kvm.cloudfront.net. 60       IN      A       13.33.165.13
```



Date/Time		Source	ZTNA Server	Real Server	Service	Result	ZTNA Rule
2024/11/28 13:42:07		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:34:07		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:32:48		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:31:27		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:30:08		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:28:47		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:27:27		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:26:07		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:24:47		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:23:28		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:22:07		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)
2024/11/28 13:20:48		userb (10.120.1.41)	doq_cert	10.1.20.5	tcp/8888	Accept	tc1 (4)

Sample logs:

```
# exec log filter field subtype ztna
```

```
# exec log display
215 logs found.
10 logs returned.
50.9% of logs has been searched.
date=2024-11-28 time=13:32:48 eventtime=1732829567500943296 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.41 srcport=45660
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.1.20.5 dstport=8888 dstintf="port1" dstintfrole="undefined" sessionid=1835553063
service="tcp/8888" proxyapptype="http" proto=6 action="accept" policyid=4 policytype="proxy-
policy" poluuid="37bb5da4-a6b4-51ef-de42-7f4108602748" policyname="tc1" trandisp="snat"
transip=10.120.1.209 transport=0 clientip=10.120.1.41 appcat="unscanned" duration=0 vip="doq_
cert" accessproxy="doq_cert" clientdevicemanageable="unknown" clientcert="no" wanin=0
rcvdbyte=0 wanout=0 lanin=0 sentbyte=0 lanout=0 fctuid="6F6248B158C74FF98905ADCE528DB1E7"
unauthuser="userb" unauthusersource="forticlient" srcremote=207.102.138.19

29: date=2024-11-28 time=13:31:27 eventtime=1732829487500544467 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.41 srcport=45640
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.1.20.5 dstport=8888 dstintf="port1" dstintfrole="undefined" sessionid=1835553062
service="tcp/8888" proxyapptype="http" proto=6 action="accept" policyid=4 policytype="proxy-
policy" poluuid="37bb5da4-a6b4-51ef-de42-7f4108602748" policyname="tc1" trandisp="snat"
transip=10.120.1.209 transport=0 clientip=10.120.1.41 appcat="unscanned" duration=0 vip="doq_
cert" accessproxy="doq_cert" clientdevicemanageable="unknown" clientcert="no" wanin=0
rcvdbyte=0 wanout=0 lanin=0 sentbyte=0 lanout=0 fctuid="6F6248B158C74FF98905ADCE528DB1E7"
unauthuser="userb" unauthusersource="forticlient" srcremote=207.102.138.19
```

2. Verify the DNS and check the logs in FortiProxy:

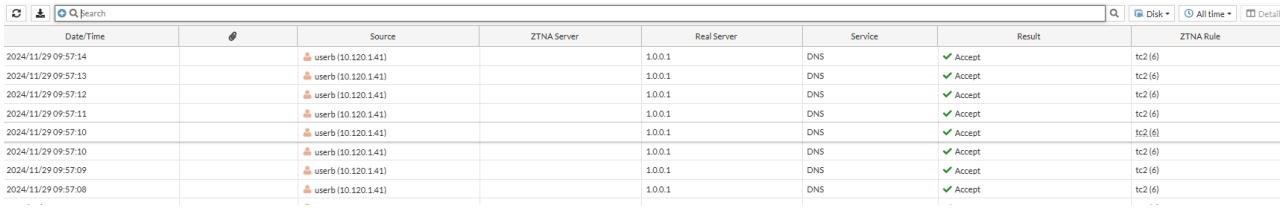
```
guodong@guodong-vm:~/Downloads$ dig @1.0.0.1 -p 53 google.com

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @1.0.0.1 -p 53 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21267
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             231     IN      A       142.251.33.110

;; Query time: 59 msec
;; SERVER: 1.0.0.1#53(1.0.0.1) (UDP)
;; WHEN: Thu Nov 28 13:49:19 PST 2024
;; MSG SIZE  rcvd: 55
```



Date/Time		Source	ZTNA Server	Real Server	Service	Result	ZTNA Rule
2024/11/29 09:57:14		userb (10.120.1.41)		1.0.0.1	DNS	Accept	tc2 (6)
2024/11/29 09:57:13		userb (10.120.1.41)		1.0.0.1	DNS	Accept	tc2 (6)
2024/11/29 09:57:12		userb (10.120.1.41)		1.0.0.1	DNS	Accept	tc2 (6)
2024/11/29 09:57:11		userb (10.120.1.41)		1.0.0.1	DNS	Accept	tc2 (6)
2024/11/29 09:57:10		userb (10.120.1.41)		1.0.0.1	DNS	Accept	tc2 (6)
2024/11/29 09:57:10		userb (10.120.1.41)		1.0.0.1	DNS	Accept	tc2 (6)
2024/11/29 09:57:09		userb (10.120.1.41)		1.0.0.1	DNS	Accept	tc2 (6)
2024/11/29 09:57:08		userb (10.120.1.41)		1.0.0.1	DNS	Accept	tc2 (6)

Sample logs:

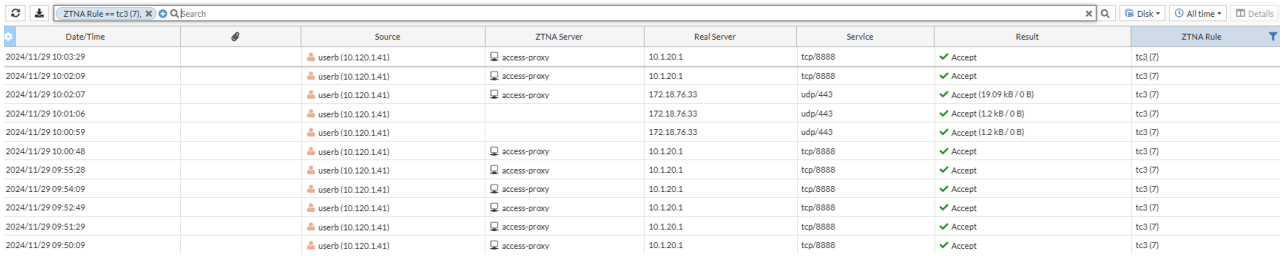
```
# exec log filter field subtype ztna

# exec log display
23 logs found.
10 logs returned.
5.1% of logs has been searched.

1: date=2024-11-29 time=09:53:09 eventtime=1732902789224747854 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.41 srcport=54305
srcintf="port1" srcintfrole="undefined" dstcountry="Australia" srccountry="Reserved"
dstip=1.0.0.1 dstport=53 dstintf="port1" dstintfrole="undefined" service="DNS"
proxyapptype="http" proto=17 action="accept" policyid=6 policytype="proxy-policy"
poluuid="245671fc-a6c5-51ef-0310-b41eac08fd57" policyname="tc2" appcat="unscanned" duration=15
wanin=0 rcvdbyte=0 wanout=0 lanin=0 sentbyte=0 lanout=0
fctuid="6F6248B158C74FF98905ADCE528DB1E7" unauthuser="userb" unauthusersource="forticlient"
srcremote=207.102.138.19
```

3. Verify traffic to http3 (QUIC) and check the logs in FortiProxy:

```
guodong@guodong-vm:~/Downloads$ sudo curl -m 10 --http3-only -kv https://172.18.76.33:443
*   Trying 172.18.76.33:443...
* Server certificate:
*  subject: CN=ubuntu
*  start date: Nov 16 11:05:41 2022 GMT
*  expire date: Nov 13 11:05:41 2032 GMT
*  issuer: CN=ubuntu
*  SSL certificate verify result: self signed certificate (18), continuing anyway.
* Connected to 172.18.76.33 (172.18.76.33) port 443
* using HTTP/3
* [HTTP/3] [0] OPENED stream for https://172.18.76.33:443/
* [HTTP/3] [0] [:method: GET]
* [HTTP/3] [0] [:scheme: https]
* [HTTP/3] [0] [:authority: 172.18.76.33]
* [HTTP/3] [0] [:path: /]
* [HTTP/3] [0] [user-agent: curl/8.10.0-DEV]
* [HTTP/3] [0] [accept: */*]
> GET / HTTP/3
> Host: 172.18.76.33
> User-Agent: curl/8.10.0-DEV
> Accept: */*
>
* Request completely sent off
< HTTP/3 200
< server: nginx/1.23.4
< date: Fri, 29 Nov 2024 18:00:31 GMT
< content-type: text/html
< content-length: 38
< last-modified: Wed, 12 Jun 2024 00:19:51 GMT
< etag: "6668e9a7-26"
< alt-svc: h3=":443"; ma=86401
< accept-ranges: bytes
<
```



Date/Time		Source	ZTNA Server	Real Server	Service	Result	ZTNA Rule
2024/11/29 10:03:29		userb (10.120.1.41)	access-proxy	10.1.20.1	tcp/8888	Accept	tc3 (7)
2024/11/29 10:02:09		userb (10.120.1.41)	access-proxy	10.1.20.1	tcp/8888	Accept	tc3 (7)
2024/11/29 10:02:07		userb (10.120.1.41)	access-proxy	172.18.76.33	udp/443	Accept (19.09 kB / 0 B)	tc3 (7)
2024/11/29 10:01:06		userb (10.120.1.41)		172.18.76.33	udp/443	Accept (1.2 kB / 0 B)	tc3 (7)
2024/11/29 10:00:59		userb (10.120.1.41)		172.18.76.33	udp/443	Accept (1.2 kB / 0 B)	tc3 (7)
2024/11/29 10:00:48		userb (10.120.1.41)	access-proxy	10.1.20.1	tcp/8888	Accept	tc3 (7)
2024/11/29 09:55:28		userb (10.120.1.41)	access-proxy	10.1.20.1	tcp/8888	Accept	tc3 (7)
2024/11/29 09:54:09		userb (10.120.1.41)	access-proxy	10.1.20.1	tcp/8888	Accept	tc3 (7)
2024/11/29 09:52:49		userb (10.120.1.41)	access-proxy	10.1.20.1	tcp/8888	Accept	tc3 (7)
2024/11/29 09:51:29		userb (10.120.1.41)	access-proxy	10.1.20.1	tcp/8888	Accept	tc3 (7)
2024/11/29 09:50:09		userb (10.120.1.41)	access-proxy	10.1.20.1	tcp/8888	Accept	tc3 (7)

Sample logs:

```
1: date=2024-11-29 time=10:03:29 eventtime=1732903409010463530 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.41 srcport=38410
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.1.20.1 dstport=8888 dstintf="port1" dstintfrole="undefined" sessionid=1366711345
service="tcp/8888" proxyapptype="http" proto=6 action="accept" policyid=7 policytype="proxy-
policy" poluuid="ecb22964-a6c7-51ef-3b66-9aed56737e89" policyname="tc3" trandisp="snat"
transip=10.120.1.209 transport=0 clientip=10.120.1.41 appcat="unscanned" duration=0 vip="ztna_
vip" accessproxy="access-proxy" clientdevicemanageable="unknown" clientcert="no" wanin=0
rcvdbyte=0 wanout=0 lanin=0 sentbyte=0 lanout=0 fctuid="6F6248B158C74FF98905ADCE528DB1E7"
unauthuser="userb" unauthusersource="forticlient" srcremote=207.102.138.19

2: date=2024-11-29 time=10:02:09 eventtime=1732903329010694544 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.41 srcport=38408
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.1.20.1 dstport=8888 dstintf="port1" dstintfrole="undefined" sessionid=1366711344
service="tcp/8888" proxyapptype="http" proto=6 action="accept" policyid=7 policytype="proxy-
policy" poluuid="ecb22964-a6c7-51ef-3b66-9aed56737e89" policyname="tc3" trandisp="snat"
transip=10.120.1.209 transport=0 clientip=10.120.1.41 appcat="unscanned" duration=0 vip="ztna_
vip" accessproxy="access-proxy" clientdevicemanageable="unknown" clientcert="no" wanin=0
rcvdbyte=0 wanout=0 lanin=0 sentbyte=0 lanout=0 fctuid="6F6248B158C74FF98905ADCE528DB1E7"
unauthuser="userb" unauthusersource="forticlient" srcremote=207.102.138.19
```

```
3: date=2024-11-29 time=10:02:07 eventtime=1732903326273388765 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.41 srcport=34650
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.18.76.33 dstport=443 dstintf="port1" dstintfrole="undefined" sessionid=1366711342
service="udp/443" proxyapptype="http" proto=17 action="accept" policyid=7 policytype="proxy-
policy" poluuid="ecb22964-a6c7-51ef-3b66-9aed56737e89" policyname="tc3" trandisp="snat"
transip=0.0.0.0 transport=0 clientip=10.120.1.41 appcat="unscanned" duration=102 vip="ztna_
vip" accessproxy="access-proxy" clientdevicemanageable="manageable" clientcert="yes" wanin=0
rcvdbyte=0 wanout=0 lanin=19092 sentbyte=19092 lanout=13250
fctuid="6F6248B158C74FF98905ADCE528DB1E7" unauthuser="userb" unauthusersource="forticlient"
srcremote=207.102.138.19

4: date=2024-11-29 time=10:01:06 eventtime=1732903266274561819 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.41 srcport=34650
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.18.76.33 dstport=443 dstintf="port1" dstintfrole="undefined" service="udp/443"
proxyapptype="http" proto=17 action="accept" policyid=7 policytype="proxy-policy"
poluuid="ecb22964-a6c7-51ef-3b66-9aed56737e89" policyname="tc3" appcat="unscanned" duration=35
wanin=0 rcvdbyte=0 wanout=0 lanin=1200 sentbyte=1200 lanout=0
fctuid="6F6248B158C74FF98905ADCE528DB1E7" unauthuser="userb" unauthusersource="forticlient"
srcremote=207.102.138.19

5: date=2024-11-29 time=10:00:59 eventtime=1732903259718201554 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.41 srcport=34650
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=172.18.76.33 dstport=443 dstintf="port1" dstintfrole="undefined" service="udp/443"
proxyapptype="http" proto=17 action="accept" policyid=7 policytype="proxy-policy"
poluuid="ecb22964-a6c7-51ef-3b66-9aed56737e89" policyname="tc3" appcat="unscanned" duration=35
wanin=0 rcvdbyte=0 wanout=0 lanin=1200 sentbyte=1200 lanout=0
fctuid="6F6248B158C74FF98905ADCE528DB1E7" unauthuser="userb" unauthusersource="forticlient"
srcremote=207.102.138.19

6: date=2024-11-29 time=10:00:48 eventtime=1732903249011046552 tz="-0800" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.41 srcport=38406
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.1.20.1 dstport=8888 dstintf="port1" dstintfrole="undefined" sessionid=1366711343
service="tcp/8888" proxyapptype="http" proto=6 action="accept" policyid=7 policytype="proxy-
policy" poluuid="ecb22964-a6c7-51ef-3b66-9aed56737e89" policyname="tc3" trandisp="snat"
transip=10.120.1.209 transport=0 clientip=10.120.1.41 appcat="unscanned" duration=0 vip="ztna_
vip" accessproxy="access-proxy" clientdevicemanageable="unknown" clientcert="no" wanin=0
rcvdbyte=0 wanout=0 lanin=0 sentbyte=0 lanout=0 fctuid="6F6248B158C74FF98905ADCE528DB1E7"
unauthuser="userb" unauthusersource="forticlient" srcremote=207.102.138.19
```

ZTNA troubleshooting and debugging commands

The following debug commands can be used to troubleshoot ZTNA issues:

Command	Description
`# diagnose endpoint fctems test-connectivity <EMS>`	Verify FortiProxy to FortiClient EMS connectivity.
`# execute fctems verify <EMS>`	Verify the FortiClient EMS's certificate.
`# diagnose test application fcnacd 2`	Dump the EMS connectivity information.
`# diagnose debug app fcnacd -1` `# diagnose debug enable`	Run real-time FortiClient NAC daemon debugs.
`# diagnose endpoint record list`	Show the endpoint record list. Optionally, add filters.
`# diagnose endpoint lls-comm send ztna find-uid <uid> <EMS_serial_number> <EMS_tenant_id>`	Query endpoints by client UID, EMS serial number, and EMS tenant ID.
`# diagnose endpoint lls-comm send ztna find-ip-vdom <ip> <vdom>`	Query endpoints by the client IP-VDOM pair.
`# diagnose wad dev query-by uid <uid> <EMS_serial_number> <EMS_tenant_id>`	Query from WAD diagnose command by UID, EMS serial number, and EMS tenant ID.
`# diagnose wad dev query-by ipv4 <ip>`	Query from WAD diagnose command by IP address.
`# diagnose firewall dynamic list`	List EMS security posture tags and all dynamic IP and MAC addresses.
`# diagnose test application fcnacd 7` `# diagnose test application fcnacd 8`	Check the FortiClient NAC daemon ZTNA and route cache.
`# diagnose wad worker policy list`	Display statistics associated with application gateway rules.

`# diagnose wad debug enable category all`
`# diagnose wad debug enable level verbose`
`# diagnose debug enable`
	Run real-time WAD debugs.

`# diagnose debug reset`	Reset debugs when completed



The WAD daemon handles proxy related processing. The FortiClient NAC daemon (fcnacd) handles FortiProxy to EMS connectivity.

Troubleshooting usage and output

1. Verify the FortiProxy to EMS connectivity and EMS certificate:

```
# diagnose endpoint fctems test-connectivity 1
Connection test was successful.
# execute fctems verify 1
EMS already verified.
# diagnose test application fcnacd 2
EMS context status:
```

```
FortiClient EMS number 1:
        name(id): emstest(1) confirmed: yes
        fetched-serial-number: FCTEMS8823005021
        fetched-tenant-id: 00000000000000000000000000000000
        user-data:
                verified capabilities: true
                verified identity: true
        interface-selection-method: 0
        verify-peer-method: 4
Websocket status: connected, oif: 0
```

2. If fcnacd does not report the proper status, run real-time fcnacd debugs:

```
# diagnose debug app fcnacd -1
# diagnose debug enable
```

3. Verify the following information about an endpoint:
   - Network information
   - Registration information
   - Client certificate information
   - Device information
   - Vulnerability status
   - Relative position with the FortiProxy

```
# dia end record list 10.120.1.26
Record #1:
                IP Address = 10.120.1.26
                MAC Address = 00:0c:29:8d:33:5c
                MAC list =
                VDOM = root (0)
                EMS serial number: FCTEMS8823005021
                EMS tenant id: 00000000000000000000000000000000
                Client cert SN: 696348D6485176EECFEC967D9E762D5166CF00EB
                Public IP address: 207.102.138.19
                Quarantined: no
                Online status: online
                Registration status: registered
                On-net status: on-net
                Gateway Interface: port1
                FortiClient version: 7.2.4
                AVDB version: 0.0
                FortiClient app signature version: 0.0
                FortiClient vulnerability scan engine version: 2.40
                FortiClient UID: 0F37F57235724AD19FADAABB1B34AE6F
                Host Name: DESKTOP-CLIUU77
                OS Type: WIN64
                OS Version: Microsoft Windows 10 Professional Edition, 64-bit (build 19045)
                Host Description:
                Domain: qa.domaintest.com
                Last Login User: userc
                Owner:
```

```
                Host Model: VMware Virtual Platform
                Host Manufacturer: VMware, Inc.
                CPU Model: Intel(R) Xeon(R) CPU E5-2630 v2 @ 2.60GHz
                Memory Size: 4095
                AV Feature: 0
                FW Feature: 0
                WF Feature: 0
                AS Feature: 0
                VS Feature: 1
                VN Feature: 1
                Last vul message received time: N/A
                Last vul scanned time: N/A
                Last vul statistic: critical=0, high=0, medium=0, low=0, info=0
                Avatar fingerprint: 05b9940c015425a375caafa28096d695be6e9ad2
                Avatar source username: userc
                Avatar source email:
                Avatar source: OS
                Phone number:
                Number of Routes: (1)
                        Gateway Route #0:
                                - IP:10.120.1.26, MAC: 00:0c:29:8d:33:5c, VPN: no
                                - Interface:port1, VFID:0, SN: FPXVULTM24000082
online records: 1; offline records: 0; quarantined records: 0; out-of-sync records: 0
```

4. Query endpoint information from WAD by UID or IP address:

```
# diagnose wad dev query-by uid 0F37F57235724AD19FADAABB1B34AE6F FCTEMS8823005021
00000000000000000000000000000000
Attr of type=0, length=83, value(ascii)=0F37F57235724AD19FADAABB1B34AE6F
Attr of type=4, length=0, value(ascii)=
Attr of type=6, length=1, value(ascii)=true
Attr of type=5, length=40, value(ascii)=696348D6485176EECFEC967D9E762D5166CF00EB
Attr of type=3, length=18, value(ascii)=EMS1_ZTNA_usergrp2
Attr of type=3, length=22, value(ascii)=MAC_EMS1_ZTNA_usergrp2
Attr of type=3, length=17, value(ascii)=EMS1_ZTNA_disk-en
Attr of type=3, length=21, value(ascii)=MAC_EMS1_ZTNA_disk-en
Attr of type=3, length=32, value(ascii)=EMS1_ZTNA_all_registered_clients
Attr of type=3, length=36, value(ascii)=MAC_EMS1_ZTNA_all_registered_clients
Attr of type=3, length=23, value(ascii)=EMS1_ZTNA_anti-virus-ok
Attr of type=3, length=27, value(ascii)=MAC_EMS1_ZTNA_anti-virus-ok
Attr of type=3, length=18, value(ascii)=EMS1_ZTNA_usergrp3
Attr of type=3, length=22, value(ascii)=MAC_EMS1_ZTNA_usergrp3
Response termination due to no more data
# diagnose wad dev query-by ipv4 10.120.1.26
Attr of type=0, length=83, value(ascii)=0F37F57235724AD19FADAABB1B34AE6F
Attr of type=4, length=0, value(ascii)=
Attr of type=6, length=1, value(ascii)=true
Attr of type=5, length=40, value(ascii)=696348D6485176EECFEC967D9E762D5166CF00EB
Attr of type=3, length=18, value(ascii)=EMS1_ZTNA_usergrp2
Attr of type=3, length=22, value(ascii)=MAC_EMS1_ZTNA_usergrp2
Attr of type=3, length=17, value(ascii)=EMS1_ZTNA_disk-en
Attr of type=3, length=21, value(ascii)=MAC_EMS1_ZTNA_disk-en
```

```
Attr of type=3, length=32, value(ascii)=EMS1_ZTNA_all_registered_clients
Attr of type=3, length=36, value(ascii)=MAC_EMS1_ZTNA_all_registered_clients
Attr of type=3, length=23, value(ascii)=EMS1_ZTNA_anti-virus-ok
Attr of type=3, length=27, value(ascii)=MAC_EMS1_ZTNA_anti-virus-ok
Attr of type=3, length=18, value(ascii)=EMS1_ZTNA_usergrp3
Attr of type=3, length=22, value(ascii)=MAC_EMS1_ZTNA_usergrp3
Response termination due to no more data
```

5. List all the dynamic ZTNA IP and MAC addresses learned from EMS:

```
# diagnose firewall dynamic list
List all dynamic addresses:
IP dynamic addresses in VDOM root(vfid: 0):
CMDB name: FCTEMS_ALL_FORTICLOUD_SERVERS
FCTEMS_ALL_FORTICLOUD_SERVERS: ID(239)
        ADDR(75.237.184.208)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 1.

CMDB name: EMS1_ZTNA_AntiVirus_ON
TAG name: AntiVirus_ON
EMS1_ZTNA_AntiVirus_ON: ID(109)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 0.

CMDB name: EMS1_ZTNA_anti-virus-software
TAG name: anti-virus-software
EMS1_ZTNA_anti-virus-software: ID(213)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 0.

CMDB name: EMS1_ZTNA_anti-virus-ok
TAG name: anti-virus-ok
EMS1_ZTNA_anti-virus-ok: ID(115)
        ADDR(10.120.1.26)
Total IP dynamic range blocks: 0.
Total IP dynamic addresses: 1.
…
```

6. Check the FortiClient NAC daemon ZTNA and route cache:

```
# diagnose test application fcnacd 7

ZTNA Cache V2:
Entry #1:

 - UID: 0F37F57235724AD19FADAABB1B34AE6F
 - EMS Fabric ID: FCTEMS8823005021:00000000000000000000000000000000
 - Domain: qa.domaintest.com
 - User: userc
 - Owner:
 - Certificate SN: 696348D6485176EECFEC967D9E762D5166CF00EB
```

```
 - online: true
 - Routes (1):
  -- Route #0: IP=10.120.1.26, vfid=0
 - FWAddrNames (10):
  -- Name (#0): EMS1_ZTNA_usergrp2
  -- Name (#1): MAC_EMS1_ZTNA_usergrp2
  -- Name (#2): EMS1_ZTNA_disk-en
  -- Name (#3): MAC_EMS1_ZTNA_disk-en
  -- Name (#4): EMS1_ZTNA_all_registered_clients
  -- Name (#5): MAC_EMS1_ZTNA_all_registered_clients
  -- Name (#6): EMS1_ZTNA_anti-virus-ok
  -- Name (#7): MAC_EMS1_ZTNA_anti-virus-ok
  -- Name (#8): EMS1_ZTNA_usergrp3
  -- Name (#9): MAC_EMS1_ZTNA_usergrp3
lls_idx_mask = 0x00000001,
```

7. Troubleshoot WAD with real-time debugs to understand how the proxy handled a client request:

```
# diagnose wad debug enable category all
# diagnose wad debug enable level verbose
# diagnose debug enable

[I][p:1608][s:2079431665][r:7] wad_dump_http_request             :2833  hreq=0x7fbfcc8cc228
Received request from client: 10.100.1.21:49974

GET /icons/ubuntu-logo.png HTTP/1.1
Host: 10.100.1.59:7831
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0
accept: image/avif,image/webp,*/*
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate, br
dnt: 1
sec-gpc: 1
referer: https://10.100.1.59:7831/
sec-fetch-dest: image
sec-fetch-mode: no-cors
sec-fetch-site: same-origin
te: trailers

[V][p:1608][s:2079431665][r:7] wad_http_marker_uri               :1270  path=/icons/ubuntu-
logo.png len=22
[V][p:1608][s:2079431665][r:7] wad_http_parse_host               :1649  host_len=16
[V][p:1608][s:2079431665][r:7] wad_http_parse_host               :1685  len=11
[V][p:1608][s:2079431665][r:7] wad_http_parse_host               :1694  len=4
[I][p:1608][s:2079431665][r:7] wad_http_str_canonicalize         :2200  enc=0
path=/icons/ubuntu-logo.png len=22 changes=0
[V][p:1608][s:2079431665][r:7] wad_http_normalize_uri            :2432  host_len=11 path_
len=22 query_len=0
[I][p:1608][s:2079431665][r:7] wad_vs_proxy_match_gwy            :4251  3:ZTNA_server01:
matching gwy with vhost(_def_virtual_host_)
[V][p:1608][s:2079431665][r:7] wad_vs_proxy_match_vhost          :4312  3:ZTNA_server01:
matching vhost by: 10.100.1.59
```

```
[V][p:1608][s:2079431665][r:7] wad_vs_matcher_map_find           :709   Empty matcher!
[V][p:1608][s:2079431665][r:7] wad_vs_proxy_match_vhost          :4315  3:ZTNA_server01: no
host matched.
[I][p:1608][s:2079431665][r:7] wad_vs_proxy_match_gwy            :4270  3:ZTNA_server01:
matching gwy by (/icons/ubuntu-logo.png) with vhost(_def_virtual_host_).
[V][p:1608][s:2079431665][r:7] wad_pattern_matcher_search        :1307  pattern-match succ:
'/icons/ubuntu-logo.png'
[I][p:1608][s:2079431665][r:7] wad_vs_proxy_match_gwy            :4288  3:ZTNA_server01:
Matched gwy(1) type(https).
[I][p:1608][s:2079431665][r:7] wad_http_req_update_by_vs_server  :1058  3:ZTNA_server01:1:
hostname after rewrite: Host: 10.120.1.78

[I][p:1608][s:2079431665][r:7] wad_http_vs_check_dst_ovrd        :1225  3:ZTNA_server01:1:
Found server: 10.120.1.78:443
[V][p:1608][s:2079431665][r:7] wad_http_req_exec_act             :15123 request
(0x7fbfcc8cc228), intercept(pass), block(0)
[V][p:1608][s:2079431665][r:7] wad_http_req_exec_act             :15215 dst_addr_type=3 wc_
nontp=0 sec_web=1 web_cache=0 req_bypass=1
[V][p:1608][s:2079431665][r:7] wad_http_req_vs_check_policy      :13895 HTTP
req=0x7fbfcc8cc228 out_intf=3, vwl=0
[V][p:1608][s:2079431665][r:7] wad_http_req_check_policy         :13627 start match policy
vd=0(ses_ctx:ct|Pvx|Mde|Hf|C|A1|Og) (10.120.1.209:6092@6->10.120.1.78:443@3) absUrl=0
[V][p:1608][s:2079431665][r:7] wad_fw_addr_match_l7_vip          :1253  matching vip:ZTNA_
server01(13) type:AP-HTTPS with vip addr:ZTNA_server01(13)
[I][p:1608][s:2079431665][r:7] wad_url_filter_req_alloc          :698   url_req=0x7fbfc8b56978
id=0
[I][p:1608][s:2079431665][r:7] wad_url_filter_rating_request     :4146  hreq=0x7fbfcc8cc228
url_req=0x7fbfc8b56978 hostname=10.100.1.59, url=/icons/ubuntu-logo.png vd=root id=0 ses_
ctx.dst=10.120.1.78 req.srv=10.120.1.78
[V][p:1608][s:2079431665][r:7] wad_url_fetch_cate2                :1535  host=10.100.1.59
ip=10.120.1.78
[I][p:1608][s:2079431665][r:7] wad_url_cate_dump_req_ctx         :280   (fetch-done):
req/wfp=1/0 cate: cate=255 webf=255 sslexempt=255 url/ip=0/0 done:
bal=0,local/user/cache/ftgd/ia_cache=1/1/1/1/0   matched[url]: block/allow/user=0/0/0 ftgd=0
sub=0 log=0 invalid=0
[I][p:1608][s:2079431665][r:7] wad_http_policy_get_cate_info     :272   get category right
away
[I][p:1608][s:2079431665][r:7] wad_url_filter_cancel             :710   type=2
data=0x7fbfcc8cc228 url_req=0x7fbfc8b56978 id=0
[I][p:1608][s:2079431665][r:7] wad_http_policy_match_one         :511   fw_pol_id=1(pol_
ctx:th|Ac|7|=p) pflag:H|W|U|Ac asyn_info=1
[I][p:1608][s:2079431665][r:7] wad_fw_policy_async_match         :7401  pol_ctx:th|Ac|7|=d
[I][p:1608][s:2079431665][r:7] wad_http_req_policy_set           :11734 match policy-id=1(pol_
ctx:th|Ac|7|=d) vd=0(ses_ctx:ct|Pvx|Mde|Hf|C|A1|Og) (10.100.1.21:49974@6 -> 10.120.1.78:443@3)
[V][p:1608][s:2079431665][r:7] wad_https_ap_pol_info_get         :11542 policy info created,
req=0x7fbfcc8cc228, ses_ctx=0x7fbfc8b9c570, info=0x7fbfc8bcfab0
[I][p:1608][s:2079431665][r:7] wad_http_req_proc_policy          :11236 ses_
ctx:ct|Pvx|Mde|Hf|C|A1|Og conn_srv=0 fwd_srv=<nil>
[I][p:1608][s:2079431665][r:7] wad_http_req_proc_policy          :11370 policy result:vf_
id=0:0 sec_profile=0x7fbfc89ad048 set_cookie=0
[W][p:1608][s:2079431665][r:7] wad_fw_policy_async_match         :7391  no policy to match.
```

```
[V][p:1608][s:2079431665][r:7] wad_setup_shaping_policy          :536   did not match any
shaping policy
[I][p:1608][s:2079431665][r:7] wad_http_urlfilter_check          :392   uri_norm=1 inval_
host=0 inval_url=0 scan-hdr/body=1/0 url local=0 block=0 user-cat=0 allow=0 ftgd=0 keyword=0
wisp=0
[I][p:1608][s:2079431665][r:7] wad_http_req_proc_waf             :1338  req=0x7fbfcc8cc228
ssl.deep_scan=1 proto=10 exempt=0 waf=(nil) body_len=18446744073709551615 ua=Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0 skip_scan=0
[V][p:1608][s:2079431665][r:7] wad_http_req_proc_antiphish       :9091  No profile
[V][p:1608][s:2079431665][r:7] wad_http_parse_auth_cookie        :1421  cookie_parsed=0
strip=1 pid=1608
[I][p:1608][s:2079431665][r:7] wad_vs_ssl_cert_sni_check         :12995 sni=10.120.1.78 len=11
name=(null): cannot find the matched SNI in the certificate CN or SAN.
[I][p:1608][s:2079431665][r:7] wad_http_srvs_ssl_tnode_get_srv   :811   found server with
matched sent sni:10.120.1.78 even cert not match, use it
[I][p:1608][s:2079431665][r:7] wad_http_srv_attach_req           :461   [0x7fbfcc8cc228] Use
old server0x7fbfcc8df280: 10.120.1.78:443
[V][p:1608][s:2079431665][r:7] wad_http_req_get_svr              :10077 http session
0x7fbfc8d76208 req=0x7fbfcc8cc228 connected
[V][p:1608][s:2079431665][r:7] wad_http_msg_start_setup_proc     :2320  msg(0x7fbfcc8cc228)
proc-setup started from: req_casb.
[V][p:1608][s:2079431665][r:7] wad_http_def_proc_msg_plan        :2282  msg(0x7fbfcc8cc228)
setting up processor(req_casb)
[V][p:1608][s:2079431665][r:7] wad_http_def_proc_msg_plan        :2282  msg(0x7fbfcc8cc228)
setting up processor(req_scan)
```



Always reset the debugs after using them:

```
# diagnose debug reset
```

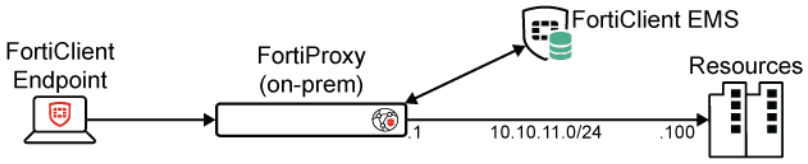
ZTNA troubleshooting scenarios

This topic describes how to troubleshoot common FortiClient endpoint IP/MAC access control issues for the following topologies:

- ZTNA access control on page 374
- IP/MAC based access control on page 376

ZTNA access control

In this topology, FortiClient endpoints use an SSL encrypted connection to the FortiProxy application gateway to access protected resources. FortiProxy works with FortiClient EMS to use a combination of IP/MAC addresses and security posture tags to control FortiClient endpoint access to resources.



This section describes how to handle the following errors:

- Invalid ZTNA certificate on page 375
- ZTNA policy mismatch on page 375

Invalid ZTNA certificate

When FortiClient attempts to access a server protected by ZTNA, an *Invalid ZTNA certificate* error is shown. This error often appears when the serial number for the ZTNA certificate differs between the endpoint and the FortiProxy.

1. Check the serial number for the ZTNA certificate on the endpoint and the FortiProxy:
   a. On the endpoint, check the serial number for the certificate.
   b. On the FortiProxy, check the serial number for the client certificate by running the following command:

```
# diagnose endpoint record list
```

2. If the serial number for the ZTNA certificate differs between the endpoint and the FortiProxy, and the serial number on the FortiProxy is comprised of zeros, check the following:
   a. For FortiClient, make sure that the endpoint is running FortiClient 7.0 or later. FortiClient versions earlier than 7.0 do not support ZTNA.
   b. For FortiClient EMS, make sure that ZTNA is enabled. Check the profile on EMS and the endpoint's summary information.
   c. For licensing, make sure that you have a ZTNA agent license entitlement. Only some license types support ZTNA.
3. If the serial numbers still do not match, deregister FortiClient from EMS, and then connect FortiClient to EMS again to trigger a new certificate signing request.

ZTNA policy mismatch

In most cases, FortiProxy denies incoming ZTNA requests because the endpoint FortiClient does not meet the tagging criteria configured in the ZTNA rule and is considered a policy mismatch.

1. On the FortiProxy, look at the ZTNA event logs and the forwarded logs.
2. Run the following commands on the ZTNA server:

```
# diagnose wad debug enable category policy
```

```
# diagnose wad debug enable level verbose
```

```
# diagnose debug enable
```

The command output contains incoming ZTNA requests and the FortiProxy process for matching the connection to a ZTNA rule.

3. Verify the zero trust tags for the endpoint:
   - On FortiClient, verify the applied tags. Click the avatar to view the zero trust tags.
   - On FortiClient EMS, verify the endpoint's tags. Go to the endpoint list and click the endpoint.
   - On FortiProxy, verify the tags using the following commands:
     - Display ZTNA cache data for all endpoints:

       ```
       # diagnose test application fcnacd 7
       ```

     - Display ZTNA cache data for an individual endpoint:

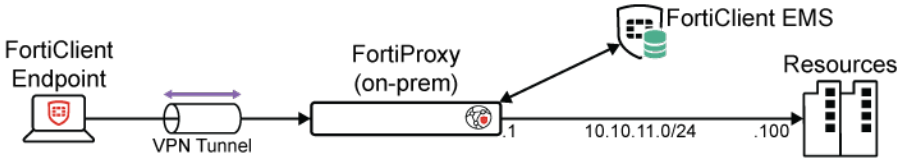
       ```
       # diagnose wad dev query-by uid <UID> <EMS S/N> <tenant ID>
       ```

4. If the tagging information differs between FortiProxy and EMS, examine the EMS tag exchange communication between FortiProxy and EMS by looking at the cmNotify and python logs in the debug diagnostics for EMS.

   For more information about FortiClient EMS diagnostics, see Generate Diagnostic Log in the FortiClient EMS Administration Guide.

IP/MAC based access control

In the following ZTNA topology, FortiClient endpoints use VPN to access resources. FortiProxy works with FortiClient EMS to use a combination of IP/MAC addresses and security posture tags to control FortiClient endpoint access to resources.



Security posture tag information missing on the FortiProxy

If the IP address for the FortiClient endpoint is not associated with a security posture tag on the FortiProxy, a firewall policy mismatch occurs, and the FortiProxy denies network access to the FortiClient endpoint.

The following workflow summarizes how FortiProxy retrieves the IP address and tags for the FortiClient endpoint to help you better understand how to troubleshoot the situation:

1. FortiClient establishes a VPN connection to the FortiProxy.
2. FortiProxy uses the API to pass FortiClient's UUID and VPN IP address to FortiClient EMS.
3. FortiProxy requests system information and tags from FortiClient based on the response from EMS.

Based on the workflow, start troubleshooting before the FortiClient endpoint attempts to establish a VPN connection to FortiProxy. On FortiProxy, run the following commands:

```
# diagnose debug application fcnacd -1
```

```
# diagnose debug console timestamp enable
```

```
# diagnose endpoint filter show-large-data yes
```

```
# diagnose debug enable
```

The following outputs illustrate how to examine the command output. The output can differ between environments. The outputs help illustrate how to understand the communication between FortiProxy and FortiClient EMS.

In the following output, FortiProxy's VPN daemon sends FortiClient's UUID and the VPN IP address to FortiClient EMS using the API. The NAC daemon makes the API call to send the details to FortiClient EMS:

```
2024-07-11 10:57:36 [ec_daemon_submit_sock_call:49] sent 244,244
[fcems_call_vpn_client_gateway_call:1151] VPN act connect (UID: 70A5C5FABBE64A9B98B6DDA3FE8AC794,
Interface: port1, IP: 10.212.134.200, VDom: root, FortiProxy-SN: FPXVULTM24000083) added to EMS
emstest(FCTEMS8823005021:00000000000000000000000000000000)
2024-07-11 10:57:36 [ec_ez_worker_base_prep_resolver:374] Outgoing interface index 0 for 1
(emstest).
2024-07-11 10:57:36 [ec_ez_worker_prep_data_url:98] request (206):
"""
{"sn_list":["FPXVULTM24000083"],"uid_list":
[{"uid":"70A5C5FABBE64A9B98B6DDA3FE8AC794","ip":"10.212.134.200","is_
delete":false,"vdom":"root","interface":"port1","sn":"FPXVULTM24000083"}],"is_snapshot":false}
"""
2024-07-11 10:57:36 [ec_ez_worker_prep_data_url:184] Full URL:
https://10.120.1.24/api/v1/fgt/gateway_details/vpn
2024-07-11 10:57:36 [ec_ez_worker_base_prep_ssl:423] verify peer method: 4, current ssl_cb:
0x6ad220, new ssl_cb: 0x6ad220
2024-07-11 10:57:36 [ec_ems_context_submit_work:519] Call submitted successfully.
    obj-id: 7, desc: REST API to send updated regarding VPN updates., entry: api/v1/fgt/gateway_
details/vpn.
2024-07-11 10:57:36 [__get_ec_fctems_certificate_info:431] ems cert ca_cn: C = US, ST =
California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress =
support@fortinet.comFCTEMS8823005021
2024-07-11 10:57:36 [__get_ec_fctems_certificate_info:432] ems cert fingerprint:
1F:17:09:BF:F3:C9:E3:3A:80:D6:30:91:36:C1:0B:76:AE:38:1B:C9:F8:B8:B2:0C:C1:28:04:A1:AF:77:85:96:7C
:39:2E:52:4A:D9:C4:00:A0:7E:0C:C3:53:68:42:49:F9:3F:41:8F:47:29:1B:81:F4:26:F9:5C:61:DF:E6:EF
2024-07-11 10:57:36 [__match_server_cert_key:487] verify_peer_method: 4
2024-07-11 10:57:36 [__match_server_cert_key:505] ret=1
2024-07-11 10:57:36 [ec_ez_worker_process:368] Processing call for obj-id: 7, entry:
"api/v1/fgt/gateway_details/vpn"
2024-07-11 10:57:36 [ec_ez_worker_process:387] reply:
"""
{"result": {"retval": 1, "message": "FortiGate VPN connection details updated successfully"},
"data": {"rejected_uid_list": []}}
"""
2024-07-11 10:57:36 [_update_obj_stats:336] Storing (7, emstest, 0)
2024-07-11 10:57:36 [ec_ez_worker_process:475] Call completed successfully.
```

```
    obj-id: 7, desc: "REST API to send updated regarding VPN updates.", entry:
"api/v1/fgt/gateway_details/vpn".
2024-07-11 10:57:38 [__ws_writefunction_once:963] received frame: opcode:TEXT(1), fin:1, mask: 0,
len: 82.
2024-07-11 10:57:38 [fcems_ws_on_text:369] WebSocket Recv(83): {"message_
type":"notification","message_body":{"notify": {"tags":{"value":true}}}}
2024-07-11 10:57:38 [ec_ems_context_update_call:393] Update didn't constitute a scheduled call for
obj-id 12
2024-07-11 10:57:38 [ec_ems_context_update_call:393] Update didn't constitute a scheduled call for
obj-id 13
2024-07-11 10:57:38 [__ws_writefunction_once:963] received frame: opcode:TEXT(1), fin:1, mask: 0,
len: 85.
2024-07-11 10:57:38 [fcems_ws_on_text:369] WebSocket Recv(86): {"message_
type":"notification","message_body":{"notify": {"sysinfo":{"value":true}}}}
2024-07-11 10:57:38 [ec_ems_context_update_call:393] Update didn't constitute a scheduled call for
obj-id 8
2024-07-11 10:57:38 [ec_ez_worker_base_prep_resolver:374] Outgoing interface index 0 for 1
(emstest).
2024-07-11 10:57:38 [ec_ez_worker_prep_data_url:98] request (142):
"""
sn_list[]=FPXVULTM24000083&updated_after=2024-07-11%2017%3A57%3A41%2E4804469&tag_uid_
offset=9C8AF06C-8585-4572-ACDC-597E6AA1B6CD&send_mac=true
"""
2024-07-11 10:57:38 [ec_ez_worker_prep_data_url:184] Full URL:
https://10.120.1.24/api/v1/report/fct/tags?sn_list[]=FPXVULTM24000083&updated_after=2024-07-
11%2017%3A57%3A41%2E4804469&tag_uid_offset=9C8AF06C-8585-4572-ACDC-597E6AA1B6CD&send_mac=true
2024-07-11 10:57:38 [ec_ez_worker_base_prep_ssl:423] verify peer method: 4, current ssl_cb:
0x6ad220, new ssl_cb: 0x6ad220
2024-07-11 10:57:38 [ec_ems_context_submit_work:519] Call submitted successfully.
    obj-id: 12, desc: REST API to get updates of tag endpoints., entry: api/v1/report/fct/tags.
2024-07-11 10:57:38 [ec_ez_worker_base_prep_resolver:374] Outgoing interface index 0 for 1
(emstest).
2024-07-11 10:57:38 [ec_ez_worker_prep_data_url:98] request (120):
"""
sn_list[]=FPXVULTM24000083&updated_after=2024-07-11%2017%3A57%3A41%2E4774466&uid_
offset=70A5C5FABBE64A9B98B6DDA3FE8AC794
"""
2024-07-11 10:57:38 [ec_ez_worker_prep_data_url:184] Full URL:
https://10.120.1.24/api/v1/report/fct/uid_tags?sn_list[]=FPXVULTM24000083&updated_after=2024-07-
11%2017%3A57%3A41%2E4774466&uid_offset=70A5C5FABBE64A9B98B6DDA3FE8AC794
2024-07-11 10:57:38 [ec_ez_worker_base_prep_ssl:423] verify peer method: 4, current ssl_cb:
0x6ad220, new ssl_cb: 0x6ad220
2024-07-11 10:57:38 [ec_ems_context_submit_work:519] Call submitted successfully.
    obj-id: 13, desc: REST API to get updates of tags associated with FCT UID., entry:
api/v1/report/fct/uid_tags.
2024-07-11 10:57:38 [__get_ec_fctems_certificate_info:431] ems cert ca_cn: C = US, ST =
California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress =
support@fortinet.comFCTEMS8823005021
2024-07-11 10:57:38 [__get_ec_fctems_certificate_info:432] ems cert fingerprint:
1F:17:09:BF:F3:C9:E3:3A:80:D6:30:91:36:C1:0B:76:AE:38:1B:C9:F8:B8:B2:0C:C1:28:04:A1:AF:77:85:96:7C
:39:2E:52:4A:D9:C4:00:A0:7E:0C:C3:53:68:42:49:F9:3F:41:8F:47:29:1B:81:F4:26:F9:5C:61:DF:E6:EF
2024-07-11 10:57:38 [__match_server_cert_key:487] verify_peer_method: 4
```

```
2024-07-11 10:57:38 [__match_server_cert_key:505] ret=1
2024-07-11 10:57:38 [__get_ec_fctems_certificate_info:431] ems cert ca_cn: C = US, ST =
California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress =
support@fortinet.comFCTEMS8823005021
2024-07-11 10:57:38 [__get_ec_fctems_certificate_info:432] ems cert fingerprint:
1F:17:09:BF:F3:C9:E3:3A:80:D6:30:91:36:C1:0B:76:AE:38:1B:C9:F8:B8:B2:0C:C1:28:04:A1:AF:77:85:96:7C
:39:2E:52:4A:D9:C4:00:A0:7E:0C:C3:53:68:42:49:F9:3F:41:8F:47:29:1B:81:F4:26:F9:5C:61:DF:E6:EF
2024-07-11 10:57:38 [__match_server_cert_key:487] verify_peer_method: 4
2024-07-11 10:57:38 [__match_server_cert_key:505] ret=1
2024-07-11 10:57:38 [ec_ez_worker_process:368] Processing call for obj-id: 13, entry:
"api/v1/report/fct/uid_tags"
2024-07-11 10:57:38 [ec_ez_worker_process:387] reply:
"""
{"result": {"retval": 1, "message": null}, "data": {"uid_offset":
"70A5C5FABBE64A9B98B6DDA3FE8AC794", "updated_after": "2024-07-11 17:57:41.4774466", "is_final":
true, "data": "eJyrVirNTIkvSUyPz8ksLilWsqqurQUAUUEH2g==", "is_zipped": true, "unzipped_size": 20}}
"""
2024-07-11 10:57:38 [fcems_json_unzip:289] unzipped:
"""
{"uid_tag_lists":{}}
"""
2024-07-11 10:57:38 [_update_obj_stats:336] Storing (13, emstest, 0)
2024-07-11 10:57:38 [ec_ez_worker_process:475] Call completed successfully.
    obj-id: 13, desc: "REST API to get updates of tags associated with FCT UID.", entry:
"api/v1/report/fct/uid_tags".
2024-07-11 10:57:38 [ec_ez_worker_base_prep_resolver:374] Outgoing interface index 0 for 1
(emstest).
2024-07-11 10:57:38 [ec_ez_worker_prep_data_url:98] request (120):
"""
sn_list[]=FPXVULTM24000083&updated_after=2024-07-11%2017%3A57%3A41%2E4614463&uid_
offset=70A5C5FABBE64A9B98B6DDA3FE8AC794
"""
2024-07-11 10:57:38 [ec_ez_worker_prep_data_url:184] Full URL:
https://10.120.1.24/api/v1/report/fct/sysinfo?sn_list[]=FPXVULTM24000083&updated_after=2024-07-
11%2017%3A57%3A41%2E4614463&uid_offset=70A5C5FABBE64A9B98B6DDA3FE8AC794
2024-07-11 10:57:38 [ec_ez_worker_base_prep_ssl:423] verify peer method: 4, current ssl_cb:
0x6ad220, new ssl_cb: 0x6ad220
2024-07-11 10:57:38 [ec_ems_context_submit_work:519] Call submitted successfully.
    obj-id: 8, desc: REST API to get updates about system info., entry: api/v1/report/fct/sysinfo.
2024-07-11 10:57:38 [__get_ec_fctems_certificate_info:431] ems cert ca_cn: C = US, ST =
California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress =
support@fortinet.comFCTEMS8823005021
2024-07-11 10:57:38 [__get_ec_fctems_certificate_info:432] ems cert fingerprint:
1F:17:09:BF:F3:C9:E3:3A:80:D6:30:91:36:C1:0B:76:AE:38:1B:C9:F8:B8:B2:0C:C1:28:04:A1:AF:77:85:96:7C
:39:2E:52:4A:D9:C4:00:A0:7E:0C:C3:53:68:42:49:F9:3F:41:8F:47:29:1B:81:F4:26:F9:5C:61:DF:E6:EF
2024-07-11 10:57:38 [__match_server_cert_key:487] verify_peer_method: 4
2024-07-11 10:57:38 [__match_server_cert_key:505] ret=1
2024-07-11 10:57:38 [ec_ez_worker_process:368] Processing call for obj-id: 8, entry:
"api/v1/report/fct/sysinfo"
2024-07-11 10:57:38 [ec_ez_worker_process:387] reply:
"""
{"result": {"retval": 1, "message": null}, "data": {"uid_offset":
```

```
"70A5C5FABBE64A9B98B6DDA3FE8AC794", "updated_after": "2024-07-11 17:57:52.3553944", "is_final":
true, "data":
"eJyFVNtu4zYQ/RVCT7uAZJAUqYuf6mubttmkTfYCFIFAi5SXgEyqFGXDG/jfO/StxrZpAQsWzxkORzPn8DXK8YTP+HIynS4yN
imnZTHN5vNJulwUk1lesmj8GvX7XpvGVkMnhVeV1xsVjSOKKUtwnhCCSD7m8KOjlPO0ZCyKo/Wuqq0xqvbamsrvO9iC46ixzuu
61cr4SstoTDABVHRd1et1tVUuGv9Bi7ig/AXg7Q1KYnyClLlAeUwzwJraXwF2jNoO7U1YGlPAQjE+Gns3qLBotYGKGtH2sNR95
dRa9145Ja/on4NwwngI/BuD891gjDbrKwSHmaqvhfkHEwrrDbRqOXsuMMYFYdCzglHoj+4AJ3hEKDyjNAWoG1atrqsjQ3E+Ipi
OSFqMSAnkRtQAY5zgOqFlkpMkLROSA/NVOLkTTp2O+nQf3hOeISZRUyJcoDxFrEZcIpolXKFSoqxBQqIUo5ygFGJkSGN7b8Rxs
vPF0y/PD4/J04fpbz9jdiarjTBDI2o/uNDW80kxujP16BpipWqvXB4TIOpuAOTOeNW++/09+qKsCf+zx49owROaQRlbin5AdJT
hH3/6Fr5Vbazbw6aClBjWtj9NMrrXtbO9bTz6rI20ux4RjB6dbVTfg8xEixZSB8HFKGPJSnv0bjXoViLIw/j7U6qTFqPPdx+y8
GlDr1x1/vD1YKWFAYJ8nR26C/zgvyqHFkZ2VhvfR0EGwgtXNTBt5ToHaBgOX5UlwzUmnFEu0pzXQjSCFrjMZFbylcpUKWSY/tk
BtXJnhTBC5jOWkhlb4oJOwJHzokwzvFwuspxxPmUZSctiAnsbJcIIKrGFfdr0XrStkjdEs3uD2HbmLaZ/g9g13xOg6WNPK2PBv
hkvQMtGagdOb/cXz984pllfTPD45dPHX5/vKcPBC0Hxa7hOdmJfQf+UA2mFZndwQwTZbKXdwNJZ628iv7MBXSVUJHl2EwGDgzu
qBTOD9V9vjmhsuMv+q5z/K+MQR6fsp2SQ/V9c/LZRT3vP8jt1LDq8HF7OGrxUCO9bfazh4Sk6HA5/ATr0vWU=", "is_
zipped": true, "unzipped_size": 1444}}
"""
2024-07-11 10:57:38 [fcems_json_unzip:289] unzipped:
"""
{"70A5C5FABBE64A9B98B6DDA3FE8AC794":{"sysinfo_update_time":"2024-07-11 17:57:52.3553944","gw_
connection_type":0,"forticlient_id":1010,"app_sig_ver":[28,825],"av_sig_ver":[1,0],"av_eng_ver":
[7,26],"fct_ver":[7,4,0],"vul_eng_ver":[3,2],"onnet":true,"online":false,"is_
registered":false,"quarantined":false,"av_running":false,"vuln_scan_running":false,"fct_
sn":"FCT8000814024842","ip":"10.120.1.33","public_ip":"207.102.138.19","mac":"00-0c-29-71-39-
17","hardware_sn":"VMware-56 4d f9 08 73 4c 5d 26-5e 9d 6f ad 30 71 39 0d","hostname":"DESKTOP-
SNBQJ04","host_manufacturer":"VMware, Inc.","host_model":"VMware7,1","cpu":"Intel(R) Xeon(R) CPU
E5-2630 v2 @ 2.60GHz","memory":"8190","os_ver":"Microsoft Windows 10 Professional Edition, 64-bit
(build 19045)","os_type":"WIN64","user_name":"guodong","group_name":"Other Endpoints","avatar_
fingerprint":"05b9940c015425a375caafa28096d695be6e9ad2","client_cert_
sn":"411DC431C4F082AC5FD89360FFE67455B461398A","feature_av":"installed","feature_
fw":"installed","feature_vpn":"installed","feature_vs":"installed","feature_wf":"installed","fct_
build_no":1658,"indirectly_connected":false,"fgt_sn":"FPXVULTM24000083","gateway_
interface":"port1","vdom":"root","gateway_mac":"00-0c-29-2b-2a-76","gateway_route_list":
[{"gateway_info":{"fgt_sn":"FPXVULTM24000083","interface":"port1","vdom":"root"},"route_info":
[{"ip":"10.120.1.33","mac":"00-0c-29-71-39-17","route_type":"direct"}]}],"user_info":
{"service":"OS"}}}
"""
2024-07-11 10:57:38 [ec_rec_add:1133] called (FTCL UID 70A5C5FABBE64A9B98B6DDA3FE8AC794).
2024-07-11 10:57:38 [ec_avatar_update:440] called (FTCL UID 70A5C5FABBE64A9B98B6DDA3FE8AC794).
2024-07-11 10:57:38 [ec_record_del_user_store:1649] deleting user store for user guodong, vfid:0
2024-07-11 10:57:38 [_update_obj_stats:336] Storing (8, emstest, 0)
2024-07-11 10:57:38 [ec_ez_worker_process:475] Call completed successfully.
    obj-id: 8, desc: "REST API to get updates about system info.", entry:
"api/v1/report/fct/sysinfo".
2024-07-11 10:57:39 [ec_ez_worker_process:368] Processing call for obj-id: 12, entry:
"api/v1/report/fct/tags"
2024-07-11 10:57:39 [ec_ez_worker_process:387] reply:
"""
{"result":{"retval":1,"message":"Returned FCT incremental tags information"},"data":{"tag_uid_
offset":"9C8AF06C-8585-4572-ACDC-597E6AA1B6CD","updated_after":"2024-07-11 17:57:41.4804469","is_
final":true,"data":"eJyqVkrOz81NzEuJL0stKs7Mz1OyMtJRKk4tykzMUbJScnMOcfUNtrAwMjYwMDUwMlTSUUpJLctMTo
0vqSxIVbJSSssvKslMzS1WqgUEAAD//4xEGAI=","is_zipped":true,"unzipped_size":74}}
"""
2024-07-11 10:57:39 [fcems_json_unzip:289] unzipped:
```

```
"""
{"command_version":2,"serial":"FCTEMS8823005021","device_type":"fortiems"}
"""
2024-07-11 10:57:39 [_update_obj_stats:336] Storing (12, emstest, 0)
2024-07-11 10:57:39 [ec_ez_worker_process:475] Call completed successfully.
    obj-id: 12, desc: "REST API to get updates of tag endpoints.", entry:
"api/v1/report/fct/tags".

2024-07-11 10:57:49 [__ws_writefunction_once:963] received frame: opcode:TEXT(1), fin:1, mask: 0,
len: 84.
2024-07-11 10:57:49 [fcems_ws_on_text:369] WebSocket Recv(85): {"message_
type":"notification","message_body":{"notify": {"avatar":{"value":true}}}}
```

Other useful CLI commands

Output the JSON-formatted list of FortiProxy interfaces (gateways) with IP and MAC addresses. This is the list that FortiProxy sends to EMS so that EMS can identify the endpoints that are directly connected to the firewall:

```
# diagnose endpoint fctems json gateway-mac-request
```

Makes EMS execute API calls to the EMS API endpoints on demand:

```
# diagnose test application fcnacd 5
```

Send the gateway list to EMS on demand. It could be useful to execute `diagnose test application fcnacd 5` right after command during troubleshooting, as EMS will have an updated list of firewall interfaces:

```
# diagnose test application fcnacd 99
```

For more commands, see ZTNA troubleshooting and debugging commands on page 367.

Policy & Objects

The *Policy & Objects* menu provides the following options:

- Policy on page 382
- Authentication Rules on page 419
- Proxy Auth Setting on page 427
- Traffic shaping on page 431
- Isolator Setting on page 468
- DNS Lookup on page 471
- Central SNAT on page 472
- PAC Policy on page 476
- Policy Test on page 480
- URL Lookup on page 481
- Decrypted Traffic Mirror on page 481
- Addresses on page 483
- Zero Trust Network Access introduction on page 232
- Internet Service Database on page 506
- Services on page 507
- Schedules on page 516
- Virtual IPs on page 521
- IP Pools on page 535

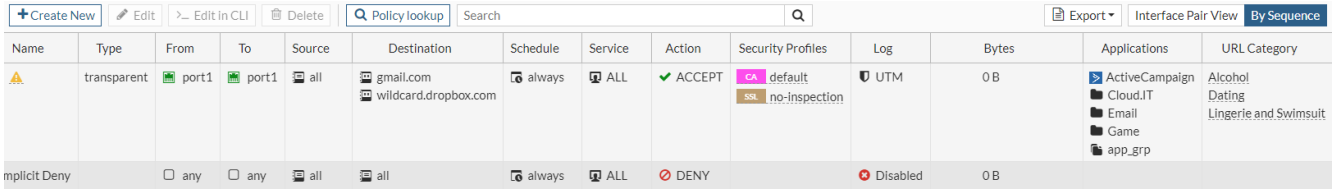
Policy

The policy list displays firewall policies in their order of matching precedence. For details about arranging policies in the policy list, see Change how the policy list is displayed.

You can add firewall policies that match HTTP traffic to be cached according to source and destination addresses and the destination port of the traffic.

Various right-click menus are available throughout the policy list. The columns displayed in the policy list can be customized, and filters can be added in a variety of ways to filter the information that is displayed. See Change how the policy list is displayed.

To view the policy list, go to *Policy & Objects* > *Policy*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Add a new policy. New policies are added to the bottom of the list. See Create or edit a policy on page 387.
Edit	Edit the selected policy. See Create or edit a policy on page 387.
Delete	Delete the selected policy.
Policy match	Use this button to find out which policy matches specific traffic from a number of policies. The matching policy is highlighted in the policy list after the lookup. The policy match is based on the `Source_interfaces/Protocol/Source_Address/Destination_Address` that matches the `source-port` and `dst-port` of the protocol.  • Policy match does not work in transparent mode. • Confirm whether the relevant route required for the policy work already exists when executing the policy match,
Search	Enter a search term to find in the policy list.
Export	Export the current view to CSV and JSON formats. Click *Export* and select *CSV* or *JSON* to download the file.
Interface Pair View/By Sequence	Select how to view the policy list: • *Interface Pair View*—Displays the policies in the order that they are checked for matching traffic, grouped by the pairs of Incoming and Outgoing interfaces. For instance, all of the policies referencing traffic from WAN1 to DMZ will be in one section. The policies referencing traffic from DMZ to WAN1 will be in another section. The sections are collapsible so that you only need to look at the sections with policies you are interested in. • *By Sequence*—Displays the policies in the order that they are checked for matching traffic without any grouping. The FortiProxy unit automatically changes the view on the policy list page to *By Sequence* whenever there is a policy containing the *any* interface. If the *Interface Pair View* is grayed out, one or more of the policies is using the *any* interface. See Policy views on page 402 for more details.
New layout/Use classic layout	Select the layout of the policy list. See Policy views on page 402 for more details.
Type	The type of policy, such as Explicit Web, Transparent, or SSH Tunnel. See Policy types on page 387.

Name	The name of the policy.
Incoming Interface	The incoming interface or interfaces.
Outgoing Interface	The outgoing interface or interfaces.
Source	The source is the source address or source user of the initiating traffic.
Destination	The destination address or address range that the policy matches. For more information, see Web cache policy address formats on page 416.
Forwarding Server	The upstream forwarding server that the policy will forward traffic to.
Schedule	The time frame that is applied to the policy. See Schedules on page 516.
Service	The service or services chosen here represent the TCP/IP suite port numbers that will most commonly be used to transport the named protocols or group of protocols. See Services on page 507.
Action	The action to be taken by the policy, such as ACCEPT, DENY, REDIRECT, or ISOLATE.
Security Profiles	All the profiles used by the policy, such as AntiVirus, Web Filter, DLP Profile, ICAP, SSL Inspection, and Content Analysis options. See Security Profiles on page 538.
Log	The logging level of the policy. Options vary depending on the policy type.
Bytes	The number of bytes.
Applications	Application names, application categories, and application groups that use the policy. See Policy matching using applications on page 412 for more details.

URL Category	URL categories that use the policy.
	For HTTPS traffic, you can configure FortiProxy to use only the FQDN category or both the hostname and path to determine a subcategory when matching traffic based on URL categories:
	`config firewall policy`
	`edit <id>`
	`set https-sub-category [enable | disable]`
	`next`
	`end`
	`enable` Enable HTTPS sub-category policy matching.

		The policy attempts deep inspection to determine the subcategory based on both hostname and path. Deep inspection may be required to extract the path.
	`disable` (default)	Disable HTTPS sub-category policy matching. The policy only uses the FQDN to determine the category, even if the traffic is already deeply inspected by `L7 match`.
Active Sessions	The number of active sessions.	
Application Control	What action is taken when an application matches.	
AV	The antivirus profile used by the policy. See Antivirus on page 541.	
Comments	Comments about the policy (up to 1023 characters).	
Destination Address	The destination addresses that the policy matches. The destination address can be used as a traffic filter.	
DNS Filter	The DNS filter profile used by the policy. See DNS Filter on page 588.	
Email Filter	The email filter profile used by the policy.	
Enforce ZTNA	Whether Zero Trust Network Access (ZTNA) is enabled or disabled. See Zero Trust Network Access introduction on page 232.	
File Filter	The file filter profile used by the policy. See File Filter on page 622.	
First Used	When the policy was first used.	
Groups	Which groups the policy matches.	
Hit Count	Number of results found.	
ICAP	The ICAP profile used by the policy. See Create or edit an ICAP profile on page 725.	
ID	The policy identifier. Policies are numbered in the order they are added to the configuration.	
IPS	Which IPS signatures the policy uses.	
Last Used	When the policy was last used.	
Packets	The number of packets.	
Protocol Options	The proxy options profile used by the policy. See Proxy Options on page 171.	
Source Address	The addresses that a policy can receive traffic from. For more information, see Web cache policy address formats on page 416.	
SSL Inspection	The SSL/SSH inspection options used by the policy. See SSL/SSH Inspection on page 625.	

Status	Select to enable a policy or clear to disable a policy. A disabled policy is out of service.
Users	Which users the policy matches.
Video Filter	The video filter profile used by the policy. See Video Filter on page 580.
VPN Tunnel	The VPN tunnel used by the policy. See VPN on page 768.
Web Application Firewall	The web application firewall profile used by the policy. See .
Web Filter	The web filter profile used by the policy. See Web Filter on page 565.
ZTNA Tag	The ZTNA tags used in the ZTNA rule that is used by the policy. See Zero Trust Network Access introduction on page 232.

Change how the policy list is displayed

Policies can be added, edited, copied and pasted, moved, and deleted. Policies can be inserted above or below existing policies and can also be disabled if needed. Note that firewall policy order affects policy matching. See Policy matching on page 407.



Moving a policy in the policy list does not change its ID, which only indicates the order in which the policies were created.

The displayed policies can be filtered by either using the search field in the toolbar or by selecting the filter icon in a column heading. The available filter options vary depending on the type of data that the selected column contains.

To help organize your policies, you can also create sections to group policies together.

Copy and paste a policy

Policies can be copied and pasted to create clones. Right-click on the policy name and then select *Copy* from the pop-up menu. Right-click in the policy name that the new clone policy will be placed next to and select *Paste Above* or *Paste Below* to insert the new policy before or after the selected policy.

Policy rules and authentication rules

Policy rules control what a user or user group can do. Authentication rules define how to authenticate a user. If a policy without a user group matches the type of traffic, authentication is not used because the user group was not specified in the policy.

For example, if a policy rule involving an explicit proxy has the Source field specifying an LDAP-based user group, any other policy rule referencing the explicit proxy is only matched if its Source field also specifies an LDAP-based group.

Create or edit a policy

New policies can be created by selecting *Create New* in the toolbar. By default, the new policy appears at the bottom of the policy list. New policies can also be created above or below an existing policy by right-clicking a policy name and selecting *Insert Empty Policy Above* or *Insert Empty Policy Below* or by copying or cutting an existing policy and then selecting *Paste Above* or *Paste Below* from the right-click menu.

Editing a policy

Policy information can be edited as required in four ways:

- By double-clicking on the sequence number of a policy or the policy name in the policy list
- By selecting a policy and then selecting *Edit* from the toolbar
- By hovering over the policy name and then selecting *Edit* (the pencil icon)
- By right-clicking on the sequence number of the policy or the policy name and selecting *Edit* from the right-click menu

The editing window for regular policies contains the same information as when creating new policies.

Policy types

There are six types of policies:

- *Explicit*—for an explicit web proxy policy.

  Use an explicit web proxy policy if you want to use the explicit web proxy.

  You can use the FortiProxy explicit web proxy to enable explicit proxying of IPv4 and IPv6 HTTP, and HTTPS traffic on one or more FortiProxy interfaces. The explicit web proxy also supports proxying FTP sessions from a web browser and proxy auto-config (PAC) to provide automatic proxy configurations for explicit web proxy users. From the CLI, you can also configure the explicit web proxy to support SOCKS sessions from a web browser.

  The explicit web and FTP proxies can be operating at the same time on the same or on different FortiProxy interfaces.

  The explicit web proxy receives web browser sessions to be proxied at FortiProxy interfaces with the explicit web proxy enabled. The explicit web proxy uses FortiProxy routing to route sessions through the FortiProxy unit to a destination interface. Before a session leaves the exiting interface, the explicit web proxy changes the source addresses of the session packets to the IP address of the exiting interface. You can configure the explicit web proxy to keep the original client IP address.
- *Transparent*—for a transparent firewall policy.

  Use a transparent firewall policy if you want to use the transparent web proxy.

  In addition to the explicit web proxy, the FortiProxy unit supports a transparent web proxy. While it does not have as many features as explicit web proxy, the transparent proxy has the advantage that nothing needs to be done on the user's system to forward supported web traffic over to the proxy. There is no need to reconfigure the browser or publish a PAC file. Everything is transparent

to the end user, hence the name. This makes it easier to incorporate new users into a proxy deployment.

You can use the transparent proxy to apply web authentication to HTTP traffic accepted by a firewall policy.

On networks where authentication based on IP address will not work, you can use the transparent web proxy to apply web authentication that is based on the user's browser and not on their IP address. This authentication method allows you to identify individual users even if multiple users on your network are connecting to the FortiProxy unit from the same IP address.

- *FTP*—for an explicit FTP proxy policy.

  Use an explicit FTP proxy policy if you want to use the explicit FTP proxy.

  You can use the FortiProxy explicit FTP proxy to enable explicit FTP proxying on one or more FortiProxy interfaces. The explicit web and FTP proxies can be operating at the same time on the same or on different FortiProxy interfaces.

  The FTP proxy receives FTP sessions to be proxied at FortiProxy interfaces with the explicit FTP proxy enabled. The FTP proxy uses FortiProxy routing to route sessions through the FortiProxy unit to a destination interface. Before a session leaves the exiting interface, the explicit FTP proxy changes the source addresses of the session packets to the IP address of the exiting interface.
- *SSH Tunnel*—to perform access control for TCP/IP port forwarding traffic that is tunneled through the SSH proxy.
- *SSH Proxy*—to apply a proxy firewall policy with user authentication on SSH sessions.
- *Wanopt*—for a WAN optimization tunnel.

  All optimized traffic passes between the FortiProxy units or between a FortiClient peer and a FortiProxy unit over a WAN optimization tunnel. Traffic in the tunnel can be sent in plain text or encrypted using AES-128bit-CBC SSL.

  Both plain text and the encrypted tunnels use TCP destination port 7810.

  Before a tunnel can be started, the peers must be configured to authenticate with each other. Then, the clientside peer attempts to start a WAN optimization tunnel with the server-side peer. Once the peers authenticate with each other, they bring up the tunnel and WAN optimization communication over the tunnel starts. After a tunnel has been established, multiple WAN optimization sessions can start and stop between peers without restarting the tunnel.

Configuring a policy

To configure an explicit policy:

Type	Select *Explicit*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
Explicit Web Proxy	If you selected *Explicit* for the policy type, select *web-proxy* or search for a policy. To create an explicit proxy policy, see Create or edit an explicit proxy on page 110.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.

Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Select *Create* to create a schedule. For more information, see Schedules on page 516.
Service	Select a service or service group that packets must match to trigger this policy. Select *Create* to create a service list. See Services on page 507. You can add multiple services or service groups.
Application	Select an application from the drop-down list. See Policy matching using applications on page 412 for more details.
Application Category	Select an application category from the drop-down list.
Application Group	Select an application group from the drop-down list. Select *Create* to create an application group.
URL Category	Select a URL category from the drop-down list.
URL Risk	Select risk levels to apply to the policy. See Web Filter Risk Level on page 659.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy. • *REDIRECT*—Redirect traffic matched by the policy to the URL specified in the Redirect URL field. • *ISOLATE*—Isolate traffic matched by the policy to the isolator server selected in the Isolator Server drop-down list.
Web Cache	Enable or disable web caching.
Reverse Cache	Enable to use reverse proxy web caching.

	This option is available only if the *Action* is *Accept* and *Web Cache* is enabled.
Web Cache For HTTPS Traffic	Enable or disable web caching for HTTPS traffic.
Transparent	Enable or disable transparent proxy.
Poolname	If you configured an IP pool, enable this option and then select the IP pool from the drop-down list.
Webproxy Profile	If you configured a web proxy profile, enable this option and then select the web proxy profile from the drop-down list. See Web Proxy Profile on page 145.
Web Proxy Forwarding Server	If you configured a web proxy forwarding server, enable this option and then select a server from the drop-down list. See Create or edit a forwarding server on page 160.
Protocol Options	Select the proxy options profilefor the policy to use. See Proxy Options on page 171.
SSL/SSH Inspection	The SSL/SSH inspection options used by the policy. See SSL/SSH Inspection on page 625.
Display Disclaimer	If you want to display a disclaimer about Internet content that is not controlled by the network access provider, select *By Domain*, *By Policy*, or *By User*. This option is available only if *Action* is set to *ACCEPT*.
Customize Messages	Enable and then edit the existing message or create a message. This option is available only if *Display Disclaimer* is set to *By Domain*, *By Policy*, or *By User*.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
AntiVirus	Enable the antivirus profile and select or create a profile from the drop-down list. See Antivirus on page 541.
Web Filter	Enable the web filter profile and select or create a profile from the drop-down list. See Web Filter on page 565.
Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 599.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 619.
DLP Profile	Enable DLP profiles and select or create a profile from the drop-down list. See Data Loss Prevention on page 660.
Content Analysis	Enable the Content Analysis profile and select or create a profile from the drop-down list. See Create or edit an Image Analysis profile on page 721.

ICAP	Enable the ICAP profile and select or create a profile from the drop-down list. See Create or edit an ICAP profile on page 725.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*, *REDIRECT*, or *ISOLATE*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Log HTTP Transaction	Configure the logging of HTTP transactions: • *Enable*—Enable HTTP transaction log. • *Disable* (default)—Disable HTTP transaction log. When enabled, you can find the HTTP transaction logs under *Log & Report > HTTP Transaction*. See Types of logs on page 1138.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. When traffic matches a pass-through policy, the firewall continues to the next policy. After FortiProxy tries to match all policies, it will set the last matched pass-through policy as the matched policy.
Enable SSH policy check	Enable or disable whether to redirect SSH traffic to the matching proxy policy. See SSH policy matching on page 415.
Extended Log	Enable or disable the recording of extended log for implicit policies. The extended log includes the useragent, referralurl, httpmethod, and statuscode fields.

To configure a transparent policy:

Type	Select *Transparent*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
ZTNA	Enable or disable Zero Trust Network Access (ZTNA). If you enable ZTNA, select whether to use *Full ZTNA* or *IP/MAC filtering*. • *Full ZTNA* allows users to securely access resources through a SSL encrypted access proxy. This simplifies remote access by eliminating the use of VPNs. • *IP/MAC filtering* uses ZTNA tags to provide an additional factor for identification and security posture check to implement role-based zero trust access.
ZTNA Server	Select one or more ZTNA servers to use.
ZTNA Tag	Select one or more ZTNA tags to use.

Incoming Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any*removes the other interfaces.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Click *Create* to create a schedule. For more information, see Schedules on page 516.
Service	Select a service or service group that packets must match to trigger this policy. Click *Create* to create a service list. See Services on page 507. You can add multiple services or service groups.
Application	Select an application from the drop-down list. See Policy matching using applications on page 412 for more details.
Application Category	Select an application category from the drop-down list.
Application Group	Select an application group from the drop-down list. Select *Create* to create an application group.
URL Category	Select a URL category from the drop-down list.
URL Risk	Select risk levels to apply to the policy. See Web Filter Risk Level on page 659.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy.

	• *DENY*—Reject traffic matched by the policy. • *REDIRECT*—Redirect traffic matched by the policy to the URL specified in the Redirect URL field. • *ISOLATE*—Isolate traffic matched by the policy to the isolator server selected in the Isolator Server drop-down list.
Web Cache	Enable or disable web caching.
Reverse Cache	Enable to use reverse proxy web caching. This option is available only if the *Action* is *Accept* and *Web Cache* is enabled.
Web Cache For HTTPS Traffic	Enable or disable web caching for HTTPS traffic.
Status	Enable or disable WAN optimization for traffic accepted by the policy. If *Status* is enabled, select *Active*, *Passive*, or *Manual*.
Profiles	If you enabled *Status* and selected *Active* or *Manual* WAN optimization, select a profile to use for WAN optimization. SeeCreate or edit a WAN optimization profile on page 739.
Passive Option	If you enabled *Status* and selected *Passive* WAN optimization, select *Default*, *Non-transparent*, or *Transparent*.
Peers	If you enabled *Status* and selected *Manual* WAN optimization, select a WAN peer. See Create or edit a WAN optimization peer on page 743.
Scan Outgoing Connections to Botnet Sites	Select *Disable* or *Block* to protect from botnet and command-and-control traffic.
Webproxy Profile	If you configured a web proxy profile, enable this option and then select the web proxy profile from the drop-down list. See Web Proxy Profile on page 145.
Web Proxy Forwarding Server	If you configured a web proxy forwarding server, enable this option and then select a server from the drop-down list. See Create or edit a forwarding server on page 160.
Force Proxy	Enable or disable whether proxying will be forced.
Protocol Options	Select the proxy options profilefor the policy to use. See Proxy Options on page 171.
SSL/SSH Inspection	The SSL/SSH inspection options used by the policy. See SSL/SSH Inspection on page 625.
Display Disclaimer	If you want to display a disclaimer about Internet content that is not controlled by the network access provider, select *By Domain*, *By Policy*, or *By User*. This option is available only if *Action* is set to *ACCEPT*.
Customize Messages	Enable and then edit the existing message or create a message.

	This option is available only if *Display Disclaimer* is set to *By Domain*, *By Policy*, or *By User*.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
AntiVirus	Enable the antivirus profile and select or create a profile from the drop-down list. See Antivirus on page 541.
Web Filter	Enable the web filter profile and select or create a profile from the drop-down list. See Web Filter on page 565.
DNS Filter	Enable the DNS filter profile and select or create a profile from the drop-down list. See DNS Filter on page 588.
Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 599.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 619.
DLP Profile	Enable DLP profiles and select or create a profile from the drop-down list. See Data Loss Prevention on page 660.
Content Analysis	Enable the Content Analysis profile and select or create a profile from the drop-down list. See Create or edit an Image Analysis profile on page 721.
ICAP	Enable the ICAP profile and select or create a profile from the drop-down list. See Create or edit an ICAP profile on page 725.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*, *REDIRECT*, or *ISOLATE*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Log HTTP Transaction	Configure the logging of HTTP transactions: • *Enable*—Enable HTTP transaction log. • *Disable* (default)—Disable HTTP transaction log. When enabled, you can find the HTTP transaction logs under *Log & Report > HTTP Transaction*. See Types of logs on page 1138.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. When traffic matches a pass-through policy, the firewall continues to the next policy. After FortiProxy tries to match all policies, it will set the last matched pass-through policy as the matched policy.

Enable SSH policy check	Enable or disable whether to redirect SSH traffic to the matching proxy policy. See SSH policy matching on page 415.
Extended Log	Enable or disable the recording of extended log for implicit policies. The extended log includes the useragent, referralurl, httpmethod, and statuscode fields.

To configure an FTP policy:

Type	Select *FTP*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Select *Create* to create a schedule. For more information, see Schedules on page 516.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
AntiVirus	Enable the antivirus profile and select or create a profile from the drop-down list. See Antivirus on page 541.

IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 619.
DLP Profile	Enable DLP profiles and select or create a profile from the drop-down list. See Data Loss Prevention on page 660.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. When traffic matches a pass-through policy, the firewall continues to the next policy. After FortiProxy tries to match all policies, it will set the last matched pass-through policy as the matched policy.

To configure an SSH tunnel policy:

Type	Select *SSH Tunnel*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
Incoming Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any*removes the other interfaces.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.

Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Click *Create* to create a schedule. For more information, see Schedules on page 516.
Service	Select a service or service group that packets must match to trigger this policy. Click *Create* to create a service list. See Services on page 507. You can add multiple services or service groups.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 599.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 619.
Logging Options	This section is available only if *Action* is set to *ACCEPT*.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. When traffic matches a pass-through policy, the firewall continues to the next policy. After FortiProxy tries to match all policies, it will set the last matched pass-through policy as the matched policy.

To configure an SSH proxy policy:

Type	Select *SSH Proxy*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.

Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Click *Create* to create a schedule. For more information, see Schedules on page 516.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 599.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 619.
Logging Options	This section is available only if *Action* is set to *ACCEPT*.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. When traffic matches a pass-through policy, the firewall continues to the next policy. After FortiProxy tries to match all policies, it will set the last matched pass-through policy as the matched policy.

To configure a WAN-optimization tunnel policy:

Type	Select *Wanopt*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Click *Create* to create a schedule. For more information, see Schedules on page 516.
Service	Select a service or service group that packets must match to trigger this policy. Click *Create* to create a service list. See Services on page 507. You can add multiple services or service groups.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy.
Web Cache	Enable or disable web caching.
Reverse Cache	Enable to use reverse proxy web caching. This option is available only if the *Action* is *Accept* and *Web Cache* is enabled.
Web Cache For HTTPS Traffic	Enable or disable web caching for HTTPS traffic.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.

AntiVirus	Enable the antivirus profile and select or create a profile from the drop-down list. See Antivirus on page 541.
Web Filter	Enable the web filter profile and select or create a profile from the drop-down list. See Web Filter on page 565.
Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 599.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 619.
DLP Profile	Enable DLP profiles and select or create a profile from the drop-down list. See Data Loss Prevention on page 660.
Content Analysis	Enable the Content Analysis profile and select or create a profile from the drop-down list. See Create or edit an Image Analysis profile on page 721.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. When traffic matches a pass-through policy, the firewall continues to the next policy. After FortiProxy tries to match all policies, it will set the last matched pass-through policy as the matched policy.

Web cache policy address formats

A source or destination address can contain one or more network addresses. Network addresses can be represented by an IP address with a netmask or an IP address range.

When representing hosts by an IP address with a netmask, the IP address can represent one or more hosts. For example, a source or destination address can be any of the following:

- a single computer, for example, `192.45.46.45`
- a subnetwork, for example, `192.168.1.*` for a class C subnet
- `0.0.0.0` matches any IP address

The netmask corresponds to the subnet class of the address being added and can be represented in either dotted decimal or CIDR format. The FortiProxy unit automatically converts CIDR-formatted netmasks to dotted decimal format. Example formats:

- netmask for a single computer: `255.255.255.255` or `/32`
- netmask for a class A subnet: `255.0.0.0` or `/8`
- netmask for a class B subnet: `255.255.0.0` or `/16`
- netmask for a class C subnet: `255.255.255.0` or `/24`

- netmask including all IP addresses: `0.0.0.0`

Valid IP address and netmask formats include:

- x.x.x.x/x.x.x.x, such as `192.168.1.0/255.255.255.0`
- x.x.x.x/x, such as `192.168.1.0/24`



An IP address `0.0.0.0` with the netmask `255.255.255.255` is not a valid source or destination address.

When representing hosts by an IP address range, the range indicates hosts with continuous IP addresses in a subnet, such as `192.168.1.[2-10]`, or `192.168.1.*`, to indicate the complete range of hosts on that subnet. You can also indicate the complete range of hosts on a subnet by entering `192.168.1.[0-255]` or `192.168.1.0-192.168.1.255`. Valid IP range formats include:

- x.x.x.x-x.x.x.x, for example, `192.168.110.100-192.168.110.120`
- x.x.x.[x-x], for example, `192.168.110.[100-120]`
- x.x.x.*, for a complete subnet, for example: `192.168.110.*`
- x.x.x.[0-255] for a complete subnet, such as `192.168.110.[0-255]`
- x.x.x.0 -x.x.x.255 for a complete subnet, such as `192.168.110.0 - 192.168.110.255`



You cannot use square brackets [ ] or asterisks * when adding addresses to the CLI. Instead you must enter the start and end addresses of the subnet range separated by a dash -. For example, `192.168.20.0-192.168.20.255` for a complete subnet and `192.168.10.10-192.168.10.100` for a range of addresses.

Device ownership

When device ownership is enabled, ownership enforcement is done at policy level. It is disabled by default.

To enable device ownership:

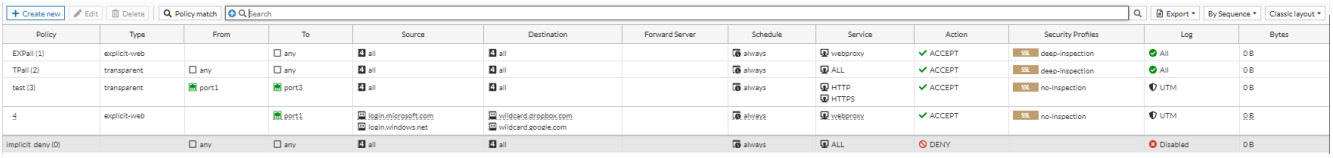
```
config firewall policy
    edit 2
        set ztna-status enable
        set ztna-ems-tag "FCTEMS_ALL_FORTICLOUD_SERVERS"
        set device-ownership enable
        ...
    next
end
```

Policy views

In *Policy & Objects* policy list pages, there are three policy views: *Interface Pair View*, *Sequence Grouping View*, and *By Sequence*. For large policy tables (thousands of policies), the *By Sequence* view will load the fastest.

Interface Pair View displays the policies in the order that they are checked for matching traffic, grouped by the pairs of incoming and outgoing interfaces in collapsible sections. The *Interface Pair View* can be used when a policy is configured with multiple interfaces. Right-click on any pair name and click *Expand All* or *Collapse All* to expand or collapse all of the pairs.

By Sequence displays policies in the order that they are checked for matching traffic without any grouping.



In *By Sequence* or *Sequence Grouping View* view, policies can be moved by their policy ID before or after another specified policy ID.

To move a policy by policy ID:

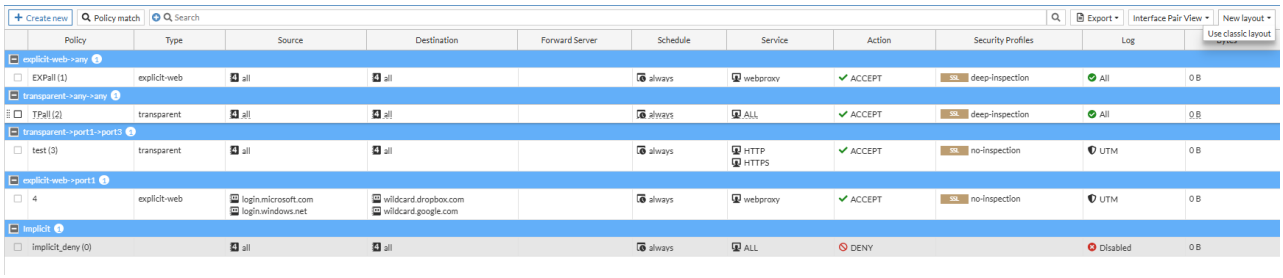
1. Go to *Policy & Objects* > *Policy*.
   Make sure *By Sequence* or *Sequence Grouping View* is selected at the top-right corner.
2. Right-click the policy you want to move and select *Move by ID*.
   The *Move by ID* pane is displayed.
3. Define the new location of the policy:
   a. Select whether the policy should be moved *Above* or *Below* the policy ID you will define in the next step.
   b. In the *Destination policy ID* field, enter the ID of the destination policy or select it from the dropdown menu.
4. If you do not want to automatically view the new location of the policy, disable *Jump to policy after move*. This feature is enabled by default.
5. Click *OK*.
   The policy will be moved to the new location.

New layout for policies

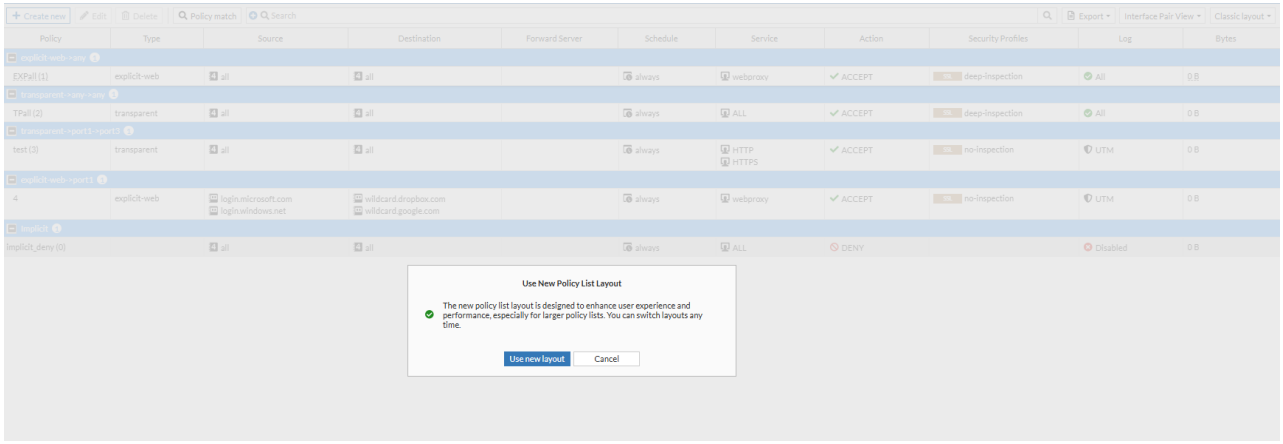
A new layout is available for the policy list with the option to alternate between the new layout and the old layout. To switch between the *Classic layout* and *New layout*, select the style from the dropdown menu.

To change from the classic layout to the new layout:

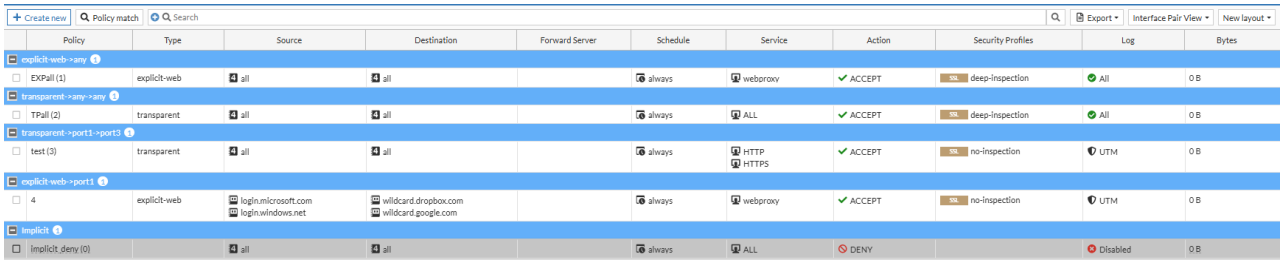
1. Go to *Policy & Objects* > *Policy*.
2. Select the *Classic layout* dropdown menu.



3. Select *Use new layout*. A confirmation message is displayed.

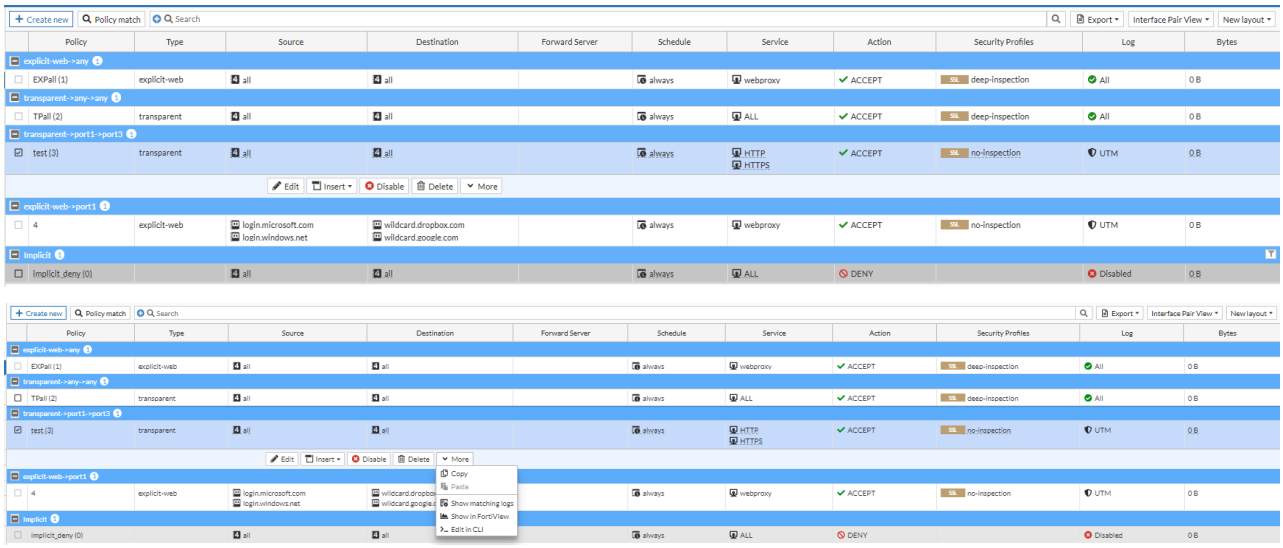


4. Click *Use new layout*. The new layout is displayed.

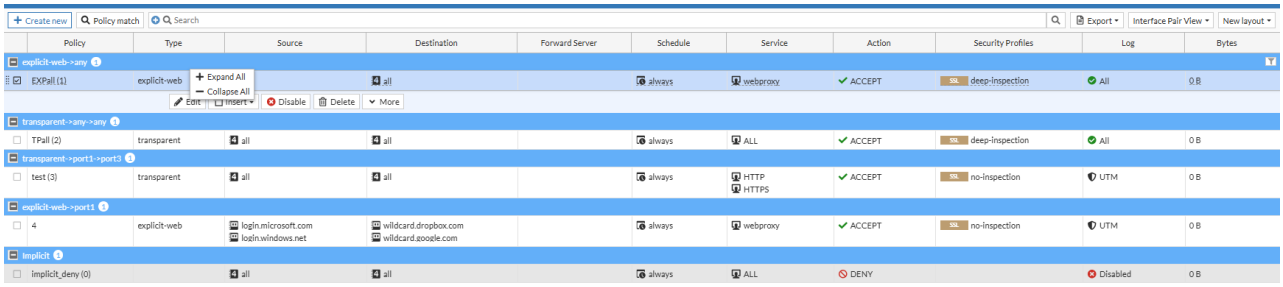


The *New layout* includes several features to enhance user experience when using the *Policy & Objects* > *Policy* page:

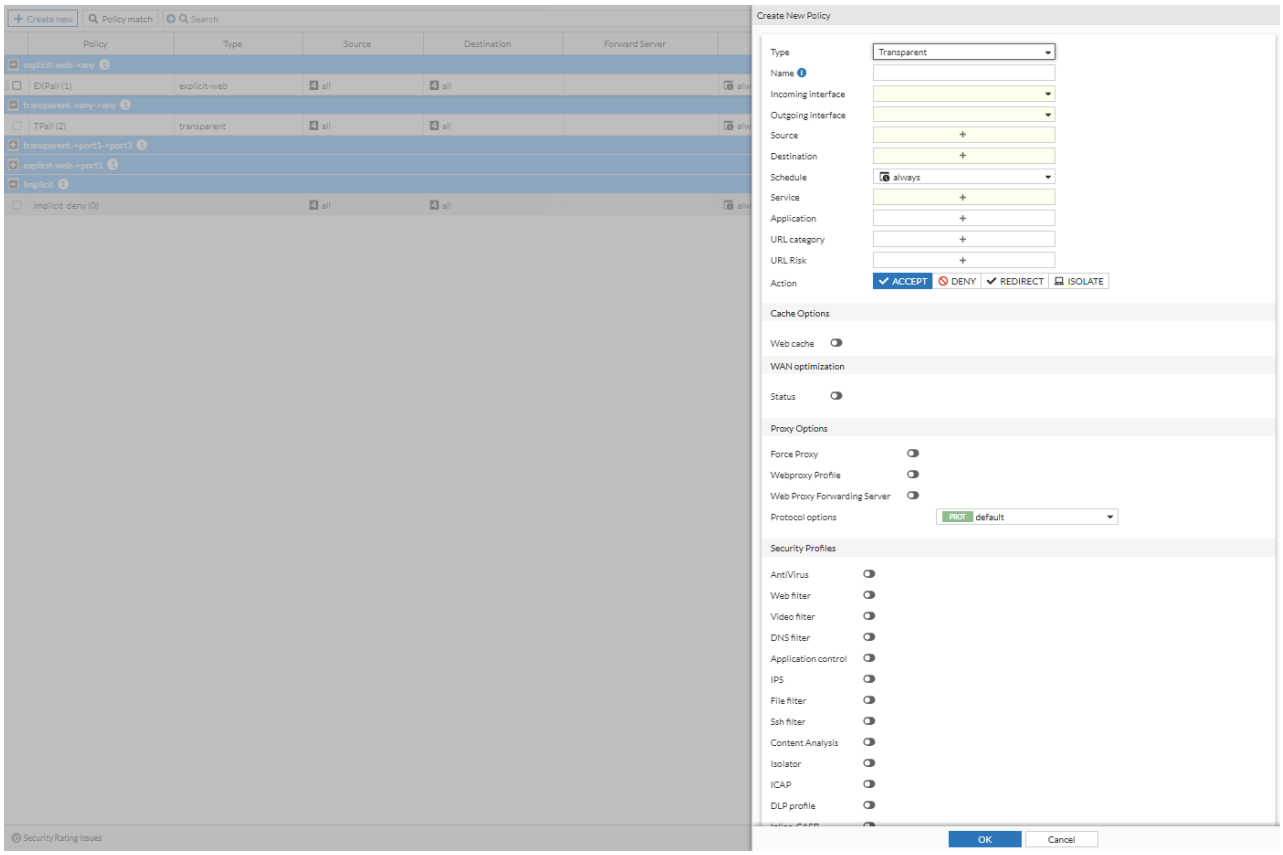
- The create, edit, and delete buttons are identified through icons instead of words. Selecting a policy also displays an inline menu with options to edit, delete, insert policies, and the option to show more options.



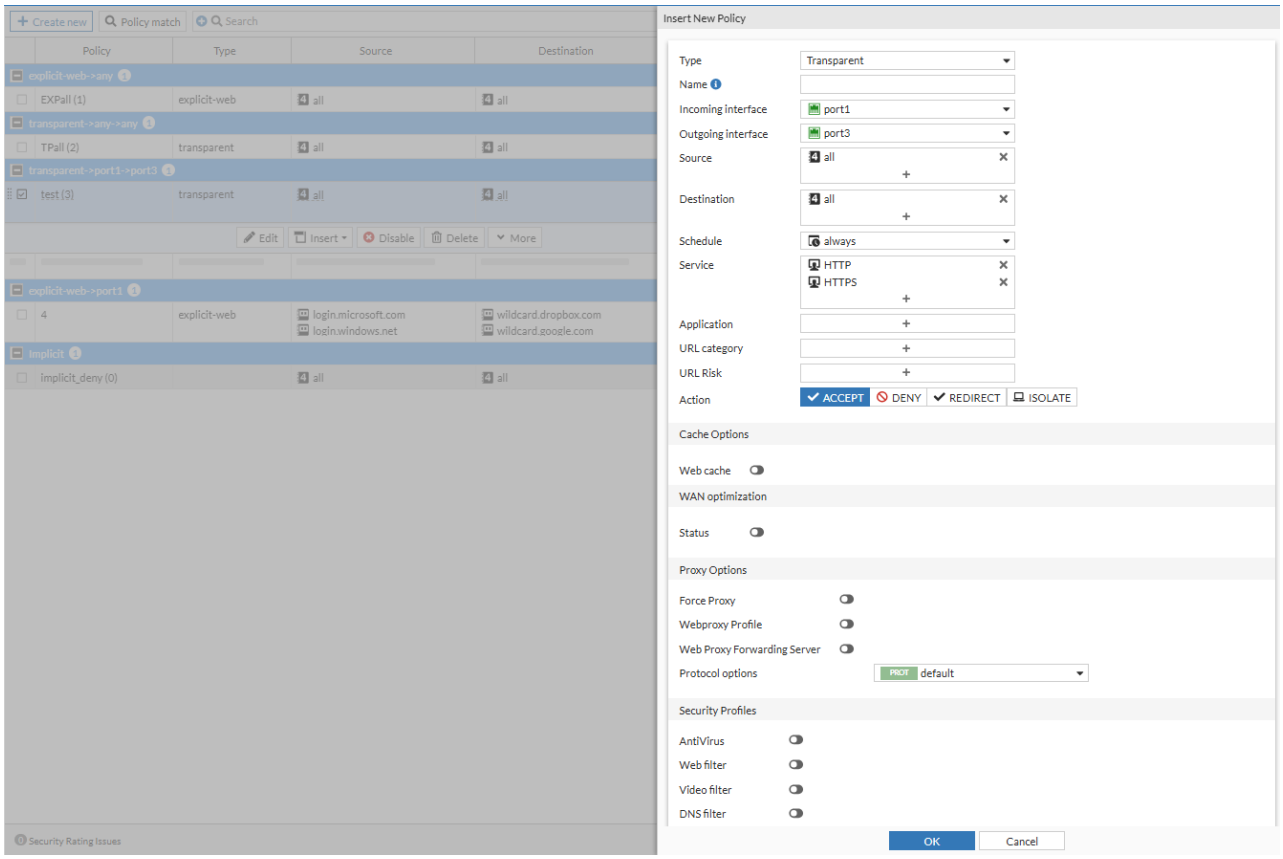
- Right-click in *Interface Pair View* to *Expand All* or *Collapse All* sections.



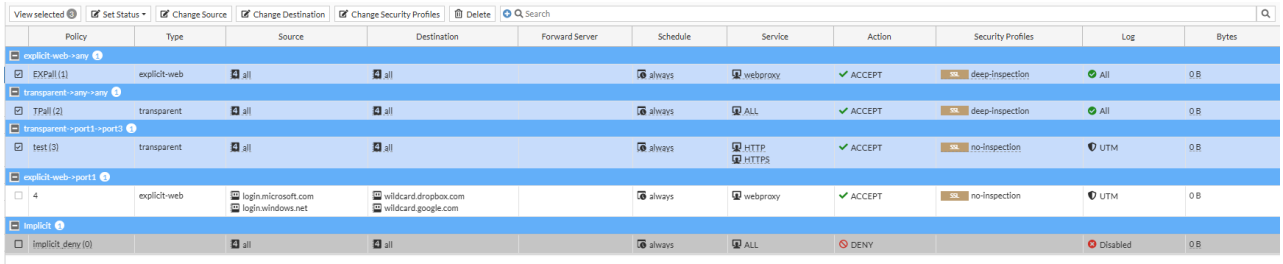
- A pane is used to create, edit, and insert policies instead of a separate page.



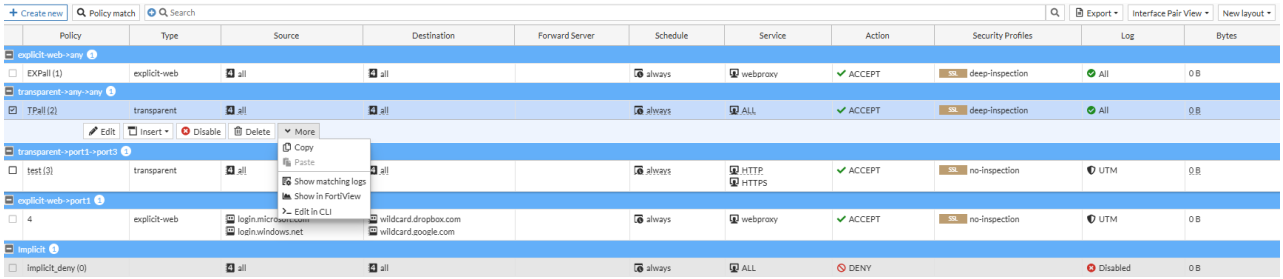
- When a policy is inserted in *Interface Pair View*, the *Incoming Interface* and *Destination Interface* fields will be automatically filled. You can confirm the location of the new policy in the right-side gutter before clicking *OK* to insert the policy.

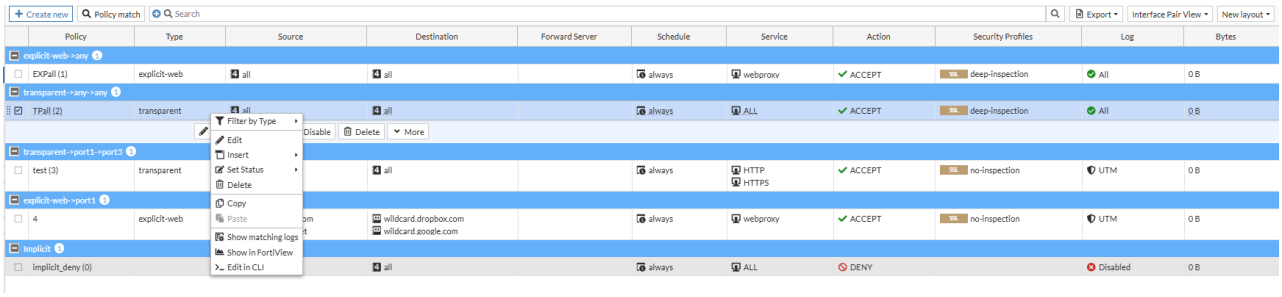


- Multiple policies can be selected at once to efficiently work with a large number of policies.

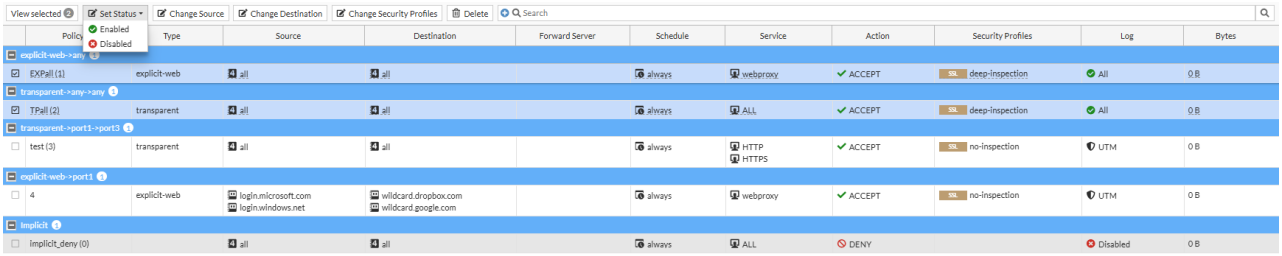


- When a single policy is selected, an inline menu opens below the row. The *More* dropdown menu includes the same expanded list of options that are available in the right-click menu.

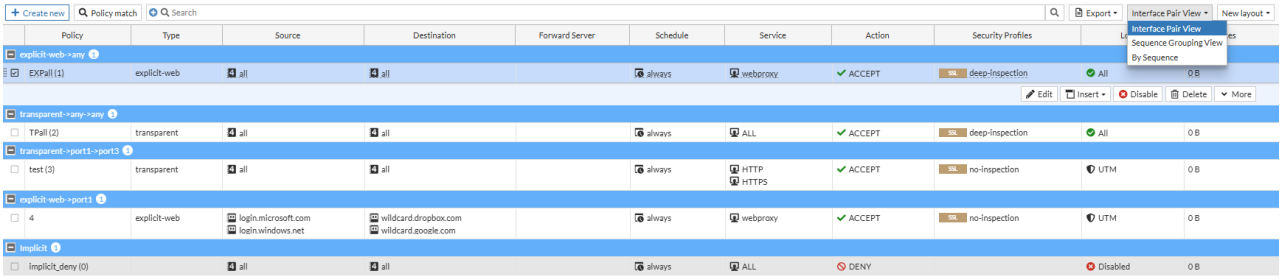




- When multiple policies are selected, the top menu bar changes to show buttons that are applicable to the multiple selections.



- The view selector drop-down includes three options: *Interface Pair View*, *Sequence Grouping View*, and *By Sequence*. For large policy tables (thousands of policies), a tooltip will specify that the *By Sequence* view will load the fastest.



Policy matching

In FortiProxy, traffic is matched against the list of configured policies sequentially from top down by comparing the policy with the session source address, destination address, and the destination port. If a policy successfully matches the traffic, the policy is applied. If not, FortiProxy continues to the next policy in the list until a match is found, in which case all subsequent policies will be ignored. If no policy match is found, the traffic is handled by the implicit policy (policy ID 0), which always denies all traffic.

By default, the implicit policy log is disabled. You can enable it using the following command:

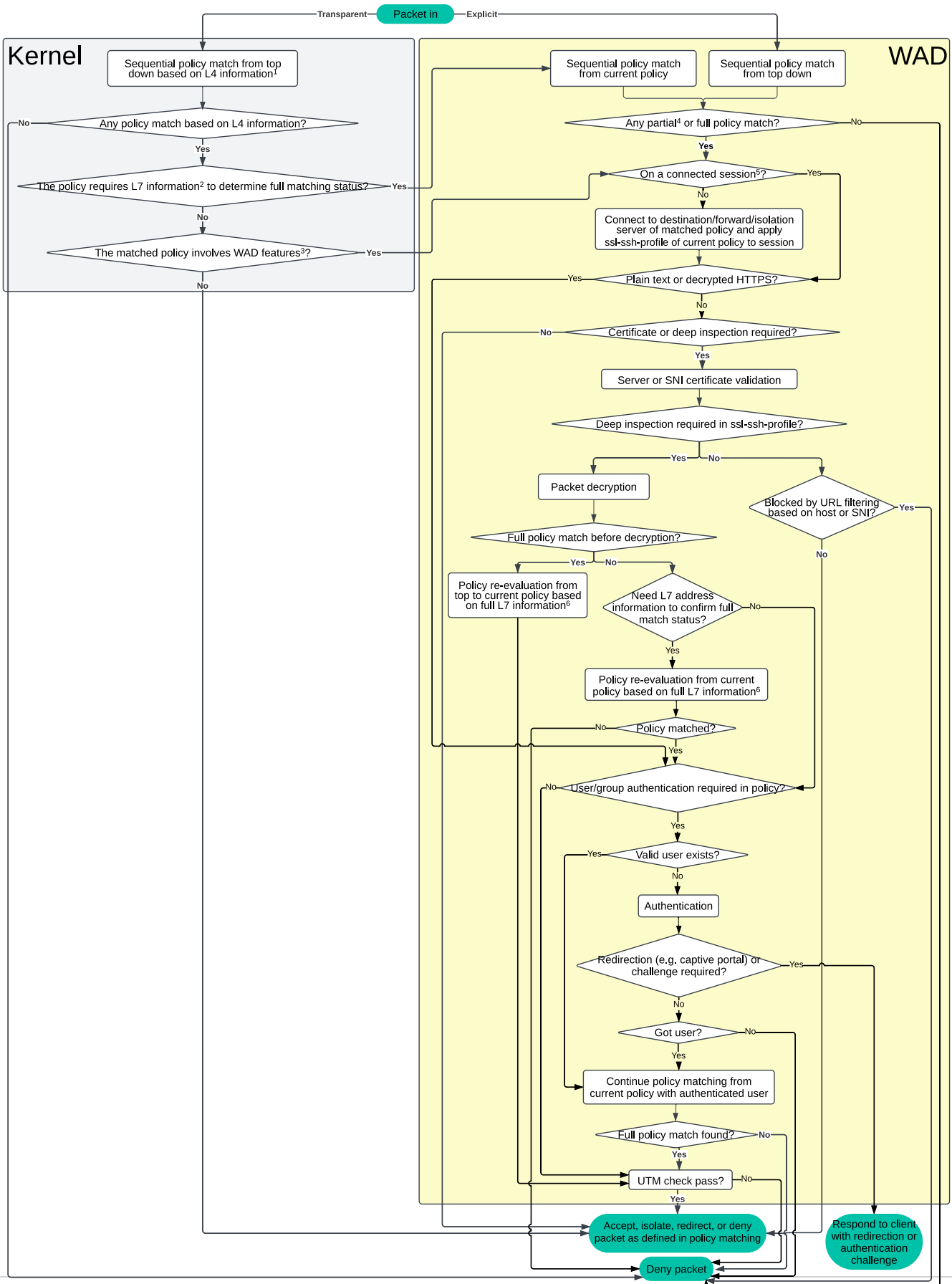
```
config log setting
    set fwpolicy-implicit-log enable
end
```

As a general rule, order the policy list from most specific to most general to prevent policies that match a wide range of traffic from superseding and effectively masking policies that match exceptions.

Transparent and explicit policy matching

- Transparent proxy traffic is initially handled by the kernel, where policies are evaluated sequentially from top down based on Layer 4 (L4) information. A packet may be redirected to the WAD engine for further processing if the matched policy (based on L4 information) requires Layer 7 (L7) information to further determine the full policy matching status or if the match policy involves WAD features, such as UTM scanning.
- Explicit proxy traffic is directly handled by the WAD engine, which performs sequential policy matching from top down.

The following diagram illustrates the policy matching process for transparent policy and explicit policy:


Transparent
Packet in
Explicit
Kernel
WAD
Sequential policy match from top down based on L4 information1
Any policy match based on L4 information?
No
Yes
The policy requires L7 information2 to determine full matching status?
Yes
No
The matched policy involves WAD features3?
Yes
No
Sequential policy match from current policy
Sequential policy match from top down
Any partial4 or full policy match?
No
Yes
On a connected session5?
Yes
No
Connect to destination/forward/isolation server of matched policy and apply ssl-ssh-profile of current policy to session
Plain text or decrypted HTTPS?
Yes
No
Certificate or deep inspection required?
No
Yes
Server or SNI certificate validation
Deep inspection required in ssl-ssh-profile?
Yes
No
Packet decryption
Blocked by URL filtering based on host or SNI?
Yes
No
Full policy match before decryption?
Yes
No
Policy re-evaluation from top to current policy based on full L7 information6
Need L7 address information to confirm full match status?
No
Yes
Policy re-evaluation from current policy based on full L7 information6
Policy matched?
No
Yes
User/group authentication required in policy?
No
Yes
Valid user exists?
Yes
No
Authentication
Redirection (e.g. captive portal) or challenge required?
Yes
No
Got user?
No
Yes
Continue policy matching from current policy with authenticated user
Full policy match found?
No
Yes
UTM check pass?
No
Yes
Accept, isolate, redirect, or deny packet as defined in policy matching
Respond to client with redirection or authentication challenge
Deny packet

1. L4 information includes interface, IP addresses, protocols, and ports.
2. L7 information includes proxy-address, inline application, authentication, URL category, etc.
3. WAD features include UTM, forward server, isolated action, deep inspection, certificate inspection, log-http-transaction, webproxy-profile, webcache, etc.
4. Partial match is an intermediate state for HTTPS packets when a policy matches a proxy-address host (SNI) but requires deep inspection to extract information from the HTTP headers to further determine the policy matching status or needs user information to match users or groups in the policy.
5. Packets on a connected session always reuse the existing connection to the server without user or group re-authentication.
6. For HTTPS packets that require deep inspection, the final matched policy from re-evaluation from top or current policy (based on full L7 information) might be different from the initial fully matched policy (based on limited information before decryption).

For more information about the overall packet flow, see Packet flow ingress and egress.

HTTPS traffic with deep inspection

For HTTPS traffic, if FortiProxy encounters a policy that matches a proxy-address host (SNI) but requires deep inspection to extract information from the HTTP headers to further determine the policy matching status, the policy is considered a partial match with an intermediate state if all of the following conditions are met:

- The traffic is HTTPS and has not yet undergone deep inspection.
- The policy involves proxy-address matching that requires extracting information from the HTTP headers.

  Exceptions:
  - Proxy-address host match is not required for `saas`-type `proxy-address`.
  - Extracting information from the HTTP headers is not required in the following cases:
    - Hostname that corresponds to no sub-category.
    - The proxy type is `method` or `ua` in explicit mode.
- The traffic does not match any entries in the policy's SSL exemption list (firewall.ssl-sshprofile.ssl-exempt).

In partial match state, FortiProxy performs deep inspection on the traffic using the established SSL connection based on the settings (forward server, isolation server, or destination server) of the partial match policy and re-evaluates whether it is a full match. Based on the evaluation result, the partial match state transitions to either a successful match or a failed match.

In case of failed match, FortiProxy resumes the full policy matching process starting from the next policy in the list until a full policy match is found. If the full match policy requires deep inspection, FortiProxy attempts the policy match again from top down in the policy list as the decrypted content may change the final policy matching result.



- Traffic that goes through partial match state is considered deeply inspected even if subsequent policies do not require deep inspection as the packet has already been decrypted and inspected.
- Since SSL decryption occurs at the SSL handshake stage, once the decryption process has started, it cannot be reversed within the same session.
- Regardless of the full policy matching result, the forward server, isolator action, and SSL SSH profile settings of all subsequent policies will be overridden by those of the partial match policy as the SSL tunnel is already established at this stage and subsequent policies modifying the forward server or isolator settings will not take effect for this session.

  Exceptions:
  - The policy's `dstaddr` contains only `category`-type `proxy-address` entries.
  - The `category` in `dstaddr` does not match the category of the traffic.

To enable/disable HTTPS sub-category policy matching when the policy uses URL category to match traffic:

```
config firewall policy
   edit <id>
      set https-sub-category [enable | disable]
   next
end
```

`enable`	Enable HTTPS sub-category policy matching. The policy attempts deep inspection to determine the subcategory based on both hostname and path.
`disable` (default)	Disable HTTPS sub-category policy matching. The policy only uses the FQDN to determine the category, even if the traffic is already deeply inspected by partial match.

To enable/disable logging for sessions in the partial match state in traffic log:

```
config web-proxy global
   set log-policy-pending [enable | disable]
end
```

To view debug logs for partial match and deep inspection:

1. Enable full debug logging: `diag wad debug enable all`.
2. Run `wad_http_req_policy_set` to verify when traffic fully matches (or partial match triggers) a policy and whether deep inspection is enabled. See example log below:

   ```
   wad_http_req_policy_set
   10430 match policy-id=3(pol_ctx:xhcf|Ad|7?oO|=7) vd=0(ses_ctx:x|P)
   wad_http_req_policy_set
   :10430 match policy-id=4(pol_ctx:xhf|Ad|7|=d) vd=0(ses_ctx:cx|Phx|)
   ```

   The `policy-id` after `match policy-id=` indicates the policy matched while the matching states at the end of `pol_ctx` show `"=7"` for a partial match triggered, requiring deep inspection, and `"=d"` for

a full match without deep inspection.

Policy matching using applications

Starting from 7.4.2, you can use applications as filters in policies without requiring web filter or application control profiles. If the traffic is allowed by the policy, packets are sent to the IPS engine for application match, and then, if enabled, UTM inspection (antivirus, IPS, DLP, and email filter) is performed.

Compared with the previous mechanism of filtering applications using ports and source/destination IPs in a policy, the new application filter automatically determines the application's identity, regardless of the dynamic port or IP change, which improves your security posture.



Inline IPS is required to use this feature. To verify that inline IPS is enabled, run the `dia wad deb ips-db status` command.

To configure an SSL Inspection & Authentication policy for Facebook and Gmail access in the CLI:

```
config firewall policy
   edit 2
      set uuid 08c7b0c6-bfc2-51ee-17b8-078effe835eb
      set srcintf "port2"
      set dstintf "port1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set utm-status enable
      set logtraffic all
      set logtraffic-start enable
      set log-http-transaction all
      set extended-log enable
      set application 15832
      set ssl-ssh-profile "deep-inspection"
      set av-profile "g-default"
      set webfilter-profile "monitor-all"
      set application-list "AP"
   next
 end
```

Logs

Traffic logs:

```
d1: date=2024-02-29 time=13:42:15 eventtime=1709242935321868122 tz="-0800" logid="0000000015"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.100.1.55 srcport=40338
srcintf="port2" srcintfrole="undefined" dstip=157.240.241.35 dstport=443 dstintf="port1"
dstintfrole="undefined" srccountry="Reserved" dstcountry="United States" sessionid=1695777498
proto=6 action="start" policyid=2 policytype="policy" poluuid="08c7b0c6-bfc2-51ee-17b8-
```

```
078effe835eb" service="HTTPS" trandisp="noop" url="https://www.facebook.com/" agent="curl/7.81.0"
appid=15832 app="Facebook" appcat="Social.Media" apprisk="medium" duration=0 sentbyte=0 rcvdbyte=0
sentpkt=0 rcvdpkt=0
```

Web filter log:

```
1: date=2024-02-29 time=13:42:15 eventtime=1709242935322088194 tz="-0800" logid="0317013312"
type="utm" subtype="webfilter" eventtype="ftgd_allow" level="notice" vd="root" policyid=2
poluuid="08c7b0c6-bfc2-51ee-17b8-078effe835eb" policytype="policy" sessionid=1695777498
transid=117440514 srcip=10.100.1.55 srcport=40338 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="6a168214-f8e3-51ec-9294-1673e0a41d9e" dstip=157.240.241.35
dstport=443 dstcountry="United States" dstintf="port1" dstintfrole="undefined" proto=6
httpmethod="GET" service="HTTPS" hostname="www.facebook.com" agent="curl/7.81.0" profile="monitor-
all" action="passthrough" reqtype="direct" url="https://www.facebook.com/" sentbyte=774
rcvdbyte=3243 direction="outgoing" msg="URL belongs to an allowed category in policy"
ratemethod="domain" cat=37 catdesc="Social Networking"
```

Application control log:

```
1: date=2024-02-29 time=13:42:15 eventtime=1709242935609343887 tz="-0800" logid="1059028704"
type="utm" subtype="app-ctrl" eventtype="signature" level="information" vd="root" appid=15832
srcip=10.100.1.55 srccountry="Reserved" dstip=157.240.241.35 dstcountry="United States"
srcport=40338 dstport=443 srcintf="port2" srcintfrole="undefined" dstintf="port1"
dstintfrole="undefined" proto=6 service="HTTPS" direction="incoming" policyid=2 poluuid="08c7b0c6-
bfc2-51ee-17b8-078effe835eb" policytype="policy" sessionid=1695777498 applist="AP" action="pass"
appcat="Social.Media" app="Facebook" hostname="www.facebook.com" incidentserialno=1278682 url="/"
agent="curl/7.81.0" httpmethod="GET" msg="Social.Media: Facebook" apprisk="medium"
```

Setting application default port as a service port

The `default-app-port-as-service` option can be used to set the application default port as a service port. This allows applications to match the policy and traffic from the application that does not match the default port is be blocked immediately the first time that traffic hits the firewall. When this option is enabled, the policy aggregates the ports used by the applications in the policy and performs a pre-match on the traffic.

```
config system settings
    set default-app-port-as-service {enable | disable}
end
```



This option can be configured on a per-VDOM level.

This setting is enabled by default on new installations. When upgrading, the setting is disabled to retain the previous behavior.

Example

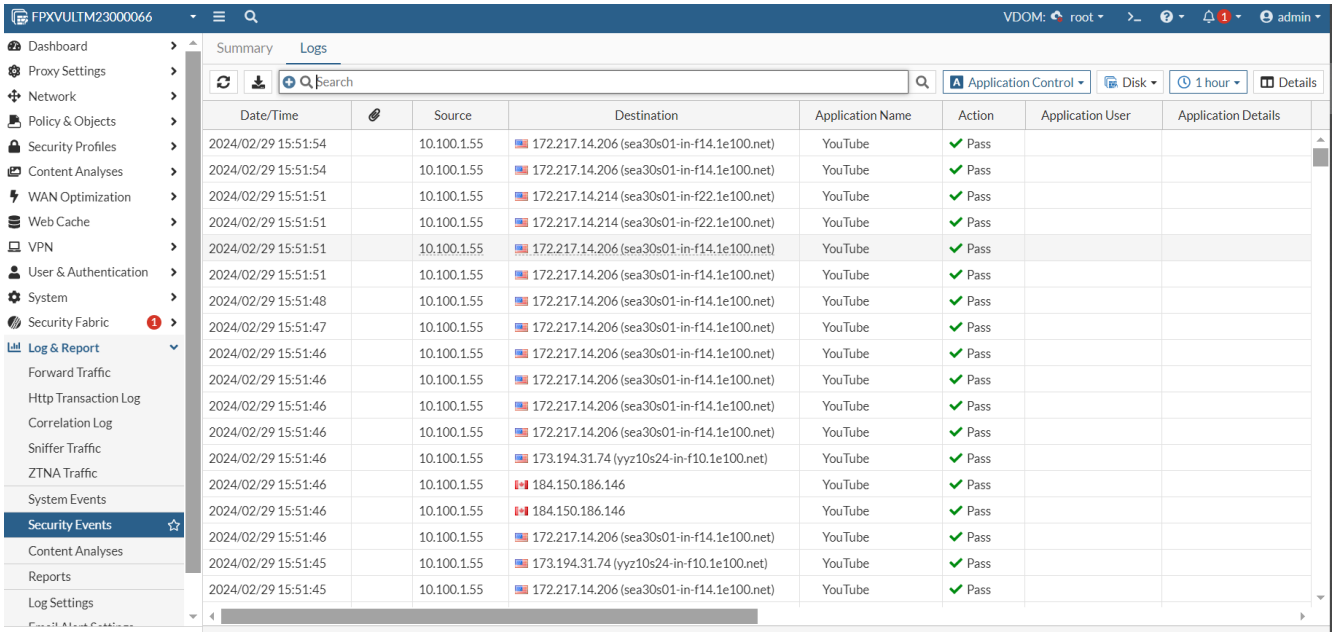
In the following example, the policy is configured to match traffic from the YouTube application:

```
config firewall policy
```

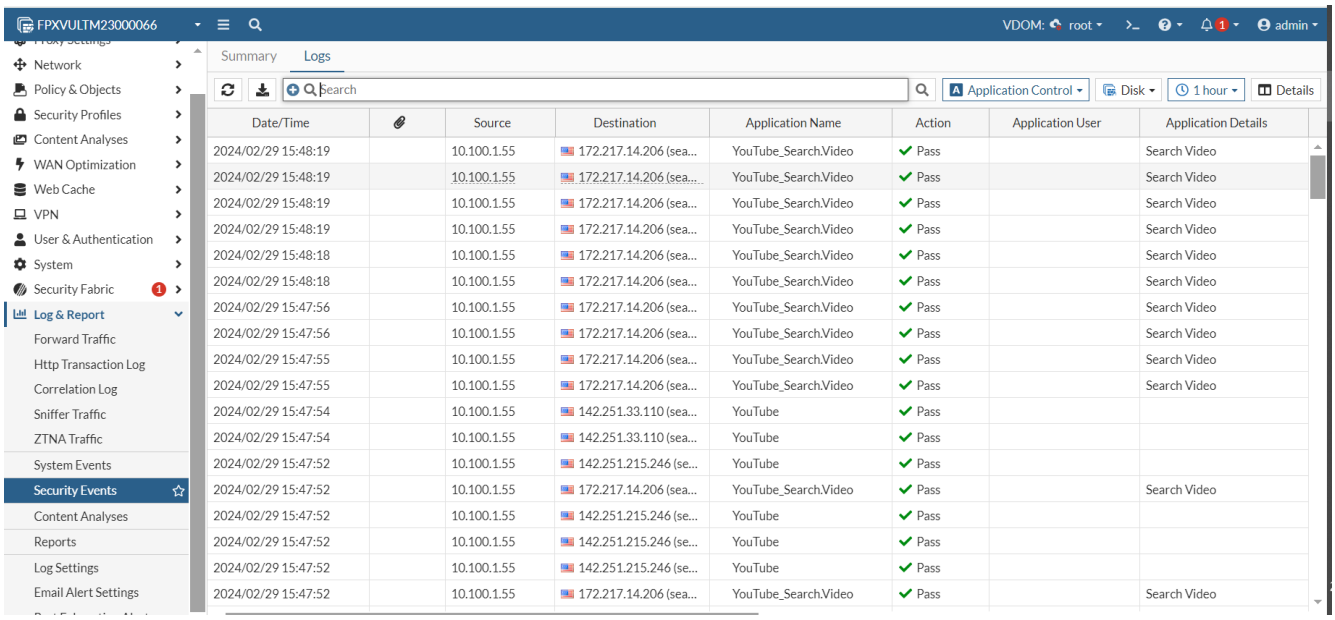
```
  edit 2
     set uuid 08c7b0c6-bfc2-51ee-17b8-078effe835eb
     set srcintf "port2"
     set dstintf "port1"
     set srcaddr "all"
     set dstaddr "all"
     set action accept
     set schedule "always"
     set service "ALL"
     set utm-status enable
     set logtraffic all
     set logtraffic-start enable
     set log-http-transaction all
     set extended-log enable
     set application 31077
     set ssl-ssh-profile "deep-inspection"
     set av-profile "g-default"
     set webfilter-profile "monitor-all"
     set application-list "AP"
  next
end
```

When traffic logging is set to *UTM* or *All*, then application control logs will be generated. To verify application logging, play some YouTube videos on a client system and then go to *Log & Report* > *Security Events* to view the *Application Control* logs.

When the `default-app-port-as-service` option is enabled, the traffic which does not match the default port is blocked immediately and only traffic log is generated. There are only logs for *YouTube*, as verified from the *Application Name* column:



When the `default-app-port-as-service` option is disabled, the traffic which does not match the default port is not be blocked and both application and traffic logs are generated. There are logs for *YouTube* and *YouTube_search.video*, as verified from the *Application Name* column:



SSH policy matching

SSH policy check is disabled by default, and can be enabled in transparent and explicit-web policies. When it is enabled, SSH policy matching will only match the SSH policy.

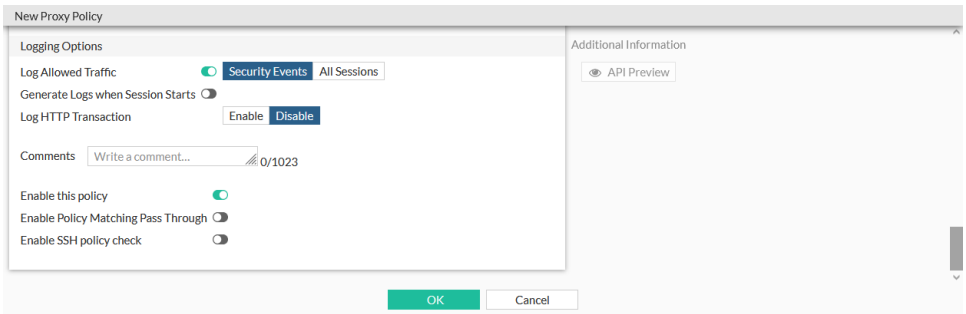
The *SSH Policy Redirect* (`ssh-policy-redirect`) command is no longer available.

To configure SSH policy check in the CLI:

```
config firewall policy
    edit <policy>
        set ssh-policy-check {disable | enable}
    next
end
```

To configure SSH policy check in the CLI:

1. Go to *Policy & Objects* > *Policy*.
2. Edit a transparent or explicit policy, or create a new policy and set *Type* to *Transparent* or *Explicit*.
3. Enable or disable *Enable SSH policy check*.



4. Click *OK*.

Web cache policy address formats

A source or destination address can contain one or more network addresses. Network addresses can be represented by an IP address with a netmask or an IP address range.

When representing hosts by an IP address with a netmask, the IP address can represent one or more hosts. For example, a source or destination address can be any of the following:

- a single computer, for example, `192.45.46.45`
- a subnetwork, for example, `192.168.1.*` for a class C subnet
- `0.0.0.0` matches any IP address

The netmask corresponds to the subnet class of the address being added and can be represented in either dotted decimal or CIDR format. The FortiProxy unit automatically converts CIDR-formatted netmasks to dotted decimal format. Example formats:

- netmask for a single computer: `255.255.255.255` or `/32`
- netmask for a class A subnet: `255.0.0.0` or `/8`
- netmask for a class B subnet: `255.255.0.0` or `/16`
- netmask for a class C subnet: `255.255.255.0` or `/24`
- netmask including all IP addresses: `0.0.0.0`

Valid IP address and netmask formats include:

- x.x.x.x/x.x.x.x, such as `192.168.1.0/255.255.255.0`
- x.x.x.x/x, such as `192.168.1.0/24`



An IP address `0.0.0.0` with the netmask `255.255.255.255` is not a valid source or destination address.

When representing hosts by an IP address range, the range indicates hosts with continuous IP addresses in a subnet, such as `192.168.1.[2-10]`, or `192.168.1.*`, to indicate the complete range of hosts on that subnet. You can also indicate the complete range of hosts on a subnet by entering `192.168.1.[0-255]` or `192.168.1.0-192.168.1.255`. Valid IP range formats include:

- x.x.x.x-x.x.x.x, for example, `192.168.110.100-192.168.110.120`
- x.x.x.[x-x], for example, `192.168.110.[100-120]`
- x.x.x.*, for a complete subnet, for example: `192.168.110.*`
- x.x.x.[0-255] for a complete subnet, such as `192.168.110.[0-255]`
- x.x.x.0 -x.x.x.255 for a complete subnet, such as `192.168.110.0 - 192.168.110.255`



You cannot use square brackets [ ] or asterisks * when adding addresses to the CLI. Instead you must enter the start and end addresses of the subnet range separated by a dash -. For example, `192.168.20.0-192.168.20.255` for a complete subnet and `192.168.10.10-192.168.10.100` for a range of addresses.

HTTP2 connection coalescing and concurrent multiplexing for virtual server load balancing

HTTP2 connection coalescing and concurrent multiplexing allows multiple HTTP2 requests to share the same TLS connection when the destination IP is the same.

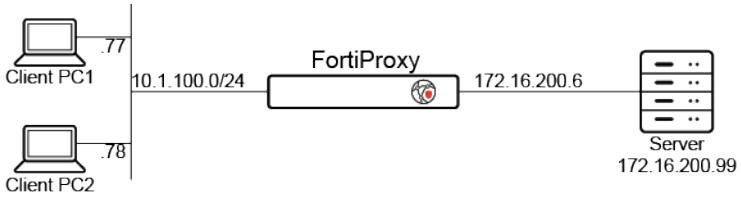
To configure the load balanced virtual server:

```
config firewall vip
    edit <name>
        set type server-load-balance
        set server-type {http | https}
        set http-multiplex {enable | disable}
        set http-multiplex-ttl <integer>
        set http-multiplex-max-request <integer>
        set http-supported-max-version {http1 | http2}
    next
end
```

`http-multiplex {enable | disable}`	Enable/disable HTTP multiplexing.
`http-multiplex-ttl <integer>`	Set the time-to-live for idle connections to servers (in seconds, 0 - 2147483647, default = 15).
`http-multiplex-max-request <integer>`	Set the maximum number of requests that the multiplex server can handle before disconnecting (0 - 2147483647, default = 0).
`http-supported-max-version {http1 | http2}`	Set the maximum supported HTTP version: • http1: support HTTP 1.1 and HTTP1. • http2: support HTTP2, HTTP 1.1, and HTTP1 (default).

Example

In this example, multiple clients submit requests in HTTP2. The requests hit the VIP address, and then FortiProxy opens a session between itself (172.16.200.6) and the server (172.16.200.99). The coalescing occurs in this session as the multiple streams share the same TLS session to connect to the same destination server.



To configure connection coalescing and concurrent multiplexing with virtual server load balancing:

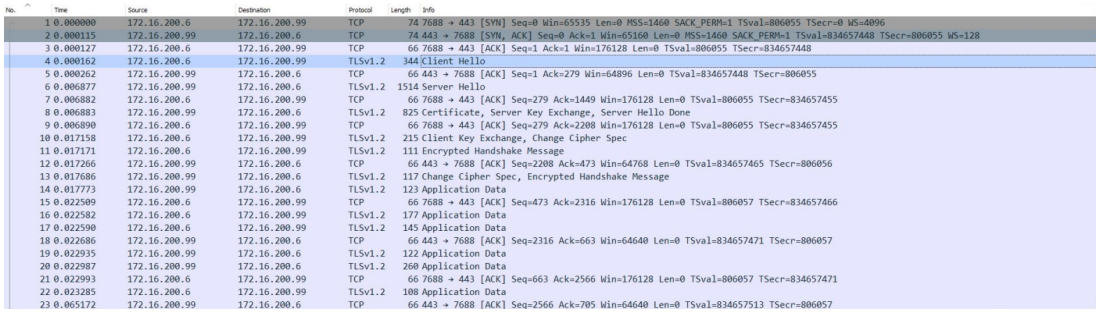
1. Configure the virtual server:

```
config firewall vip
    edit "vip-test"
        set type server-load-balance
        set extip 10.1.100.222
        set extintf "port2"
        set server-type https
        set extport 443
        config realservers
            edit 1
                set ip 172.16.200.99
                set port 443
            next
        end
        set http-multiplex enable
        set ssl-mode full
        set ssl-certificate "Fortinet_SSL"
    next
end
```

2. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "vip-test"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "deep-inspection-clone"
        set av-profile "av"
        set logtraffic all
        set nat enable
    next
end
```

3. Get the clients to access the VIP address (10.1.100.222). The FortiProxy shares the first TLS connection with second TLS connection.
4. Verify the sniffer packet capture on the FortiProxy server side. There is one client hello.

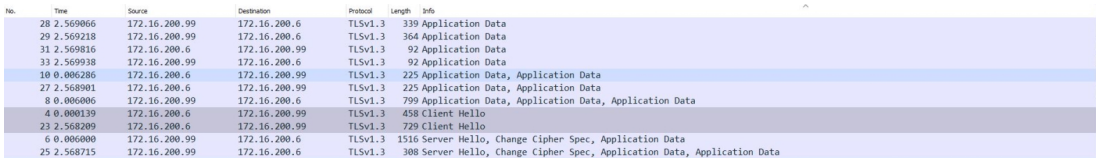


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.200.6	172.16.200.99	TCP	74	7688 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=806055 TSecr=0 WS=4096
2	0.000115	172.16.200.99	172.16.200.6	TCP	74	443 → 7688 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=834657448 TSecr=806055 WS=128
3	0.000127	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=1 Ack=1 Win=176128 Len=0 TSval=806055 TSecr=834657448
4	0.000162	172.16.200.6	172.16.200.99	TLSv1.2	344	Client Hello
5	0.000262	172.16.200.99	172.16.200.6	TCP	66	443 → 7688 [ACK] Seq=1 Ack=279 Win=64896 Len=0 TSval=834657448 TSecr=806055
6	0.006877	172.16.200.99	172.16.200.6	TLSv1.2	1514	Server Hello
7	0.006882	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=279 Ack=1449 Win=176128 Len=0 TSval=806055 TSecr=834657455
8	0.006883	172.16.200.99	172.16.200.6	TLSv1.2	825	Certificate, Server Key Exchange, Server Hello Done
9	0.006890	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=279 Ack=2208 Win=176128 Len=0 TSval=806055 TSecr=834657455
10	0.017158	172.16.200.6	172.16.200.99	TLSv1.2	215	Client Key Exchange, Change Cipher Spec
11	0.017171	172.16.200.6	172.16.200.99	TLSv1.2	111	Encrypted Handshake Message
12	0.017266	172.16.200.99	172.16.200.6	TCP	66	443 → 7688 [ACK] Seq=2208 Ack=473 Win=64768 Len=0 TSval=834657465 TSecr=806056
13	0.017686	172.16.200.99	172.16.200.6	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
14	0.017773	172.16.200.99	172.16.200.6	TLSv1.2	123	Application Data
15	0.022509	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=473 Ack=2316 Win=176128 Len=0 TSval=806057 TSecr=834657466
16	0.022582	172.16.200.6	172.16.200.99	TLSv1.2	177	Application Data
17	0.022590	172.16.200.6	172.16.200.99	TLSv1.2	145	Application Data
18	0.022686	172.16.200.99	172.16.200.6	TCP	66	443 → 7688 [ACK] Seq=2316 Ack=663 Win=64640 Len=0 TSval=834657471 TSecr=806057
19	0.022935	172.16.200.99	172.16.200.6	TLSv1.2	122	Application Data
20	0.022987	172.16.200.99	172.16.200.6	TLSv1.2	260	Application Data
21	0.022993	172.16.200.6	172.16.200.99	TCP	66	7688 → 443 [ACK] Seq=663 Ack=2566 Win=176128 Len=0 TSval=806057 TSecr=834657471
22	0.023285	172.16.200.6	172.16.200.99	TLSv1.2	108	Application Data
23	0.065172	172.16.200.99	172.16.200.6	TCP	66	443 → 7688 [ACK] Seq=2566 Ack=705 Win=64640 Len=0 TSval=834657513 TSecr=806057

5. Disable HTTP multiplexing:

```
config firewall vip
    edit "vip-test"
        config realservers
            edit 1
                set type ip
                set ip 172.16.200.99
                set port 443
            next
        end
        set http-multiplex disable
    next
end
```

6. Verify the sniffer packet capture. This time, the FortiProxy does reuse the TLS connection, so there are two client hellos sent to the real server.



No.	Time	Source	Destination	Protocol	Length	Info
28	2.569066	172.16.200.99	172.16.200.6	TLSv1.3	339	Application Data
29	2.569218	172.16.200.99	172.16.200.6	TLSv1.3	364	Application Data
31	2.569816	172.16.200.6	172.16.200.99	TLSv1.3	92	Application Data
33	2.569938	172.16.200.99	172.16.200.6	TLSv1.3	92	Application Data
10	0.006286	172.16.200.6	172.16.200.99	TLSv1.3	225	Application Data, Application Data
27	2.568901	172.16.200.6	172.16.200.99	TLSv1.3	225	Application Data, Application Data
8	0.006006	172.16.200.99	172.16.200.6	TLSv1.3	799	Application Data, Application Data, Application Data
4	0.000139	172.16.200.6	172.16.200.99	TLSv1.3	458	Client Hello
23	2.568209	172.16.200.6	172.16.200.99	TLSv1.3	729	Client Hello
6	0.006000	172.16.200.99	172.16.200.6	TLSv1.3	1516	Server Hello, Change Cipher Spec, Application Data
25	2.568715	172.16.200.99	172.16.200.6	TLSv1.3	308	Server Hello, Change Cipher Spec, Application Data, Application Data

Authentication Rules

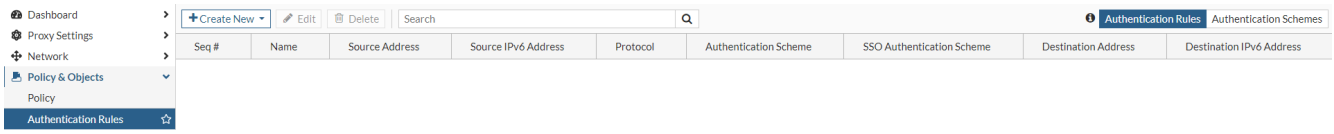
Authentication rules are used to receive user identity, based on the values set for the protocol and source address. If a rule fails to match based on the source address, there will be no other attempt to match the rule; however, the next policy will be attempted. This occurs only when:

- There is an authentication rule, but no authentication method has been set (under `config authentication scheme`), so the user identity cannot be found.
- The user is successfully matched in the rule but fails to match the current policy.

After a rule is positively matched through the protocol and/or source address, the authentication is checked (with `active-auth-method` and `sso-auth-method`). These methods point to schemes, as defined under `config authentication scheme`.

When you combine authentication rules and schemes, you have granular control over users and IP addresses, creating an efficient process for users to successfully match a criteria before matching the policy.

To manage authentication rules, go to *Policy & Objects* > *Authentication Rules*.

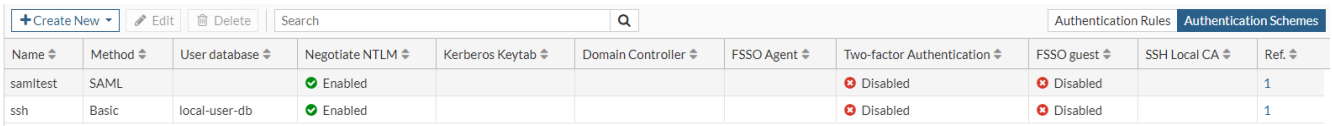


Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an authentication rule or authentication scheme. See Create or edit an authentication rule on page 422.
Edit	Modify an authentication rule or authentication scheme. See Create or edit an authentication rule on page 422.
Delete	Remove an authentication rule or rules.
Search	Enter a search term to find in the list.
Authentication Rules/Authentication Schemes	Select *Authentication Rules* to see a list of authentication rules. Select *Authentication Schemes* to see a list of authentication schemes.
Name	The name of the authentication rule.
Source Address	The source IPv4 addresses, address groups, *all*, or *none*.
Source IPv6 Address	The source IPv6 addresses, address groups, *all*, or *none*.
Protocol	The protocol that is matched for the rule.
Authentication Scheme	The authentication scheme that is being used. To create an authentication scheme, see Create or edit an authentication scheme on page 424.
SSO Authentication Scheme	The single sign-on authentication method.
Destination Address	The destination IPv4 addresses, address groups, *all*, or *none*.
Destination IPv6 Address	The destination IPv6 addresses, address groups, *all*, or *none*.
Comments	An optional description of the authentication rule.
IP-based Authentication	Whether IP-based authentication is enabled or disabled.
Status	Whether the rule is enabled or disabled.

To manage authentication schemes, go to *Policy & Objects* > *Authentication Rules* and then click *Authentication Schemes*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

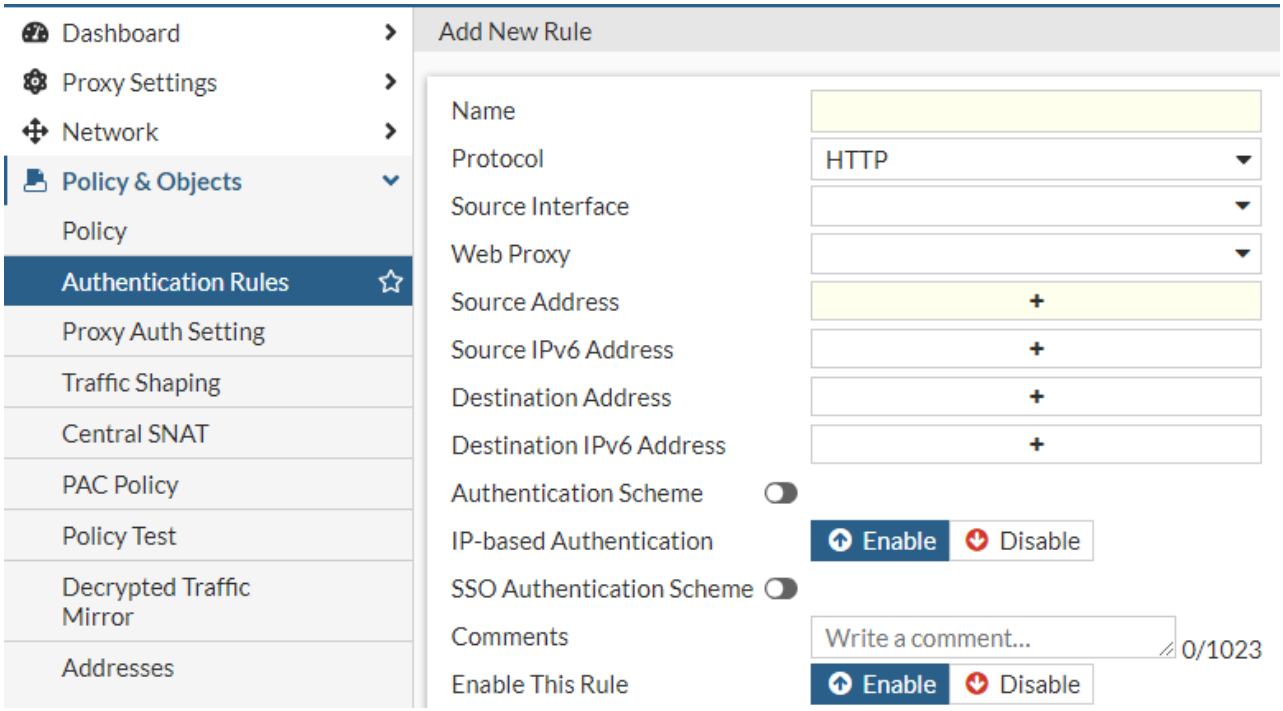
The following options are available:

Create New	Create an authentication scheme. See Create or edit an authentication scheme on page 424.
Edit	Edit an authentication scheme. See Create or edit an authentication scheme on page 424
Delete	Delete an authentication scheme or schemes.
Search	Enter a search term to find in the list.
Authentication Rules/Authentication Schemes	Select *Authentication Rules* to see a list of authentication rules. Select *Authentication Schemes* to see a list of authentication schemes.
Name	The name of the authentication scheme.
Method	The authentication method: *NTLM*, *Basic*, *Digest*, *Form-based*, *Negotiate*, *SAML*, *SSH Public Key*, or *Fortinet Single Sign-On (FSSO)*.
User database	The name of the user database to use.
Negotiate NTLM	Whether NTLM negotiation is required.
Kerberos Keytab	The file containing the shared secret for Kerberos authentication.
Domain Controller	The domain controller.
FSSO Agent	The FSSO agent.
Two-factor Authentication	Whether two-factor authentication is required.
FSSO guest	Whether FSSO-guest authentication is required.
SSH Local CA	Which CA certificate is being used.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an authentication rule

To create an authentication rule:

1. In the authentication rule list, select *Create New* > *Authentication Rules* from the toolbar.



2. Configure the following:

Name	The name of the authentication rule.
Protocol	Select which protocol is matched for the rule.
Source Interface	Select the source interface for the rule.
Web Proxy	Select the web proxy for the rule.
Source Address	Select the source IPv4 addresses, address groups, *all*, or *none*. Required for web-proxy authentication.
Source IPv6 Address	Select the source IPv6 address or address groups, *all*, or *none*. Required for web-proxy authentication.
Destination Address	The destination IPv4 addresses, address groups, *all*, or *none*.
Destination IPv6 Address	The destination IPv6 addresses, address groups, *all*, or *none*.
Authentication Scheme	Enable *Authentication Scheme* to use an authentication scheme and then select which authentication scheme to use. To create an authentication scheme, see Create or edit an authentication scheme on page 424.
IP-based Authentication	Select *Enable* if you want to use IP-based authentication.

SSO Authentication Scheme	If you selected *Enable* for IP-based authentication, enable *SSO Authentication Scheme* if you want to use single sign-on method and then select which single sign-on method to use.
Comments	Enter an optional description of the rule.
Enable This Rule	Select *Enable* or *Disable* to control whether the authentication rule is used or ignored.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

3. Click *OK* to create the new authentication rule.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

To edit an authentication rule:

1. Select the authentication rule you want to edit and then click *Edit* from the toolbar or double-click on the rule in the rule table.
2. Edit the rule information as required and click *OK* to apply your changes.

To set the authentication rule in the CLI:

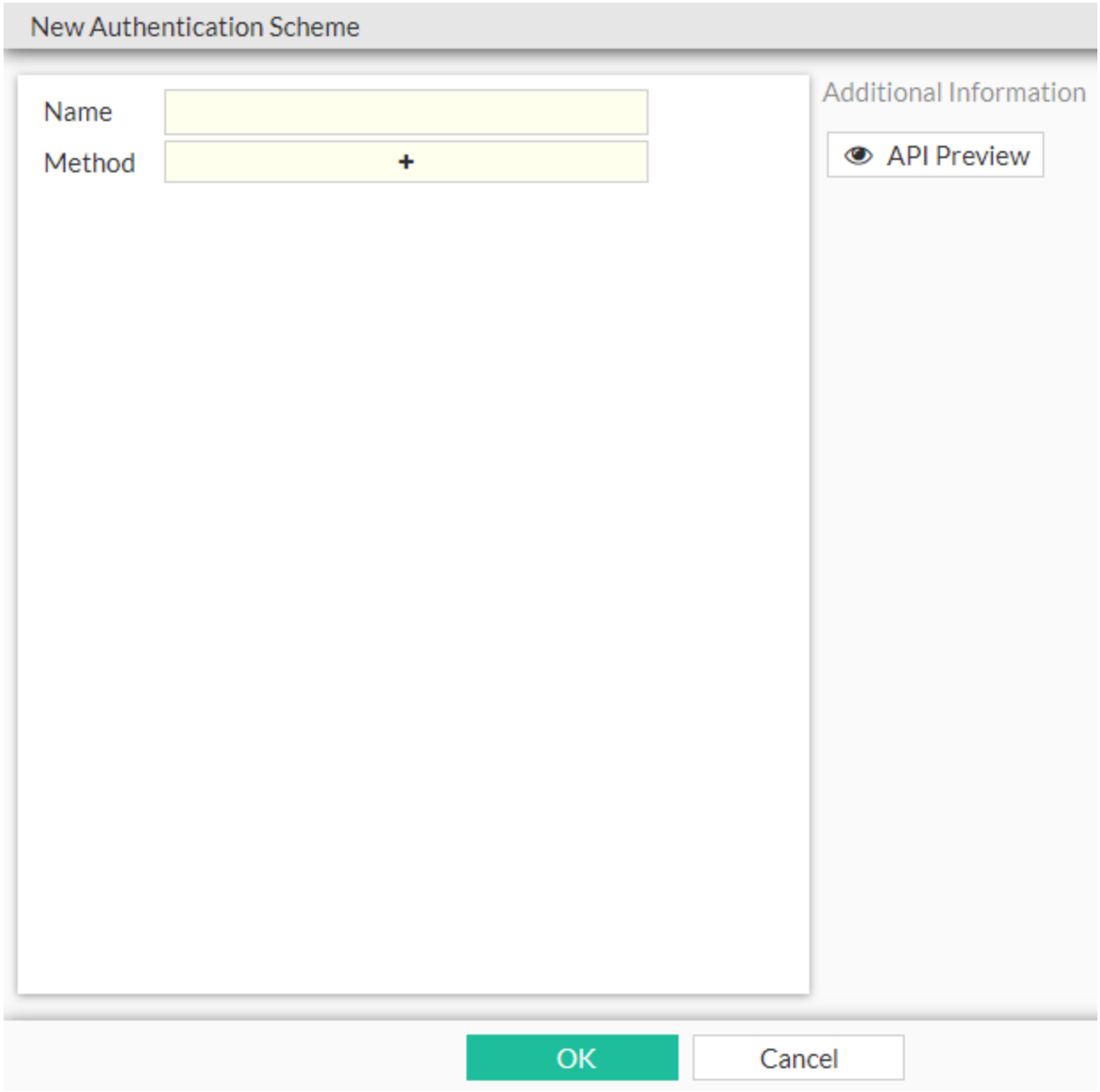
```
config authentication rule
   edit <name of rule>
      set status [enable|disable]
      set protocol [http|ftp|socks|ssh]
      set web-proxy <explicit_proxy_entity>
      set srcintf <name of incoming (ingress) interface>
      set srcaddr <name of IPv4 source address>
      set dstaddr <name of IPv4 destination address>
      set srcaddr6 <name of address object>
      set ip-based [enable|disable]
      set active-auth-method <string>
      set sso-auth-method <string>
      set web-auth-cookie [enable|disable]
      set transaction-based [enable|disable]
      set web-portal [enable|disable]
      set comments <string>
   next
end
```

Refer to config authentication rule in the CLI guide for more information.

Create or edit an authentication scheme

To create an authentication scheme:

1. In the authentication scheme list, select *Create New* > *Authentication Schemes* from the toolbar.



2. Configure the following:

Name	Enter the name of the authentication scheme.
Method	Select the authentication methods: • *Basic* • *Certificate*

	• *Digest* • *Form-based* • *Fortinet Single Sign-On (FSSO)* • *Negotiate* • *NTLM* • *RADIUS Single-Sign-On (RSSO)* • *SAML* • *SSH Public Key* Multi-methods supports *Basic*, *NTLM*, and *Negotiate*. For agentless NTML authentication, see Agentless NTLM support on page 426.
Negotiate NTLM	Enable/disable authentication negotiation for NTLM. When disabled, access is limited for non-domain users while using proxy authentication. This option is only available when the method includes *Negotiate*.
Kerberos keytab	Select the file containing the shared secret for Kerberos authentication.
Domain Controller	If you selected *NTLM*, select the domain controller.
User database	Select which user database to use.
Two-factor authentication	Move the slider to control whether two-factor authentication is required.
FSSO Agent	Move the slider to select the FSSO agent to use.
FSSO guest	Move the slider to control whether FSSO-guest authentication is required.
SSH local CA	Select which CA certificate to use.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

3. Click *OK* to create the new authentication scheme.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

To edit an authentication scheme:

1. Select the authentication scheme you want to edit and then click *Edit* from the toolbar or double-click on the scheme in the scheme table.
2. Edit the scheme information as required and click *OK* to apply your changes.

To create an authentication scheme in the CLI:

```
config authentication scheme
   edit <name>
      set method {ntlm | basic | digest | form | negotiate | fsso | rsso | ssh-publickey | cert |
            saml | saml-sp}
      set domain-controller <string>
      set fsso-agent-for-ntlm <string>
      set fsso-guest {enable | disable}
      set kerberos-keytab <string>
      set negotiate {enable | disable}
      set negotiate-ntlm {enable | disable}
      set require-tfa {enable | disable}
      set saml-ipd-portal <string>
      set ssh-ca <string>
      set user-database <auth_server>
   next
end
```

The following methods are available:

- `basic`—Basic HTTP authentication. This is the default method.
- `digest`—Digest HTTP authentication.
- `ntlm`—NTLM authentication. For agentless NTML authentication, see Agentless NTLM support on page 426. To configure the domain source when doing NTML authentication, see Domain name source when doing NTLM authentication on page 427.
- `form`—Form-based HTTP authentication.
- `negotiate`—Negotiate authentication.
- `fsso`—FSSO authentication.
- `rsso`—RADIUS Single Sign-On authentication.
- `saml`—SAML-IDP authentication (requires external FortiAuthenticator).
- `saml-sp`—SAML-IDP authentication with FortiProxy as the service provider.
- `publickey`—Public-key-based SSH authentication.
- `x-auth-user`—User from HTTP x-authenticated-user header.

Agentless NTLM support

Agentless NTLM authentication can be configured directly from the FortiProxy unit to the Domain Controller using the SMB protocol (no agent is required).

NOTE: This authentication method is only supported for proxy policies.

Syntax

NOTE: The `set domain-controller` command is only available when `method` is set to `ntlm` and/or `negotiate-ntlm` is set to `enable`.

```
config authentication scheme
   edit <name>
      set method ntlm
      set domain-controller <dc-setting>
   next
end

config user domain-controller
   edit <name>
      set ip-address <dc-ip>
      set port <port> // The default is 445.
      set domain-name <dns-name>
      set ldap-server <name>
   next
end
```

Domain name source when doing NTLM authentication

When doing NTLM authentication, the domain is extracted based on the following:

1. If the domain controller has a domain name configured, it is used.
2. Otherwise, if the NTLM type 3 message, from the user, is configured, it is used.
3. Otherwise, if the domain name from the NTLM type 2 message, from the DC, is configured, it is used.

To configure the domain name source, if it is not set:

```
config user domain-controller
    edit "adfs-dc"
        set ip-address 192.168.130.200
        unset domain-name
        set domain-name-src {server | client}
        set ldap-server "adfsldap"
    next
end
```

The domain name can be extracted from either the server's (DC) data, or from the client's data.

Proxy Auth Setting

This submenu provides settings for configuring authentication timeout, protocol support, authentication certificates, authentication schemes, and captive portals. When user authentication is

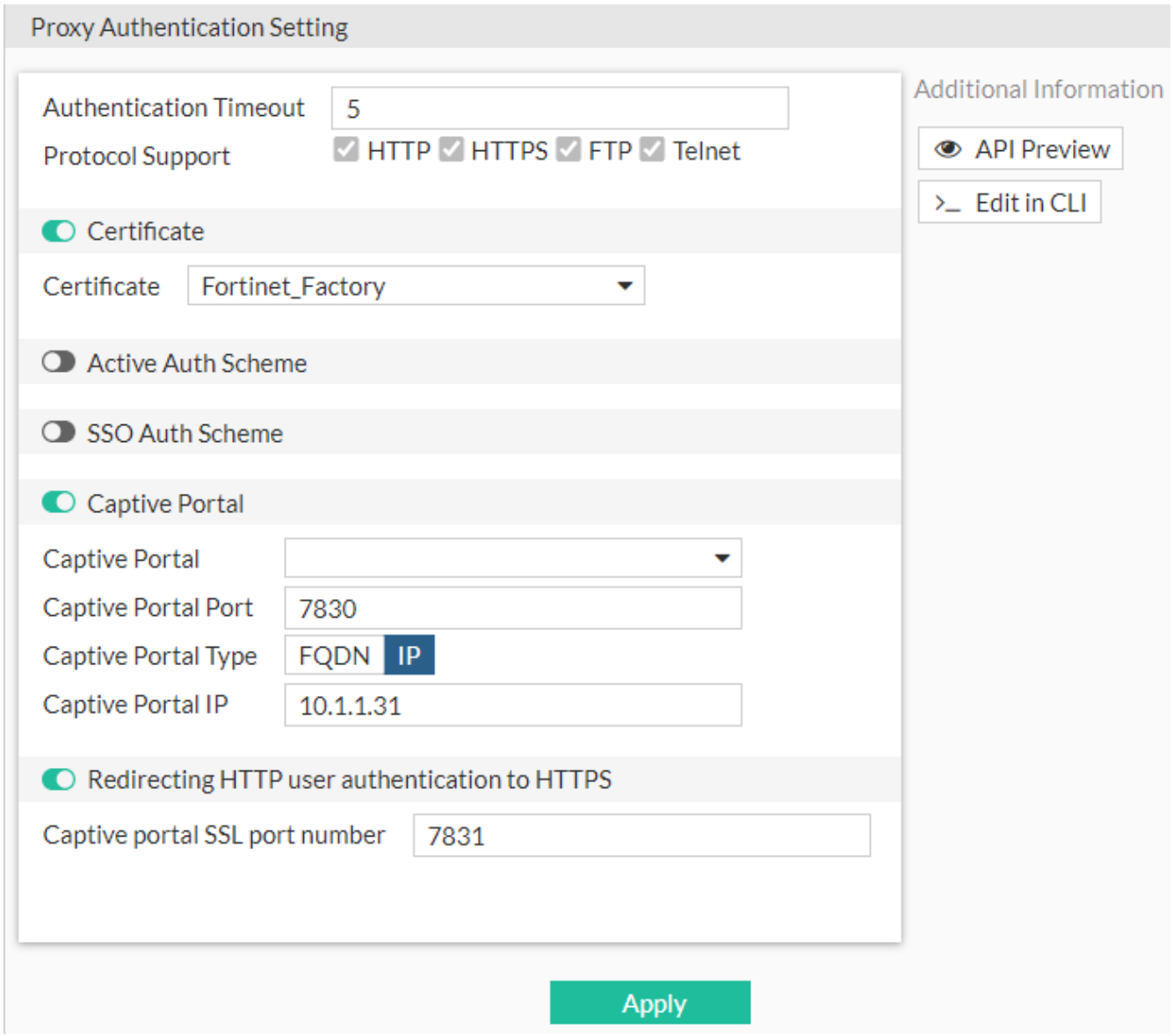
enabled within a security policy, the authentication challenge is normally issued for any of the four protocols (depending on the connection protocol):

- HTTP (can also be set to redirect to HTTPS)
- HTTPS
- FTP
- Telnet

The selections control which protocols support the authentication challenge. Users must connect with a supported protocol first so that they can subsequently connect with other protocols. If HTTPS is selected as a method of protocol support, the user can authenticate with a customized local certificate.

When you enable user authentication within a security policy, the security policy user is challenged to authenticate. For user ID and password authentication, users must provide their user names and passwords. For certificate authentication (HTTPS or HTTP redirected to HTTPS only), you can install customized certificates on the unit, and the users can also have customized certificates installed on their browsers. Otherwise, users see a warning message and have to accept a default Fortinet certificate.

To configure proxy authentication settings, go to *Policy & Objects > Proxy Auth Settings*.



Configure the following settings and then select *Apply* to save your changes:

Authentication Timeout	Enter the amount of time, in minutes, that an authenticated firewall connection can be idle before the user must authenticate again. From 1 to 480 minutes. The default is 5.
Protocol Support	Select the protocols to challenge during firewall user authentication from the following: • *HTTP* • *HTTPS* • *FTP* • *Telnet*

Certificate	If you want to use a local certificate for authentication, enable *Certificate* and then select the certificate. The default is *Fortinet_Factory*.
Active Auth Scheme	If you want to use an active authentication scheme, enable *Active Auth Scheme* and then select which scheme to use. To create an authentication scheme, see Create or edit an authentication scheme on page 424.
SSO Auth Scheme	If you want to use a single-sign-on authentication scheme, enable *SSO Auth Scheme* and then select which scheme to use.
Captive Portal	If you want use a captive portal to authenticate web users, enable *Captive Portal* and then select a captive portal. Enter the captive port number and select the portal type. If you select *IP* as the captive portal type, enter the captive portal IP address.
Redirecting HTTP user authentication to HTTPS	Enable *Redirecting HTTP user authentication to HTTPS* if you want HTTPS user authentication used instead of HTTP user authentication and then enter the captive portal SSL port number.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.
Edit in CLI	Click to open a CLI console window to view and edit the setting in the CLI. If there are multiple CLI settings on the page, the CLI console shows the first setting.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

To configure the authentication settings in the CLI:

```
config authentication setting
   set active-auth-scheme <string>
   set sso-auth-scheme <string>
   set captive-portal <string>
   set captive-portal-port <integer value from 1 to 65535; default is 0>
   set auth-https {enable | disable}
   set captive-portal-ssl-port <integer value from 1 to 65535; default is 7831>
end
```

- `active-auth-scheme`—Active authentication method.
- `sso-auth-scheme`—SSO authentication method.

- `captive-portal`—Captive portal host name.
- `captive-portal-port`—Captive portal port number.
- `auth-https`—Enable or disable redirecting HTTP user authentication to HTTPS.
- `captive-portal-ssl-port`—Captive portal SSL port number.

Traffic shaping

A FortiProxy provides quality of service (QoS) by applying bandwidth limits and prioritization to network traffic. Traffic shaping is one technique used by the FortiProxy to provide QoS. A basic approach to traffic shaping is to prioritize higher priority traffic over lower priority traffic during periods of traffic congestion. This provides a stabilizing effect for important traffic while throttling less important traffic.

The FortiProxy delivers traffic shaping with queuing. Before a packet egresses an interface, it is first enqueued to a queue using an algorithm such as RED or FIFO. The kernel dequeues the packet based on the HTB algorithm before sending it out. When traffic exceeds the configured bandwidth limits, traffic is delayed for transport until bandwidth frees up. Traffic may be dropped if the queues are full.

Configuration methods

The following table lists the methods to configure traffic shaping on the FortiProxy and their capabilities in order of preference. If both methods are configured, the first will be preferred over the second.

Method	Traffic queuing	Traffic prioritization	Guaranteed and maximum bandwidth limits
Traffic shaping profile on page 441	Yes	Traffic is placed into classes. A total of 30 classes are available. For each class, traffic can be configured into five priority levels.	When applying a traffic shaping profile to an interface's egress shaping profile, you can configure it to use up to 100% of the interface's configured bandwidth between all the classes, regardless of the configured priority in each class. The guaranteed bandwidth is always honored.

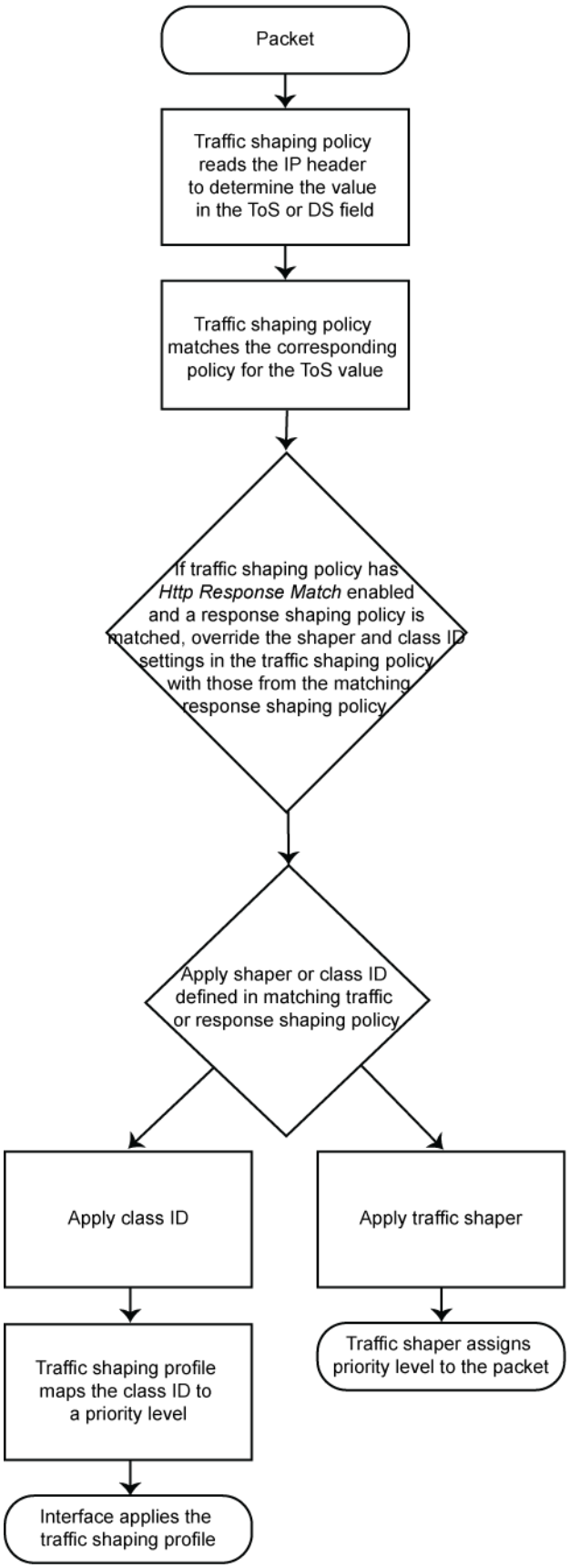
Method	Traffic queuing	Traffic prioritization	Guaranteed and maximum bandwidth limits
Traffic shaper	No	Traffic can be prioritized into the high (2), medium (3), or low (4) levels. When traffic is below the guaranteed bandwidth of the shaper, the traffic is automatically applied the critical level (1).	No hard limit on the guaranteed bandwidth. Administrators allocate guaranteed bandwidth to all the traffic shapers for an interface and ensure that the sum does not exceed the total outbandwidth of the interface. Traffic under the guaranteed bandwidth of a traffic shaper is given priority 1. If the total traffic with priority 1 exceeds the total outbandwidth, traffic can be dropped.

The following topics provide information about configuring traffic shaping:

- Traffic shaping policies on page 432
- Response shaping policies NEW on page 439
- Traffic shaping profile on page 441
- Traffic shapers on page 444
- DSCP marking in firewall shaping policies on page 453
- Examples on page 454

Traffic shaping policies

A traffic shaping policy is a rule that matches traffic to a traffic shaper or assign them to a class based on certain IP header fields and/or upper layer criteria. The matching traffic will apply a traffic shaper, class ID, or assign a DSCP DiffServ tag to the outgoing traffic. For example, it can match traffic based on source and destination IP, service, application, and URL category. One common use case is to match traffic based on the ToS or DS (differentiated services) field in the IP header. This allows Type of Service or Differentiated Services (DiffServ) tags to be read from traffic from a downstream device and prioritized accordingly on the FortiProxy based on the traffic shaper or the shaping profile applied on the interface.


Packet
Traffic shaping policy reads the IP header to determine the value in the ToS or DS field
Traffic shaping policy matches the corresponding policy for the ToS value
If traffic shaping policy has *Http Response Match* enabled and a response shaping policy is matched, override the shaper and class ID settings in the traffic shaping policy with those from the matching response shaping policy
Apply shaper or class ID defined in matching traffic or response shaping policy
Apply class ID
Apply traffic shaper
Traffic shaping profile maps the class ID to a priority level
Traffic shaper assigns priority level to the packet
Interface applies the traffic shaping profile

The traffic shaping policies must be placed in the correct order in the traffic shaping policy list page to obtain the desired results. Policies are matched from top-down, so the traffic shaping policies should be arranged in a sequence that places the more granular policies above general policies.

The policy can be configured by going to *Policy & Objects > Traffic Shaping* and selecting the *Traffic Shaping Policies* tab. If the menu does not display the traffic shaping settings, go to *System > Feature Visibility* and enable *Traffic Shaping*.

Configuring traffic shaping policies

A traffic shaping policy can be split into two parts:

- Options used to match the traffic
- Options used to apply actions to the matched traffic

The following options can be configured for traffic matching criteria. Some options can only be configured from the CLI.

GUI option (under ***Policy & Objects > Traffic Shaping > Traffic Shaping Policies***)	CLI option (under `config firewall shaping-policy`)	Description
Source		
Address	`set srcaddr <address_object>`	Select the address object to match the source IP.
Destination		
Address	`set dstaddr <address_object>`	Select the address object to match the destination IP.
Service Type	`set service-type [service|internet-service]`	Select the service type: firewall service or internet service.
Service	`set service <name1>, <name2>`	Select the firewall service or service group for the traffic.

Internet Service	`set internet-service-name <name>`
	`set internet-service-group <group>`
	`set internet-service-custom <custom>`
	`set internet-service-custom-group <custom_group>`
		Select the internet service to match the destination of the incoming traffic. Internet service currently cannot be used with destination address and service.

Schedule	`set schedule <schedule>`	Enable to select a schedule (one-time, recurring, or group).
Users	`set users <name1>, <name2>, ...`	Select the authenticated users to apply this traffic shaping policy to.

GUI option (under *Policy & Objects > Traffic Shaping > Traffic Shaping Policies*)	CLI option (under `config firewall shaping-policy`)	Description
Groups	`set groups <name1>, <name2>, ...`	Select the authenticated user groups to apply this traffic shaping policy to.

The following options can be configured for actions to apply to the matched traffic:

GUI option	CLI option	Description
Outgoing interface	`set dstintf <interface>`	Select the destination interface that the traffic shaping applies to (required).
Apply shaper		
Shared shaper	`set traffic-shaper <shaper>`	Select the shared shaper to be applied to traffic in the ingress-to-egress direction. For example, on traffic that egresses on the wan interface, the shaper is applied to upload or outbound traffic.
Reverse shaper	`set traffic-shaper-reverse <shaper>`	Select the reverse shaper to be applied to traffic in the egress-to-ingress direction. For example, on traffic that egresses on the wan interface, the shaper is applied to download or inbound traffic.
Per-IP shaper	`set per-ip-shaper <shaper>`	Select the per-IP shaper. Per-IP shapers affect downloads and uploads. The allotted bandwidth applies to each individual IP. In a shared shaper, the allotted bandwidth applies to all IPs.
Assign shaping class ID		
Traffic shaping class ID	`set class-id <class>`	Set the class ID to apply the matching traffic. Class IDs are further prioritized within a traffic shaping profile and applied to an interface.

n/a	`set diffserv-forward {enable | disable}`
	`set diffservcode-forward <code>`
	`set diffserv-reverse {enable | disable}`
	`set diffservcode-reverse <code>`
		Specify the settings to apply a DSCP tag to the forward or reverse traffic. The DiffServ code is in 6-bit binary format.
		These options can only be configured in the CLI.

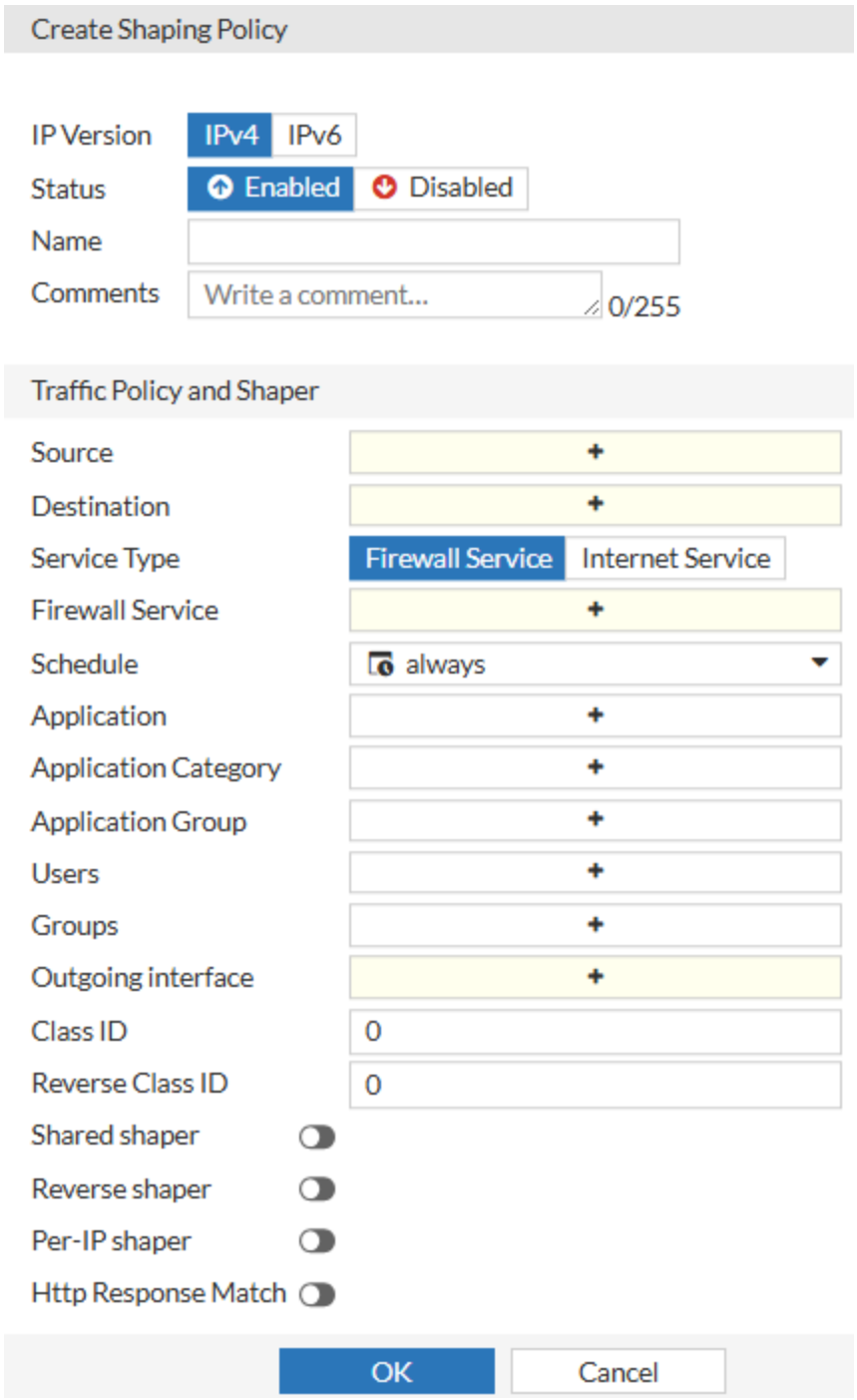
Traffic shapers and class IDs can be applied at the same time when configuring traffic shaping policies. However, to reduce the complexity, it is recommended to use one method over the other.

The following topics include examples with traffic shaping policies:

- Response shaping policies NEW on page 439
- Interface-based traffic shaping profile on page 454
- Shared traffic shaper on page 444
- Per-IP traffic shaper on page 448

Create or edit a traffic-shaping policy

Select *Create New* to open the *Create Shaping Policy* window. To change a traffic-shaping policy, select a policy and then click *Edit*.



Configure the following settings in the *New Shaping Policy* window or the *Edit Shaping Policy* window and then click *OK*:

IP Version	Select *IPv4* or *IPv6*.
Status	Policies are enabled by default. To disable to policy, click *Disabled*.
Name	Specify the name of the traffic shaping policy.

Comment	Enter any additional information that might be needed by administrators, as a reminder of the policy's purpose and scope. This setting is optional.
Source	Select or create the source address, address group, user, or user group that the traffic must match. You can select multiple sources in multiple categories.
Destination	Select or create the destination address or address group that the traffic must match. You can select multiple destinations in both categories.
Service Type	Select whether firewall services or Internet services are used for this policy.
Firewall Service	If you selected *Firewall Service* as the service type, select one or more firewall services that the traffic must match.
Internet Service	If you selected *Internet Service* as the service type, select one or more Internet services that the traffic must match.
Schedule	Select a schedule (one-time, recurring, or group) from the drop-down list for the traffic shaping policy, which allows different traffic shaping for different days or different hours of the day without administrative intervention. Select *Create* to create a schedule. The default is *always,* which means the shaping policy is always applied. For more information, see Schedules on page 516.
Application	Select an application from the drop-down list.
Application Category	Select an application category from the drop-down list.
Application Group	Select an application group from the drop-down list. Select *Create* to create an application group.
Users	Select one or more users that the traffic must match.
Groups	Select one or more user groups that traffic must match.
Outgoing Interface	Set this to the external interface that the traffic must match.
class-id	The class ID of a traffic shaper for outgoing packets.
class-id-reverse	The class ID of a traffic shaper for incoming packets.
Shared shaper	Enable or disable Shared traffic shaper on page 444.
Reverse shaper	Enable or disable reverse traffic shapers.
Per-IP shaper	Enable or disable Per-IP traffic shaper on page 448.
Http Response Match NEW	Enable matching HTTP response shaping policies. When enabled, FortiProxy looks for matching response shaping policies. If a match is found, the settings in the matching response shaping policy will override the settings in this traffic shaping policy.

API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

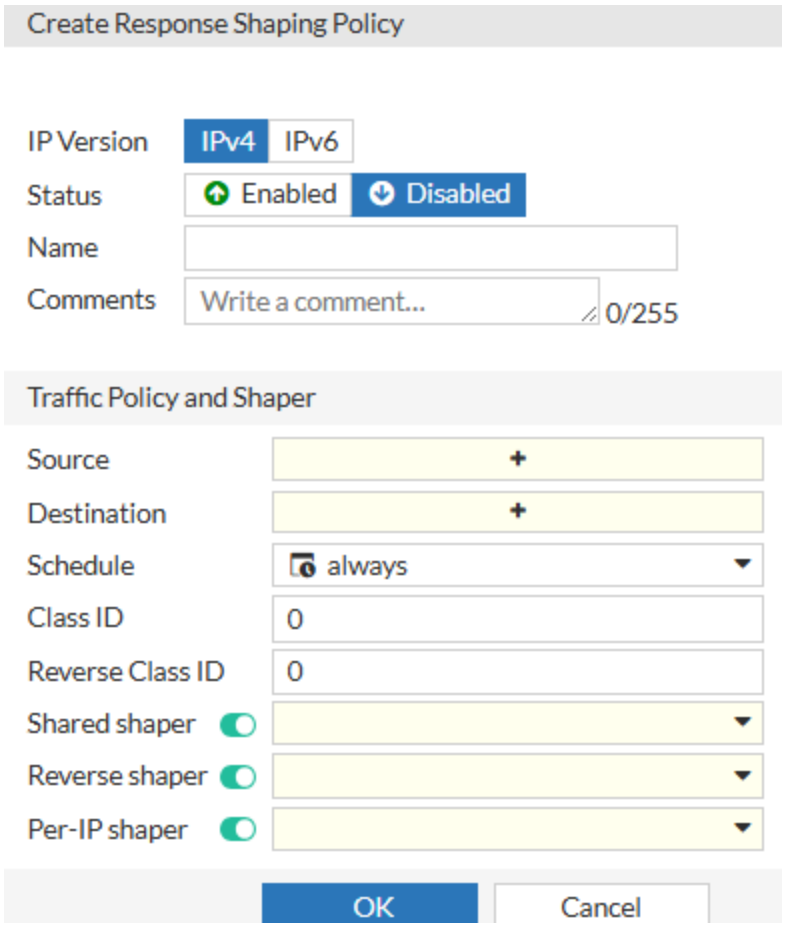
Response shaping policies NEW

A response shaping policy is a specialized type of traffic shaping policy that works on the top of a traffic shaping policy to further match the traffic based on certain HTTP response header fields. When *Http Response Match* is enabled in a traffic shaping policy, any traffic that matches the traffic shaping policy is further evaluated against the list of response shaping policies. If a match is found, the traffic will be mapped to the traffic shaper or assigned to the class defined in the response shaping policy instead of the ones defined in the original matching traffic shaping policy.

The response shaping policies must be placed in the correct order in the response shaping policy list page to obtain the desired results. Policies are matched from top-down, so the response shaping policies should be arranged in a sequence that places the more granular policies above general policies.

To create or edit a response shaping policy:

1. Go to *Policy & Objects* > *Traffic Shaping* and select the *Response Shaping Policies* tab.
   If the menu does not display the traffic shaping settings, go to *System* > *Feature Visibility* and enable *Traffic Shaping*.
2. Select *Create New* to open the *Create Response Shaping Policy* window or select a policy and then click *Edit* to change a response shaping policy.
3. Configure the following options:



IP Version	Select *IPv4* or *IPv6*.
Status	Policies are enabled by default. To disable to policy, click *Disabled*.
Name	Specify the name of the response shaping policy.
Comment	Enter any additional information that might be needed by administrators, as a reminder of the policy's purpose and scope. This setting is optional.
Source	Select or create the source address, address group, user, or user group that the traffic must match. You can select multiple sources in multiple categories.
Destination	Select or create the destination proxy address(es) that the traffic must match. The destination proxy address(es) must be the *Response Header* type. See Proxy address on page 488 for more details.

Schedule	Select a schedule (one-time, recurring, or group) from the drop-down list for the response shaping policy, which allows different traffic shaping for different days or different hours of the day without administrative intervention. Select *Create* to create a schedule. The default is *always,* which means the shaping policy is always applied. For more information, see Schedules on page 516.
Class ID	The class ID of a traffic shaper for outgoing packets.
Reverse Class ID	The class ID of a traffic shaper for incoming packets.
Shared shaper	Enable or disable Shared traffic shaper on page 444.
Reverse shaper	Enable or disable reverse traffic shapers.
Per-IP shaper	Enable or disable Per-IP traffic shaper on page 448.

4. Click *OK*.

Alternatively, use the `config firewall response-shaping-policy` command.

See Traffic shaping based on HTTP response NEW on page 463 for an end-to-end configuration example.

Traffic shaping profile

A traffic shaping profile allows traffic shaping to be configured Up to 30 classes can be defined, with prioritization and bandwidth limits configured for each class.

Configuring traffic shaping profiles

The main steps to configure traffic shaping are:

1. Configure the traffic shaping policy, and assign matched traffic to a class (see Traffic shaping policies on page 432).
2. Create a traffic shaping profile and apply traffic bandwidth, prioritization and/or queuing per class.
3. Configure the interface outbandwidth/inbandwidth and apply a shaping profile to the interface.

Creating a traffic shaping profile

A traffic shaping profile consists of the class ID, settings per class ID, and the default class ID for traffic that does not match any traffic shaping policies. A class can be configured in the GUI as part of a traffic shaping profile or policy. In the CLI, a traffic class must be defined before it can be assigned within a traffic shaping profile. Class IDs range from 2 - 31, and they can be reused between different traffic shaping profiles.

When creating a traffic shaping profile, you can configure the following options per class.

GUI option	CLI option	Description
Default	`set default-class-id <class-id>`	Set the default class ID. Each profile must have one default class ID. The default class ID can be changed at any time.
Traffic shaping class ID	`set class-id <integer>`	Set the class ID (2 - 31).
Guaranteed bandwidth	`set guaranteed-bandwidth-percentage <integer>`	Set the percentage of the outbandwidth that will be guaranteed for the class ID.
Maximum bandwidth	`set maximum-bandwidth-percentage <integer>`	Set the percentage of the outbandwidth that will be the maximum bandwidth for the class ID.
Priority	`set priority {top | critical | high | medium | low}`	Select the priority level for the class ID.

To configure a traffic shaping profile in the GUI:

1. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Profiles* tab, and click *Create New*.
2. Enter the profile name, and optionally enter a comment.
3. In the *Traffic Shaping Classes* section, click *Create New*.
4. Configure the traffic shaping class ID settings (*Traffic shaping class ID*, *Guaranteed bandwidth*, *Maximum bandwidth*, and *Priority*).
5. Click *OK*.
6. Create more shaping classes as needed (the total guaranteed bandwidth of all classes cannot exceed 100%).
7. Click *OK*.

To configure a traffic shaping profile in the CLI:

1. Configure the shaping class:

```
config firewall traffic-class
    edit <integer>
        set class-name <string>
    next
end
```

2. Configure the shaping profile:

```
config firewall shaping-profile
    edit <name>
        set type {policing | queuing}
        set default-class-id <class-id>
        config shaping-entries
            edit <id>
```

```
                set class-id <integer>
                set priority {top | critical | high | medium | low}
                set guaranteed-bandwidth-percentage <integer>
                set maximum-bandwidth-percentage <integer>
            next
        end
    next
end
```

Configuring the interface outbandwidth and inbandwidth

You must configure the following settings on an interface that has traffic shaping applied to egressing/ingressing traffic: assign a traffic shaping profile and configure the outbound/inbound bandwidth.

Since traffic shaping is often configured on the WAN interface for egressing/ingressing traffic, the outbound/inbound bandwidth is effectively the upstream/downstream bandwidth allowed by your ISP.

To configure traffic shaping on an interface:

1. Go to *Network* > *Interfaces* and double-click an interface to edit it.
2. In the *Traffic Shaping* section, depending on your needs, enable *Outbound shaping profile* or *Inbound shaping profile* or both.
3. Select a profile for each enabled option.
4. Enable *Outbound bandwidth* or *Inbound shaping profile* or both, depending on your previous configuration.
5. Specify a value for each enabled option.
6. Click *OK*.

Verifying that the traffic is being shaped

In this example, three traffic classes are defined in the traffic shaping profile assigned to port1. The outbandwidth configured on port1 is 1000 Kbps. Each class has an `allocated-bandwidth`, `guaranteed-bandwidth`, `max-bandwidth`, and `current-bandwidth` value.

- The `guaranteed-bandwidth` and `max-bandwidth` are rates that are converted from the percentage of outbandwidth configured for each class. For example, `class-id` 2 has 10% `guaranteed-bandwidth`, equivalent to 100 Kbps, and 100% `max-bandwidth` equivalent to 1000 Kbps.
- The `allocated-bandwidth` displays the real-time bandwidth allocation for the traffic class based on all available factors. This value changes as traffic demand changes.
- The `current-bandwidth` displays the real-time bandwidth usage detected for the traffic class.

To verify that traffic is being shaped by the traffic shaping profile:

Enable debug flow to view the live traffic as it matches a traffic shaping policy:

```
# diagnose debug flow show function-name enable
# diagnose debug flow filter <filters>
```

```
# diagnose debug flow trace start <repeat_number>
# diagnose debug enable
```

Traffic shapers

The following topics provide more information about traffic shapers:

- Shared traffic shaper on page 444
- Per-IP traffic shaper on page 448
- Changing traffic shaper bandwidth unit of measurement on page 450
- Multi-stage DSCP marking and class ID in traffic shapers on page 451

Shared traffic shaper

Shared traffic shaper is used in a firewall shaping policy to indicate the priority and guaranteed and maximum bandwidth for a specified type of traffic use.

The maximum bandwidth indicates the largest amount of traffic allowed when using the policy. You can set the maximum bandwidth to a value between 1 and 16776000 Kbps. The GUI displays an error if any value outside this range is used. If you want to allow unlimited bandwidth, use the CLI to enter a value of 0.

The guaranteed bandwidth ensures that there is a consistent reserved bandwidth available. When setting the guaranteed bandwidth, ensure that the value is significantly less than the interface's bandwidth capacity. Otherwise, the interface will allow very little or no other traffic to pass through, potentially causing unwanted latency.

In a shared traffic shaper, the administrator can prioritize certain traffic as high, medium, or low. FortiProxy provides bandwidth to low priority connections only when high priority connections do not need the bandwidth. For example, you should assign a high traffic priority to a policy for connecting a secure web server that needs to support e-commerce traffic. You should assign less important services a low priority.

When you configure a shared traffic shaper, you can apply bandwidth shaping per policy or for all policies. By default, a shared traffic shaper applies traffic shaping evenly to all policies that use the shared traffic shaper.

When configuring a per-policy traffic shaper, FortiProxy applies the traffic shaping rules defined for each security policy individually. For example, if a per-policy traffic shaper is configured with a maximum bandwidth of 1000 Kbps, any security policies that have that traffic shaper enabled get 1000 Kbps of bandwidth each.

If a traffic shaper for all policies is configured with a maximum bandwidth of 1000 Kbps, all policies share the 1000 Kbps on a first-come, first-served basis.

The configuration is as follows:

```
config firewall shaper traffic-shaper
   edit "share1"
      set guaranteed-bandwidth 15
      set maximum-bandwidth 80000000
      set bandwidth-unit gbps
```

```
        set per-policy enable
        set diffserv enable
       set dscp-marking-method multi-stage
       set exceed-bandwidth 16
       set exceed-dscp 011111
       set maximum-dscp 111111
        set overhead 3
       set diffservcode 000110
   next
end
```

The shared traffic shaper selected in the traffic shaping policy affects traffic in the direction defined in the policy. For example, if the source port is LAN and the destination is WAN1, the traffic shaping affects the flow in this direction only, affecting the outbound traffic's upload speed. You can define the traffic shaper for the policy in the opposite direction (reverse shaper) to affect the inbound traffic's download speed. In this example, that would be from WAN1 to LAN.

Only traffic through forward traffic shapers will be included in FortiView; reverse and per-IP shapers are not included.

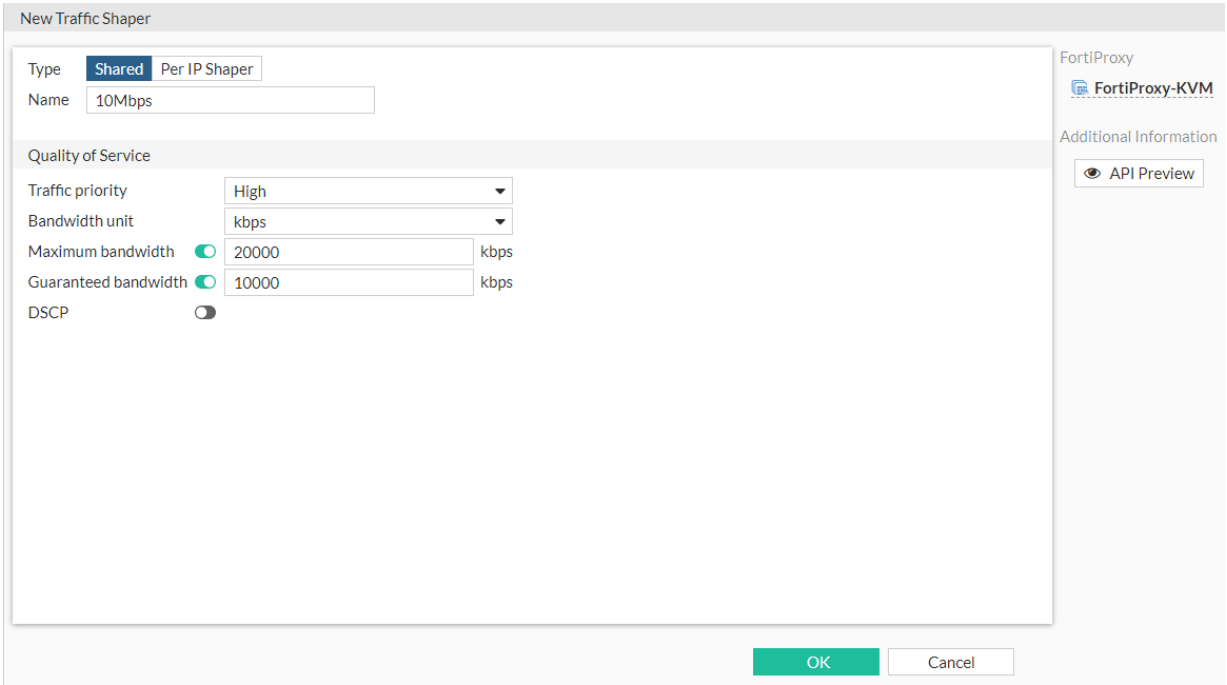
Traffic shapers can be added to a multicast policy when multicast routing is enabled.

The following example shows how to apply different speeds to different types of service. The example configures two shared traffic shapers to use in two firewall shaping policies. One policy guarantees a speed of 10 Mbps for VoIP traffic. The other policy guarantees a speed of 1 Mbps for other traffic. In the example, FortiProxy communicates with a PC using port10 and the Internet using port9.

To configure shared traffic shapers in the GUI:

1. Create a firewall policy:
   a. Go to *Policy & Objects > Policy* and click *Create New*.
   b. Set the *Name* to *Internet Access*.
   c. Set the *Incoming Interface* to *port10*.
   d. Set the *Outgoing Interface* to *port9*.
   e. Set the *Source* and *Destination* to *all*.
   f. Set the *Schedule* to *always*.
   g. Set the *Service* to *ALL*.
   h. Click *OK*.
2. Create the shared traffic shapers:
   a. Go to *Policy & Objects > Traffic Shaping*, select the *Traffic Shapers* tab, and click *Create New*.
   b. Set the *Name* to *10Mbps*. This shaper is for VoIP traffic.
   c. Set the *Traffic Priority* to *High*.
   d. Enable *Max Bandwidth* and enter *20000*.

e. Enable *Guaranteed Bandwidth* and enter *10000*.



f. Click *OK*.

g. Repeat the above steps to create another traffic shaper named *1Mbps* with the *Traffic Priority* set to *Low*, the *Max Bandwidth* set to *10000*, and the *Guaranteed Bandwidth* set to *1000*.

3. Create a firewall shaping policy for VoIP traffic:

a. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.

b. Set the *Name* to *VoIP_10Mbps_High*.

c. Set the *Source* and *Destination* to *all*.

d. Set the *Service* to all VoIP services.

e. Set the *Outgoing Interface* to *port9*.

f. Enable *Shared shaper* and select *10Mbps*.

g. Enable *Reverse shaper* and select *10Mbps*.

h. Click *OK*.

4. Repeat the sub-steps in step 3 to create another firewall shaping policy named *Other_1Mbps_Low* for other traffic, with the *Source* and *Destination* set to *all*, *Service* set to *ALL*, *Outgoing Interface* set to *port9*, and *Shared shaper* and *Reverse shaper* set to *1Mbps*.

To configure shared traffic shapers in the CLI:

1. Create a firewall policy:

```
config firewall policy
   edit 1
      set name "Internet Access"
      set srcintf "port10"
      set dstintf "port9"
      set srcaddr "all"
      set dstaddr "all"
```

```
        set action accept
        set schedule "always"
        set service "ALL"
        set fsso disable
        set nat enable
    next
end
```

2. Create the shared traffic shapers:

```
config firewall shaper traffic-shaper
    edit "10Mbps"
        set guaranteed-bandwidth 10000
        set maximum-bandwidth 20000
    next
    edit "1Mbps"
        set guaranteed-bandwidth 1000
        set maximum-bandwidth 10000
        set priority low
    next
end
```

3. Create a firewall shaping policy:

```
config firewall shaping-policy
    edit 1
        set name "VOIP_10Mbps_High"
        set service "H323" "IRC" "MS-SQL" "MYSQL" "RTSP" "SCCP" "SIP" "SIP-MSNmessenger"
        set dstintf "port9"
        set traffic-shaper "10Mbps"
        set traffic-shaper-reverse "10Mbps"
        set srcaddr "all"
        set dstaddr "all"
    next
    edit 2
        set name "Other_1Mbps_Low"
        set service "ALL"
        set dstintf "port9"
        set traffic-shaper "1Mbps"
        set traffic-shaper-reverse "1Mbps"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

To check the statuses of shared traffic shapers:

```
# diagnose firewall shaper traffic-shaper list
name 10Mbps
maximum-bandwidth 2500 KB/sec
guaranteed-bandwidth 1250 KB/sec
current-bandwidth 0 B/sec
priority 2
tos ff
packets dropped 0
bytes dropped 0

name 1Mbps
maximum-bandwidth 1250 KB/sec
guaranteed-bandwidth 125 KB/sec
```

```
current-bandwidth 0 B/sec
priority 4
tos ff
packets dropped 0
bytes dropped 0
```

Per-IP traffic shaper

With per-IP traffic shaping, you can limit each IP address's behavior to avoid a situation where one user uses all of the available bandwidth. In addition to controlling the maximum bandwidth used per IP address, you can also define the maximum number of concurrent sessions for an IP address. For example, if you apply a per-IP shaper of 1 Mbps to your entire network, FortiProxy allocates each user/IP address 1 Mbps of bandwidth. Even if the network consists of a single user, FortiProxy allocates them 1 Mbps. If there are ten users, each user gets 1 Mbps of bandwidth, totaling 10 Mbps of outgoing traffic.

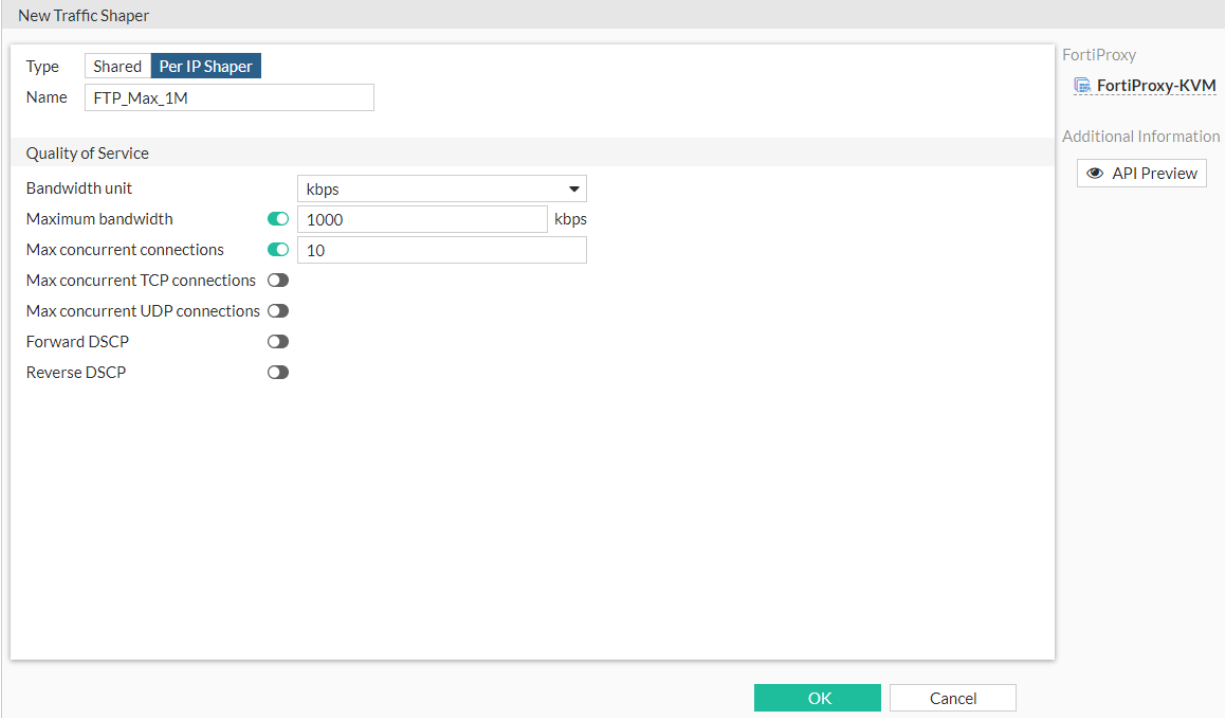
For shared shapers, all users share the set guaranteed and maximum bandwidths. For example, if you set a shared shaper for all PCs using an FTP service to 10 Mbps, all users uploading to the FTP server share the 10 Mbps.

Shared shapers affect upload speed. If you want to limit the download speed from the FTP server in the example, you must configure the shared shaper as a reverse shaper. Per-IP shapers apply the speed limit on both upload and download operations. Only traffic through forward traffic shapers will be included in FortiView; reverse and per-IP shapers are not included.

The following example shows how to apply a per-IP shaper to a traffic shaping policy. This shaper assigns each user a maximum bandwidth of 1 Mbps and allows each user to have a maximum of ten concurrent connections to the FTP server. In the example, FortiProxy communicates with users using port10 and the FTP server using port9.

To configure a per-IP traffic shaper in the GUI:

1. Create a firewall policy:
   a. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
   b. Set the *Name* to *FTP Access*.
   c. Set the *Incoming Interface* to *port10*.
   d. Set the *Outgoing Interface* to *port9*.
   e. Set the *Source* to *all*.
   f. Set the *Destination* to *FTP_Server*.
   g. Set the *Schedule* to *always*.
   h. Set the *Service* to *ALL*.
   i. Click *OK*.
2. Create the per-IP traffic shaper:
   a. Go to *Policy & Objects > Traffic Shaping*, select the *Traffic Shapers* tab, and click *Create New*.
   b. Set *Type* to *Per IP Shaper*.
   c. Enter the *Name* (*FTP_Max_1M*). This shaper is for VoIP traffic.
   d. Enable *Max Bandwidth* and enter *1000*.
   e. Enable *Max Concurrent Connections* and enter *10*. This means that each user can have up to ten concurrent connections to the FTP server.



f. Click *OK*.

3. Create a firewall shaping policy:
   a. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.
   b. Enter the *Name* (*FTP speed 1M*).
   c. Set the *Source* to the addresses and users that require access to the FTP server.
   d. Set the *Destination* to *FTP_Server*.
   e. Set the *Service* to *ALL*.
   f. Set the *Outgoing Interface* to *port9*.
   g. Enable *Per-IP shaper* and select *FTP_Max_1M*.
   h. Click *OK*.

To configure a per-IP traffic shaper in the CLI:

1. Create a firewall policy:

```
config firewall policy
   edit 1
      set name "FTP Access"
      set srcintf "port10"
      set dstintf "port9"
      set srcaddr "all"
      set dstaddr "FTP_Server"
      set action accept
      set schedule "always"
      set service "ALL"
      set fsso disable
      set nat enable
   next
```

```
   end
```

2. Create the per-IP traffic shaper:

```
config firewall shaper per-ip-shaper
   edit "FTP_Max_1M"
      set max-bandwidth 1000
      set max-concurrent-session 10
   next
end
```

3. Create a firewall shaping policy:

```
config firewall shaping-policy
   edit 1
      set name "FTP speed 1M"
      set service "ALL"
      set dstintf "port9"
      set per-ip-shaper "FTP_Max_1M"
      set srcaddr "PC1" "WinPC" "PC2"
      set dstaddr "FTP_Server"
   next
end
```

To check the status of a per-IP traffic shaper:

```
# diagnose firewall shaper per-ip-shaper list
```

The output should resemble the following:

```
name FTP_Max_1M
maximum-bandwidth 125 KB/sec
maximum-concurrent-session 10
tos ff/ff
packets dropped 0
bytes dropped 0
addr=10.1.100.11 status: bps=0 ses=3
```

Changing traffic shaper bandwidth unit of measurement

Bandwidth speeds are measured in kilobits per second (Kbps), and bytes that are sent and received are measured in megabytes (MB). In some cases, this can cause confusion depending on whether your ISP uses kilobits per second (Kbps), kilobytes per second (KBps), megabits per second (Mbps), or gigabits per second (Gbps).

You can change the unit of measurement for traffic shapers in the CLI.

To change the bandwidth unit of measurement for a shared traffic shaper:

```
config firewall shaper traffic-shaper
    edit <traffic_shaper_name>
        set bandwidth-unit {kbps | mbps | gbps}
    next
end
```

To change the bandwidth unit of measurement for a per-IP traffic shaper:

```
config firewall shaper per-ip-shaper
    edit <traffic_shaper_name>
        set bandwidth-unit {kbps | mbps | gbps}
    next
end
```

Multi-stage DSCP marking and class ID in traffic shapers

Traffic shapers have a multi-stage method so that packets are marked with a different differentiated services code point (DSCP) and `class id` at different traffic speeds. Marking packets with a different DSCP code is for the next hop to classify the packets. The FortiProxy benefits by marking packets with a different `class id`. Combined with the egress interface shaping profile, the FortiProxy can handle the traffic differently according to its `class id`.

Rule	DSCP code	Class ID
speed < guarantee bandwidth	`diffservcode`	`class id` in shaping policy
guarantee bandwidth < speed < exceed bandwidth	`exceed-dscp`	`exceed-class-id`
exceed bandwidth < speed	`maximum-dscp`	`exceed-class-id`

This example sets the following parameters:

- When the current bandwidth is less than 50 Kbps, mark packets with `diffservcode` 100000 and set `class id` to 10.
- When the current bandwidth is between 50 Kbps and 100 Kbps, mark packets with `exceed-dscp` 111000 and set `exceed-class-id` to 20.
- When the current bandwidth is more than 100 Kbps, mark packets with `maximum-dscp` 111111 and set `exceed-class-id` to 20.

To set multi-stage DSCP marking and class ID in a traffic shaper:

```
config firewall shaper traffic-shaper
    edit "50k-100k-150k"
        set guaranteed-bandwidth 50
        set maximum-bandwidth 150
        set diffserv enable
        set dscp-marking-method multi-stage
        set exceed-bandwidth 100
        set exceed-dscp 111000
        set maximum-dscp 111111
        set diffservcode 100000
    next
end
```

```
config firewall shaping-policy
     edit 1
         set service "ALL"
         set dstintf PORT2
         set srcaddr "all"
         set dstaddr "all"
         set class-id 10
     next
end
```

Traffic shapers also have an overhead option that defines the per-packet size overhead used in rate computation.

To set the traffic shaper overhead option:

```
config firewall shaper traffic-shaper
    edit "testing"
        set guaranteed-bandwidth 50
        set maximum-bandwidth 150
        set overhead 14 <range from 0 to 100>
    next
end
```

Example

This example shows how to mark QA traffic with a different DSCP according to real-time traffic speed.

To configure the firewall address:

```
config firewall address
    edit QA_team
        set subnet 10.1.100.0/24
    next
end
```

To configure the firewall shaper traffic shaper:

```
config firewall shaper traffic-shaper
    edit "500k-1000k-1500k"
        set guaranteed-bandwidth 500
        set maximum-bandwidth 1500
        set diffserv enable
        set dscp-marking-method multi-stage
        set exceed-bandwidth 1000
        set exceed-dscp 111000
        set maximum-dscp 111111
        set diffservcode 100000
    next
end
```

```
config firewall shaping-policy
    edit QA_team
        set service "ALL"
        set dstintf port1
        set traffic-shaper "500k-1000k-1500k"
        set traffic-shaper-reverse "500k-1000k-1500k"
        set srcaddr "QA_team"
        set dstaddr "all"
    next
end
```

DSCP marking in firewall shaping policies

Use the `diffserv-forward` and `diffserv-reverse` fields in firewall shaping policies to perform DSCP marking in firewall shaping policies to change the DSCP tag on egress traffic. Traffic is allowed or blocked according to the Differentiated Services Code Point (DSCP) values in the incoming packets. When DSCP marking on `firewall shaper traffic-shaper` and `firewall shaping-policy` both apply to the same session, `shaper traffic-shaper` overrides `shaping-policy`.

The following CLI variables in `config firewall shaping-policy` are used to mark the packets:

`diffserv-forward {enable | disable}`	Enable/disable changing a packet's DiffServ values to the value specified in `diffservcode-forward` (default = disable).
`diffservcode-forward <dscp_value>`	The value that packet's DiffServ is set to (default = 000000). This variable is only available when `diffserv-forward` is enabled.
`diffserv-reverse {enable | disable}`	Enable/disable changing a packet's reverse (reply) DiffServ values to the value specified in `diffservcode-rev` (default = disable).
`diffservcode-rev <dscp_value>`	The value that packet's reverse (reply) DiffServ is set to (default = 000000). This variable is only available when `diffserv-rev` is enabled.

Example

A FortiProxy has a traffic shaping policy to mark traffic from the QA team with a DSCP value of 100000, while reverse traffic is marked with 000011. To configure the FortiProxy:

```
config firewall shaping-policy
    edit 1
        set name "QA Team 50MB"
        set service "ALL"
        set dstintf "port3"
        set traffic-shaper "50MB/s"
        set traffic-shaper-reverse "50MB/s"
        set diffserv-forward enable
        set diffserv-reverse enable
        set srcaddr "QA"
```

```
        set dstaddr "all"
        set diffservcode-forward 100000
        set diffservcode-rev 000011
    next
end
```

Examples

This section includes the following traffic shaping configuration examples:

- Interface-based traffic shaping profile on page 454
- Ingress traffic shaping profile on page 459
- Traffic shaping based on HTTP response NEW on page 463

Interface-based traffic shaping profile

A traffic shaping policy can be used for interface-based traffic shaping by organizing traffic into 30 class IDs. The shaping profile defines the percentage of the interface bandwidth that is allocated to each class. Each traffic class ID is shaped to the assigned speed according to the outgoing bandwidth limit configured to the interface.

Traffic classification

A shaping policy classifies traffic and organizes it into different class IDs, based on matching criteria. For traffic matching a criteria, you can choose to put it into 30 different shaping classes, identified by class ID 2 to 31.

You must select an outgoing interface for the traffic. The shaping policy is only applied when the traffic goes to one of the selected outgoing interfaces.

Criterion	Description
Source	• Address: match the source address of the traffic to the selected address or address group. • User: use the user credentials of the traffic to match the selected user or user group. At least one address, address group, or internet service must also be selected. • Internet service: match the traffic to the selected internet service. Internet services cannot be used if addresses or address or groups are used.
Destination	• Address: match the destination address of the traffic to the selected address or address group. • Internet service: match the traffic to the selected internet service. Internet services cannot be used if addresses or address or groups are used.

Criterion	Description
Schedule	Match the current date and time to the selected schedule. You can select a one-time schedule, recurring schedule, or schedule group. This setting is optional.
Service	Match the service of the traffic to the selected service or service group.
Users	Match the user of the traffic.
Groups	Match the user group(s) of the traffic.



When multiple items are selected in one criterion, it is considered a match when traffic matches any one of them.

Traffic prioritization

Shaping profiles define how different shaping classes of traffic are prioritized. For each class, you can define three prioritization strategies: guaranteed bandwidth, maximum bandwidth, and priority.

For each shaping profile, a default shaping class must be defined. Traffic is prioritized based on the default shaping group in the following two circumstances:

- All traffic to the outgoing interface that does not match to any shaping policy
- Traffic with a shaping group that is not defined in a shaping profile

Prioritization strategy	Description
Guaranteed bandwidth	The percentage of the link speed that is reserved for the shaping group. The total guaranteed bandwidth for all shaping groups cannot exceed 100%.
Maximum bandwidth	The maximum percentage of the link speed that the shaping group can use.
Priority	The shaping class priority: top, critical, high, medium, or low. When groups are competing for bandwidth on the interface, the group with the higher priority wins.

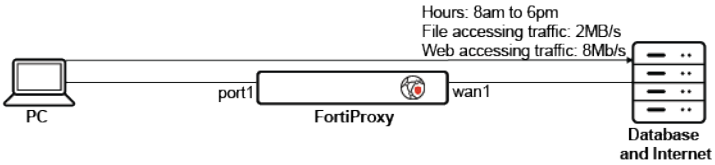
Applying a shaping profile to an interface

Traffic shaping is accomplished by configuring the outgoing bandwidth and outgoing shaping profile on an interface. The shaping profile uses the outgoing bandwidth of the interface as the maximum link speed, and it only works when the outgoing bandwidth is configured.

This example shows how to apply interface-based traffic shaping to web and file accessing traffic according to a schedule:

- The link speed of the wan1 interface is 10 Mb/s.
- File access can use up to 2 Mb/s from 8:00 AM to 6:00 PM.

- Web access can use 8 Mb/s from 8:00 AM to 6:00 PM.



Create a recurring schedule in the GUI

To create a recurring schedule in the GUI:

1. Go to *Policy & Objects* > *Schedules*.
2. Click *Create New* > *Schedule*.
3. Configure a recurring schedule called *Day_Hours* for everyday from 8:00 AM to 6:00 PM.
4. Click *OK*.

Putting the traffic into shaping classes

To create a traffic shaping policy and class ID for web accessing traffic in the GUI:

1. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.
2. Configure the policy by referring to Create or edit a traffic-shaping policy on page 436. Set *Service Type* to *Firewall Service* and select web accessing services under *Firewall Service*, such as *HTTP* and *HTTPS*. Set *Outgoing interface* to *wan1*.
3. Click *OK*.

To create a traffic shaping policy and class ID for the file accessing traffic in the GUI:

1. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.
2. Configure the policy by referring to Create or edit a traffic-shaping policy on page 436. Set *Service Type* to *Firewall Service* and select file accessing services under *Firewall Service*, such as *ASF3*, *FTP* and *SMB*. Set *Outgoing interface* to *wan1*.
3. Click the *Traffic shaping class ID* drop down then click *Create*.
4. Click *OK*.

To put the traffic into shaping classes in the CLI:

1. Create a recurring schedule:

```
config firewall schedule recurring
 edit "Day_Hours"
  set start 08:00
  set end 18:00
  set day sunday monday tuesday wednesday thursday friday saturday
 next
end
```

2. Create the traffic class IDs:

```
config firewall traffic-class
    edit 3
        set class-name "Web Access"
    next
    edit 4
        set class-name "File Access"
    next
end
```

3. Create the web and file accessing traffic shaping policies:

```
config firewall shaping-policy
    edit 2
        set name "web_access_day_hours"
        set comment "Limit web accessing traffic to 8Mb/s in day time"
        set service "HTTP" "HTTPS"
        set schedule "Day_Hours"
        set dstintf "wan1"
        set class-id 3
        set srcaddr "all"
        set dstaddr "all"
    next
    edit 3
        set name "file_access_day_hours"
        set comment "Limit file accessing traffic to 2Mb/s during the day"
        set service "AFS3" "FTP" "FTP_GET" "FTP_PUT" "NFS" "SAMBA" "SMB" "TFTP"
        set schedule "Day_Hours"
        set dstintf "wan1"
        set class-id 4
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

Allocating bandwidth to the shaping classes

A traffic shaping profile defines the guaranteed and maximum bandwidths each class receives. In this example, file access can use up to 2 Mb/s and web access can use 8 Mb/s.

To create a traffic shaping profile using the GUI:

1. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Profiles* tab, and click *Create New*.
2. Enter a name for the profile, such as *Day_Hours_Profile*.
3. Configure a default traffic shaping class:
   This class has a high priority, meaning that when the other classes have reached their guaranteed bandwidths, this default class will use the rest of the available bandwidth.

   a. Enter the class ID you specified in the *Putting the traffic into shaping classes* section.
   b. Configure the following settings, then click *OK*:

Guaranteed bandwidth	30
Maximum bandwidth	100
Priority	High

4. Configure a web accessing traffic shaping class:
   When other types of traffic are competing for bandwidth, this class is guaranteed to 6 Mb/s, or 60% of the bandwidth.
   a. In the *Traffic Shaping Classes* table click *Create New*.
   b. Configure the following settings, then click *OK*:

Traffic shaping class ID	Web Access
Guaranteed bandwidth	60
Maximum bandwidth	80
Priority	Medium

5. Configure a file accessing traffic shaping class:
   When other types of traffic are competing for bandwidth, this group is guaranteed to 1 Mb/s, or 10% of the bandwidth.
   a. In the *Traffic Shaping Classes* table click *Create New*.
   b. Configure the following settings, then click *OK*:

Traffic shaping class ID	File Access
Guaranteed bandwidth	10
Maximum bandwidth	20
Priority	Medium

6. Click *OK*.

To create a traffic shaping profile using the CLI:

```
config firewall shaping-profile
    edit "Day_Hours_Profile"
        set default-class-id 2
        config shaping-entries
            edit 1
                set class-id 2
                set guaranteed-bandwidth-percentage 30
                set maximum-bandwidth-percentage 100
            next
            edit 2
                set class-id 3
                set priority medium
                set guaranteed-bandwidth-percentage 60
```

```
                set maximum-bandwidth-percentage 80
            next
            edit 3
                set class-id 4
                set priority medium
                set guaranteed-bandwidth-percentage 10
                set maximum-bandwidth-percentage 20
            next
        end
    next
end
```

Defining the available bandwidth on an interface

In this example, the link speed of the wan1 interface is 10 Mb/s.

To set the bandwidth of the wan1 interface in the GUI:

1. Go to *Network > Interfaces*.
2. Edit the wan1 interface.
3. Under Traffic Shaping, enable *Outbound shaping profile* and select the profile that you just created, *Day_Hours_Profile*.
4. Enable *Outbound Bandwidth* and set it to *10000* Kbps.
5. Click *OK*.

To set the bandwidth of the wan1 interface in the CLI:

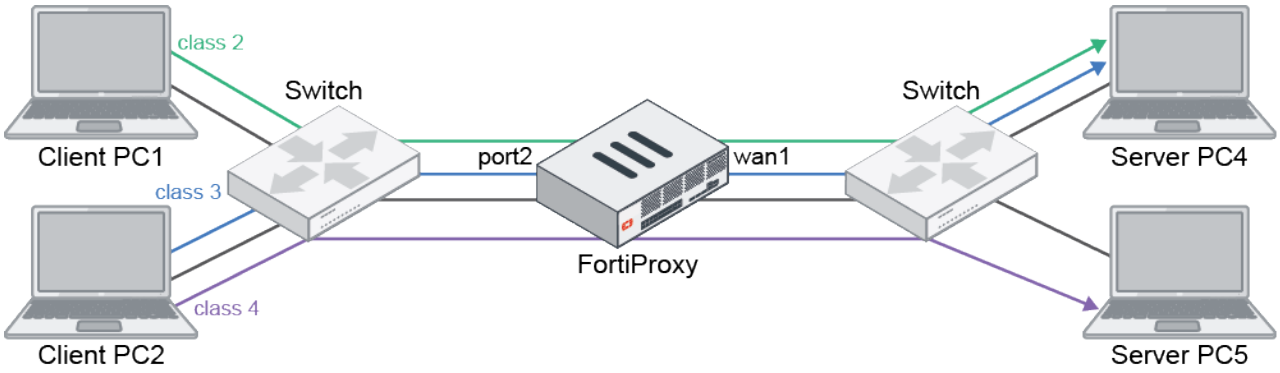
```
config system interface
    edit "wan1"
        set egress-shaping-profile "Day_Hours_Profile"
        set outbandwidth 10000
    next
end
```

Ingress traffic shaping profile

A traffic shaping profile can be applied to an interface for traffic in the ingress direction. Similar to an egress traffic shaping profile, the guaranteed bandwidth and priority of the profile will be respected when an interface receives inbound traffic. When congestion occurs, any remaining bandwidth will be allotted to classes based on priority.

Example

In this example, the port2 interface has a total inbound bandwidth of 100 Mbps. Traffic from certain clients to certain servers are assigned different classes.



IPv6 traffic from any client PCs to server PCs is assigned class 5.

For each class, the priority, guaranteed bandwidth, and maximum bandwidth are as follows:

Class	Priority	Guaranteed bandwidth	Maximum bandwidth
2	Low	10%	60%
3	High	20%	100%
4	High	30%	100%
5	Medium	10%	50%

Bandwidth will first be allotted to each class according to its guaranteed bandwidth. Then remaining available bandwidth will be allotted to class 3 and 4 first based on their priority. The allocation will be proportional to their guaranteed bandwidth ratio.

To configure ingress traffic shaping:

1. Configure the client and server addresses:

```
config firewall address
    edit "pc1"
        set subnet 10.1.100.11 255.255.255.255
    next
    edit "pc2"
        set subnet 10.1.100.22 255.255.255.255
    next
    edit "pc4"
        set subnet 172.16.200.44 255.255.255.255
    next
    edit "pc5"
        set subnet 172.16.200.55 255.255.255.255
    next
end
```

2. Configure the class IDs:

```
config firewall traffic-class
    edit 2
        set class-name "class2"
```

```
    next
    edit 3
        set class-name "class3"
    next
    edit 4
        set class-name "class4"
    next
    edit 4
        set class-name "class5"
    next
end
```

3. Configure traffic shaping policies to assign classes to each group of traffic.
   a. Configure a policy to assign traffic from PC1 to PC4 in class 2:

```
config firewall shaping-policy
    edit 1
        set name "shaping policy 1"
        set service "ALL"
        set dstintf "wan1"
        set class-id 2
        set srcaddr "pc1"
        set dstaddr "pc4"
    next
end
```

   b. Configure a policy to assign traffic from PC2 to PC4 in class 3:

```
config firewall shaping-policy
    edit 2
        set name "shaping policy 2"
        set service "ALL"
        set dstintf "wan1"
        set class-id 3
        set srcaddr "pc2"
        set dstaddr "pc4"
    next
end
```

   c. Configure a policy to assign traffic from PC2 to PC5 in class 4:

```
config firewall shaping-policy
    edit 3
        set name "shaping policy 3"
        set service "ALL"
        set dstintf "wan1"
        set class-id 4
        set srcaddr "pc2"
        set dstaddr "pc5"
    next
end
```

d. Configure a policy to assign all IPv6 traffic to class 5:

```
config firewall shaping-policy
    edit 4
        set name "shaping policy 4"
        set ip-version 6
        set service "ALL"
        set dstintf "wan1"
        set class-id 5
        set srcaddr6 "all"
        set dstaddr6 "all"
    next
end
```

4. Configure a shaping profile to set the priority, and the guaranteed and maximum bandwidth percentages for each class:

```
config firewall shaping-profile
    edit "ingShapeProfile"
        set default-class-id 2
        config shaping-entries
            edit 2
                set class-id 2
                set priority low
                set guaranteed-bandwidth-percentage 10
                set maximum-bandwidth-percentage 60
            next
            edit 3
                set class-id 3
                set guaranteed-bandwidth-percentage 20
                set maximum-bandwidth-percentage 100
            next
            edit 4
                set class-id 4
                set guaranteed-bandwidth-percentage 30
                set maximum-bandwidth-percentage 100
            next
            edit 5
                set class-id 5
                set priority medium
                set guaranteed-bandwidth-percentage 10
                set maximum-bandwidth-percentage 50
            next
        end
    next
end
```

5. Configure the inbandwidth and apply the ingress shaping profile on port2:

```
config system interface
    edit "port2"
        set ip 10.1.100.1 255.255.255.0
        set inbandwidth 100000
```

```
        set ingress-shaping-profile "ingShapeProfile"
        config ipv6
            set ip6-address 2000:10:1:100::1/64
        end
    next
end
```

Inbandwidth must be configured for traffic shaping to take effect.

6. Configure firewall policies to allow IPv4 and IPv6 traffic to go through. Since traffic shaping is for inbound traffic on port2, the policy is defined from port2 to wan1:

```
config firewall policy
    edit 20
        set uuid d9f9be4c-eaab-51ed-41d6-783cecc11c0c
        set srcintf "port2"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

```
config firewall policy
    edit 21
        set uuid c535a92a-eaac-51ed-6e6c-3943f8c2dc8f
        set srcintf "port2"
        set dstintf "wan1"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

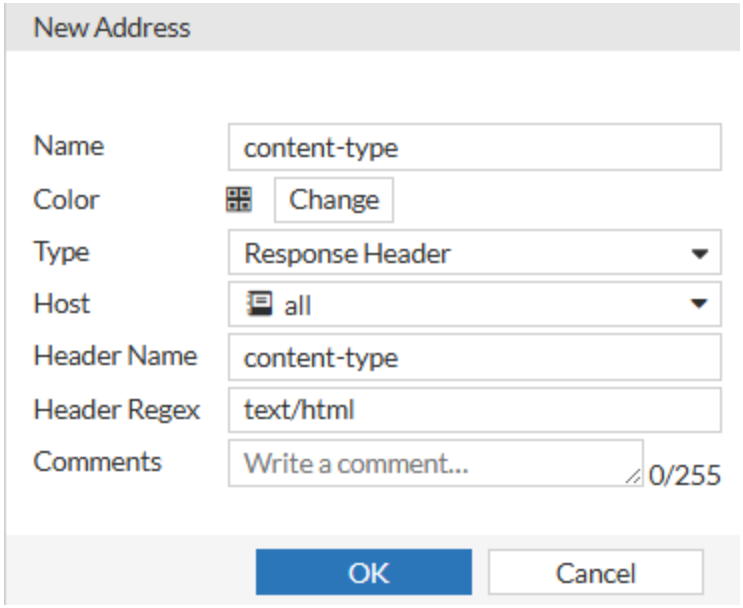
Traffic shaping based on HTTP response NEW

You can configure traffic shaping based on HTTP response by configuring a proxy address of the *Response Header* type, enabling *Http Response Match* in the traffic shaping policy, and then creating a response shaping policy that defines the overriding shaping behavior (for matching traffic) and references the proxy address.

Example

The following configuration example assigns high priority to traffic with the HTTP header "content-type" field set to "text/html":

1. Create a proxy address of the *Response Header* type with the header set to "text/html":
   a. Go to *Policy & Objects* > *Addresses*.
   b. In the *Proxy* tab, click *Create New* > *Address*.
   c. Set the following:
      - *Name* to *content-type*,
      - *Type* to *Response Header*,
      - *Host* to *all*,
      - *Header Name* to *content-type*
      - *Header Regex* to *text/html*.



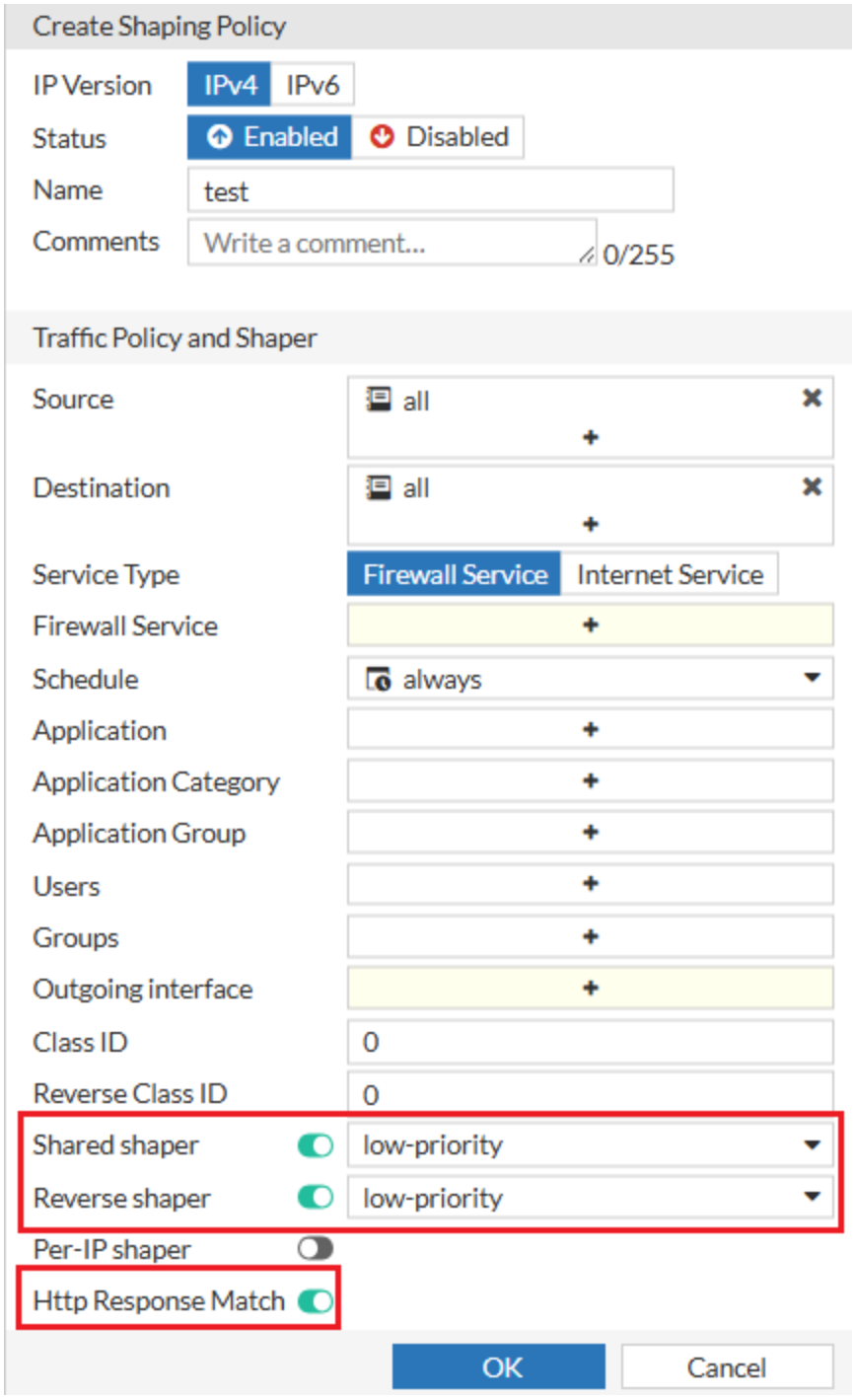
   d. Click *OK*.

   Alternatively, use the following command in the CLI:

```
config firewall proxy-address
   edit "content-type"
      set uuid adcb49a0-05aa-51f0-f432-5740ef86a4a4
      set type response-header
      set host "all"
      set header-name "content-type"
      set header "text/html"
   next
end
```

2. Enable the new *Http Response Match* option in your traffic shaping policy to enable matching HTTP response shaping policies. Note that the traffic shaping policy uses the low priority shapers.
   a. Go to *Policy & Objects* > *Traffic Shaping*.
   b. In the *Traffic Shaping Policies* tab, click *Create New* .
   c. Set the following:
      - *Name* to *test*,
      - *Source* to *all*,
      - *Destination* to *all*
      - *Shared shaper* to *low priority*.

- *Reverse shaper* to *low priority*.
- *Http Response Match* to *Enable*.



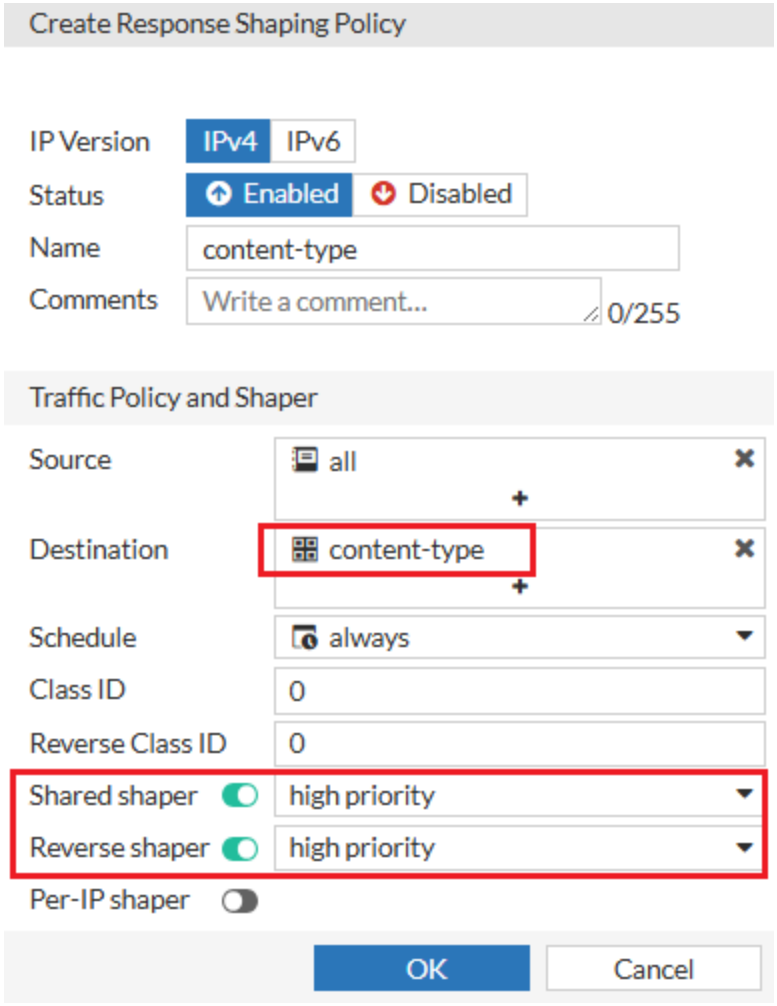
d. Click *OK*.

Alternatively, use the following command option in the CLI:

```
config firewall shaping-policy
   edit 2
      set uuid 8c299866-04e6-51f0-a1e2-8f76f7856ab0
      set dstaddr "all"
```

```
        set service "all"
        set http-response-match enable
        set dstintf "any"
        set traffic-shaper "low-priority"
        set per-ip-shaper "low-priority"
        set srcaddr "all"
    next
end
```

3. Create a response shaping policy to define the shaping behavior and reference the response header address (you created in step 1) in destination address. Note that the response shaping policy uses the high priority shapers.
   a. Go to *Policy & Objects* > *Traffic Shaping*.
   b. In the *Response Shaping Policies* tab, click *Create New* .
   c. Set the following:
      - *Name* to *content-type*,
      - *Source* to *all*,
      - *Destination* to *content-type*
      - *Shared shaper* to *high priority*.
      - *Reverse shaper* to *high priority*.



d. Click *OK*.

Alternatively, use the following new command in the CLI:

```
config firewall response-shaping-policy
   edit content-type
      set uuid a0edf572-0378-51f0-f0f6-8f924dccfd53
      set dstaddr "content-type"
      set traffic-shaper "high-priority"
      set traffic-shaper-reverse "high_priority"
      set srcaddr "all"
   next
end
```

Sample debug output for a successful match:

```
HTTP/1.1 204 No Content
Date: Thu, 10 Apr 2025 18:36:56 GMT
Content-Type: text/html
Server: HTTP server (unknown)
X-XSS-Protection: 0
[V][p:1240][s:2][r:3] __wad_hauth_user_node_hold :2741 wad_http_resp_shaping_policy_init (12818):
      holding node 0x7f93ebc3a310
[I][p:1240][s:2][r:3] wad_http_policy_match_one :538 fw_pol_id=1(pol_ctx:th|Ad|7|=p) pflag:H|W|U|A
      asyn_info=1
[I][p:1240][s:2][r:3] wad_fw_policy_async_match :6820 pol_ctx:th|Ad|7|=d
[V][p:1240][s:2][r:3] wad_http_resp_setup_shaping_policy:12567 Newly matched response shaping policy
      1
[V][p:1240][s:2][r:3] __wad_hauth_user_node_put :2752 wad_fw_pol_async_ctx_close (6030): putting
      node(ref=4) 0x7f93ebc3a310
[V][p:1240][s:2][r:3] wad_shaper_results__update :260 applying response shaping policy=1 priority=0
      uuid=16557
[I][p:1240][s:2][r:3] wad_apply_shared_shaper :740 apply shared shaper high-priority(forward) and
      <none> (reverse) uuid 16557
[I][p:1240][s:2][r:3] wad_redirect_init_tuple :621 init tuple: 10.120.1.1:54947 -> 10.120.1.209:8080
[I][p:1240][s:2][r:3] wad_apply_shared_shaper :740 apply shared shaper high-priority(forward) and
      <none> (reverse) uuid 16557
[I][p:1240][s:2][r:3] wad_redirect_init_tuple :621 init tuple: 10.120.1.209:52250 ->
      142.251.33.110:80
[I][p:1240][s:2][r:3] wad_http_fwd_non_cacheable_resp :2867 resp(0x7f93ec3937f0) starts processing.
```

Sample event log

```
date=2025-04-10 time=11:51:54 eventtime=1744311114101621457 tz="-0700" logid="0000000010"
      type="traffic" subtype="forward" level="notice" vd="root" srcip=10.120.1.1 srcport=55458
      srcintf="port1" srcintfrole="undefined" dstcountry="United States" srccountry="Reserved"
      dstip=142.251.33.110 dstport=80 dstintf="port1" dstintfrole="undefined" sessionid=6
      service="HTTP" proxyapptype="web-proxy" proto=6 action="accept" policyid=14 policytype="proxy-
      policy" poluuid="af600584-13de-51f0-c3a4-da80c372aaac" trandisp="snat" transip=10.120.1.209
      transport=56226 clientip=10.120.1.1 appcat="unscanned" duration=1 wanin=141 rcvdbyte=141
      wanout=98 lanin=121 sentbyte=121 lanout=141 shapersentname="high-priority"
      shaperdropsentbyte=0 shaperrcvdname="high-priority" shaperdroprcvdbyte=0
```

Isolator Setting

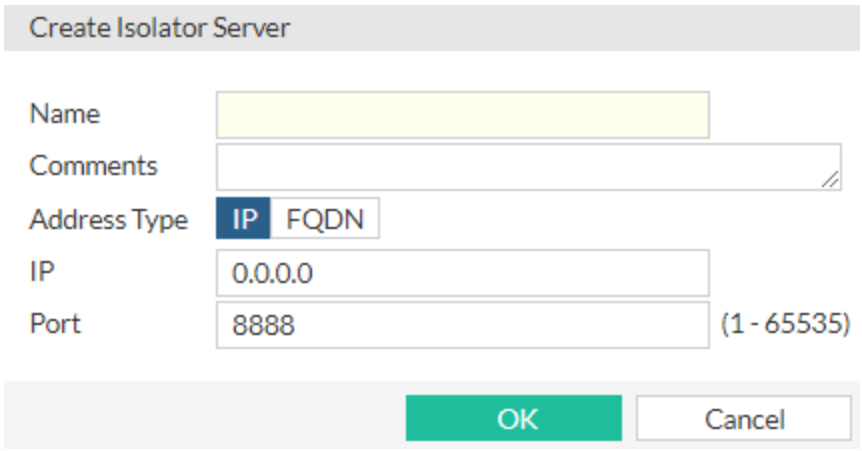
Configure an isolator server, profile, or setting:

- Servers on page 468
- Profiles on page 469
- Setting on page 470

.

Servers

Configure an isolator server for the FortiProxy to forward isolation requests to.



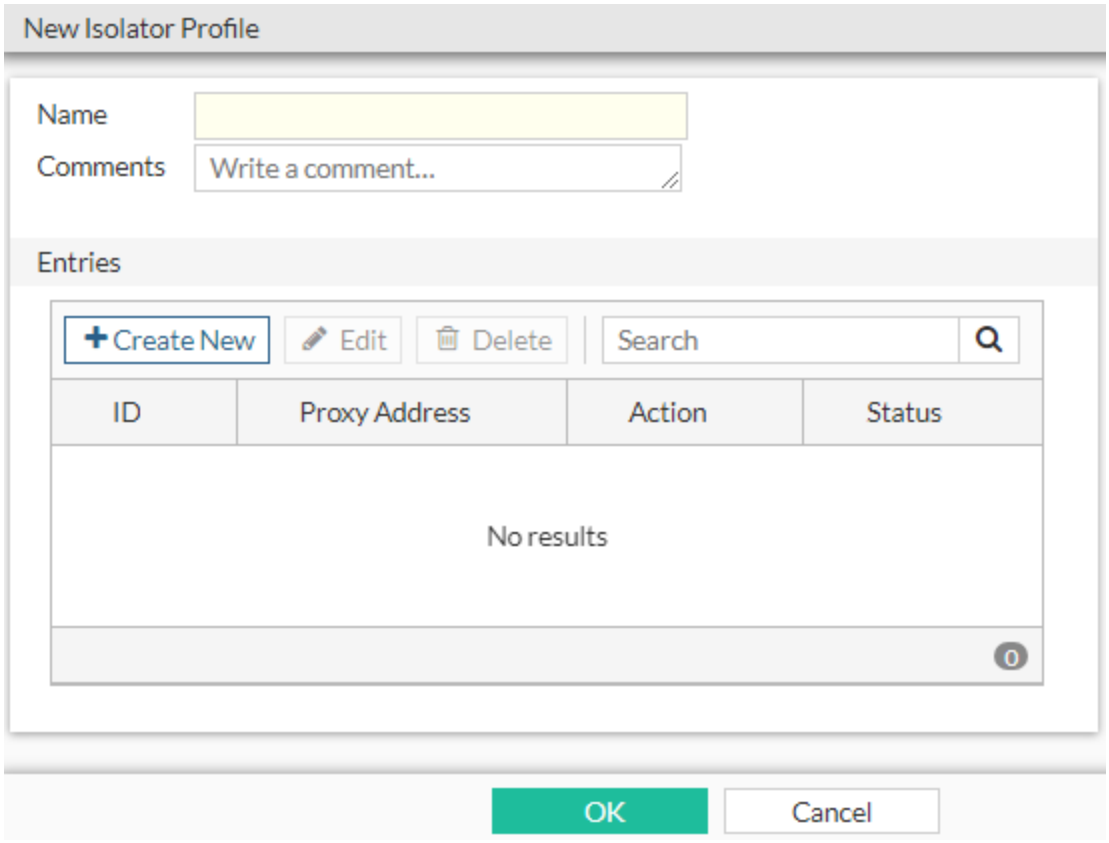
To configure an isolator server in the GUI, go to *Policy & Objects* > *Isolator Setting* > *Servers*, select an existing isolator server and then click *Edit* or click *Create New* to create a new one. Configure the following options, and click *OK*.

Name	Enter the name of the isolator server.
Comments	Enter an optional description of the isolator server.
Address Type	Select the type of isolator server address, either *IP* or *FQDN*.
IP	If you selected *IP* for the address type, enter the IP address of the isolator server.
FQDN	If you selected *FQDN* for the address type, enter the fully qualified domain name of the isolator server.
Port	Enter the port number of the isolator server.

To configure an isolator server in the CLI, use the `config web-proxy isolator-server` command.

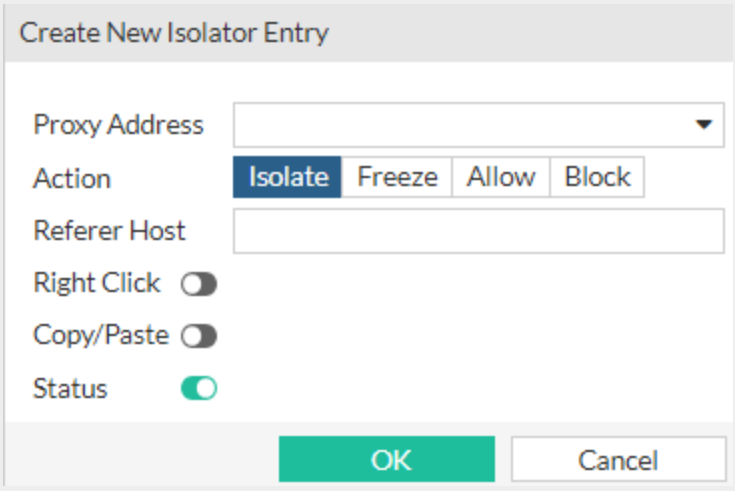
Profiles

Configure an isolator profile to define the isolation behavior.



To configure an isolator profile in the GUI, go to *Policy & Objects* > *Isolator Setting* > *Profiles*, select an existing isolator profile and then click *Edit* or click *Create New* to create a new one. Configure the following options, and click *OK*.

Name	Enter the name of the isolator profile.
Comments	Enter an optional description of the isolator profile.
Entries	Select an existing entry and click *Edit* or click *Create New* to create a new one. Configure the following options and click *OK*:

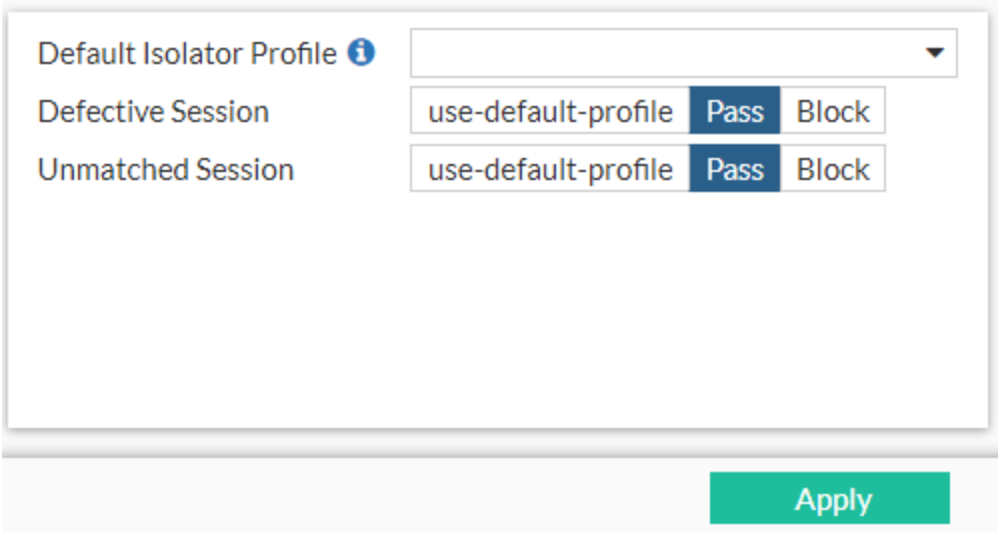


Proxy Address	Select the proxy address for this isolator profile entry.
Action	Select the action for this isolator entry: • **Isolate**—Open the website in an isolator instead of the client. • **Freeze**—Freeze the website. The user is able to unfreeze and get access to the website when they accept the risk. • **Block**—Block the traffic to the website. • **Allow**—Bypass the traffic to the website.
Referer Host	Host of the referer.
Right Click	Specifies whether to allow client users to right click on mouse to display a menu.
Copy/Paste	Specifies whether to allow client users to copy and paste from keyboard.
Status	Enable/disable this isolator entry.

To configure an isolator profile in the CLI, use the `config isolator profile` command.

Setting

Configure the default isolator profile and/or configure the action to perform on rating requests for isolator sessions that do not match any existing policies (unmatched-session) or have missing information (defective-session).



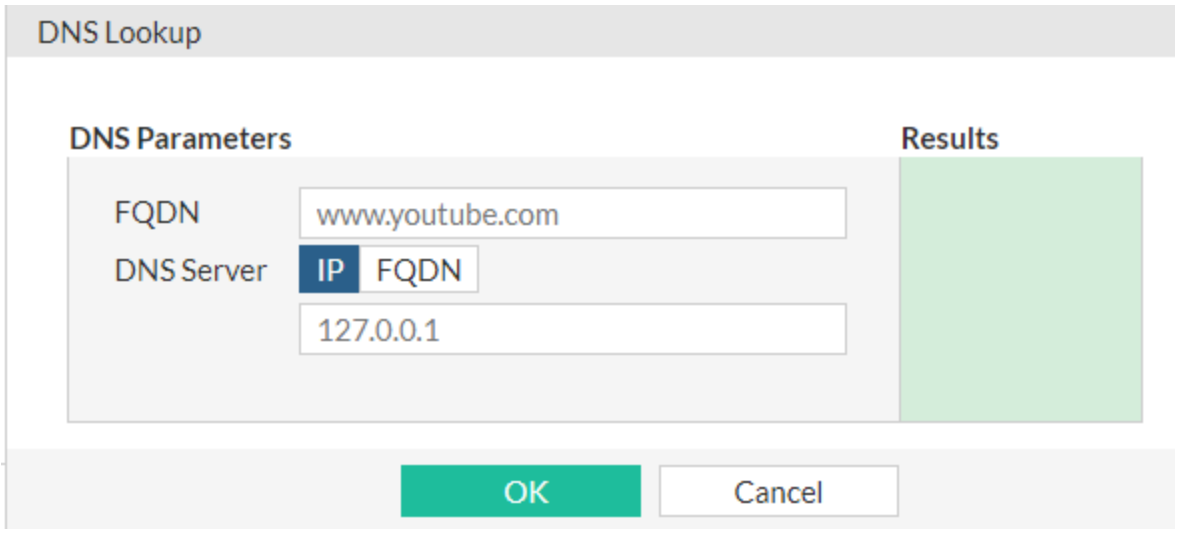
To configure isolator settings in the GUI, go to *Policy & Objects* > *Isolator Setting* > *Setting*, configure the following options, and click *Apply*.

Default Isolator Profile	Select a profile that will used when no policy is matched. You can select an existing isolator profile from the list or create a new one. By default, no profile is selected.
Defective Session	Select the action to perform on rating requests for isolator sessions that do not match any existing policies. • Use the action defined in the default isolator profile. • Bypass defective sessions • Block defective sessions
Unmatched Session	Select the action to perform on rating requests for isolator sessions that have missing information. • Use the action defined in the default isolator profile. • Bypass unmatched sessions • Block unmatched sessions

To configure isolator settings in the CLI, use the `config isolator setting` command.

DNS Lookup

You can check the associated IPs (20 entries maximum) for a specific domain (FQDN) on a specific DNS server.



To view the associated IPs for a domain on a specific DNS server:

1. Go to *Policy & Objects* > *DNS Lookup*
2. Configure the following settings:

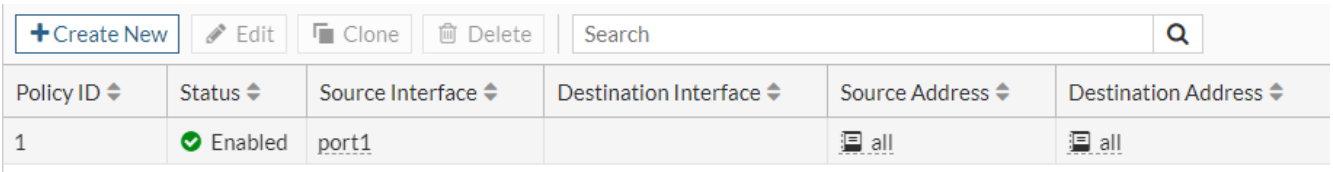
FQDN	Enter the domain name.
DNS Server	Select *IP* or *FQDN* and enter the source IP address or domain of the DNS server for which you want to check the associated IPs.

3. Click *OK*. The results show the associated IPs for the specified domain on the specified DNS server.

Central SNAT

NAT is a process used to modify or translate either the source or destination IP address or port in a packet header. The primary use for NAT is to allow multiple network devices on a private network to be represented by a single public IP address when they browse the Internet.

The FortiProxy unit applies the NAT settings from matching central Source Network Address Translation (SNAT) policies. Go to *Policy & Objects* > *Central SNAT* to create a central SNAT policy.



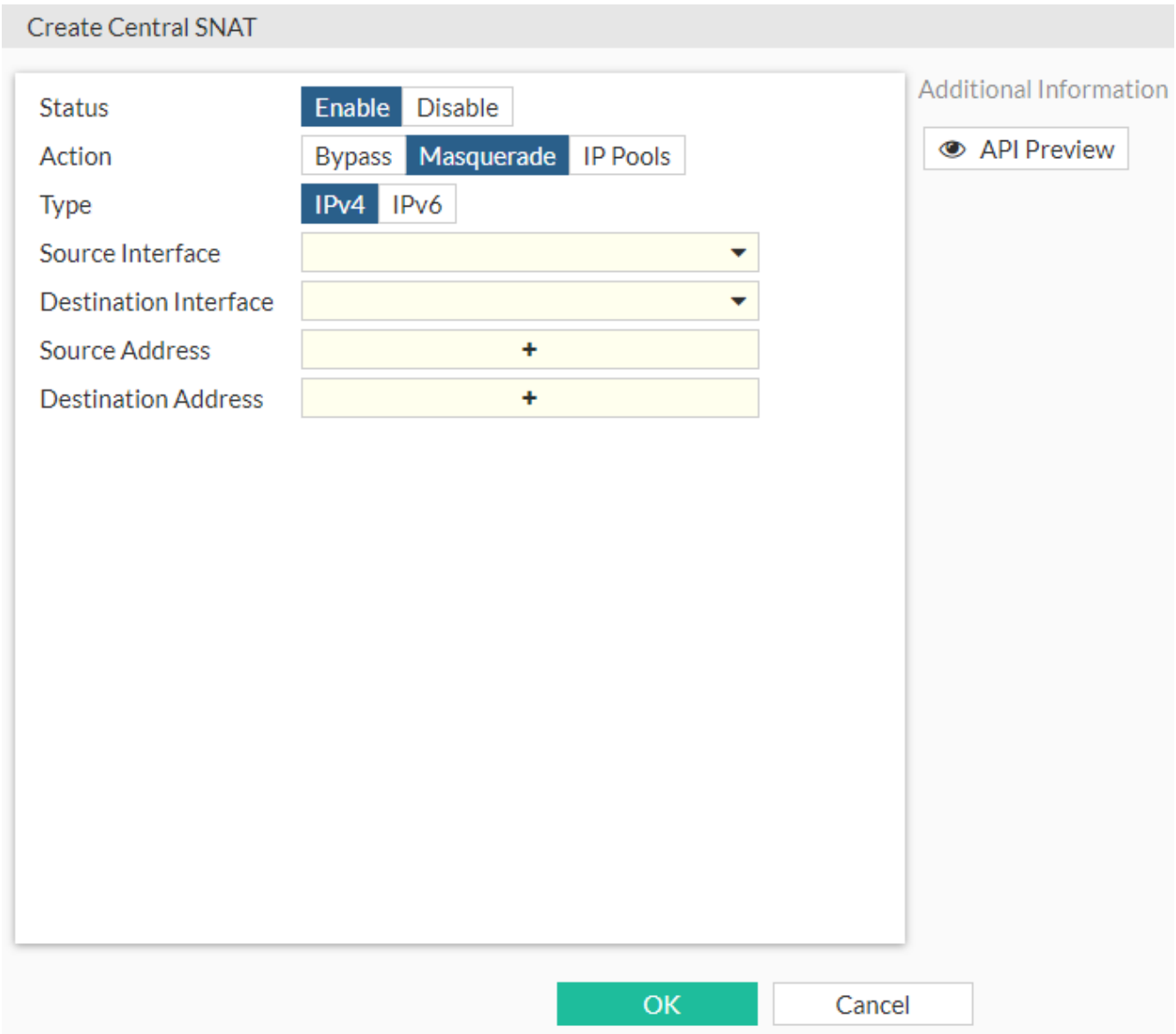
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Select to open the *Create Central SNAT* window. See Create or edit a central SNAT policy on page 473.
Edit	Edit the selected central SNAT policy. See Create or edit a central SNAT policy on page 473.
Clone	Copy an existing central SNAT policy.
Delete	Delete the selected central SNAT policy.
Search	Enter a search term to find in the list.
Policy ID	SNAT identifier.
Status	The status is either *enable* (active) or *disable* (inactive).
Source Interface	The source interface name is either a port or *any*.
Destination Interface	The destination interface name.
Source Address	The source addresses and address groups.
Destination Address	The destination addresses and address groups.
Action	The central SNAT action is *Bypass*, *Masquerade*, or *IP Pools*.
nat-ippool	The name of the NAT IP pool.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a central SNAT policy

Select *Create New* to open the *Create Central SNAT* window. To change a central SNAT policy, select the policy and then click *Edit*.



Configure the following settings in the *Create Central SNAT* window or the *Edit Central SNAT* window and then click *OK*:

Status	Select *Enable* make the central SNAT policy is active.
Action	Select one of the following options for the central SNAT action: • *Bypass*—Do not perform network address translation (NAT). • *Masquerade*—Use a single IP address to protect multiple IP addresses in a LAN. • *IP Pools*—Use an IP address from an IP pool. An IP pool defines a single IP address or a range of IP addresses to be used as the source address for the duration of the session. These assigned addresses are used instead of the IP address assigned to that FortiProxy interface.

Type	Select *IPv4* or *IPv6*.
Source Interface	Select one of the available interfaces from the drop-down list.
Destination Interface	Select one of the available interfaces from the drop-down list.
Source Address **Source IPv6 Address**	Click +. A window slides out from the right. Here, you can select from the available addresses and address groups. Select one or more items to add to the field. Clicking on an object in this window while it is highlighted removes it from the field. Multiple selections are allowed. For more information on addresses, see Addresses on page 483.
Destination Address **Destination IPv6 Address**	Click +. A window slides out from the right. Here, you can select from the available addresses and address groups. Select one or more items to add to the field. Clicking on an object in this window while it is highlighted removes it from the field. Multiple selections are allowed. For more information on addresses, see Addresses on page 483.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

To create a central SNAT policy in the CLI:

```
config firewall central-snat-map
   edit <policy_identifier>
      set status {enable | disable}
      set action {bypass | masquerade | ippool}
      set ipv6 {enable | disable}
      set srcintf <source_interface_name>
      set dstintf <destination_interface_name>
      set src-addr <original_address>
      set dst-addr <original_address>
   end
```

For example, to create an IPv4 central SNAT policy:

```
config firewall central-snat-map
   edit 1
      set status enable
      set action masquerade
```

```
      set ipv6 disable
      set srcintf port2
      set dstintf port1
      set src-addr "all"
      set dst-addr "all"
   end
```

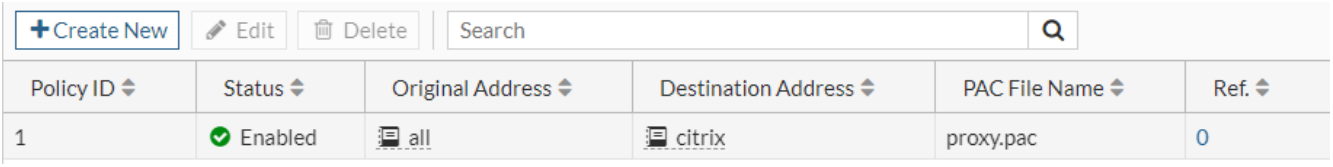
For example, to create an IPv6 central SNAT policy:

```
config firewall central-snat-map
   edit 1
      set status enable
      set action ippool
      set ipv6 enable
      set srcintf port1
      set dstintf port3
      set src-addr6 "all"
      set dst-addr6 "all"
      set nat-ippool6 "pool6"
   end
```

PAC Policy

Proxy auto-config (PAC) files automatically choose the appropriate proxy server for browsers and other user agents. Not every user in an organization has the same proxy server requirements. Supporting multiple PAC files provides granular control. To manage multiple PAC files, you use PAC policies.

To see a list of available PAC policies in the GUI, go to *Policies & Objects* > *PAC Policy*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

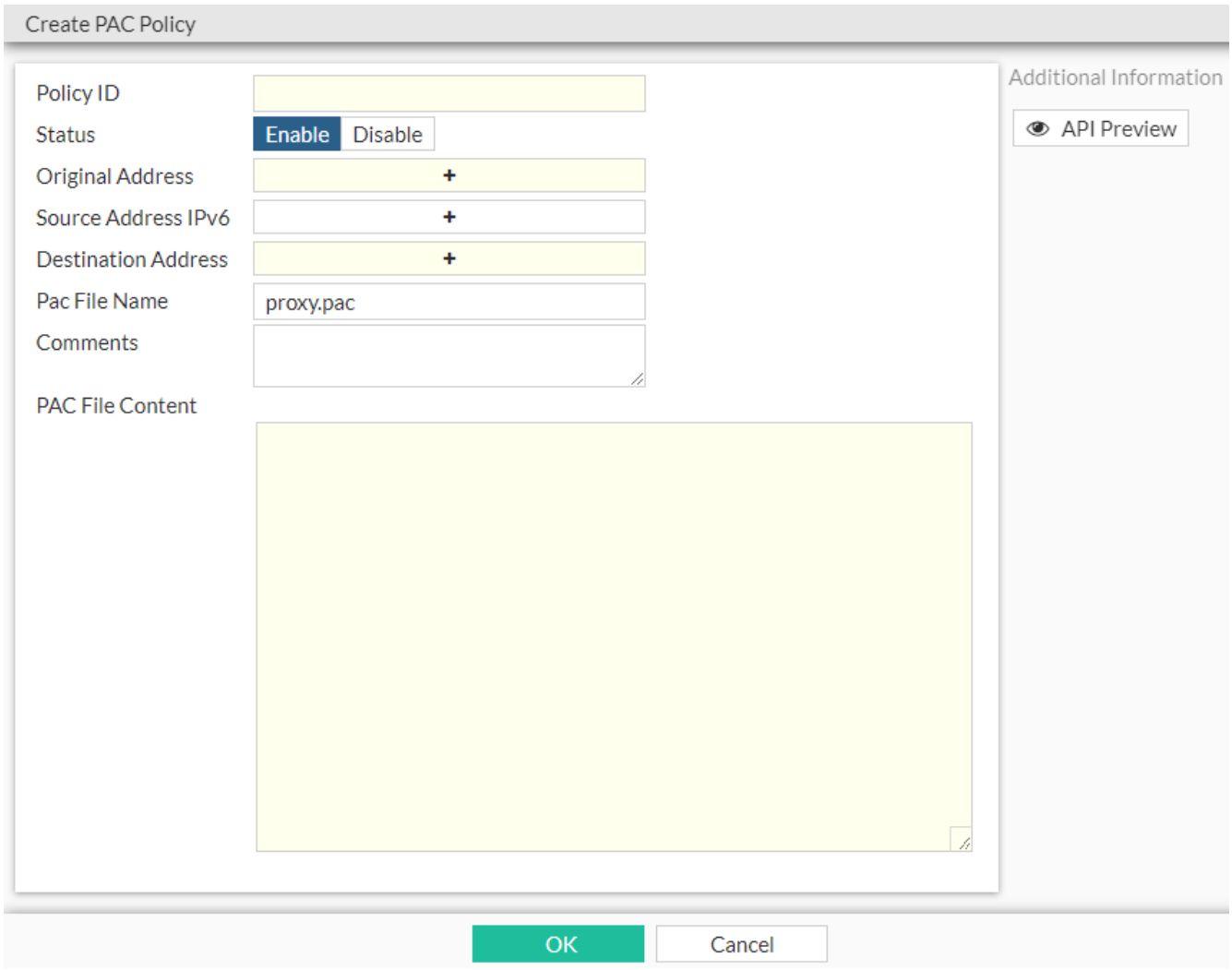
The following options are available:

Create New	Select to open the *Create PAC Policy* window. See Create or edit a PAC policy on page 477.
Edit	Edit the selected PAC policy. See Create or edit a PAC policy on page 477.
Delete	Delete the selected PAC policy.
Search	Enter a search term to find in the list.

Policy ID	The PAC policy identifier.
Status	The status is enabled or disabled.
Original Address	The source address of the initiating traffic.
Destination Address	The destination address that the policy matches.
PAC File Name	The name of the PAC file.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a PAC policy

Select *Create New* to open the *Create PAC Policy* window. To change a PAC policy, select a policy and then click *Edit*.



Configure the following settings in the *Create PAC Policy* window or the *Edit PAC Policy* window and then click *OK*:

Policy ID	Enter the PAC policy identifier.
Status	Click *Enable* to make the policy active.
Original Address	Enter the source IPv4 address of the initiating traffic.
Source Address IPv6	Enter the source IPv6 address of the initiating traffic.
Destination Address	Enter the destination address that the policy matches.
Pac File Name	Enter the name of the PAC file.
Comments	Enter an optional description of the PAC policy.
PAC File Content	Type or copy and paste a PAC file.

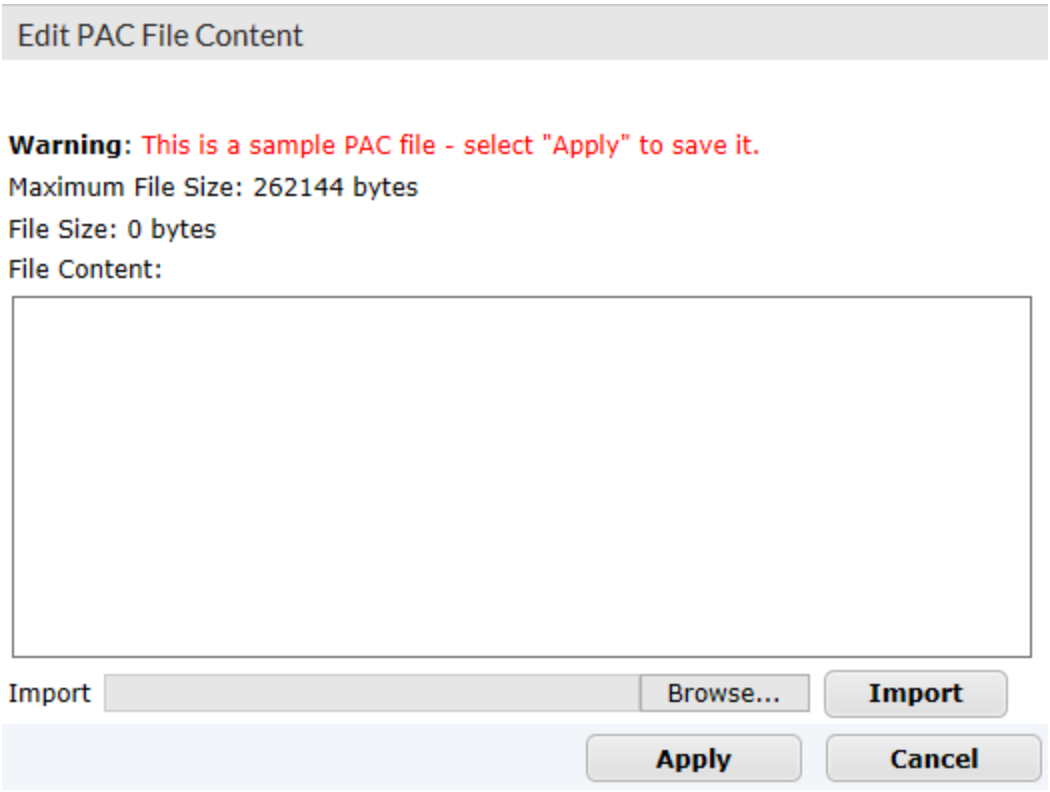
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Edit a PAC file

In the Create PAC Policy window or Edit PAC Policy window, click *Edit* to open the *Edit PAC File Content* window.



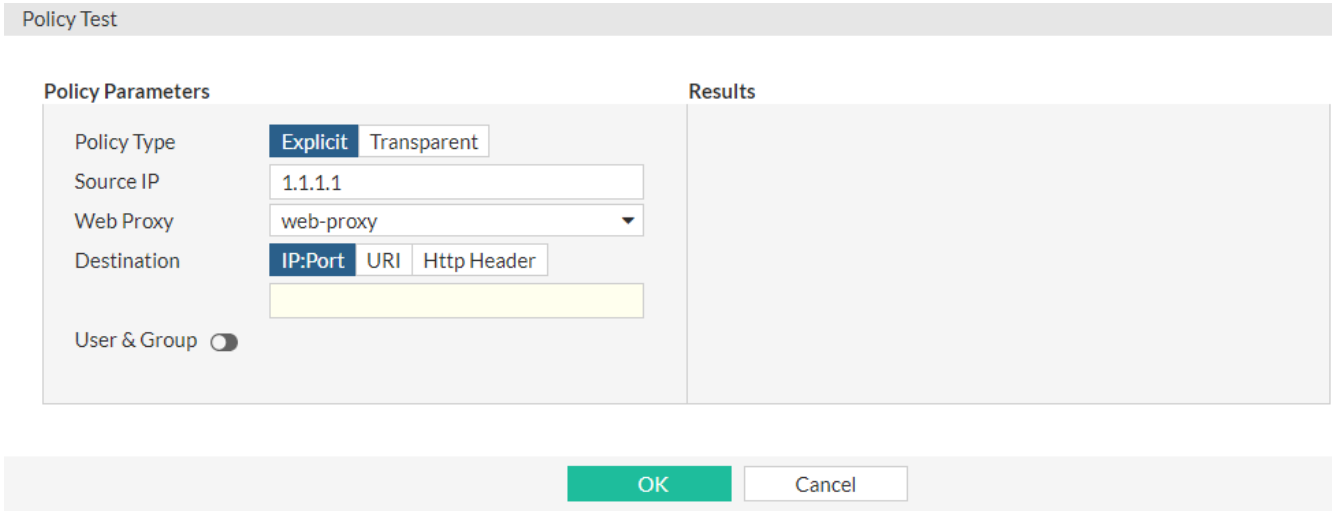
To add content to a PAC file:

1. If you have a PAC file, select *Browse*, navigate to the PAC file, select *Open,* and then select *Import*. After you import the PAC file, you can edit the content in the text box.

2. If you do not have a PAC file, you can type the content into the text box or copy and paste the content into the text box.
3. Click *Apply*.

Policy Test

You can check the configuration of explicit web proxy policies and transparent firewall policies to confirm that they are set up correctly.



The combination of policy type and source IP address forms the source traffic to test.

If a URI or HTTP header is specified as the destination, the policy test uses a DNS lookup to determine the actual IP address and port number of the destination traffic. If the client's DNS lookup differs from the device's DNS lookup, the policy used for the test might be different that the policy used on the client's traffic.

To test a policy:

1. Go to *Policy & Objects* > *Policy Test*.
2. Configure the following settings:

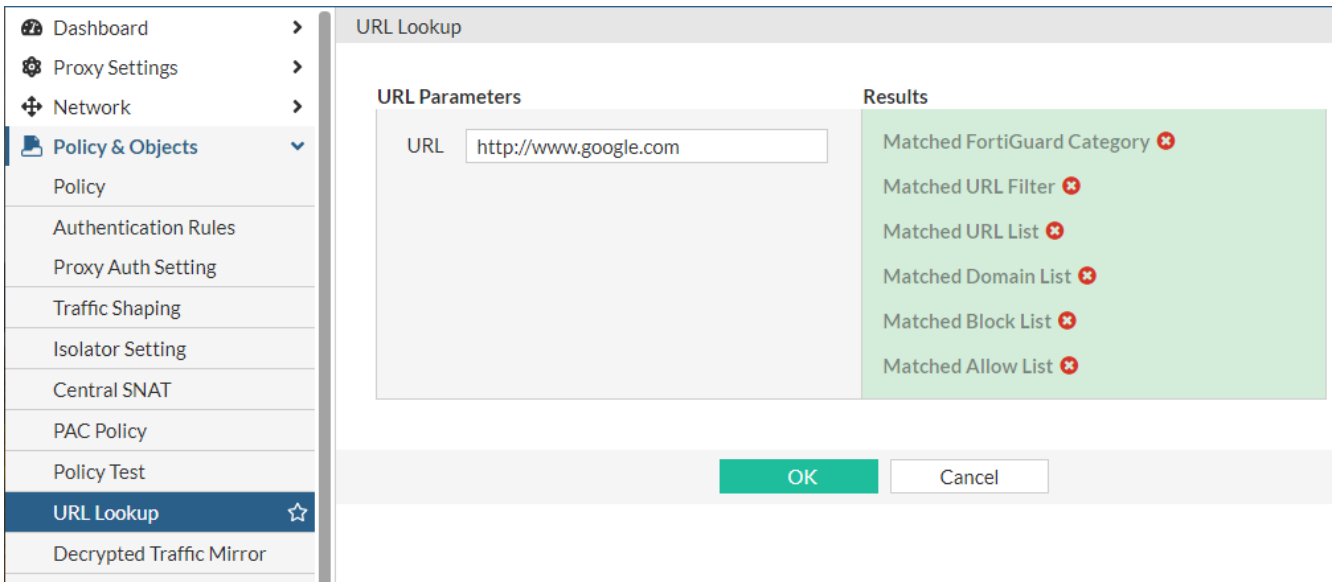
Policy Test	Select whether you want to test an *Explicit* or *Transparent* policy.
Source IP	Enter the source IP address.
Web Proxy	If you selected *Explicit*, select *web-proxy* or search for an explicit web proxy. To create an explicit web proxy, see Create or edit an explicit proxy on page 110.
Source Interface	If you selected *Transparent*, enter the source interface.
Destination	Select *IP:Port*, *URI*, or *HTTP Header* and enter the destination.

User & Group	If you want to test a specific user or user group, enable *User & Group* and then select one user or user group.

3. Click *OK*. The results show the policy configuration if a policy matches the parameters.

URL Lookup

You can check if a website has been rated and what category and classification it is filed as. If you find a site that has been wrongly categorized, use this page to request that the site be re-evaluated: https://www.fortiguard.com/webfilter.

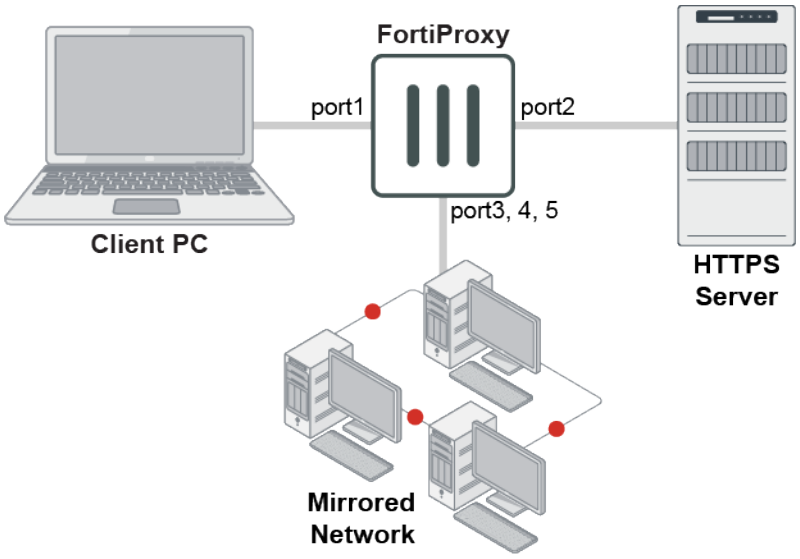


To view the associated IPs for a domain on a specific DNS server:

1. Go to *Policy & Objects* > *URL Lookup*
2. Enter the URL of the website.
3. Click *OK*. The results show the category and classification the websiteis filed as.

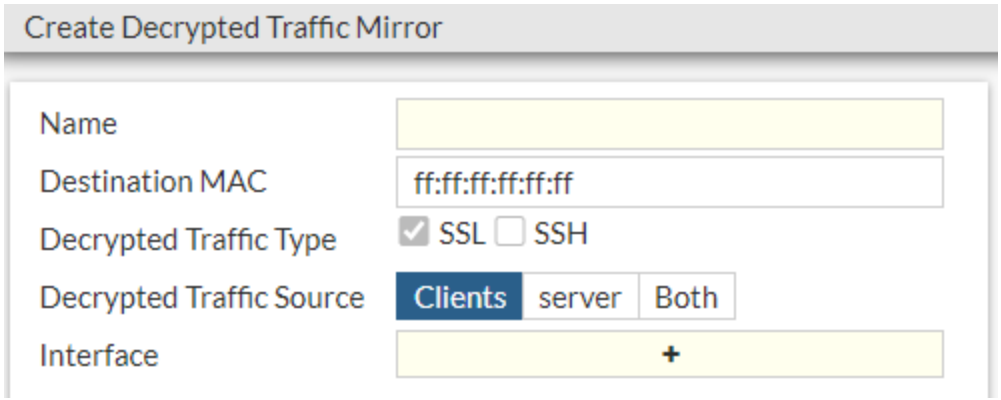
Decrypted Traffic Mirror

SSL mirroring allows the FortiProxy unit to decrypt and mirror traffic to a designated port. A decrypted traffic mirror profile can be applied to explicit, transparent, SSH tunnel, and SSH proxy policies when the custom-deep-inspection, deep-inspection, or deep-test SSL/SSH inspection security profile is selected. SSL inspection is automatically enabled when you enable a security profile on the policy configuration page.



To configure SSL mirroring in a policy:

1. Create a decrypted traffic mirror profile by selecting *Create New* under *Policy & Objects* > *Dycrypted Traffic Mirror* in the GUI. Configure the following options:



Name	Enter the name of the decrypted traffic mirror profile.
Destination MAC	Enter the destination MAC address for the mirrored traffic.
Decrypted Traffic Type	Select whether decrypted SSL traffic, decrypted SSH traffic, or both are mirrored.
Decrypted Traffic Source	Select whether decrypted client-side traffic, decrypted server-side traffic, or both are mirrored.
Interface	Select which interfaces will have decrypted traffic mirrored. Fortinet recommends that you mirror the traffic to a dedicated interface or virtual interface.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if

	the user is logged in as an administrator that has read-only GUI permissions.

Alternatively, use the `config firewall decrypted-traffic-mirror` command. For example:

```
config firewall decrypted-traffic-mirror
   edit "1"
      set dstmac ff:ff:ff:ff:ff:ff
      set traffic-type ssl ssh
      set traffic-source both
      set interface "port1"
   next
end
```

2. Configure the policy to enable SSL traffic mirroring:

```
config firewall policy
   edit 1
      set type explicit-web
      set name "All"
      set uuid 10e62d76-7c94-51ee-fa3a-ae92170cea18
      set dstintf "port1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "webproxy"
      set explicit-web-proxy "web-proxy"
      set utm-status enable
      set logtraffic all
      set log-http-transaction all
      set decrypted-traffic-mirror "1"
      set ssl-ssh-profile "Deep_Custom".
      set webfilter-profile "default"
   next
end
```

To verify and troubleshoot issues with traffic mirroring, use the *Network* > *Diagnostics on page 218* tab to capture and analyze the mirrored traffic.

Addresses

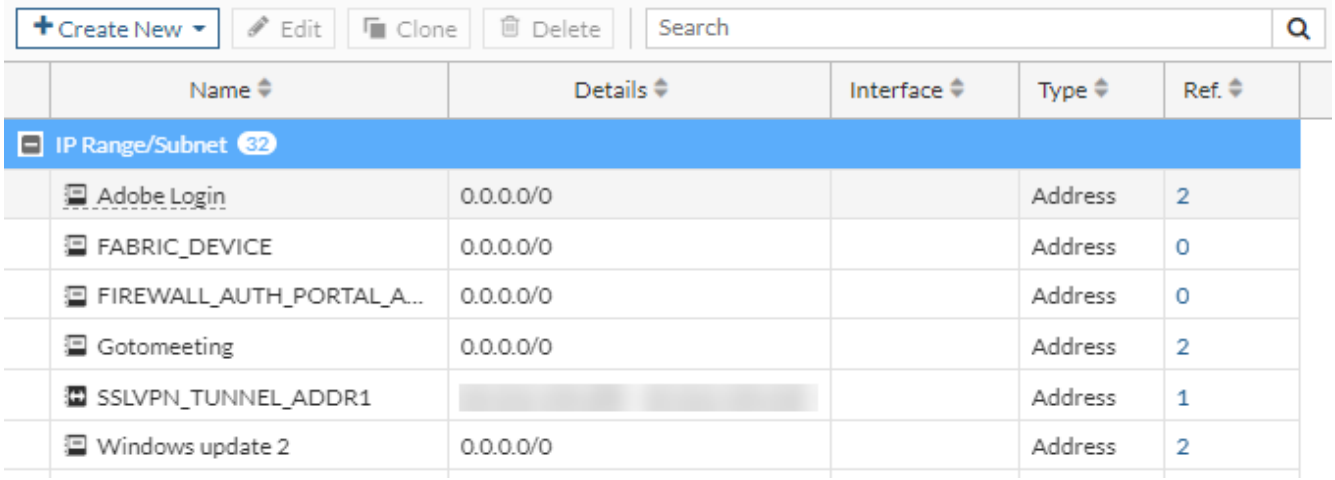
Web cache addresses and address groups define the network addresses that you use when configuring source and destination addresses for security policies. The FortiProxy unit compares the IP addresses contained in packet headers with security policy source and destination addresses to determine if the security policy matches the traffic. Addresses can be IPv4 addresses and address ranges, IPv6 addresses, and fully qualified domain names (FQDNs).



Be careful if employing FQDN web cache addresses. Using a fully qualified domain name in a security policy, while convenient, does present some security risks because policy matching then relies on a trusted DNS server. If the DNS server becomes compromised, security policies requiring domain name resolution might no longer function properly.

Web cache addresses in the address list are grouped by type: Address, Address Group, IPv6 Address, IPv6 Address Group, Proxy Address, Proxy Group, IPv6 Proxy Address, IPv6 Proxy Group. A FortiProxy unit's default configurations include all address, which represents any IPv4 IP address on any network. You can also add a firewall address list when configuring a security policy.

To view the address list, go to *Policy & Objects* > *Addresses*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

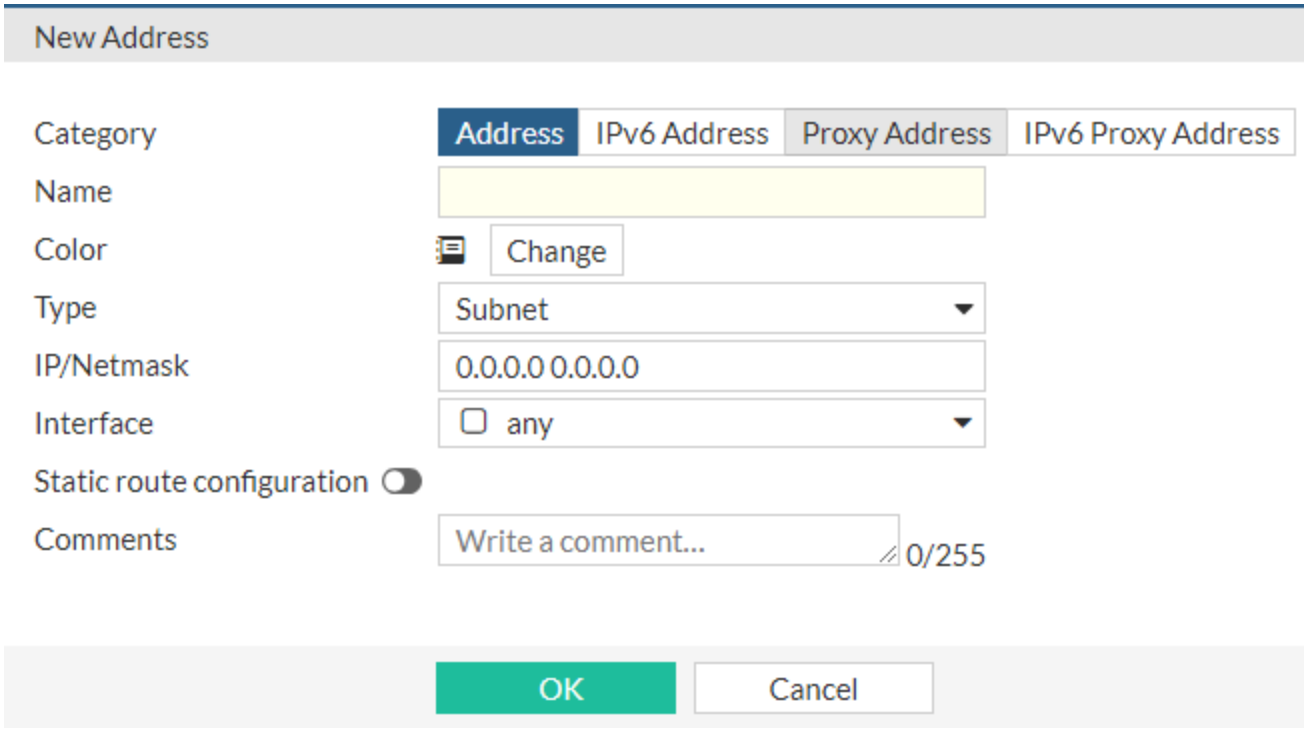
The following options are available:

Create New > Address	Add a new address. See Create or edit an address on page 485.
Create New > Address Group	Add a new address group. See Create or edit an address group on page 501.
Create New > IPv6 Address Template	Add an IPv6 address template. See Create or edit an IPv6 address template on page 502.
Edit	Edit the selected address. See Create or edit an address on page 485 or Create or edit an address group on page 501
Clone	Make a copy of the selected address or address group.
Delete	Remove the selected address or address group. This icon appears only if a policy or address group is not currently using the address.
Search	Search for text in any column.
Name	The name of the address.
Details	The domain name.
Interface	The interface to which the address is bound.

Type	Select the type of address: *FQDN*, *Geography*, *IP Range*, *Subnet*, *Wildcard FQDN*, *Dynamic SDN address*, *IPv6 Subnet*, *URL Pattern*, *Host Regex Match*, *URL Category*, *HTTP Method*, *User Agent*, *HTTP Header*, *Advanced (Source)*, or *Advanced (Destination)*.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Comments	Optional description of the address.
Exclude Members	Addresses excluded from an address group.
Routable	Whether the IP address can be used for routing.

Create or edit an address

Select *Create New* > *Address* to open the *New Address* window.



To open the *Edit Address* window, select an address and then click *Edit*.

Configure the following settings in the *New Address* window or the *Edit Address* window and then click *OK*:

Category	Select *Address*, *IPv6 Address*, *Proxy Address*, or *IPv6 Proxy Address*.
Name	Enter a name for the address. Addresses must have unique names.
Color	Select *Change* to choose a color for the icon.
Type	If you selected *Address* for the category, select one of the following: • *Subnet* • *IP Range* • *FQDN* • *Geography* • *Dynamic* • *Device (MAC Address)* If you selected *IPv6 Address* for the category, select one of the following: • *IPv6 Subnet* • *IPv6 Range* • *IPv6 FQDN* • *IPv6 Geography* • *IPv6 Fabric Connector Address* • *IPv6 Template* • *Device (MAC Address)* If you selected *Proxy Address* or *IPv6 Proxy Address* for the category, select one of the following. Refer to Proxy address on page 488 for more information about each proxy address type. • *Host Regex Match* • *URL Pattern* • *URL Category* • *URL List* • *HTTP Method* • *User Agent* • *HTTP Header* • *Advanced (Source)* • *Advanced (Destination)* • *addr_type_saas*
IP/Netmask	If you selected *Subnet* as the IPv4 address type, enter the IP address and netmask.
IP Range	If you selected *IP Range*as the IPv4 address type or you selected *IPv6 Range* as the IPv6 address type, enter an IP address range separated by a hyphen. See Web cache policy address formats.

FQDN	If you selected *FQDN* as the IPv4 address type or *IPv6 FQDN* as the IPv6 address type, enter the fully qualified domain name.
Country/Region	If you selected *Geography* as the IPv4 address type or *IPv6 Geography* as the IPv6 address type, select the country or region.
Sub Type	If you selected Dynamic as the IPv4 address type, select *ClearPass*, *Fabric Connector Address*, *FortiNAC Tag*, *FortiVoice Tag*, *Fortinet Single Sign-On (FSSO)*, or *Switch Controller NAC Policy Tag*.
SPT (System Posture Token)	If you selected *ClearPass* as the *Sub Type*, select *Checkup*, *Healthy*, *Infected*, *Quarantine*, *Transient*, or *Unknown*.
SDN Connector	If you selected *Fabric Connector Address* as the *Sub Type* or *IPv6 Fabric Connector Address* as the IPv6 address type, select an existing SDN connector or create a new one. See External Connectors on page 1106.
FSSO Group	If you selected *Fortinet Single Sign-On (FSSO)* as the *Sub Type*, select an existing FSSO group or create a new one. See Create or edit a user group on page 809.
MAC address	If you selected *Device (MAC Address)* as the *Sub Type* or *Type*, enter the MAC address or range of MAC addresses.
IPv6 Address	If you selected *IPv6 Subnet* as the IPv6 address type, enter the IPv6 address.
IPv6 Address Template	If you selected *IPv6 Template* as the IPv6 address type, select an existing IPv6 address template or create one. See Create or edit an IPv6 address template on page 502.
Host Type	If you selected *IPv6 Template* as the IPv6 address type, select *any* or *specific*. If you select *specific*, enter the host name.
Interface	Select the interface to which you want to bind the IPv4 address. Select *any* if you want to bind the IP address with the interface when you create a policy.
Host	Enter or select the host name.
Host Regex Pattern	If you selected *Host Regex Match* as the proxy address type, enter the appropriate string.
URL Path Regex	If you selected *URL Pattern* or *Advanced (Destination)* as the proxy address type, enter the appropriate string.
URL Category	If you selected *URL Category* or *Advanced (Destination)* as the proxy address type, select the FortiGuard web filter category or categories.
URL List	If you selected *URL List* as the proxy address type, select a URL list from the list.

Request Method	If you selected *HTTP Method* or *Advanced (Source)* as the proxy address type, select *CONNECT*, *DELETE*, *GET*, *HEAD*, *OPTIONS*, *POST*, *PUT*, or *TRACE*.
User Agent	If you selected *User Agent* or *Advanced (Source)* as the proxy address type, select a browser or browsers.
Header Name	If you selected *HTTP Header* as the proxy address type, enter the header name.
Header Regex	If you selected *HTTP Header* as the proxy address type, enter the appropriate string value.
Request Method	If you selected *Advanced (Source)* as the proxy address type, select *CONNECT*, *DELETE*, *GET*, *HEAD*, *OPTIONS*, *POST*, *PUT*, or *TRACE*.
HTTP Header	If you selected *Advanced (Source)* as the proxy address type, enter the name and value of the header.
Static Route Configuration	Enabling this feature includes the address in the listing of named addresses when setting up a static route. This option is available only when the *Type* is *FQDN*, IP Range, or *Subnet*.
Comments	Optionally, enter a description of the address.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Proxy address

The following proxy address types are available for firewall policies:

- Host Regex Match on page 489
- URL Pattern on page 490
- URL Category on page 491
- URL List on page 492
- HTTP Method on page 493
- User Agent on page 495
- HTTP Header on page 496

- Advanced (Source) on page 497
- Advanced (Destination) on page 498
- Response Header on page 500 NEW

Fast policy match

The fast policy match function improves the performance of IPv4 explicit and transparent web proxies on FortiProxy devices.

When enabled, after the firewall policies are configured, the FortiProxy builds a fast searching table based on the different firewall policy matching criteria. When fast policy matching is disabled, web proxy traffic is compared to the policies one at a time from the beginning of the policy list.

Fast policy matching is enabled by default, and can be configured with the following CLI command:

```
config web-proxy global
    set fast-policy-match {enable | disable}
end
```

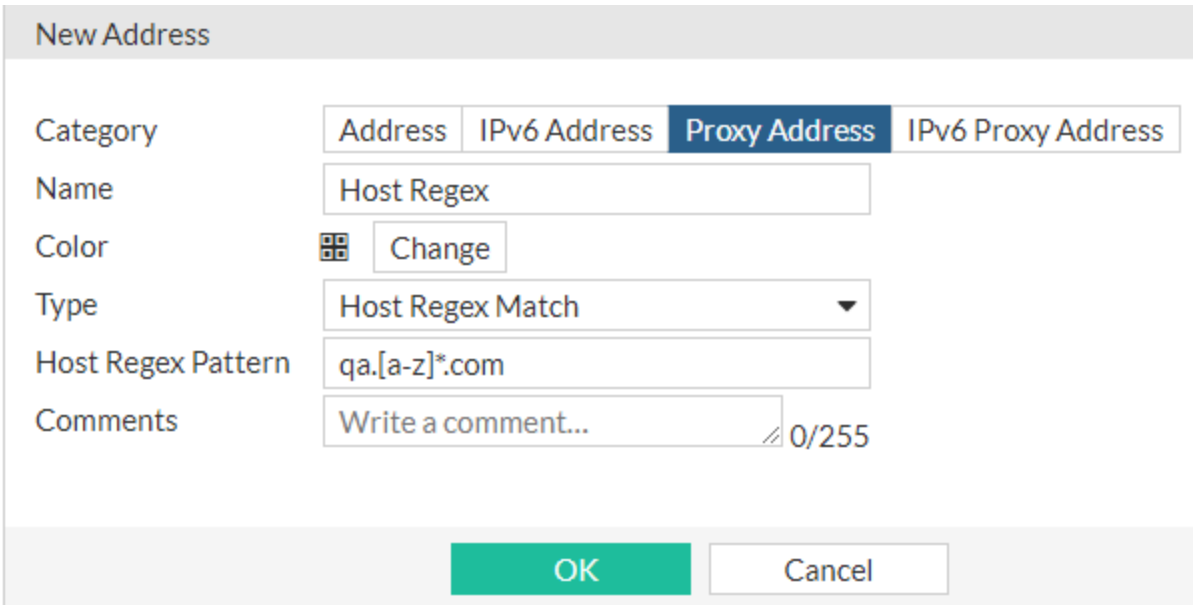
Host Regex Match

In this address type, a user can create a hostname as a regular expression to match the Host field in the Layer 7 header of a packet. Once created, the hostname address can be selected as a destination of a firewall policy. This means that a policy will only allow or block requests that match the regular expression.

This example creates a host regex match address with the pattern *qa.[a-z]*.com*.

To create a host regex match address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *Host Regex*,
   - *Type* to *Host Regex Match*, and
   - *Host Regex Pattern* to *qa.[a-z]*.com*.



4. Click *OK*.

To create a host regex match address in the CLI:

```
config firewall proxy-address
    edit "Host Regex"
        set type host-regex
        set host-regex "qa.[a-z]*.com"
    next
end
```

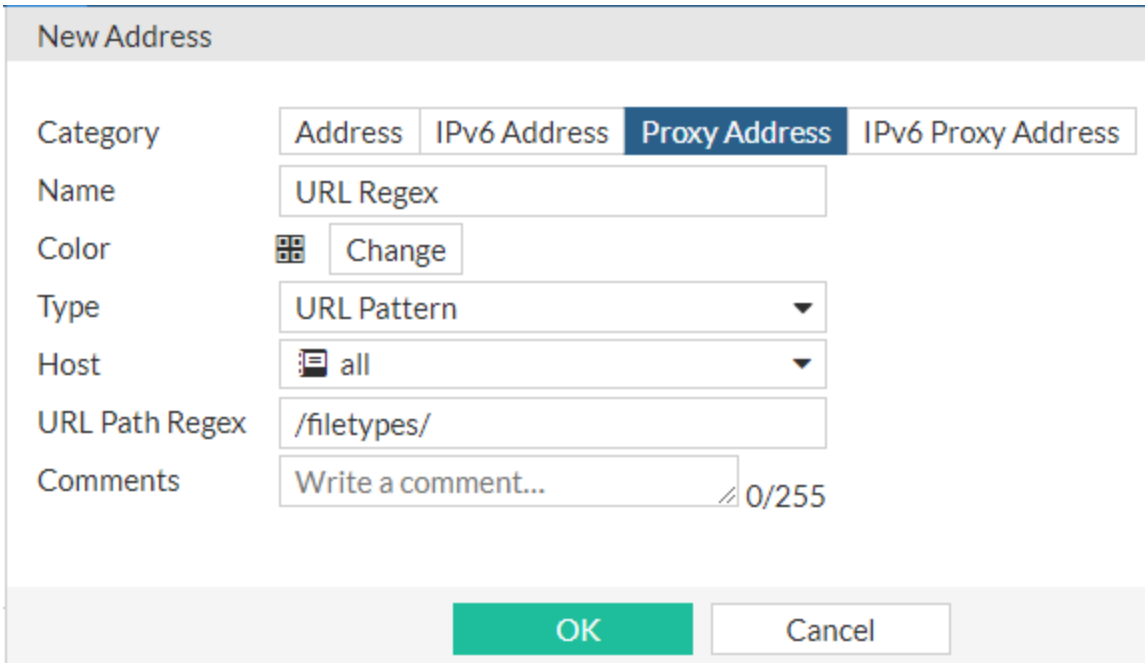
URL Pattern

In this address type, a user can create a URL path as a regular expression. Once created, the path address can be selected as a destination of a firewall policy. This means that a policy will only allow or block requests that match the regular expression.

This example creates a URL pattern address with the pattern */filetypes/*.

To create a URL pattern address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *URL Regex*,
   - *Type* to *URL Pattern*,
   - *Host* to *all*, and
   - *URL Path Regex* to */filetypes/*.



4. Click *OK*.

To create a URL pattern address in the CLI:

```
config firewall proxy-address
    edit "URL Regex"
        set type url
        set host "all"
        set path "/filetypes/"
    next
end
```

URL Category

In this address type, a user can create a URL category based on a FortiGuard URL ID. Once created, the address can be selected as a destination of a firewall policy. This means that a policy will only allow or block requests that match the URL category.

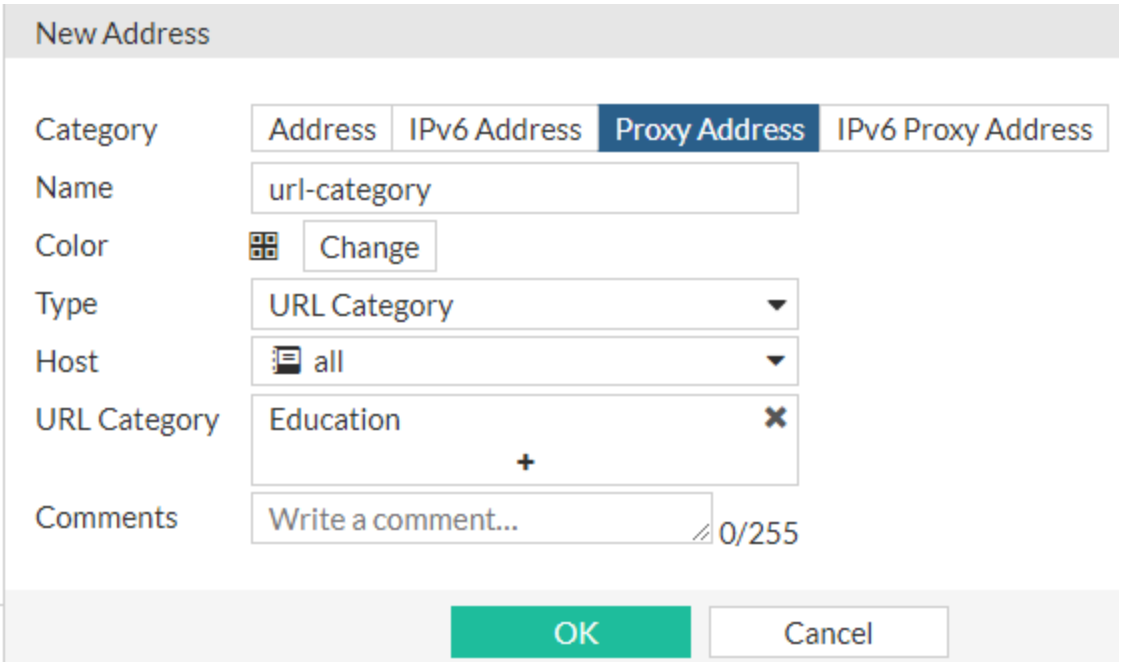
The example creates a URL category address for URLs in the *Education* category. For more information about categories, see https://fortiguard.com/webfilter/categories.

For information about creating and using custom local and remote categories, see Web Rating Overrides on page 650.

To create a URL category address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.

3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *url-category*,
   - *Type* to *URL Category*,
   - *Host* to *all*, and
   - *URL Category* to *Education*.



4. Click *OK*.

To create a URL category address in the CLI:

```
config firewall proxy-address
    edit "url-category"
        set type category
        set host "all"
        set category 30
    next
end
```

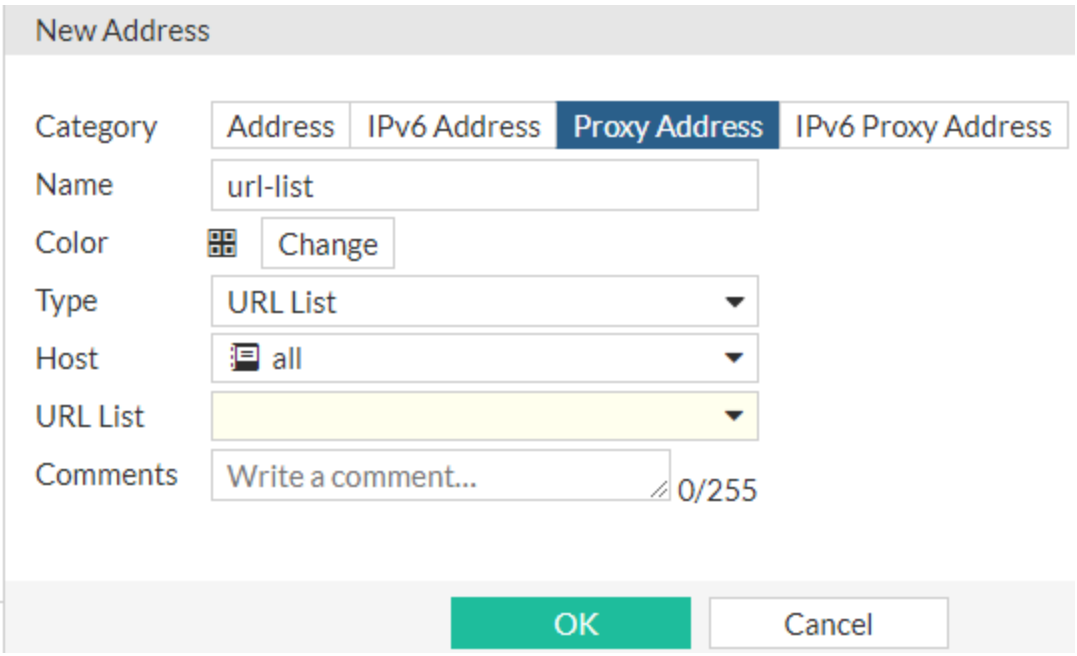
To see a list of all the categories and their numbers, when editing the address, enter `set category ?`.

URL List

In this address type, a user can create a URL list based on an existing web filter URL list that you created under *Security Profiles > Web Filter URL List*. Once created, the URL list can be selected as a destination of a firewall policy. This means that a policy will only allow or block requests that match the URL list.

To create a URL list address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *url-list*,
   - *Type* to *URL List*,
   - *Host* to *all*, and
   - *URL List* to one that is available. If no URL list is available, create one under *Security Profiles* > *Web Filter URL List*.



4. Click *OK*.

To create a URL list address in the CLI:

1. If no web filter URL list is defined, use the config webfilter url-list command to define one.
2. Create a URL list address by referencing the web filter URL list:

```
config firewall proxy-address
   edit "url-list"
      set type url-list
      set host "all"
      set url list "example-list"
   next
end
```

HTTP Method

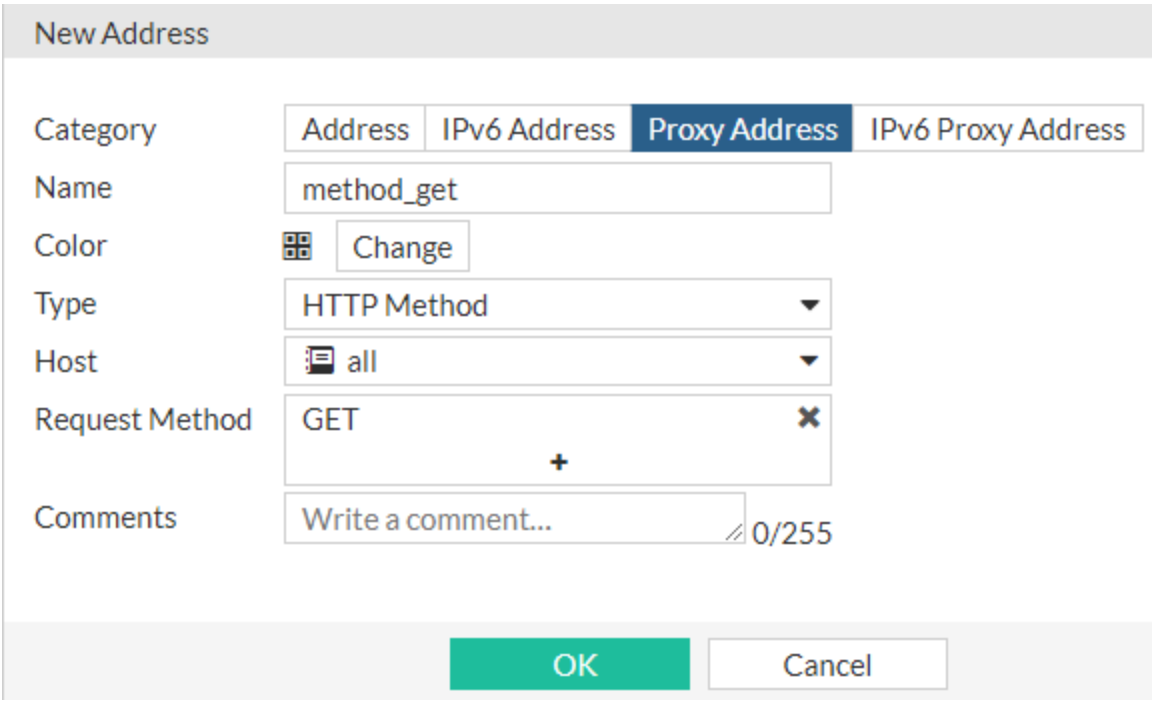
In this address type, a user can create an address based on the HTTP request methods that are used. Multiple method options are supported, including: *CONNECT*, *DELETE*, *GET*, *HEAD*, *OPTIONS*, *POST*,

PUT, and *TRACE*. Once created, the address can be selected as a source of a firewall policy. This means that a policy will only allow or block requests that match the selected HTTP method.

The example creates a HTTP method address that uses the GET method.

To create a HTTP method address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *method_get*,
   - *Type* to *HTTP Method*,
   - *Host* to *all*, and
   - *Request Method* to *GET*.



4. Click *OK*.

To create a HTTP method address in the CLI:

```
config firewall proxy-address
    edit "method_get"
        set type method
        set host "all"
        set method get
    next
end
```

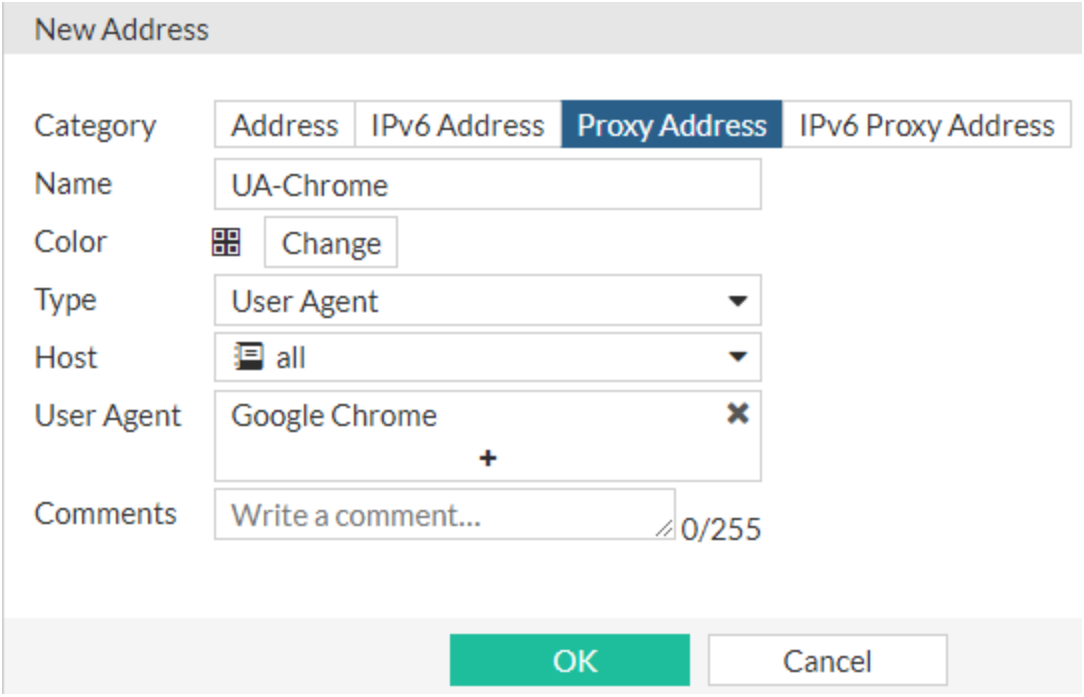
User Agent

In this address type, a user can create an address based on the names of the browsers that are used as user agents. Multiple browsers are supported, such as Chrome, Firefox, Internet Explorer, and others. Once created, the address can be selected as a source of a firewall policy. This means that a policy will only allow or block requests from the specified user agent.

This example creates a user agent address for Google Chrome.

To create a user agent address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *UA-Chrome*,
   - *Type* to *User Agent*,
   - *Host* to *all*, and
   - *User Agent* to *Google Chrome*.



4. Click *OK*.

To create a user agent address in the CLI:

```
config firewall proxy-address
    edit "UA-Chrome"
        set type ua
        set host "all"
        set ua chrome
```

```
    next
end
```

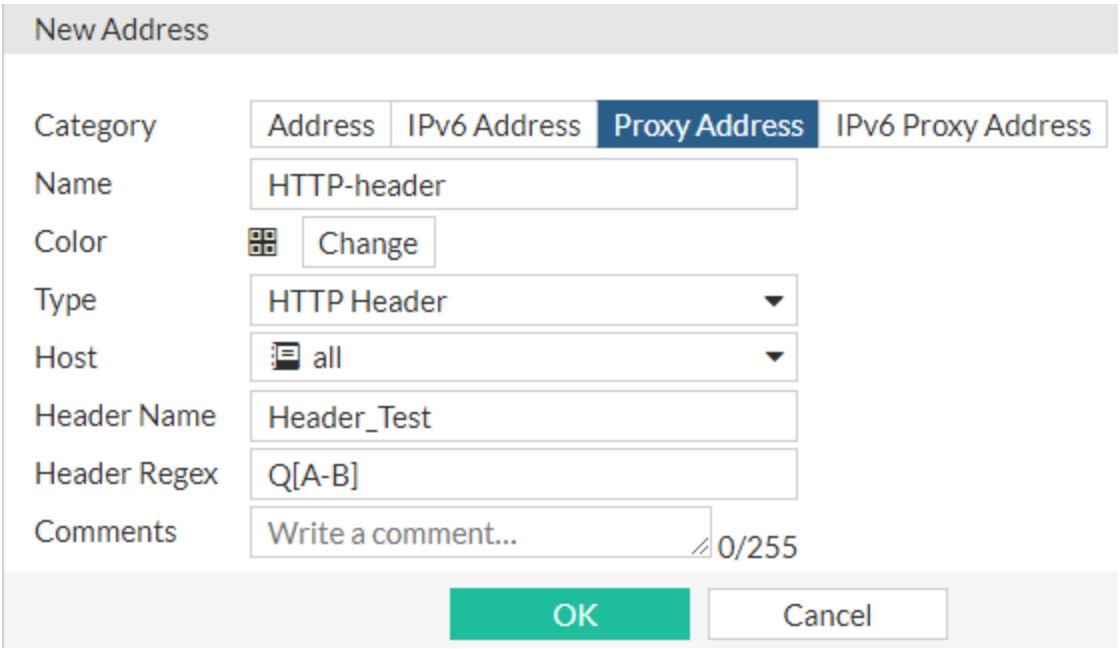
HTTP Header

In this address type, a user can create a HTTP header as a regular expression. Once created, the header address can be selected as a source of a firewall policy. This means that a policy will only allow or block requests where the HTTP header matches the regular expression.

This example creates a HTTP header address with the pattern *Q[A-B]*.

To create a HTTP header address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *HTTP-header*,
   - *Type* to *HTTP Header*,
   - *Host* to *all*,
   - *Header Name* to *Header_Test*, and
   - *Header Regex* to *Q[A-B]*.



4. Click *OK*.

To create a HTTP header address in the CLI:

```
config firewall proxy-address
    edit "method_get"
```

```
        set type header
        set host "all"
        set header-name "Header_Test"
        set header "Q[A-B]"
    next
end
```

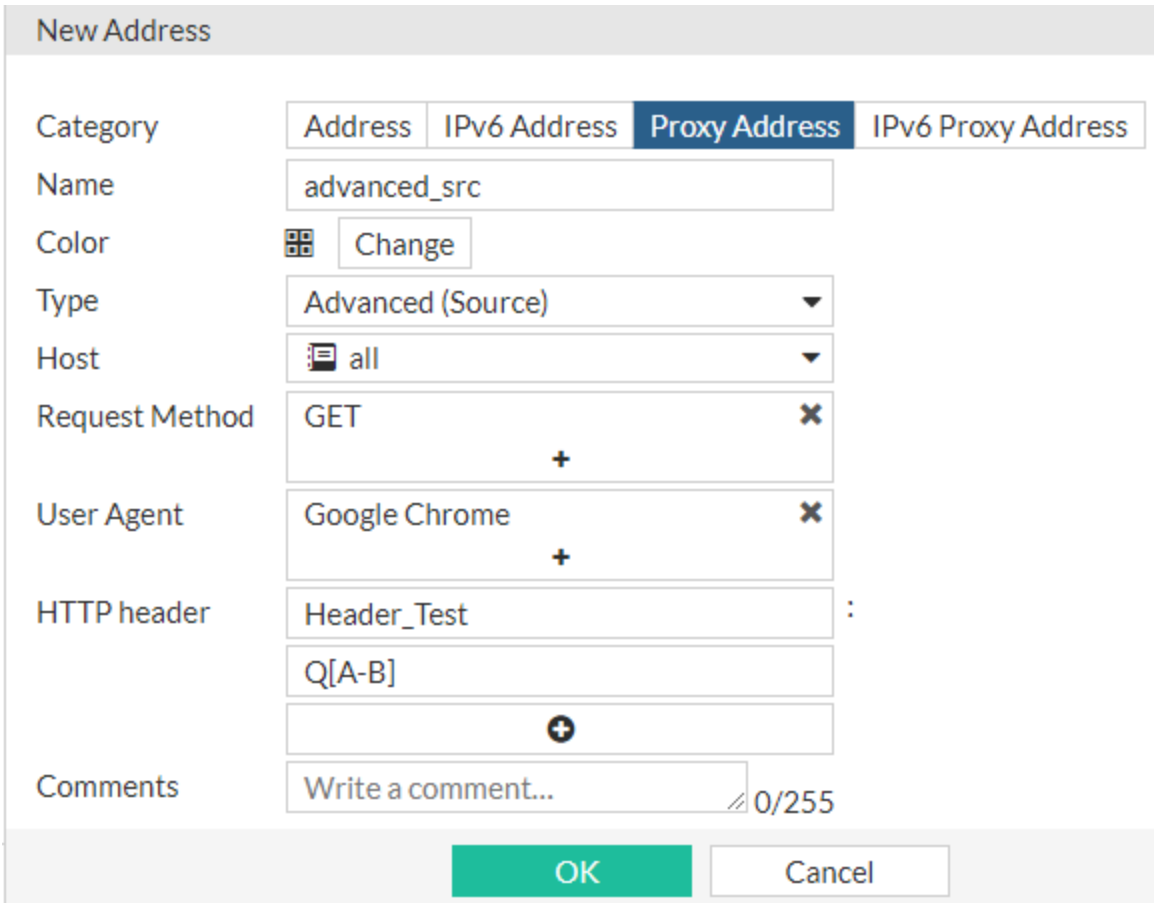
Advanced (Source)

In this address type, a user can create an address based on multiple parameters, including HTTP method, User Agent, and HTTP header. Once created, the address can be selected as a source of a firewall policy. This means that a policy will only allow or block requests that match the selected address.

This example creates an address that uses the get method, a user agent for Google Chrome, and an HTTP header with the pattern *Q[A-B]*.

To create an advanced (source) address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *advanced_src*,
   - *Type* to *Advanced (Source)*,
   - *Host* to *all*,
   - *Request Method* to *GET*,
   - *User Agent* to *Google Chrome*, and
   - *HTTP header* to *Header_Test* : *Q[A-B]*.



4. Click *OK*.

To create an advanced (source) address in the CLI:

```
config firewall proxy-address
    edit "advance_src"
        set type src-advanced
        set host "all"
        set method get
        set ua chrome
        config header-group
            edit 1
                set header-name "Header_Test"
                set header "Q[A-B]"
            next
        end
    next
end
```

Advanced (Destination)

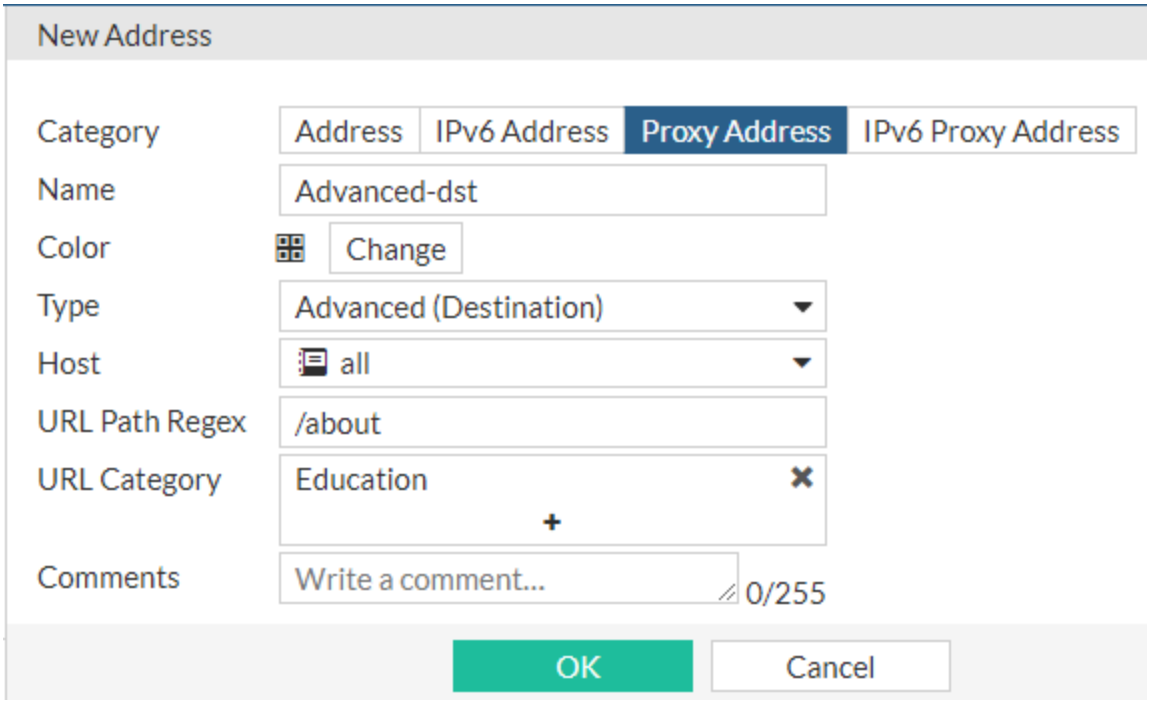
In this address type, a user can create an address based on URL pattern and URL category parameters. Once created, the address can be selected as a destination of a firewall policy. This means that a

policy will only allow or block requests that match the selected address.

This example creates an address with the URL pattern */about* that are in the *Education* category. For more information about categories, see https://fortiguard.com/webfilter/categories.

To create an advanced (destination) address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *Advanced-dst*,
   - *Type* to *Advanced (Destination)*,
   - *Host* to *all*,
   - *URL Path Regex* to */about*, and
   - *URL Category* to *Education*.



4. Click *OK*.

To create an advanced (destination) address in the CLI:

```
config firewall proxy-address
    edit "Advanced-dst"
        set type dst-advanced
        set host "ubc"
        set path "/about"
        set category 30
    next
end
```

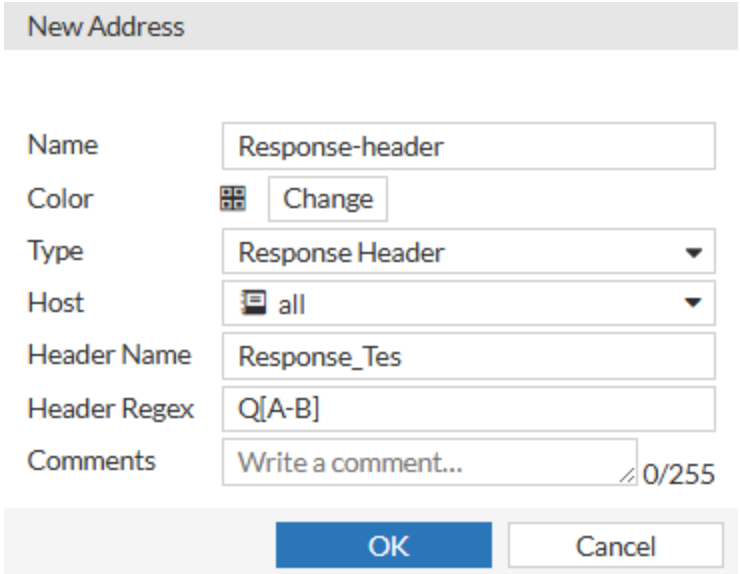
Response Header

In this address type, a user can create a HTTP response header as a regular expression. Once created, the response header address can be selected as a destination of a response shaping policy. This means that a response shaping policy will only apply the traffic shaping behavior where the response header matches the regular expression.

This example creates a response header address with the pattern *Q[A-B]*.

To create a response header address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. In the *Proxy* tab, click *Create New* > *Address*.
3. Set the following:
   - *Name* to *Response-header*,
   - *Type* to *Response Header*,
   - *Host* to *all*,
   - *Header Name* to *Response_Test*
   - *Header Regex* to *Q[A-B]*.



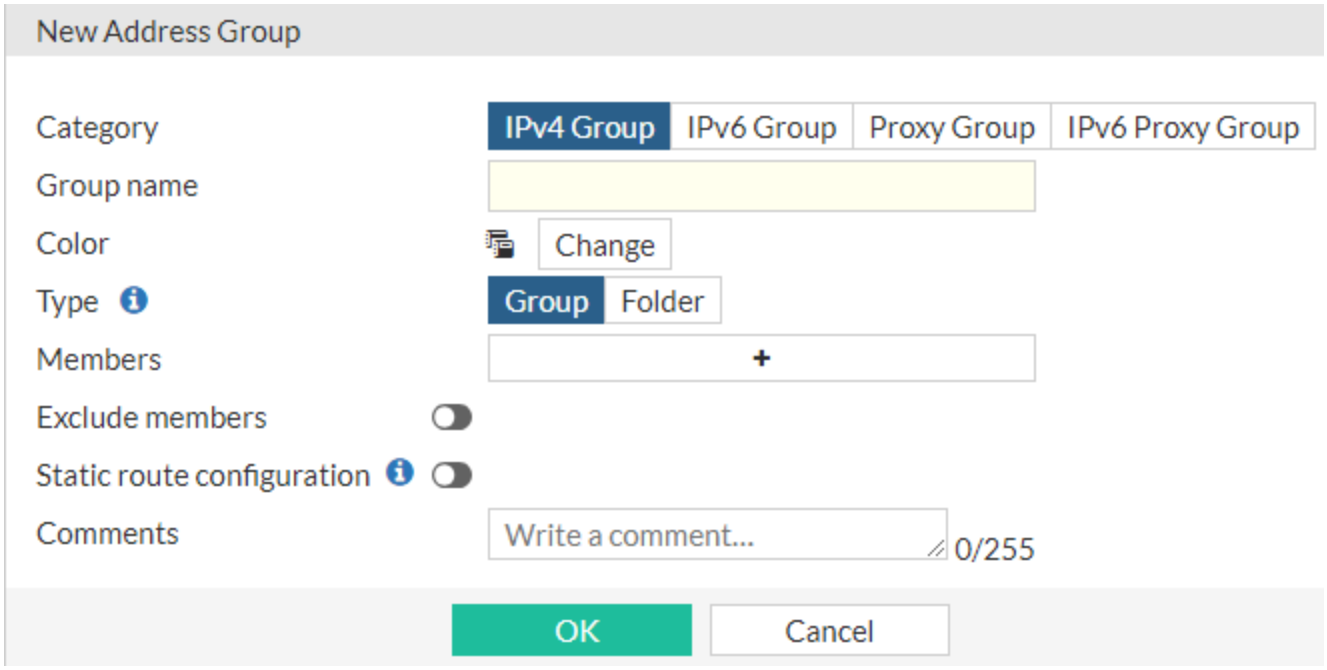
4. Click *OK*.

To create a response header address in the CLI:

```
config firewall proxy-address
    edit "method_get"
        set type response-header
        set host "all"
        set header-name "Header_Test"
        set header "Q[A-B]"
    next
end
```

Create or edit an address group

Select *Create New* > *Address Group* to open the *New Address Group* window.



To open the *Edit Address Group* window, select an address group and then click *Edit*.

Configure the following settings in the *New Address Group* window or the *Edit Address Group* window and then click *OK*:

Category	Select *IPv4 Group*, *IPv6 Group*, *Proxy Group*, or *IPv6 Proxy Group*.
Group name	Enter a name to identify the address group. Addresses, address groups, and virtual IPs must have unique names.
Color	Select *Change* to choose a color for the icon.
Type	If you selected *IPv4 Group*, select *Group* or *Folder*. If you selected *Proxy Group* or *IPv6 Proxy Group*, select *Source Group* or *Destination Group*.
Members	Select the addresses to add to the address group. When *Category* is *Proxy Group* or *IPv6 Proxy Group*, select the Proxy address on page 488 or group from the list.
Exclude Members	Enable *Exclude Members* and then select the addresses to exclude from the address group.
Static Route Configuration	Enabling this feature includes the address in the listing of named addresses when setting up a static route. This option is available only if *Category* is *IPv4 Group* and every member of the address group has *Static Route Configuration* enabled.

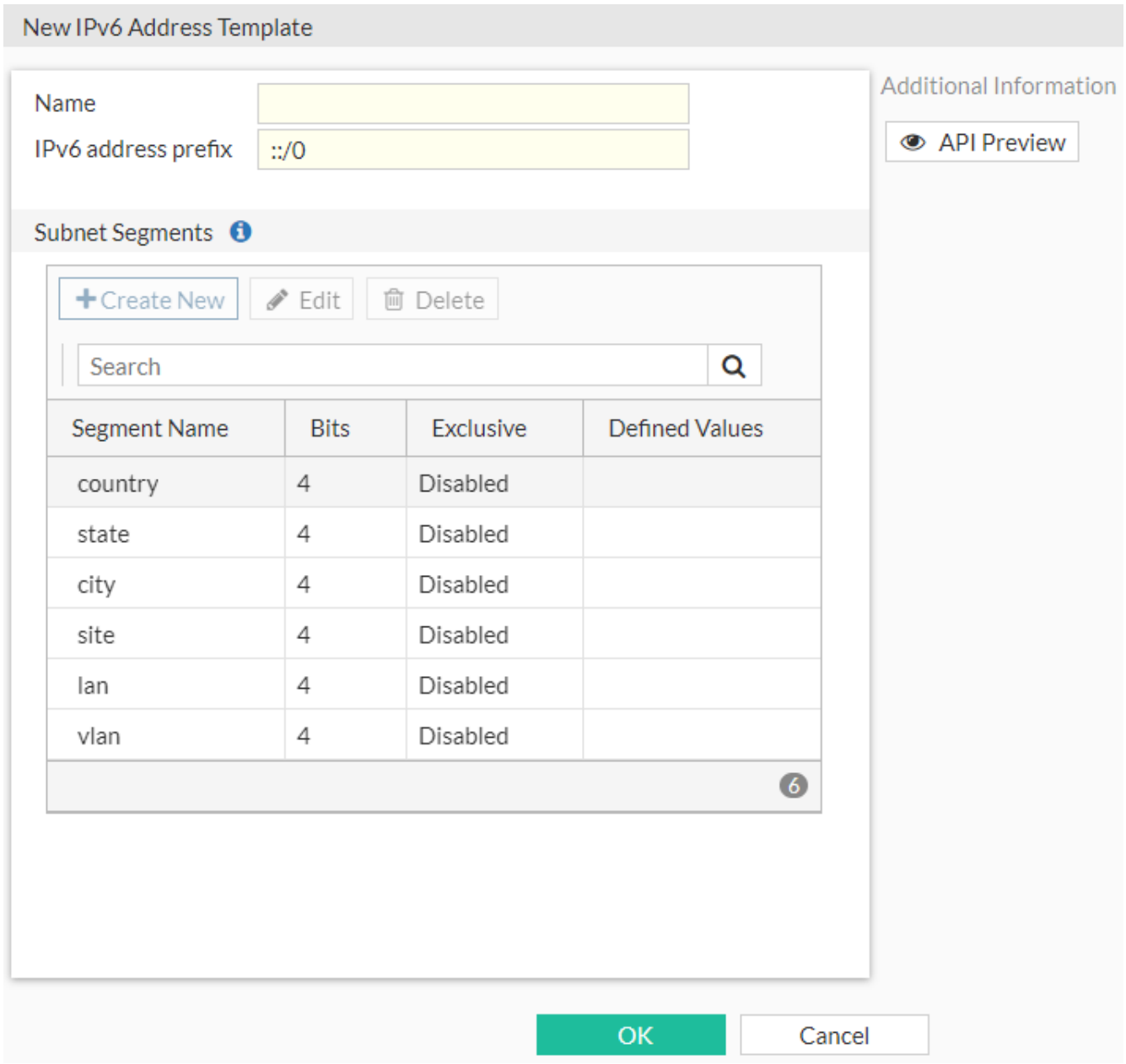
Comments	Optionally, enter a description of the address group.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create or edit an IPv6 address template

Select *Create New* > *IPv6 Address Template* to open the *New IPv6 Address Template* window.



To open the *Edit IPv6 Address Template* window, select an IPv6 address template and then click *Edit*.

Configure the following settings in the *New IPv6 Address Template* window or the *Edit IPv6 Address Template* window and then click *OK*:

Name	Enter a name for the IPv6 address template.
IPv6 address prefix	Enter the IPv6 address prefix.
Subnet Segments	Select a maximum of six segments. Each segment can have a maximum of 16 bits.
Create New	You cannot create a subnet segment.

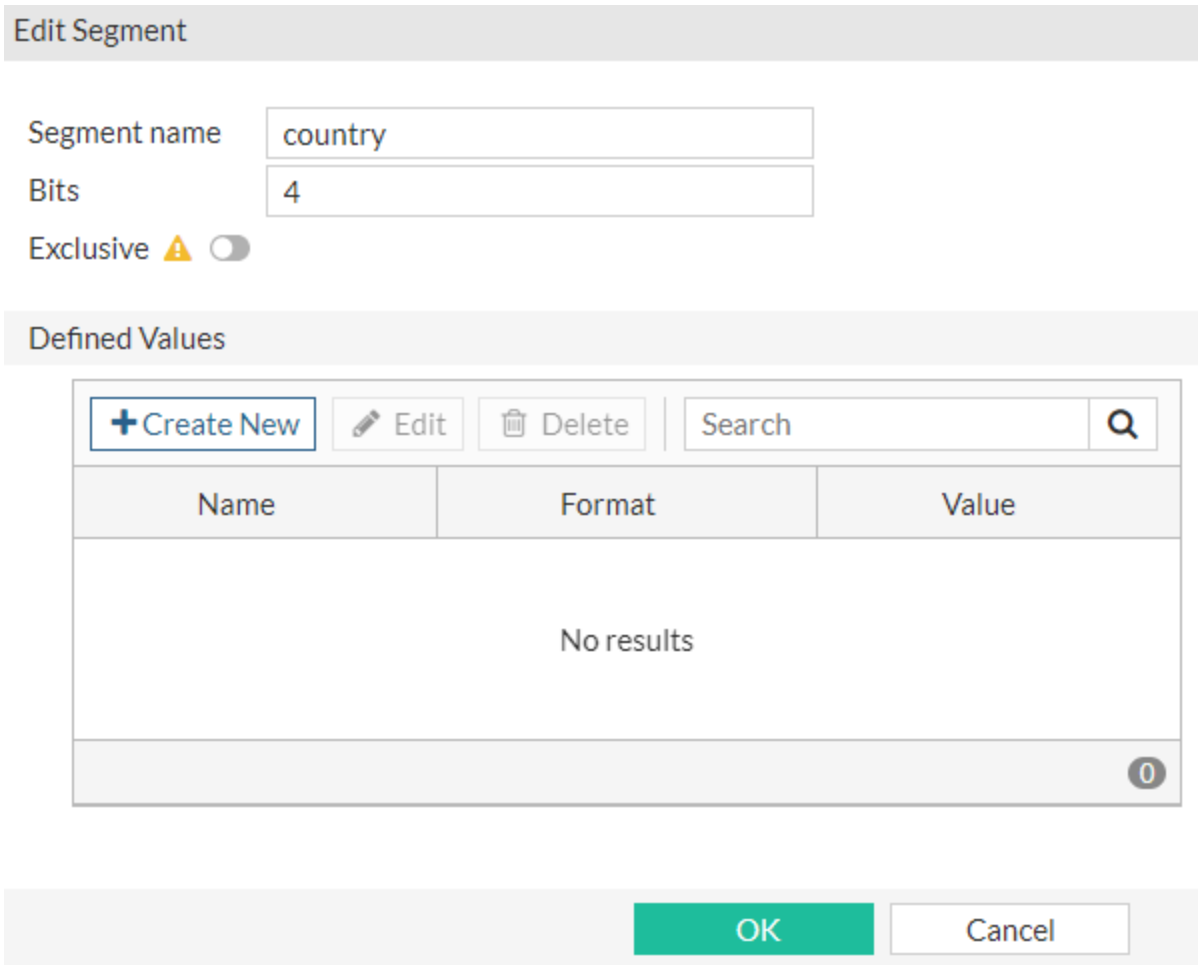
Edit	Select a subnet segment and click *Edit*. See Edit a subnet segment on page 504.
Delete	Delete the selected subnet segment.
Search	Search for text in any column.
Segment Name	The name of the subnet segment.
Bits	The number of bits used by the subnet segment.
Exclusive	*Enabled* means that the subnet segment is exclusive, and the user must select from predefined values for the segment.
Defined Values	Predefined values for an exclusive segment.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.
References	Click to open the object usage page to show which other configuration are referencing the object.
Edit in CLI	Click to open a CLI console window to view and edit the setting in the CLI. If there are multiple CLI settings on the page, the CLI console shows the first setting.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Edit a subnet segment

Select a subnet segment and click *Edit* to open the *Edit Segment* window.



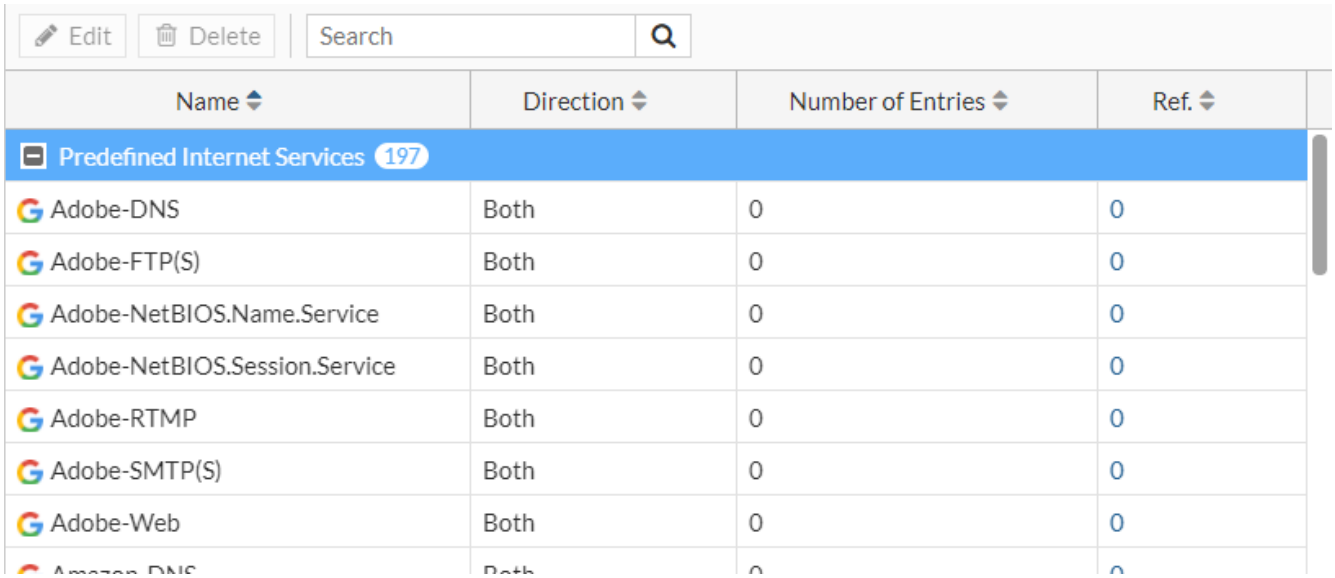
Configure the following settings in the *Edit Segment* window and then click *OK*:

Name	You can change the name of the segment.
Bits	You can change the number of bits for the segment. Each segment can have a maximum of 16 bits.
Exclusive	Enable this option to make a segment exclusive so that the user must select from predefined values for the segment. **NOTE:** You need to define at least one value before enabling *Exclusive*.
Defined Values	You can create defined values for exclusive segments.
Create New	Create the predefined values for an exclusive segment.
Edit	Select a value and then click *Edit* to change the value.
Delete	Delete the selected value.
Search	Search for text in any column.
Name	The name of the segment value.
Format	The format of the segment value.

Value	The value of the segment.

Internet Service Database

To view the Fortinet database of cloud-based applications, go to *Policy & Objects* > *Internet Service Database*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

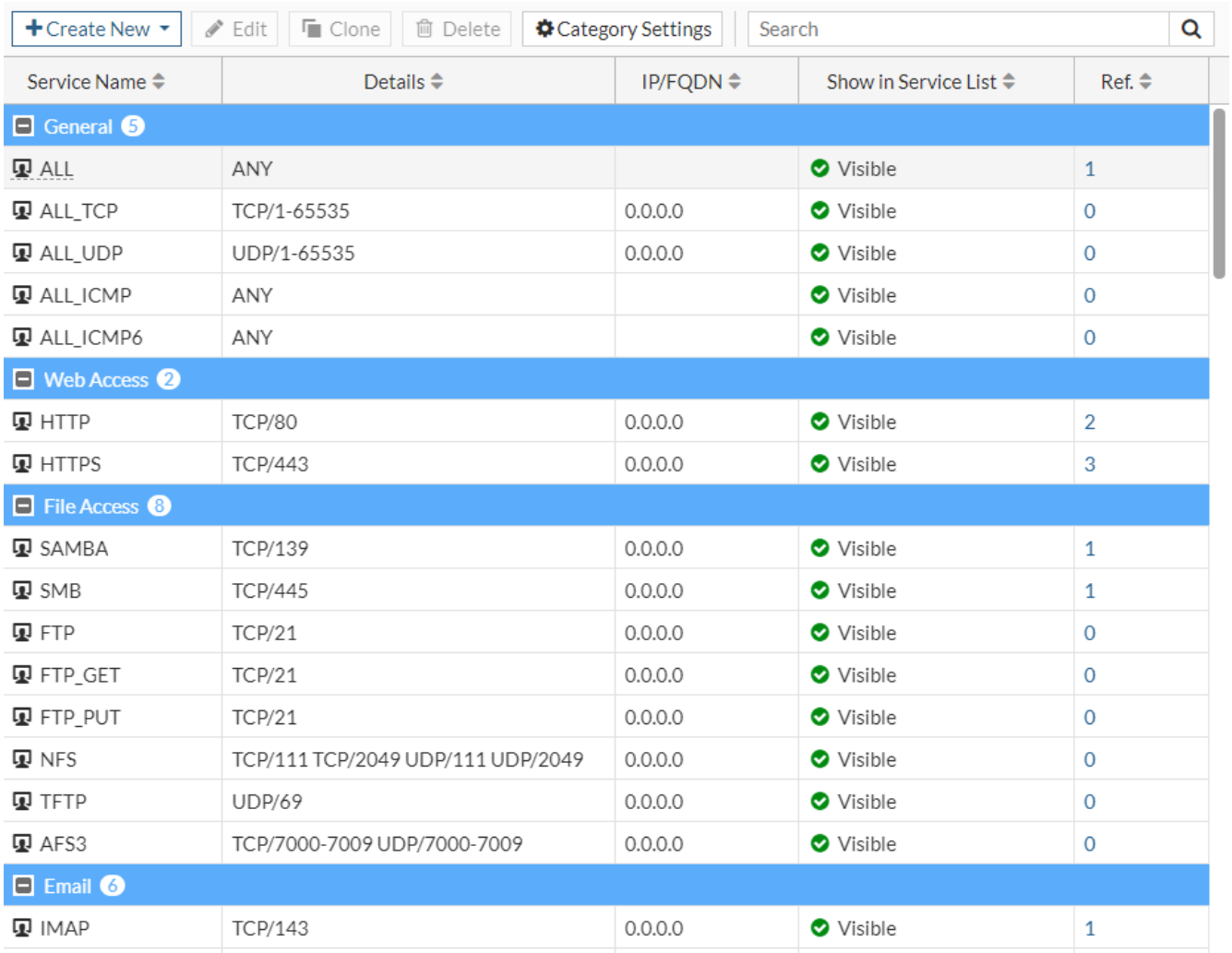
The following options are available:

Edit	Predefined Internet services cannot be changed.
Delete	Predefined Internet services cannot be deleted.
Search	Enter a search term to search the database.
Name	The name of the Internet service.
Direction	Which direction is supported for the Internet service.
Number of Entries	The number of entries in the database.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.

Services

Web cache services define one or more protocols and port numbers associated with each service. Web cache policies use service definitions to match session types. You can organize related services into service groups to simplify your policy list.

If you need to create a web cache policy for a service that is not in the predefined service list, you can add a custom service. Custom services are configured in *Policy & Objects* > *Services*.



Service Name	Details	IP/FQDN	Show in Service List	Ref.
General 5				
ALL	ANY		Visible	1
ALL_TCP	TCP/1-65535	0.0.0.0	Visible	0
ALL_UDP	UDP/1-65535	0.0.0.0	Visible	0
ALL_ICMP	ANY		Visible	0
ALL_ICMP6	ANY		Visible	0
Web Access 2				
HTTP	TCP/80	0.0.0.0	Visible	2
HTTPS	TCP/443	0.0.0.0	Visible	3
File Access 8				
SAMBA	TCP/139	0.0.0.0	Visible	1
SMB	TCP/445	0.0.0.0	Visible	1
FTP	TCP/21	0.0.0.0	Visible	0
FTP_GET	TCP/21	0.0.0.0	Visible	0
FTP_PUT	TCP/21	0.0.0.0	Visible	0
NFS	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	Visible	0
TFTP	UDP/69	0.0.0.0	Visible	0
AFS3	TCP/7000-7009 UDP/7000-7009	0.0.0.0	Visible	0
Email 6				
IMAP	TCP/143	0.0.0.0	Visible	1

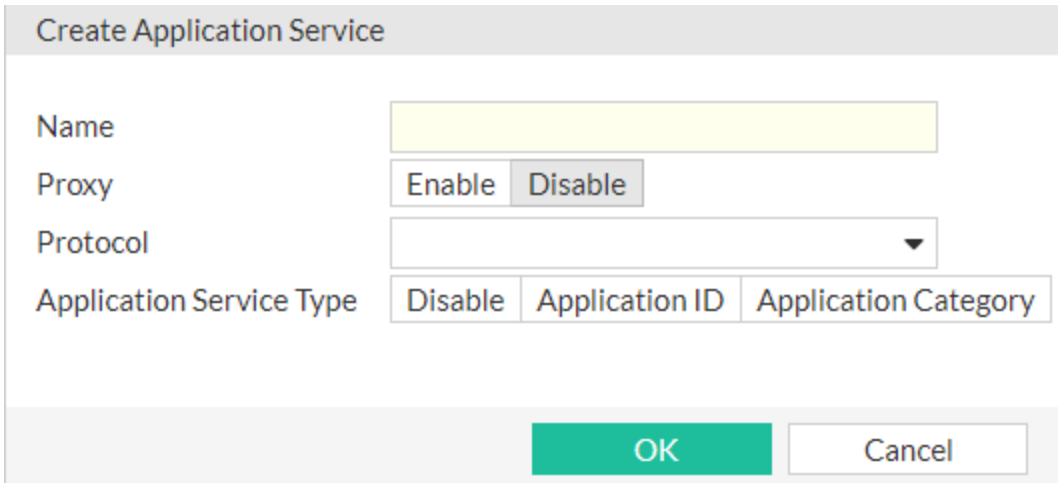
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an application service, service, service group, or category. See Create or edit an application service on page 508, Create or edit a service on page 509, Create or edit a service group on page 511, and Create a service category on page 515.
Edit	Edit the selected service.
Clone	Make a copy of the selected service.
Delete	Remove the selected custom service. This icon appears only if a service is not currently being used in a web cache policy.
Category Settings	Edit the order in which the categories are displayed in the list when viewing the list by category.
Search	Search for text in any column.
Service Name	The name of the custom service.
Details	Destination port or ports.
IP/FQDN	The IP address or FQDN of the service.
Show in Service List	Whether or not the service is shown in the service list.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Comments	Optional description of the service.
Protocol	The protocol type for the service.
Type	The type of service, such as *Firewall*, *Explicit Proxy*, or *Firewall Group*.

Create or edit an application service

Select *Create New* > *Application Service* to open the *Create Application Service* window.



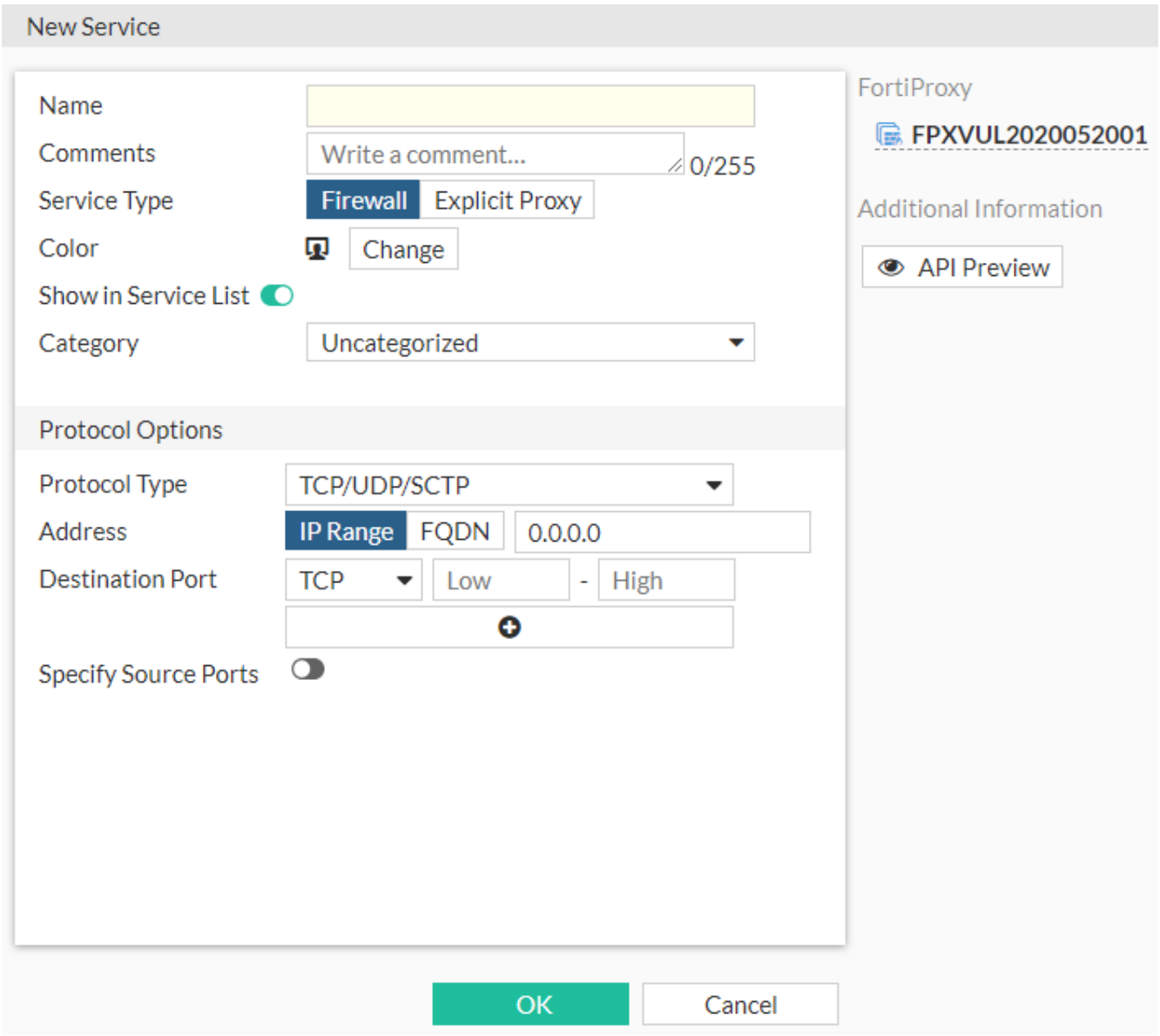
To open the *Edit Application Service* window, select an application service and then click *Edit*.

Configure the following settings in the *Create Application Service* window or *Edit Application Service* window and then click *OK*:

Name	Enter a name for the application service.
Proxy	Enable or disable the new application service.
Protocol	Select the protocol that the application service will use.
Application Service Type	Select *Disable*, *Application ID*, or *Application Category*.
Application ID	If you selected *Application ID*, click + to open the *Select Entries* window. Select one or more entries and then select *Close*.
Application category	If you selected an *Application Service Type* of *Application category*, click + to open the *Select Entries* window. Select one or more entries and then select *Close*.
TCP Port Range	If you selected *TCP/UDP/SCTP* or *ALL*, enter a range of TCP ports.

Create or edit a service

Select *Create New* > *Service* to open the *New Service* window.



To open the Edit Service window, select a service and then click *Edit*.

Configure the following settings in the *New Service* window or *Edit Service* window and then click *OK*:

Name	Enter a name for the custom service.
Comments	Optionally, enter a description of the service.
Service Type	Select the service type: *Firewall* or *Explicit Proxy*.
Color	Select *Change* to choose a color for the icon.
Show in Service List	Enable to show the service in the service list.

Category	Select the category for the service: *Uncategorized*; *Application*; *General*; *Web Access*; *File Access*; *Email*; *Network Services*; *Authentication*; *Remote Access*; *Tunneling*, *VoIP, Messaging & Other Applications*; or *Web Proxy*. You can create new service categories. See Create a service category on page 515.
Protocol Type	Select the type of protocol for the service. • If *Service Type* is *Firewall*, select one of: *TCP/UDP/SCTP*, *ICMP*, *ICMP6*, or *IP*. • If *Service Type* is *Explicit Proxy*, select one of: *ALL*, *CONNECT*, *FTP*, *HTTP*, *SOCKS_TCP*, or *SOCKS_UDP*.
Address	Select *IP Range* or *FQDN* and then enter the range of IP addresses or the FQDN for the service. Separate IP addresses with a hyphen.
Destination Port	Select *TCP*, *UDP*, or *SCTP* and then enter a range of port numbers.
Specify Source Ports	Enable and then enter a range of port numbers.
Type	Enter the ICMP type number for the ICMP protocol configuration. This option is only available if *Protocol Type* is set to *ICMP* or *ICMP6*.
Code	Enter the ICMP code number for the ICMP protocol configuration. This option is only available if *Protocol Type* is set to *ICMP* or *ICMP6*.
Protocol Number	Enter the protocol number for the IP protocol configuration. This option is only available if *Protocol Type* is set to *IP*.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create or edit a service group

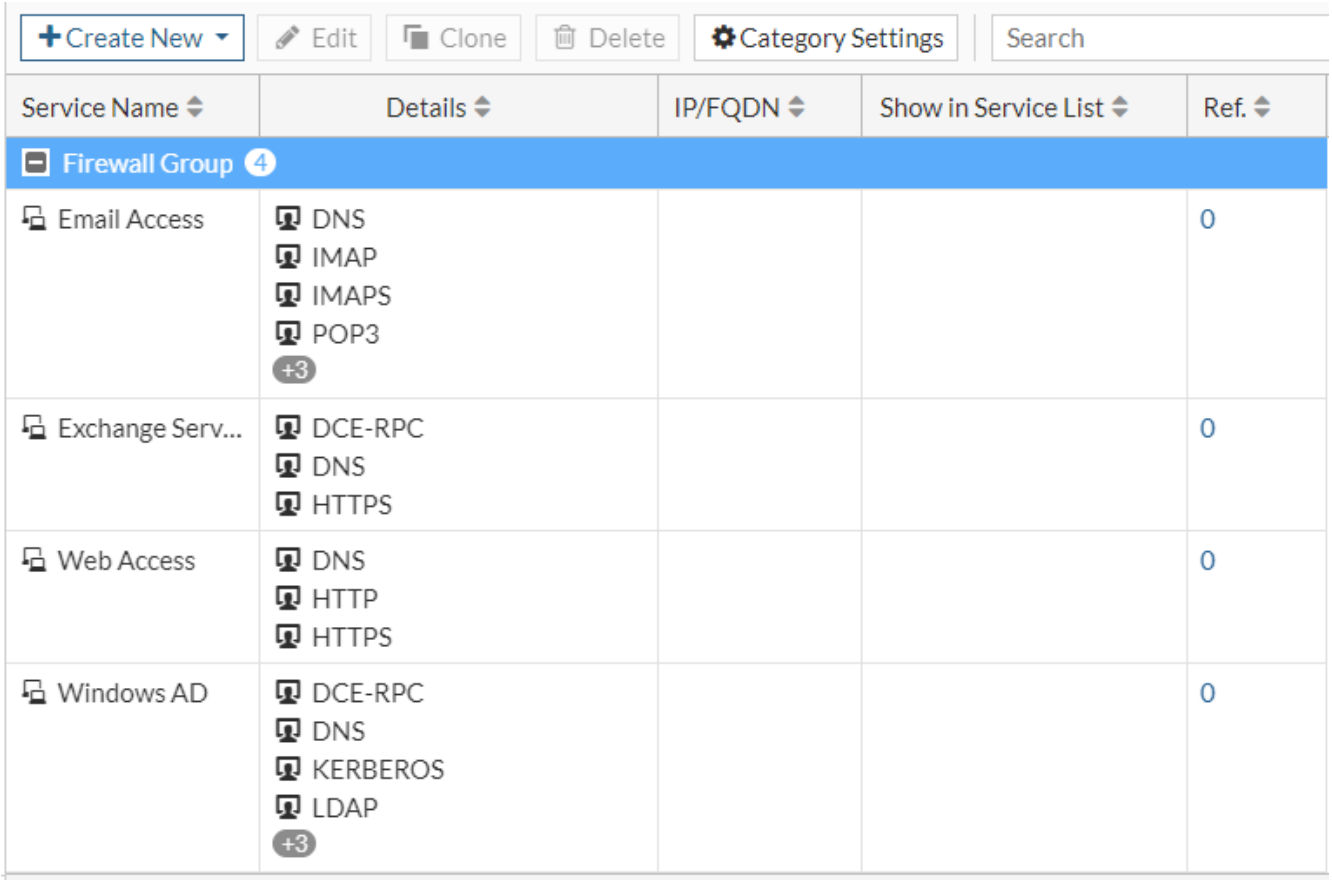
You can organize multiple services into a service group to simplify your policy list. For example, instead of having five identical policies for five different but related services, you can combine the five services into a single service group that is used by a single policy.

Service groups cannot contain other service groups.

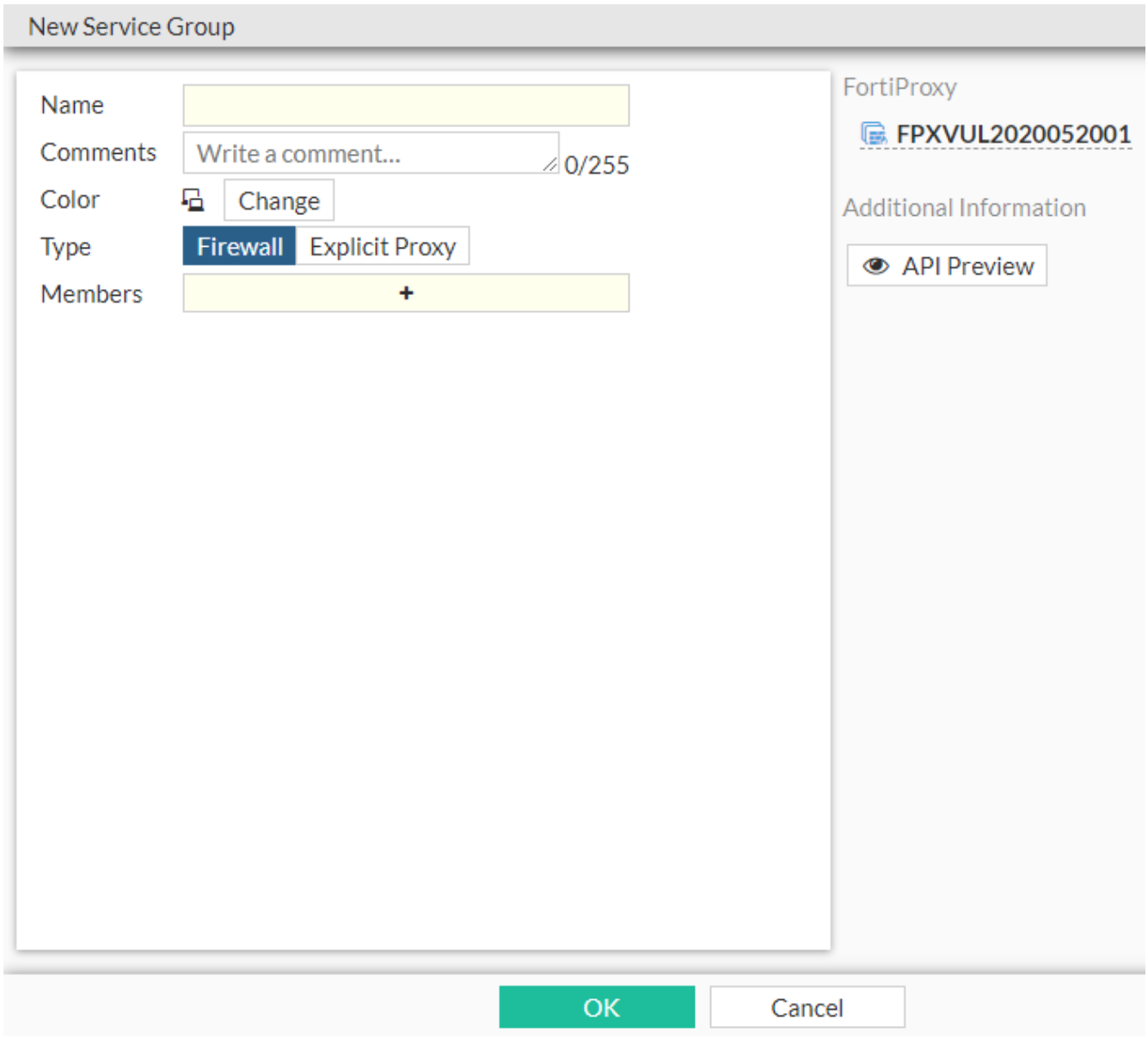
Configure a service group using the following CLI commands:

```
config firewall service group
   edit <name>
      set member // Address group member.
      set explicit-proxy // Enable or disable the explicit web proxy service group.
      set comment            // Comment.
      set color              // GUI icon color.
   next
end
```

Service groups are listed in the Firewall Group category.



Select *Create New* > *Service Group* to open the *New Service Group* window.



To open the *Edit Service Group* window, select a firewall group and then click *Edit*.

Configure the following settings in the *New Service Group* window or the *Edit Service Group* window and then click *OK*:

Name	Enter a name for the service group.
Comments	Optionally, enter a description of the service group.
Color	Select *Change* to choose a color for the icon.
Type	Select the type of service group, either *Firewall* or *Explicit Proxy*.
Members	Select the services to add to the service group.

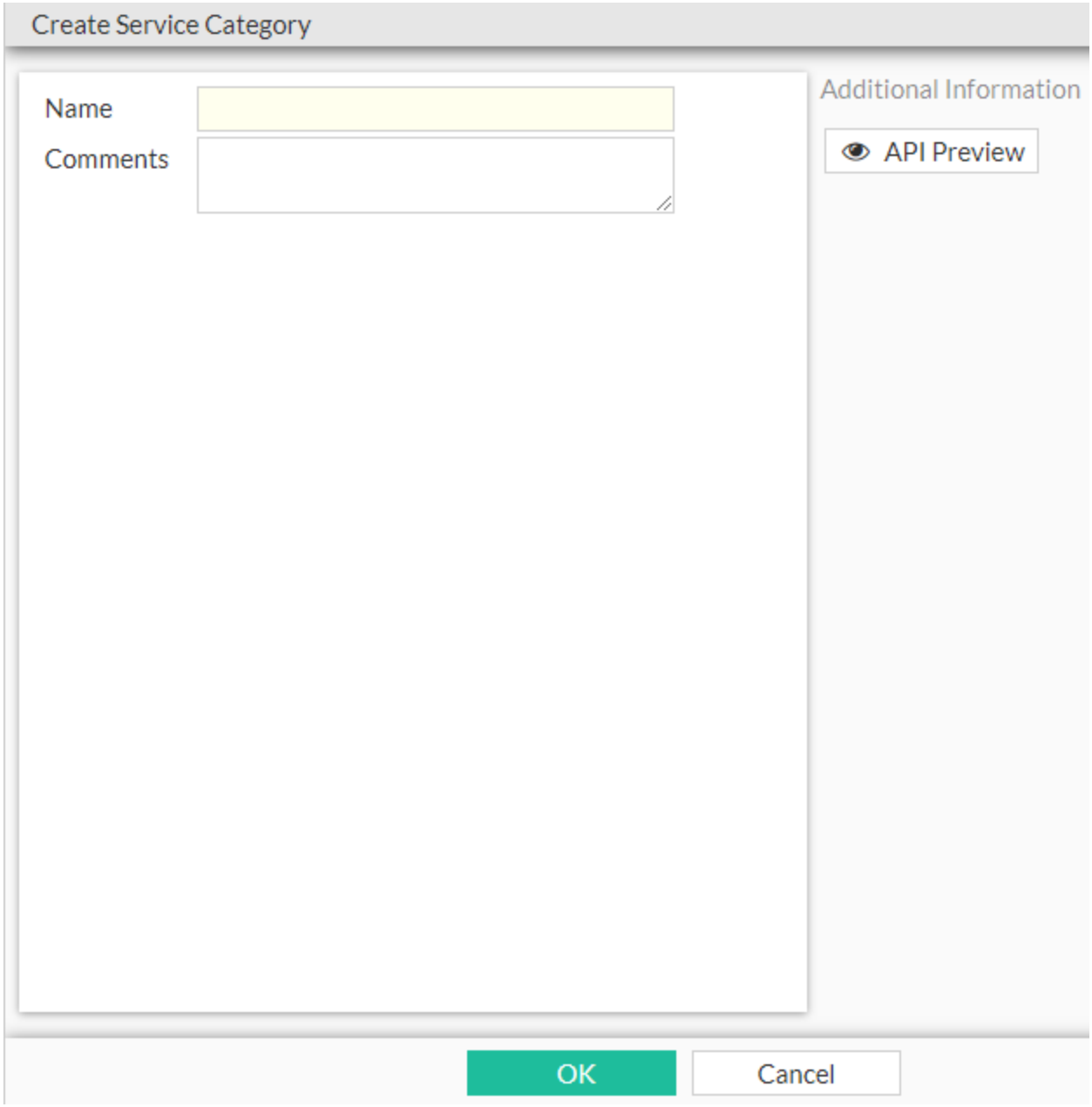
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create a service category

1. Go to *Policy & Objects* > *Services* and select *Create New* > *Category*.



2. Enter a name for the new category in the *Name* field.
3. Optionally, enter a description of the category in the *Comments* field.
4. Click *OK* to create the new service category.

Schedules

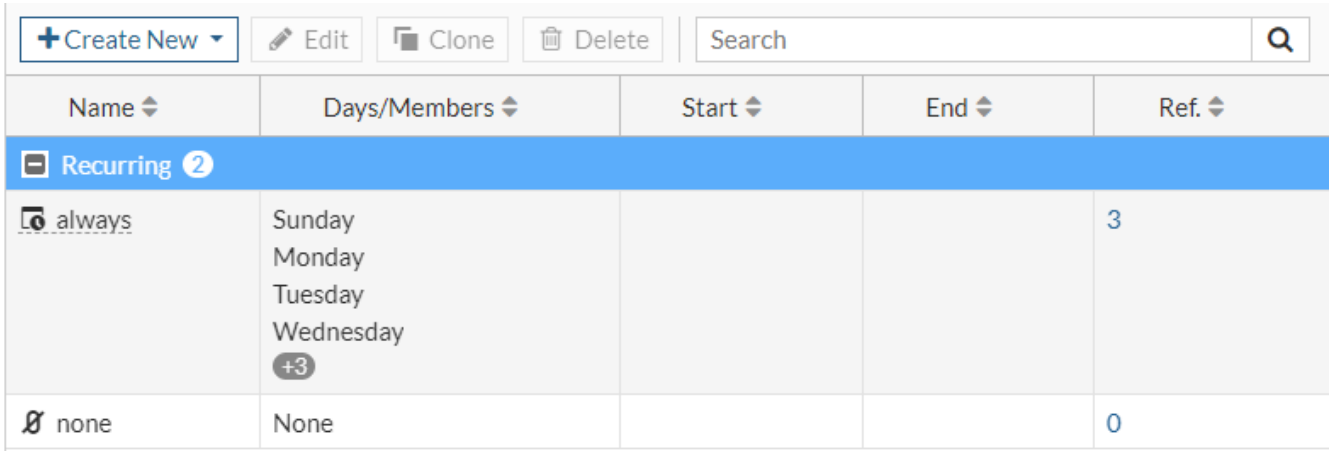
When you add security policies on a FortiProxy unit, those policies are always on, policing the traffic through the device. Schedules control when policies are in effect.

The schedule list lists all of the schedules. Recurring and one-time schedules can be created, edited, and deleted as needed.

You can create a recurring schedule that activates a policy during a specified period of time. If a recurring schedule has a stop time that is earlier than the start time, the schedule will take effect at the start time but end at the stop time on the next day. You can use this technique to create recurring schedules that run from one day to the next. To create a recurring schedule that runs for 24 hours, set the start and stop times to 00.

You can create one-time schedules, which are schedules that are in effect only once for the period of time specified in the schedule.

To manage schedules, go to *Policy & Objects* > *Schedules*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

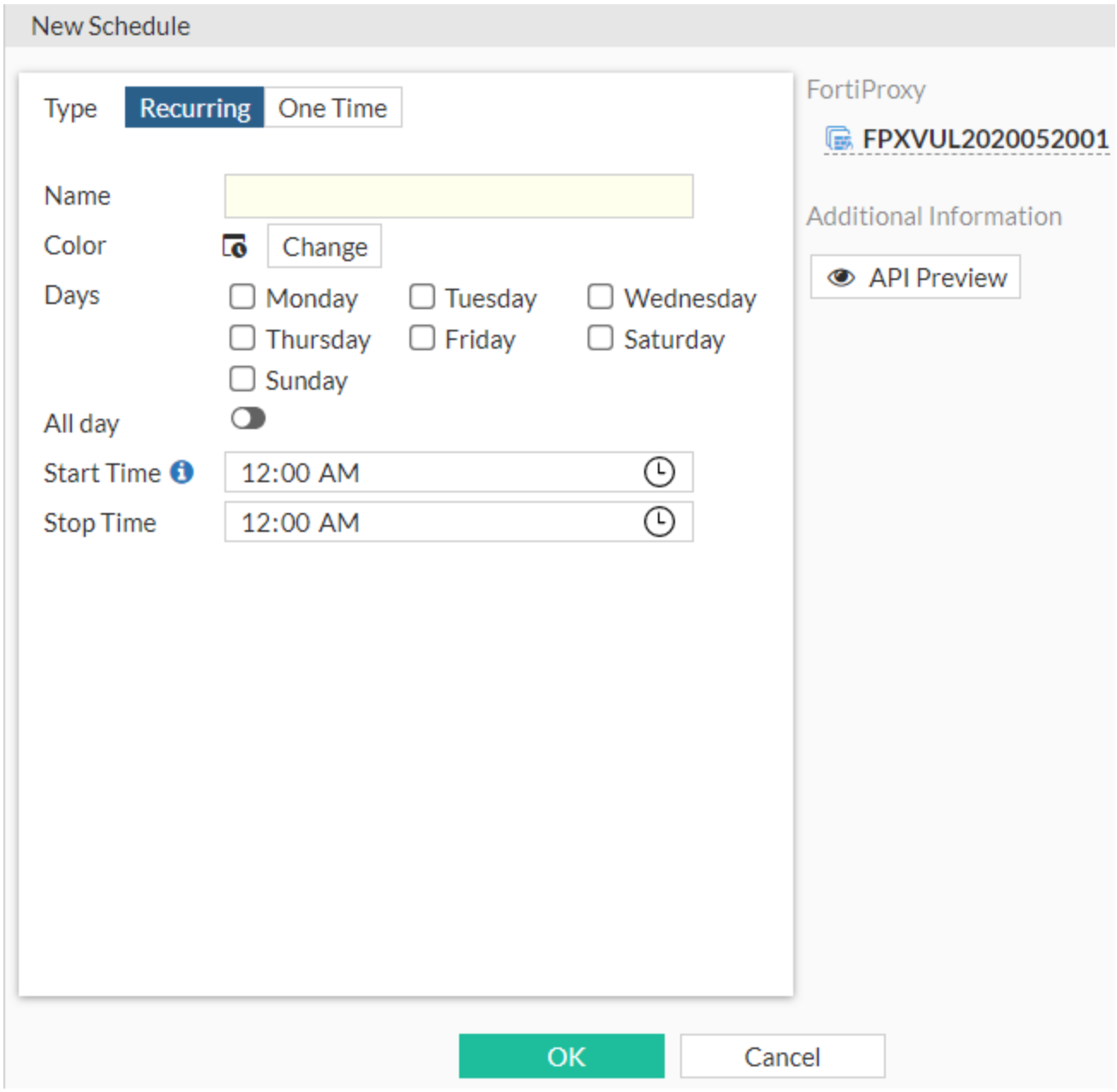
Create New	Create a schedule or a schedule group. See Create or edit a schedule on page 517 or Create or edit a schedule group on page 519.
Edit	Edit the selected schedule or schedule group. See Create or edit a schedule on page 517 or Create or edit a schedule group on page 519.
Clone	Make a copy of the selected schedule or schedule group.
Delete	Remove the selected schedule. This icon is only available if the selected schedule is not currently being used in a policy.
Search	Enter a search term to search the schedule list.

Name	The name of the schedule.
Days/Members	The days of the week that the schedule is configured to be active.
Start	The time of day that the schedule is configured to start.
End	The time of day that the schedule is configured to end.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Type	The type of schedule, either *Recurring* or *One-Time*.

Create or edit a schedule

When you add security policies on a FortiProxy unit, those policies are always on, policing the traffic through the device. Schedules control when policies are in effect.

Select *Create New* > *Schedule*to open the *New Schedule* window.



To open the *Edit Schedule* window, select a schedule and then click *Edit*.

Configure the following settings in the *New Schedule* window or the *Edit Schedule* window and then click *OK*:

Type	Select *Recurring* or *One- Time*.
Name	Enter a name for the schedule.
Color	Click *Change* to choose a color for the icon.
Days	If you selected a recurring schedule, select the days of the week when the schedule will be active.

All Day	If you selected a recurring schedule and the scheduled time is the whole day, enable *All Day*. If the schedule is for specific times during the day, disable *All Day*.
Start Date	If you select a one-time schedule, select the year, month, and day that the schedule will start. The start date must be earlier than the stop date.
Start Time	If you select a recurring schedule and disable *All Day* of if you select a one-time schedule, select the start time for the schedule.
End Date	If you select a one-time schedule, select the year, month, and day that the schedule will stop. The end date must be later than the start date.
Stop Time	If you select a recurring schedule and disable *All Day* of if you select a one-time schedule, select the stop time for the schedule. If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will run for 24 hours.
Pre-expiration event log	If you select a one-time schedule, enable this option to generate an event log before the schedule expires and then enter the number of days before the expiration that the event log will be generated, from 1 to 100.
Number of days before	If you select a one-time schedule, enter the number of days before the schedule expires to generate an event log. The range is 1-100 days).
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

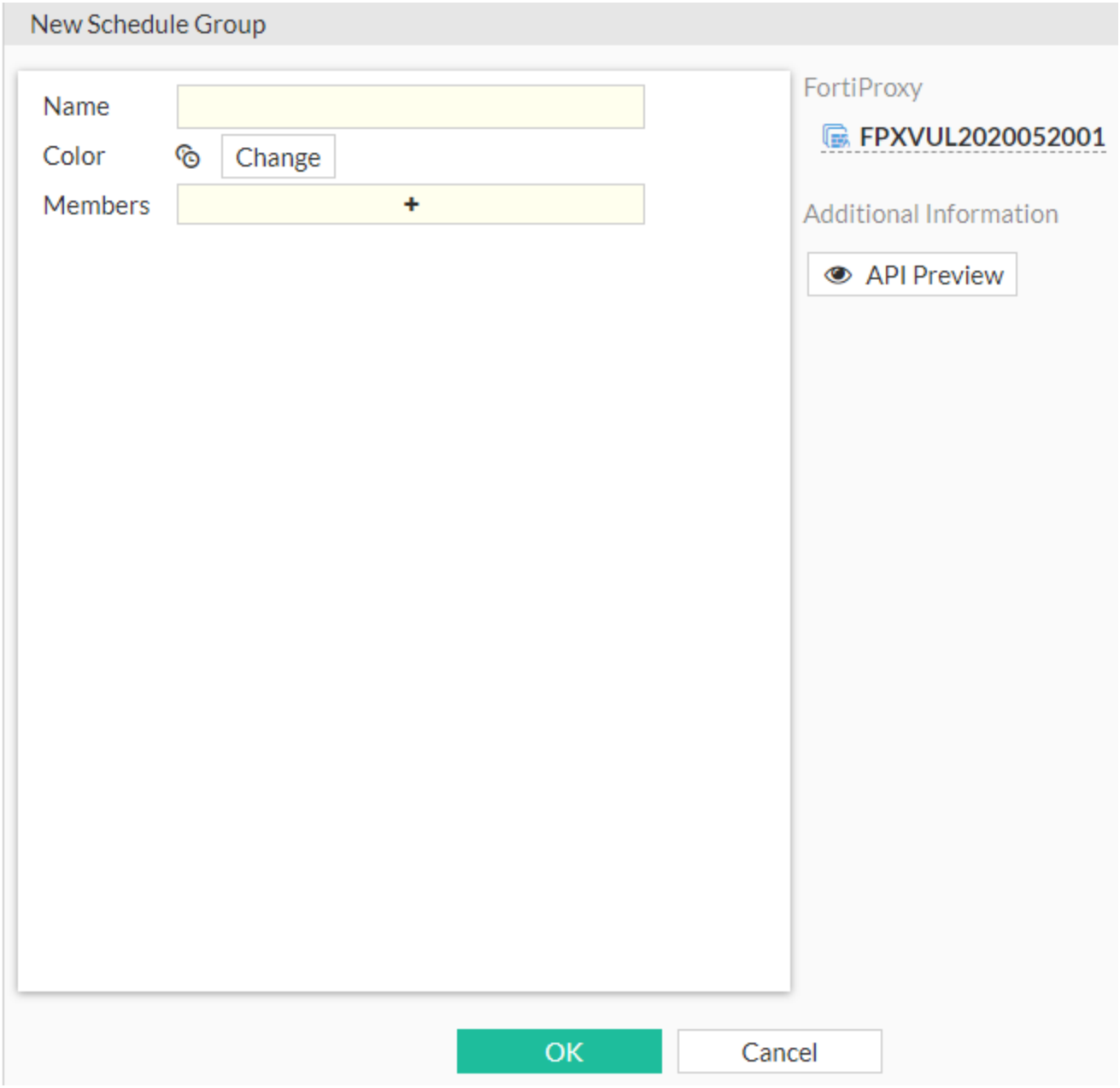
1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create or edit a schedule group

You can organize multiple schedules into a schedule group to simplify your security policy list. For example, instead of having five identical policies for five different but related schedules, you might combine the five schedules into a single schedule group that is used by a single security policy.

Schedule groups can contain both recurring and one-time schedules. Schedule groups cannot contain other schedule groups.

Select *Create New* > *Schedule Group*to open the *New Schedule Group* window.



To open the *Edit Schedule Group* window, select a schedule group and then click *Edit.*

Configure the following settings in the *New Schedule Group* window or the *Edit Schedule Group* window and then click *OK*:

Name	Enter the name of the schedule group.
Color	Click *Change* to choose a color for the icon.

Members	Select the schedules that you want to have included in the group from the drop-down menu.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Virtual IPs

Static Virtual IPs (VIP) are used to map external IP addresses to internal IP addresses. This is also called destination NAT, where a packet's destination is being NAT'd, or mapped, to a different address.

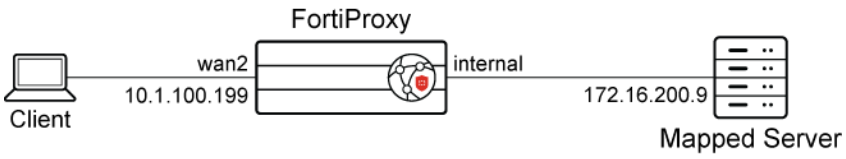
Static VIPs are commonly used to map public IP addresses to resources behind the FortiProxy unit that use private IP addresses. A static on-to-one VIP is when the entire port range is mapped. A port forwarding VIP is when the mapping is configured on a specific port or port range. See Virtual IPs with port forwarding on page 527 for more information.



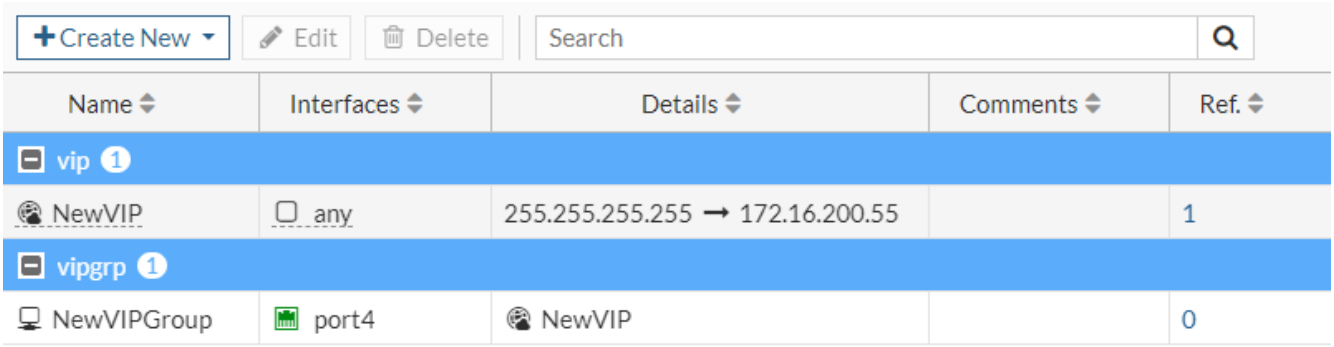
VIPs are considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). In this case, the FortiProxy is considered a destination for those IP addresses and can receive reply traffic at the application layer successfully.

However, as a side-effect, once a VIP has been configured, even if it is never used in a policy, the FortiProxy considers it as a local address and will not forward traffic based on the routing table. Therefore, any unused VIPs should be deleted to prevent any unexpected behavior.

Sample configuration



To view the virtual IPs, go to *Policy & Objects* > *Virtual IPs*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

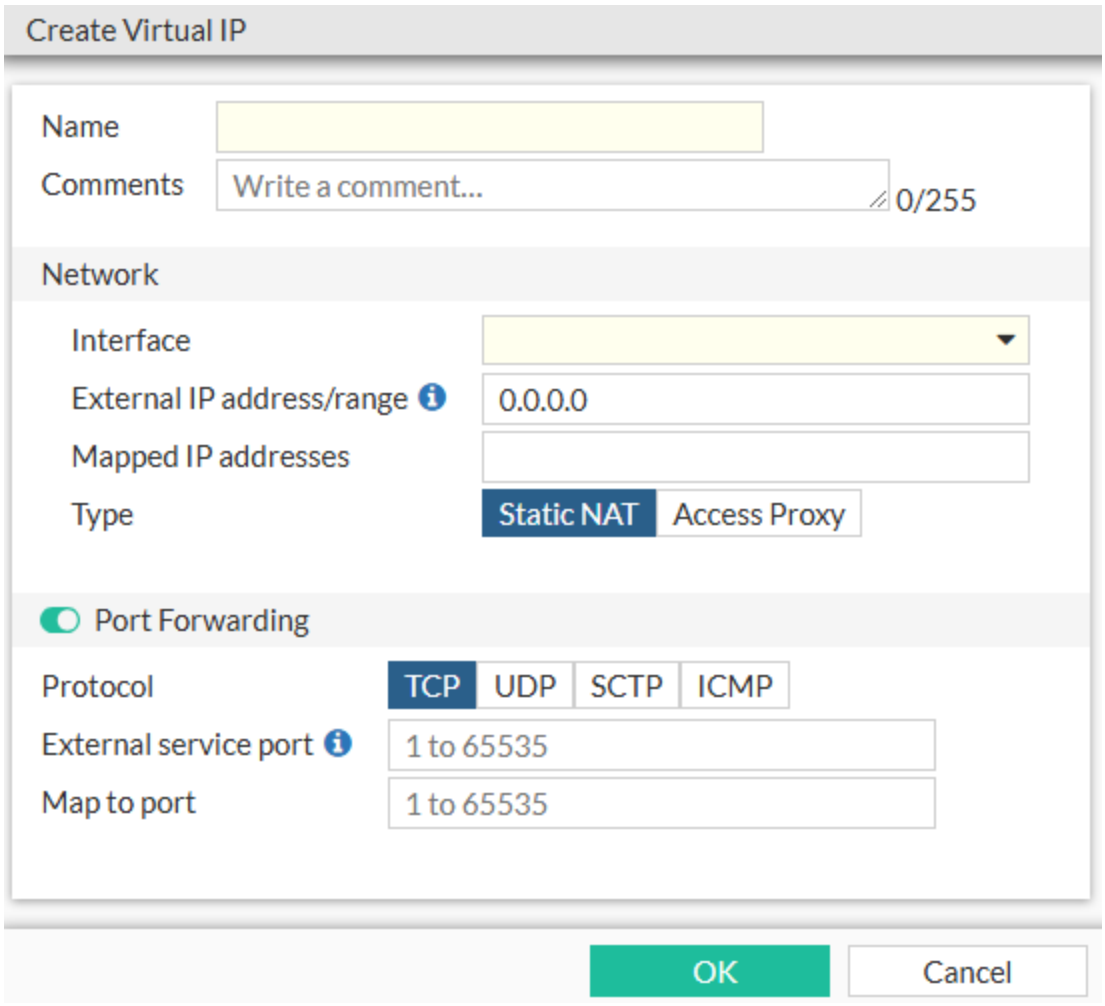
Create New > Virtual IP	Add a new virtual IP. See Create or edit a virtual IP on page 522.
Create New > Virtual IP Group	Add a new virtual IP group. See Create or edit a virtual IP group on page 526.
Edit	Edit the selected virtual IP or virtual IP group. See Create or edit a virtual IP on page 522 or Create or edit a virtual IP group on page 526
Delete	Remove the selected virtual IP or virtual IP group.
Search	Search for text in any column.
Name	The name of the virtual IP or virtual IP group.
Interfaces	The domain name.
Details	The interface to which the virtual IP or virtual IP group is bound.
Comments	Optional description of the virtual IP or virtual IP group.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
extip	External IP address or range for the virtual IP.

Create or edit a virtual IP

Virtual IPs can be configured for IPv4 and then be added to a policy. FortiProxy does not check whether VIPs overlap. As a result, you can configure multiple VIPs with the same external interface and IP. However, you can view overlapping VIPs in the security rating report. See Viewing VIP overlap in security rating reports on page 525.

To configure a VIP in the GUI:

1. Go to *Policy & Objects* > *Virtual IPs*.
2. Click *Create New* and select *Virtual IP* .
3. Configure the following settings:



Name		Enter a name for the VIP.
Comments		Enter a description of the VIP.
Network		
	Interface (`extintf`)	The external interface that the policy source interface must match. For example, if the external interface is port1, then the VIP can be used in a policy from port1 to port3, but not in a policy from port2 to port3. If the external interface is *any*, then the VIP can be used in any policy.

	External IP address/range (extip)	In a static NAT VIP, the external IP address is the IP address that the FortiProxy listens for traffic on. When the external interface is not *any*, 0.0.0.0 can be used to make the external IP address equivalent to the external interface's IP address. The external IP address is also used to perform SNAT for the mapped server when the server outbound traffic with a destination interface that matches the external interface. The policy must also have NAT enabled.
	Mapped IP addresses (mappedip)	The IPv4 address or range that the internal resource is being mapped to.
	Type (type)	Type of the virtual IP: • *Static NAT* - Use an external IP address or address range. • *Access Proxy* - Used for ZTNA. See ZTNA HTTPS access proxy example on page 292 for details.
Port Forwarding (portforward)		Enable port forwarding and display additional options, such as the port (mappedport) to map to. See Virtual IPs with port forwarding on page 527 for more information.
	Protocol (protocol)	Select the protocol to use when forwarding packets to the port.
	External service port (extport)	Enter the external service port range to be mapped to a port range on the destination network.
	Map to port (mappedport)	Enter the mapped IPv4 port range on the destination network.

4. Click *OK* to save the VIP.

To create a virtual IP in the CLI:

```
config firewall vip
   edit "Internal_WebServer"
      set extip 10.1.100.199
      set extintf "any"
      set mappedip "172.16.200.55"
   next
end
```

To apply a virtual IP to policy in the CLI:

```
config firewall policy
    edit 8
        set name "Example_Virtual_IP_in_Policy"
```

```
        set srcintf "wan2"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "Internal_WebServer"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

Viewing VIP overlap in security rating reports

There is no overlap check for VIPs, so there are no constraints when configuring multiple VIPs with the same external interface and IP. A new security rating report alerts users of any VIP overlaps.

To configure two VIPs with the same external interface and IP:

```
config firewall vip
    edit "test-vip44-1"
        set extip 10.1.100.154
        set mappedip "172.16.200.156"
        set extintf "port24"
    next
    edit "test-vip44-1_clone"
        set extip 10.1.100.154
        set mappedip "172.16.200.156"
        set extintf "port24"
        set src-filter 10.1.100.11
    next
end
```



No error message appears regarding the overlapping VIPs.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create or edit a virtual IP group

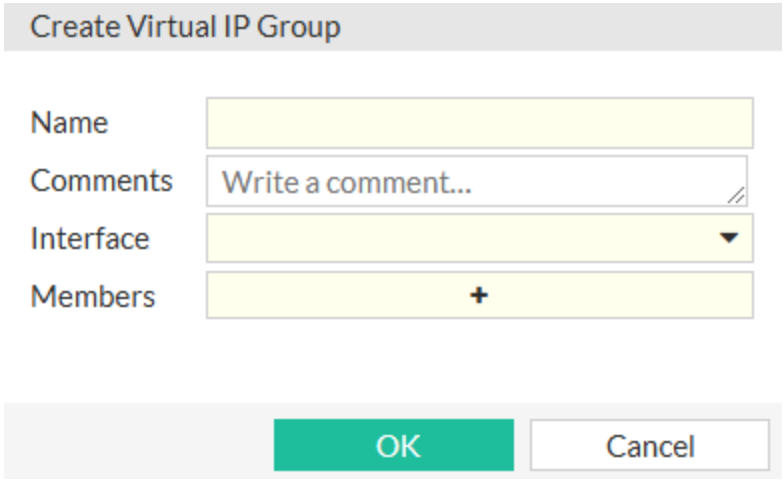
Just like other addresses, virtual IP addresses (VIPs) can be organized into groups for ease of administration when multiple VIPs are used together in policies. If you have multiple virtual IPs that are likely to be associated to common policies, you can create a virtual IP group and add the group to the policies instead of adding individual VIPs to each of the policies .If the VIP group members change, or a group member's settings change (such as the IP address and port), then those changes are automatically updated in the corresponding policies.

Different VIP types can be added to the same group. The following table summarizes which VIP types are allowed and not allowed to be members of a VIP group.

VIP types allowed as members	VIP types not allowed as members
• Static NAT • Load balance	• Access proxy

To configure a VIP group in the GUI:

1. Go to *Policy & Objects* > *Virtual IPs*.
2. Click *Create New* and select *Virtual IP Group*.
3. Configure the following settings:



Name	Enter a unique name to identify the virtual IP group.
Comments	Optionally, enter a description of the virtual IP group.
Interface	Use the drop-down menu to select the interface if all of the VIPs are on the same interface. If any of the VIPS are on different interfaces or if any of them are associated with the "any" option, choose the any option for the group.
Members	Select the virtual IPs to add to the virtual IP group.

4. Click *OK* to save the VIP group.

To configure a VIP group in the CLI:

```
config firewall vipgrp
    edit <name>
        set interface <name>
        set member <vip1> <vip2> ...
    next
end
```

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Virtual IPs with port forwarding

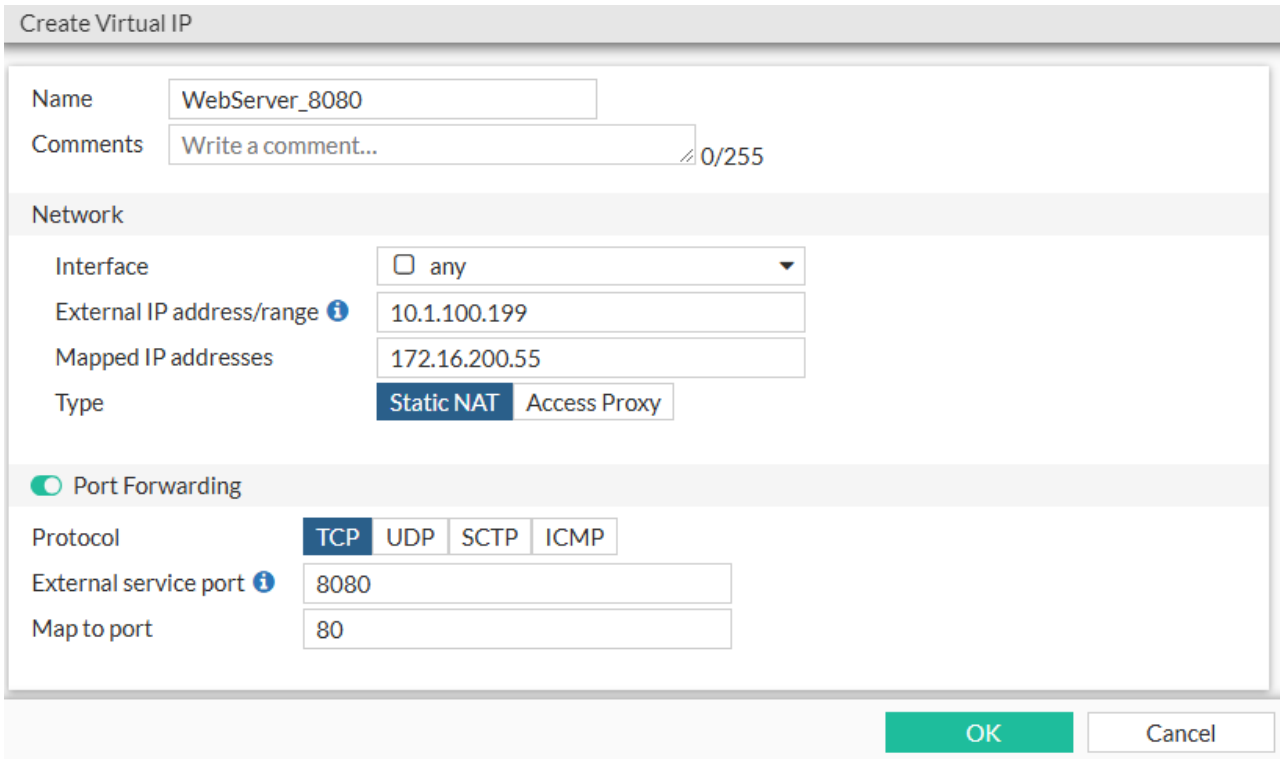
If you need to hide the internal server port number or map several internal servers to the same public IP address, enable port-forwarding for Virtual IP.

This topic shows how to use virtual IPs to configure port forwarding on a FortiProxy unit. This example has one public external IP address. We map TCP ports 8080, 8081, and 8082 to different internal WebServers' TCP port 80. This allows remote connections to communicate with a server behind the firewall.

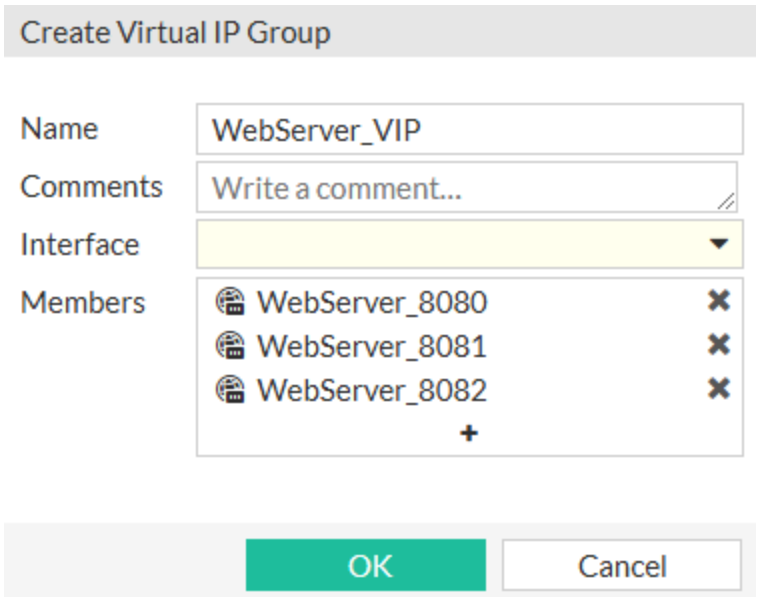
Sample configuration

To create a virtual IP with port forwarding in the GUI:

1. Go to *Policy & Objects* > *Virtual IPs*.
2. Click *Create New* > *Virtual IP*.
3. Enter a unique name for the virtual IP.
4. Configure the fields in the *Network* section. For example:
   - Set *Interface* to *any*.
   - Set *External IP address/range* to *10.1.100.199*.
   - Set *Mapped IP addresses* to *172.16.200.55*.
   - Set Type to *Static NAT*.
5. Enable *Port Forwarding* and configure the fields. For example:
   - Set *Protocol* to *TCP*.
   - Set *External service port* to *8080*.
   - Set *Map to port* to *80*.



6. Click *OK*.
7. Follow the above steps to create two additional virtual IPs.
   a. For one virtual IP:
      - Use a different *Mapped IP address/range*, for example *172.16.200.56*.
      - Set *External service port* to *8081*.
      - Use the same *Map to port* number: *80*.
   b. For the other virtual IP:
      - Use a different *Mapped IP address/range*, for example *172.16.200.57*.
      - Set *External service port* to *8082*.
      - Use the same *Map to port* number: *80*.
8. Create a *Virtual IP Group* and put the above three virtual IPs into that group:
   a. Go to *Policy & Objects > Virtual IPs*.
   b. Click *Create New > Virtual IP Group*.
   c. Enter a name for the group.
   d. Add the three previously created virtual IPs as members.



e. Click *OK*.

To see the results:

1. Apply the above virtual IP to the policy.
2. The results are:
   - Access 10.1.100.199:8080 from external network and FortiProxy maps to 172.16.200.55:80 in internal network.
   - Access 10.1.100.199:8081 from external network and FortiProxy maps to 172.16.200.56:80 in internal network.
   - Access 10.1.100.199:8082 from external network and FortiProxy maps to 172.16.200.57:80 in internal network

Virtual server load balance

This topic shows a special virtual IP type: virtual server. Use this type of VIP to implement server load balancing.

The FortiProxy server load balancing contains all the features of a server load balancing solution. You can balance traffic across multiple backend servers based on multiple load balancing schedules including:

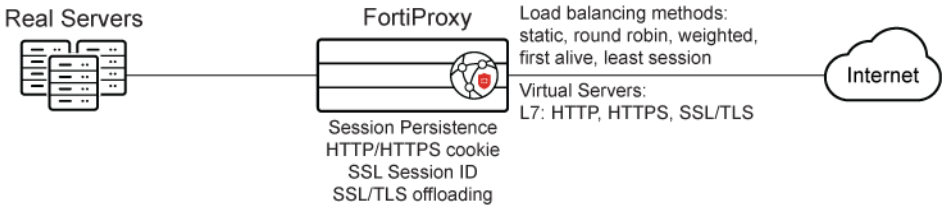
- Static (failover)
- Round robin
- Weighted (to account for different sized servers or based on the health and performance of the server including round trip time and number of connections)

The load balancer supports HTTP, HTTPS, IMAPS, POP3S, SMTPS, and SSL/TLS protocols. Session persistence is supported based on the SSL session ID based on an injected HTTP cookie, or based on the HTTP or HTTPS host. SSL/TLS load balancing includes protection from protocol downgrade

attacks. Server load balancing is supported on most FortiProxy devices and includes up to 10,000 virtual servers on high-end systems.

FortiProxy HTTP and HTTPS server load balancing does not support load balancing based on URL routing. You can use FortiWeb server pools or FortiADC server load balancing to load balance sessions to two or more URL based routes.

Sample topology



SSL/TLS offloading

FortiProxy SSL/TLS offloading is designed for the proliferation of SSL/TLS applications. The key exchange and encryption/decryption tasks are offloaded to the FortiProxy unit where they are accelerated using FortiASIC technology which provides significantly more performance than a standard server or load balancer. This frees up valuable resources on the server farm to give better response to business operations. Server load balancing offloads most SSL/TLS versions including SSL 3.0, TLS 1.0, and TLS 1.2, and supports full mode or half mode SSL offloading with DH key sizes up to 4096 bits.

FortiProxy SSL offloading allows the application payload to be inspected before it reaches your servers. This prevents intrusion attempts, blocks viruses, stops unwanted applications, and prevents data loss. SSL/TLS content inspection supports TLS versions 1.0, 1.1, and 1.2 and SSL versions 1.0, 1.1, 1.2, and 3.0.

Virtual server requirements

When creating a new virtual server, you must configure the following options:

- Virtual Server Type.
- Load Balancing Methods.
- Session persistence (optional).
- Virtual Server IP (External IP Address).
- Virtual Server Port (External Port).
- Real Servers (Mapped IP Address & Port).

Virtual server types

Select the protocol to be load balanced by the virtual server. You can apply additional server load balancing features such as *Persistence* and *HTTP Multiplexing*.

HTTP	Select *HTTP* to load balance only HTTP sessions with the destination port number that matches the *Virtual Server Port* setting. Change *Virtual Server Port* to match the destination port of the sessions to be load balanced (usually port 80 for HTTP sessions). You can enable *HTTP Multiplexing*. You can also set *Persistence* to *HTTP Cookie* to enable cookie-based persistence.
HTTPS	Select *HTTPS* to load balance only HTTPS sessions with the destination port number that matches the *Virtual Server Port* setting. Change *Virtual Server Port* to match the destination port of the sessions to be load balanced (usually port 443 for HTTPS sessions). You can enable *HTTP Multiplexing*. You can also set *Persistence* to *HTTP Cookie* to enable cookie-based persistence, or you can set *Persistence* to *SSL Session ID*.
IMAPS	Select *IMAPS* to load balance only IMAPS sessions with the destination port number that matches the *Virtual Server Port* setting. Change *Virtual Server Port* to match the destination port of the sessions to be load balanced (usually port 993 for IMAPS sessions). You can also set *Persistence* to *SSL Session ID*.
POP3S	Select *POP3S* to load balance only POP3S sessions with the destination port number that matches the *Virtual Server Port* setting. Change *Virtual Server Port* to match the destination port of the sessions to be load balanced (usually port 995 for POP3S sessions). You can also set *Persistence* to *SSL Session ID*.
SMTPS	Select *SMTPS* to load balance only SMTPS sessions with the destination port number that matches the *Virtual Server Port* setting. Change *Virtual Server Port* to match the destination port of the sessions to be load balanced (usually port 465 for SMTPS sessions). You can also set *Persistence* to *SSL Session ID*.
SSL	Select *SSL* to load balance only SSL sessions with the destination port number that matches the *Virtual Server Port* setting. Change *Virtual Server Port* to match the destination port of the sessions to be load balanced. You can also set *Persistence* to *SSL Session ID*.

Load balancing methods

The load balancing method defines how sessions are load balanced to real servers. When a real server is down or not responding, no traffic will be sent to it.

Static	The traffic load is statically spread evenly across all real servers. Sessions are not assigned according to how busy individual real servers are. This load balancing method provides some persistence because all sessions from the same source address always go to the same real server. Because the distribution is stateless, so if a real server is added, removed, or goes up or down, the distribution is changed and persistence might be lost.

Round Robin	Directs new requests to the next real server. This method treats all real servers as equals regardless of response time or the number of connections. This method does not direct requests to real servers that down or non responsive.
Weighted	Real servers with a higher weight value receive a larger percentage of connections. Set the real server weight when adding a real server.
Least Session	Directs requests to the real server that has the least number of current connections. This method works best in environments where the real servers or other equipment you are load balancing all have similar capabilities. This load balancing method uses the FortiProxy session table to track the number of sessions being processed by each real server. The FortiProxy unit cannot detect the number of sessions actually being processed by a real server.
First Alive	Directs sessions to the first live real server. This load balancing schedule provides real server failover protection by sending all sessions to the first live real server. If a real server fails, all sessions are sent to the next live real server. Sessions are not distributed to all real servers so all sessions are processed by the first real server only.

Session persistence

Use persistence to ensure a user is connected to the same real server every time the user makes an HTTP, HTTPS, or SSL request that is part of the same user session. For example, if you are load balancing HTTP and HTTPS sessions to a collection of eCommerce web servers, when users make a purchase, they will be starting multiple sessions as they navigate the eCommerce site. In most cases, all the sessions started by this user during one eCommerce session should be processed by the same real server. Typically, the HTTP protocol keeps track of these related sessions using cookies. HTTP cookie persistence ensure all sessions that are part of the same user session are processed by the same real server.

When you configure persistence, the FortiProxy unit load balances a new session to a real server according to the load balance method. If the session has an HTTP cookie or an SSL session ID, the FortiProxy unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server.

Real servers

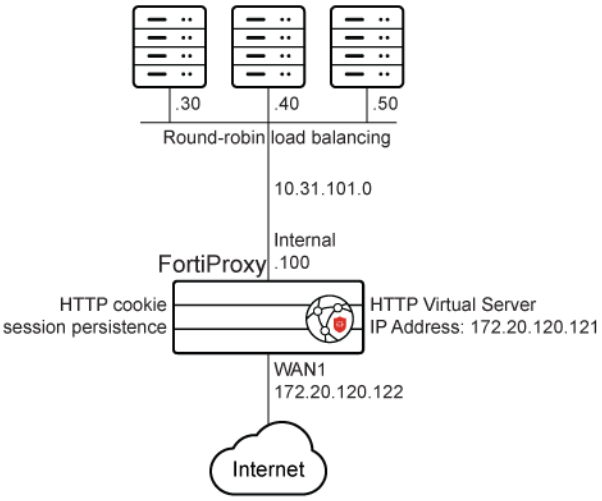
Add real servers to a load balancing virtual server to provide information the virtual server requires to send sessions to the server. A real server configuration includes the IP address of the real server and port number the real server receives sessions on. The FortiProxy unit sends sessions to the real server's IP address using the destination port number in the real server configuration.

When configuring a real server, you can also specify the weight (if the load balance method is set to *Weighted*) and you can limit the maximum number of open connections between the FortiProxy unit and the real server. If the maximum number of connections is reached for the real server, the FortiProxy unit automatically switches all further connection requests to other real servers until the connection number drops below the limit. Setting *Maximum Connections* to 0 means that the FortiProxy unit does not limit the number of connections to the real server.

Sample of HTTP load balancing to three real web servers

This example describes the steps to configure the load balancing configuration below. In this configuration, a FortiProxy unit is load balancing HTTP traffic from the Internet to three HTTP servers on the internal network. HTTP sessions are accepted at the wan1 interface with destination IP address 172.20.120.121 on TCP port 8080, and forwarded from the internal interface to the web servers. When forwarded, the destination address of the session is translated to the IP address of one of the web servers.

This load balancing configuration also includes session persistence using HTTP cookies and round-robin load balancing for the real servers.



General steps:

1. Create a load balance virtual server with three real servers. This can only done in the CLI
2. Add the load balancing virtual server to a policy as the destination address.

Configure a load balancing virtual server

To configure HTTP load balancing to three real web servers:

```
config firewall vip
    edit "Vserver-HTTP-1"
        set type server-load-balance
        set extip 172.20.120.121
        set extintf "any"
        set server-type http
        set ldb-method round-robin
        set persistence http-cookie
        set extport 8080
        config realservers
            edit 1
                set type ip
```

```
                set ip 10.31.101.30
                set port 80
            next
            edit 2
                set type ip
                set ip 10.31.101.40
                set port 80
            next
            edit 3
                set type ip
                set ip 10.31.101.50
                set port 80
            next
        end
    next
end
```

To create a policy that includes the load balance virtual server as the destination address:

GUI:

1. Go to *Policy & Objects > Policy*.
2. Click *Create New*.
3. Set the following:
   - *Name* to *LB-policy*
   - *Incoming Interface* to *wan1*
   - *Outgoing Interface* to *internal*
   - *Source* to *all*
   - *Destination* to *Vserver-HTTP-1*
   - *Schedule* to *always*
   - *Service* to *ALL*
   - *Action* to *ACCEPT*
4. Enable *AntiVirus* and select an antivirus profile.
5. Click *OK*.

CLI:

```
config firewall policy
    edit 2
        set name "LB-policy"
        set srcintf "wan1"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "Vserver-HTTP-1"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
```

```
    next
end
```

Results

Traffic accessing 172.20.120.121:8080 is forwarded in turn to the three real servers.

If the access request has an http-cookie, FortiProxy forwards the access to the corresponding real server according to the cookie.

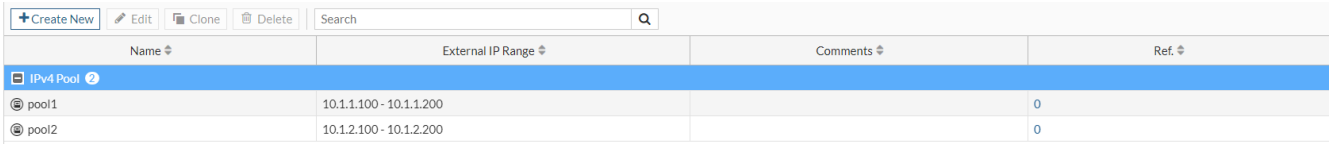
IP Pools

IP pools are a mechanism that allow sessions leaving the FortiProxy unit to use NAT. An IP pool defines a single IP address or a range of IP addresses to be used as the source address for the duration of a session. These assigned addresses are used instead of the IP address assigned to that FortiProxy interface.

IP pools are considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). In this case, the FortiProxy is considered a destination for those IP addresses and can receive reply traffic at the application layer successfully.

However, as a side-effect, once an IP pool has been configured, even if it is never used in a policy, the FortiProxy considers it as a local address and will not forward traffic based on the routing table. Therefore, any unused IP pools should be deleted to prevent any unexpected behavior.

To see which IP pools are configured, go to *Policy & Objects* > *IP Pools*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

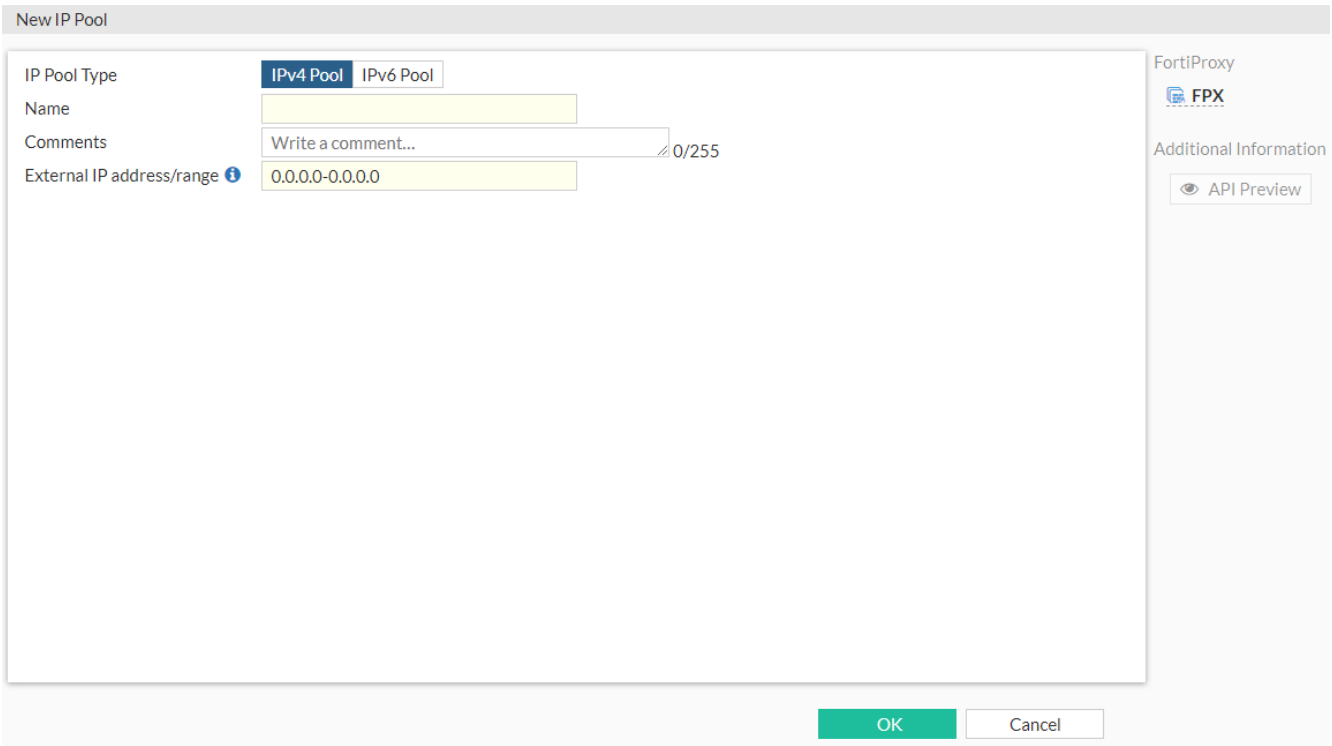
The following options are available:

Create New	Create an IP pool. See Create or edit an IP pool on page 536.
Edit	Edit the selected IP pool. See Create or edit an IP pool on page 536.
Clone	Make a copy of the selected IP pool.
Delete	Remove the selected IP pool.
Search	Enter a search term to search the IP pool list.

Name	The name of the IP pool.
External IP Range	The lowest and highest IP addresses in the range.
Comments	An optional description of the IP pool.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.

Create or edit an IP pool

Select *Create New* to open the *New IP Pool* window.



To open the *Edit IP Pool* window, select an IP pool and then click *Edit*.

Configure the following settings in the *New IP Pool* window or *Edit IP Pool* window and then click *OK*:

To create an IP pool:

IP Pool Type	Select *IPv4 Pool* if your IP pool contains IPv4 addresses or select *IPv6 Pool* if your IP pool contains IPv6 addresses.
Name	Enter a name for the IP pool in the *Name* field.

Comments	Add an optional description of the IP pool.
External IP address/range	Enter the lowest and highest IP addresses in the range. Separate IP addresses with a hyphen. If you only want a single address used, enter the same address in both fields.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Security Profiles

The FortiProxy unit combines a number of security features to protect your network from threats. As a whole, these features, when included in a single Fortinet security appliance, are referred to as security profiles.

A profile is a group of settings that you can apply to one or more firewall policies. Each Security Profile feature is enabled and configured in a profile, list, or sensor. These are then selected in a security policy and the settings apply to all traffic matching the policy. For example, if you create an antivirus profile that enables antivirus scanning of HTTP traffic, and select the antivirus profile in the security policy that allows your users to access the World Wide Web, all of their web browsing traffic will be scanned for viruses.

Because you can use profiles in more than one security policy, you can configure one profile for the traffic types handled by a set of firewall policies requiring identical protection levels and types, rather than repeatedly configuring those same profile settings for each individual security policy.

For example, while traffic between trusted and untrusted networks might need strict protection, traffic between trusted internal addresses might need moderate protection. To provide the different levels of protection, you might configure two separate sets of profiles: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks. FortiProxy does not modify the original payload if no security action is taken.

This section covers the following topics:

- Antivirus on page 541
- Web Filter on page 565
- Video Filter on page 580
- DNS Filter on page 588
- Application Control on page 598
- Intrusion Prevention on page 618
- File Filter on page 622
- SSL/SSH Inspection on page 625
- Application Signatures on page 644
- IPS Signatures on page 647
- Web Rating Overrides on page 650
- Web Profile Overrides on page 654
- Profile Groups on page 657
- Data Loss Prevention on page 660
- DLP File Pattern on page 717

The following are brief descriptions of the security profiles and their features.

Antivirus

Your FortiProxy unit stores a virus signature database that can identify more than 15,000 individual viruses. FortiProxy models that support additional virus databases are able to identify hundreds of

thousands of viruses. With a FortiGuard Antivirus subscription, the signature databases are updated whenever a new threat is discovered.

Antivirus also includes file filtering. When you specify files by type or by file name, the FortiProxy unit will block the matching files from reaching your users.

FortiProxy units with a hard drive or configured to use a FortiAnalyzer unit can store infected and blocked files that you can examine later.

Web filter

Web filtering includes a number of features you can use to protect or limit your users' activity on the web.

FortiGuard Web Filtering is a subscription service that allows you to limit access to web sites. More than 60 million web sites and two billion web pages are rated by category. You can choose to allow or block each of the 77 categories.

URL filtering can block your network users from access to URLs that you specify.

Web content filtering can restrict access to web pages based on words and phrases appearing on the web page itself. You can build lists of words and phrases, each with a score. When a web content list is selected in a web filter profile, you can specify a threshold. If a user attempts to load a web page and the score of the words on the page exceeds the threshold, the web page is blocked.

You can create overrides to web filter profiles as well.

Video filter

With the video filter profile, you can filter YouTube videos by channel ID for a more granular override of a single channel, user, or video. The video filter profile is currently supported in proxy-based policies and requires SSL deep inspection.

DNS filter

The FortiProxy will inspect DNS traffic to any DNS server, so long as the policy has DNS inspection enabled. The FortiProxy will intercept DNS requests, regardless of the destination IP, and redirect it to the FortiGuard Secure DNS server—this is separate from the FortiGuard DNS server.

The Secure DNS server will resolve and rate the FQDN and send a DNS response which includes both IP and rating of the FQDN back to the FortiProxy, where it will handle the DNS response according to the DNS filter profile.

Application control

Although you can block the use of some applications by blocking the ports they use for communications, many applications do not use standard ports to communicate. Application control can detect the network traffic of more than 1,000 applications, improving your control over application communication.

You can also write custom signatures tailored to your network.

Intrusion protection

The FortiProxy Intrusion Protection System (IPS) protects your network against hacking and other attempts to exploit vulnerabilities of your systems. More than 3,000 signatures are able to detect exploits against various operating systems, host types, protocols, and applications. These exploits can be stopped before they reach your internal network.

You can also write custom signatures tailored to your network.

File filter

The file filter allows the FortiProxy unit to block files passing through based on file type based on the file's metadata only and not on file size or file content. A DLP sensor must be configured to block files based on size or content, such as SSN numbers, credit card numbers, or regular expression pattern. The file filter can be applied directly to firewall policies.

SSL/SSH inspection

SSL/SSH inspection (otherwise known as *deep inspection*) is used to scan HTTPS traffic in the same way that HTTP traffic can be scanned. This allows the FortiProxy to receive and open up the encrypted traffic on behalf of the client, then the traffic is re-encrypted and sent on to its intended destination.

Individual Deep Inspection profiles can be created, depending on the requirements of the policy. Depending on the profile, you can:

- Configure which CA certificate will be used to decrypt the SSL encrypted traffic
- Configure which SSL protocols will be inspected
- Configure which ports will be associated with which SSL protocols for inspection
- Configure whether or not to allow invalid SSL certificates
- Configure whether or not SSH traffic will be inspected

Data loss prevention

Data loss prevention (DLP) allows you to define the format of sensitive data. The FortiProxy unit can then monitor network traffic and stop sensitive information from leaving your network. Rules for U.S. social security numbers, Canadian social insurance numbers, as well as Visa, Mastercard, and American Express card numbers are included.

Order of execution of security profiles

1. Check the IP ban of the UTM quarantine.
2. For transparent HTTPS traffic, process TLS ClientHello with/without SNI:
   a. Check the firewall policy to determine what to allow or deny and which security profiles to apply, including TLS inspection mode, forwarding proxy, and so on.
   b. Check the TLS exemption of deep inspection if necessary.
   c. Check the URL filtering of the web-filtering profile based on hosts learned from TLS negotiation and whether web-filter-based exemptions need to be applied.
   d. Apply TLS sanity checks.

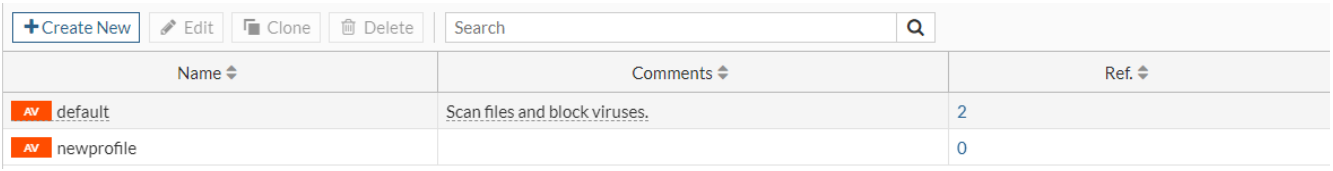
   e. If no deep inspection is needed, forward the traffic back and force with only possible IPS scans.
3. Process the HTTP request headers for plantext HTTP or decrypted HTTPS traffic:
   a. Check the firewall policy on the HTTP request to determine whether to allow or deny and which security profiles to apply:
      i. Check the TLS inspection mode for the HTTP CONNECT request.
      ii. Determine the forwarding proxy for plantext HTTP.
   b. Check the URL filtering of the web-filtering profile based on the URL in the HTTP request.
   c. Apply the video filter profile if necessary.
   d. Apply the web application profile (WAF) on the HTTP headers if necessary.
   e. Apply the web proxy profile to the HTTP request header.
   f. Perform a botnet check in the IPS profile if necessary.
   g. Apply the ICAP profile to forward the HTTP request headers to the ICAP server.
   h. Apply the IPS sensor and Application Control profiles to the HTTP request headers.
4. Process the HTTP request streaming data of the body if the body exists:
   a. Apply the web application profile (WAF) on the HTTP request body if necessary.
   b. Apply the stream-based file filtering, web content filtering, and antivirus scanning.
   c. Apply the IPS sensor and Application Control profiles to the HTTP request body.
   d. Apply the ICAP profile to forward the HTTP request body to the ICAP server.
5. Process the HTTP request whole body if the body exists:
   a. Apply file filtering, web content filtering, antivirus scanning, and DLP to the whole HTTP request.
6. Process the HTTP response headers:
   a. Apply the web application profile (WAF) on the HTTP headers if necessary.
   b. Apply the web proxy profile to the HTTP response headers.
   c. Apply the ICAP profile to forward the HTTP response headers to the ICAP server.
   d. Apply the IPS sensor and Application Control profiles to the HTTP response headers.
7. Process the HTTP response streaming data of the body if the body exists:
   a. Apply the web application profile (WAF) on the HTTP response body if necessary.
   b. Apply the stream-based file filtering, web content filtering, and antivirus scanning.
   c. Apply the IPS sensor and Application Control profiles to the HTTP response body.
   d. Apply the ICAP profile to forward the HTTP response body to the ICAP server.
8. Process the HTTP response whole body if the body exists:
   a. Apply file filtering, web content filtering, antivirus scanning, and DLP to the whole HTTP response.

Antivirus

An antivirus profile contains specific configuration information that defines how the traffic within a policy is examined and what action can be taken based on the examination. Multiple antivirus profiles

can be created for different antivirus scanning requirements. These profiles can then be applied to firewall policies.

To view available antivirus profiles, go to *Security Profiles* > *AntiVirus*.



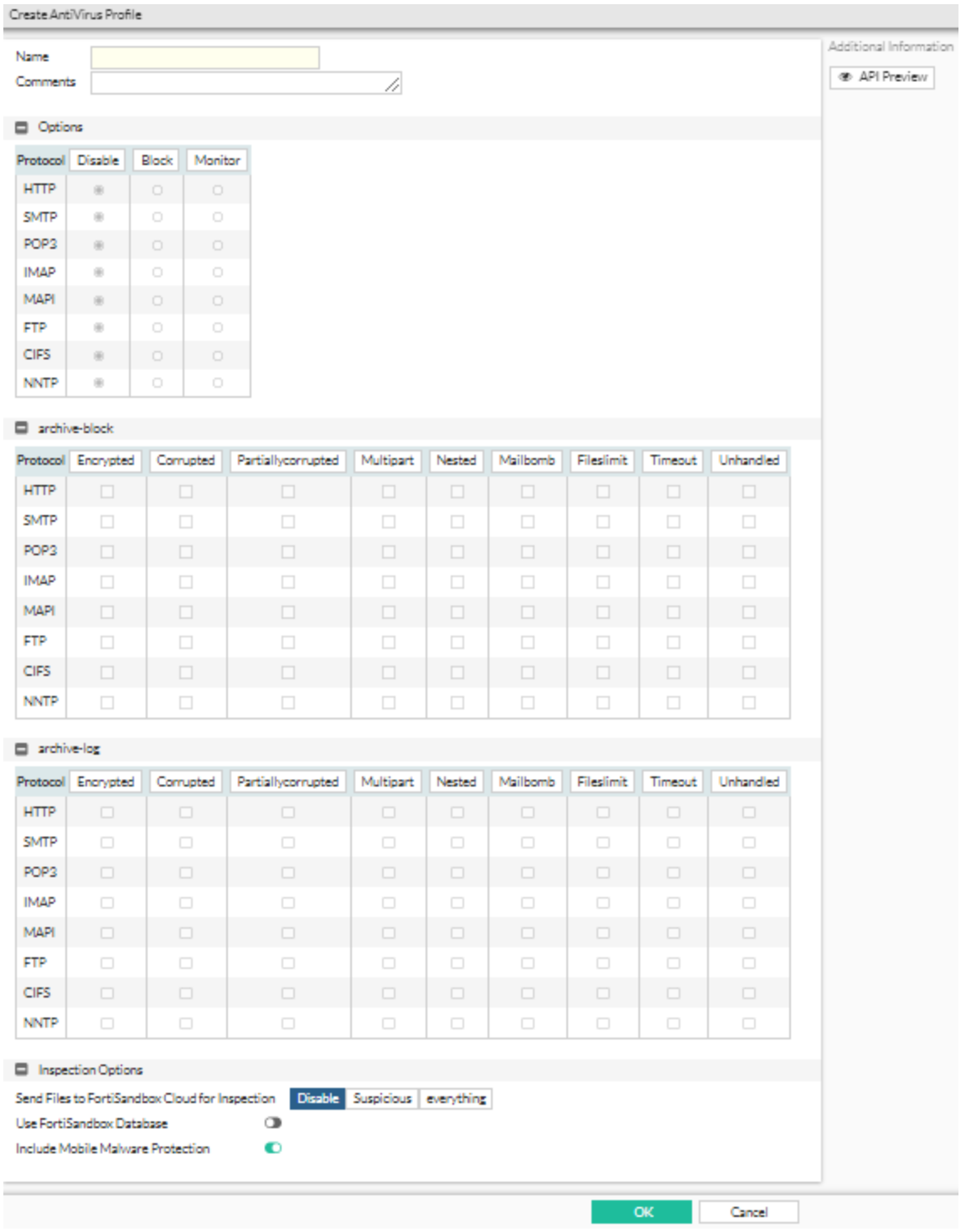
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an antivirus profile. See Create or edit an antivirus profile on page 542.
Edit	Modify the selected antivirus profile. See Create or edit an antivirus profile on page 542.
Clone	Make a copy of the selected antivirus profile.
Delete	Remove the selected antivirus profile.
Search	Enter a search term to find in the list.
Name	The name of the antivirus profile.
Comments	An optional description of the antivirus profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an antivirus profile

Click *Create New* to open the *Create AntiVirus Profile* window.



Select an antivirus profile and then click *Edit* to open the *Edit AntiVirus Profile* window.

Configure the following settings in the *Create AntiVirus Profile* window and then click *OK*:

Name	Enter the name of the antivirus profile.

Comments	Optionally, enter a description of the profile.
Options	For each protocol, enable or disable antivirus scanning, blocking, and monitoring.
Outbreak Prevention	FortiGuard Virus Outbreak Protection Service (VOS) allows the FortiProxy antivirus database to be subsidized with third-party malware hash signatures curated by FortiGuard. The hash signatures are obtained from FortiGuard's Global Threat Intelligence database. The antivirus database queries FortiGuard with the hash of a scanned file. If FortiGuard returns a match, the scanned file is deemed to be malicious. Enabling the AV engine scan is not required to use this feature.
Scanning Files by FortiNDR Server	For each protocol, select to disable, block, or monitor. Refer to Using FortiNDR inline scanning with antivirus on page 556 for more details.
Content Disarm	Content disarm and reconstruction (CDR) allows the FortiProxy unit to sanitize Microsoft Office documents and PDF files (including those that are in ZIP archives) by removing active content, such as hyperlinks, embedded media, JavaScript, macros, and so on from the files (disarm) without affecting the integrity of its textual content (reconstruction). It allows network administrators to protect their users from malicious document files. Files processed by CDR can be stored locally for quarantine on FortiAnalyzer, FortiSandbox, or FortiProxy models with a hard disk. The original copies can also be obtained in the event of a false positive. CDR is supported on HTTP, SMTP, POP3, and IMAP. **NOTE:** SMTP splice and client-comfort mode are not supported.
Archive Block	For each protocol, select the types of archive files to block.

Archive file type	Description
Encrypted	Archive files that are encrypted with an encryption key or a password.
Corrupted	Archive files that contain damaged or missing data, making them unusable or impossible to open.
Partially Corrupted	Archive files where part of the content can be extracted but the other parts are damaged. Unlike corrupted archive files, partially corrupted ones may still allow some content to be extracted, making them trickier to detect.
Multipart	Archive files that are split into many smaller

Archive file type	Description
	parts.
Nested	Archive files that contain other archive files, creating multiple layers of compression.
Mailbomb	Archive files with a big compression ratio.
Timeout	Archive files for which the scanning takes too long and exceeds the timeout threshold, indicating evasion attempts or overly complex files.  This timeout is an internal parameter in the AV Engine and is not configurable.
Unhandled	Archive files that cannot be opened, processed, and scanned due to unsupported formats, proprietary compression, or other issues.

Archive Log	For each protocol, select the file types to log.
Send Files to FortiSandbox Cloud for Inspection	If you want files to be inspected by FortiSandbox Cloud, select *Suspicious* or *everything*. Refer to Using FortiSandbox post-transfer scanning with antivirus on page 550 and FortiSandbox inline scanning on page 552 for more details.
Use FortiSandbox Database	Enable this option to use the FortiSandbox database.
Include Mobile Malware Protection	Enable this option to protect mobile devices from malware.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Stream-based antivirus scan for FTP, SFTP, and SCP

Stream-based antivirus scanning is supported for FTP, SFTP, and SCP protocols.

- Stream-based antivirus scanning optimizes memory usage for large archive files by decompressing the files on the fly and scanning the files as they are extracted.
- File types can be determined after scanning a few KB, without buffering the entire file.
- Viruses can be detected even if they are hiding in the middle or end of a large archive.
- When scanning smaller files, traffic throughput is improved by scanning the files directly on the proxy based WAD daemon, without invoking scanunit.

Stream-based scanning is the default scan mode. To disable steam-based scanning, the scan mode can be set to legacy mode, and the archive will only be scanned after the entire file has been received.

To configure stream-based scan:

```
config antivirus profile
    edit <string>
        ...
        set scan-mode {default* | legacy}
        ...
    next
end
```

Configuring threat feed and outbreak prevention without AV engine scan

In the CLI, users can enable malware threat feeds and outbreak prevention without performing an antivirus scan. In the GUI and CLI, users can choose to use all malware thread feeds, or specify the ones that they want to use. Replacement messages have been updated for external block lists.

```
config antivirus profile
    edit <name>
        config http
            set av-scan {disable | block | monitor}
            set outbreak-prevention {disable | block | monitor}
            set external-blocklist {disable | block | monitor}
            set quarantine {enable | disable}
        end
        ...
        set outbreak-prevention-archive-scan {enable | disable}
        set external-blocklist-enable-all {enable | disable}
        set external-blocklist <source>
    next
end
```

To configure malware threat feeds and outbreak prevention without performing an AV scan in the CLI:

```
config antivirus profile
    edit "Demo"
```

```
        set mobile-malware-db enable
        config http
            set av-scan disable
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set content-disarm disable
        end
        config ftp
            set av-scan disable
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
        end
        config imap
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set executables default
            set content-disarm disable
        end
        config pop3
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set executables default
            set content-disarm disable
        end
        config smtp
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set executables default
            set content-disarm disable
        end
        config mapi
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set executables default
        end
        config nntp
```

```
            set av-scan disable
            set outbreak-prevention disable
            set external-blocklist disable
            set quarantine disable
            set emulator enable
        end
        config cifs
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
        end
        config ssh
            set av-scan disable
            set outbreak-prevention disable
            set external-blocklist disable
            set quarantine disable
            set emulator enable
        end
        set outbreak-prevention-archive-scan enable
        set external-blocklist-enable-all disable
        set external-blocklist "malhash1"
        set av-virus-log enable
        set av-block-log enable
        set extended-log disable
        set scan-mode default
    next
end
```

In this example, configuring the quarantine setting is done in each protocol (`set quarantine`). The malware threat feed is also specified (`set external-blocklist-enable-all disable`) to the threat connector, malhash1 (`set external-blocklist "malhash1"`).

Content disarm and reconstruction for antivirus

Content disarm and reconstruction (CDR) allows the FortiProxy to sanitize Microsoft Office documents and PDF files (including those that are in ZIP archives) by removing active content, such as hyperlinks, embedded media, JavaScript, macros, and so on from the files (disarm) without affecting the integrity of its textual content (reconstruction). It allows network administrators to protect their users from malicious document files.

Files processed by CDR can be stored locally for quarantine on FortiAnalyzer, FortiSandbox, or FortiProxy models with a hard disk. The original copies can also be obtained in the event of a false positive.

CDR is supported on HTTP, SMTP, POP3, and IMAP. **NOTE:** SMTP splice and client-comfort mode are not supported.

Support and limitations

- CDR can only be performed on Microsoft Office documents and PDF files.
- Local Disk CDR quarantine is only possible on FortiProxy models that contain a hard disk.
- CDR is only supported on HTTP, SMTP, POP3, IMAP.
  - SMTP splice and client-comfort mode is not supported.
- CDR can only work on files in .ZIP type archives.

Configuring the feature

To configure antivirus to work with CDR, you must enable CDR on your antivirus profile, set the quarantine location, and then fine tune the CDR detection parameters.

To configure CDR:

1. Go to Security Profiles > AntiVirus.
2. Edit an antivirus profile or create a new one.
3. Under *Content Disarm*, enable the options that you want.
4. Select a quarantine location from the available options:
   - *FortiSandbox*—Saves the original document file to a connected FortiSandbox.
   - *File Quarantine*—Saves the original document file to disk (if possible) or a connected FortiAnalyzer based on the FortiProxy log settings (`config log fortianalyzer setting`).
   - *Discard*—The default setting, which discards the original document file.
5. Select the action that is taken when an error occurs:
   - *Block*—Block file when there is a CDR error.
   - *Log Only*—Log the CDR error but allow the file to pass.
   - *Ignore*—When there is a CDR error, let the file pass but do not log the error.
6. Click *OK*.

To edit the CDR detection parameters:

By default, stripping of all active Microsoft Office and PDF content types are enabled. In this example, stripping macros in Microsoft Office documents is disabled.

```
config antivirus profile
   edit <antivirus_profile_name>
      config content-disarm
         set office-macro disable
         set detect-only {enable | disable}
         set cover-page {enable | disable}
         set error-action {block | log-only | ignore}
      end
   next
end
```

Where:

detect-only	Only detect disarmable files, do not alter content. Disabled by default.
cover-page	Attach a cover page to the file's content when the file has been processed by CDR. Enabled by default.

Advanced configurations

This section includes the following:

- Using FortiSandbox post-transfer scanning with antivirus on page 550
- FortiSandbox inline scanning on page 552
- Using FortiNDR inline scanning with antivirus on page 556

Using FortiSandbox post-transfer scanning with antivirus

Antivirus profiles can submit potential zero-day viruses to FortiSandbox for inspection. Based on FortiSandbox's analysis, the FortiProxy can supplement its own antivirus database with FortiSandbox's threat intelligence to detect files determined as malicious or suspicious. This augments the FortiProxy antivirus with zero-day detection.

The FortiProxy first examines the file for any known viruses. When a match is found, the file is tagged as known malware. If no match is found, the files are forwarded to FortiSandbox using the following options:

- *All Supported Files*: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.
- *Suspicious Files Only*: files classified by the antivirus as having any possibility of active content are forwarded to FortiSandbox.

To enable FortiSandbox inspection in FortiProxy:

1. Enable FortiSandbox cloud by running the following command:

```
config system global
  set gui-fortigate-cloud-sandbox enable
end
```

2. Activate the FortiSandbox connection by running the following command:

```
execute forticloud-sandbox region
  0 Europe
  1 Global
  2 US
  3 Japan
  Please select cloud sandbox region[0-3]:0
```

```
Cloud sandbox region is selected: Europe
```

3. Configure the FortiSandbox scanning options in an antivirus profile:
   a. Go to *Security Profiles* > *AntiVirus*.
   b. Create, edit, or clone an antivirus profile.
   c. In the *Inspection Options* section, set *Send files to FortiSandbox for inspection* to *analytics-suspicious* or *analytics-everything*.
   d. Enable *Use FortiSandbox Database*.
   e. Click *OK*.

FortiProxy diagnostics

To view the detection count:

```
# diagnose test application quarantined 7
Total: 0

Statistics:
        vfid: 0, detected: 2, clean: 1252, risk_low: 6, risk_med: 2, risk_high: 1, limit_reached:0
```

To verify the address is configured correctly:

```
# diagnose test application quarantined 1
…
fortisandbox-fsb1 is enabled: analytics, realtime=yes, taskfull=no
addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no. ssl_opt=3, hmac_alg=0
…
```

To run the diagnostics for real-time debugging:

```
# diagnose debug application quarantined -1
# diagnose debug enable
```

To check the FortiGate Cloud server status:

```
# diagnose test application forticloud 3
…
    Active APTServer status:  up
```

FortiSandbox diagnostics

To run the OFTP debug for advanced debugging:

```
# diagnose-debug device <client serial number>
```

FortiSandbox inline scanning

When inline scanning is enabled, the client's file is held while it is sent to FortiSandbox for inspection. During this time, the FortiProxy may apply client comforting. For example, leaking a certain amount of bytes at a certain time interval to the client. Once a verdict is returned, the appropriate action (allow or block) is performed on the held file. If there is an error connecting to the FortiSandbox or a timeout on the FortiSandbox scanning the file within the default 50 seconds, the file can be passed, logged, or blocked based on FortiProxy's configuration.

Inline scanning requires a FortiSandbox appliance running version 4.4.5 or later, and the FortiSandbox must be reachable by port 4443. This feature is not supported on FortiSandbox Cloud. See Understanding Inline Block feature in the FortiSandbox Best Practices for more information.



FortiSandbox inline scanning is disabled by default. FortiSandbox inline scanning is best used in conjunction with AV engine scanning since there is a higher rate of detection by using both at the same time.

To enable FortiSandbox inline scanning globally:

```
config system fortisandbox
    set status enable
    set inline-scan {enable | disable}
    set server <fortisandbox_server_ip>
end
```

To configure the FortiSandbox scanning options in an antivirus profile:

```
config antivirus profile
    edit <name>
        set fortisandbox-mode {inline | analytics-suspicious | analytics-everything}
        set fortisandbox-error-action {ignore | log-only | block}
        set fortisandbox-timeout-action {ignore | log-only | block}
        set fortisandbox-max-upload <integer>
        config {http | ftp | imap | pop3 | smtp | mapi | cifs | ssh}
            set av-scan {disable | block | monitor}
            set fortisandbox {disable | block | monitor}
        end
    next
end
```

`fortisandbox-mode {inline | analytics-suspicious | analytics-everything}`	Set the FortiSandbox scan mode: • `inline`: FortiSandbox inline scanning • `analytics-suspicious`: FortiSandbox post-transfer scanning; submit supported files if heuristics or other methods determine they are suspicious • `analytics-everything`: FortiSandbox post-transfer scanning; submit supported files and known infected files (default)

`fortisandbox-error-action {ignore | log-only | block}`	Set the action to take if FortiSandbox inline scanning encounters an error reaching the FortiSandbox: • `ignore`: take no action • `log-only`: log the FortiSandbox inline scan error, but allow the file (default) • `block`: block the file upon FortiSandbox inline scan error
`fortisandbox-timeout-action {ignore | log-only | block}`	Set the action to take if FortiSandbox inline scanning encounters a scan timeout: • `ignore`: take no action • `log-only`: log the FortiSandbox inline scan timeout, but allow the file (default) • `block`: block the file upon FortiSandbox inline scan timeout
`fortisandbox-max-upload <integer>`	Set the maximum size of files that can be uploaded to FortiSandbox (1 - 396, default = 10).
`av-scan {disable | block | monitor}`	Enable the antivirus scan service. Set to `block` or `monitor` to work with FortiSandbox (default = `disable`).
`fortisandbox {disable | block | monitor}`	Set the protocol level parameter for FortiSandbox file scanning: • `disable` (default), `block`, and `monitor` are available for inline scanning • `disable` (default) and `monitor` are available for post-transfer scanning

Basic configuration

This example assumes that *Inline Block Policy* is already enabled in FortiSandbox for the FortiProxy with selected risk levels. The inline block policy in this example blocks all risk levels: malicious, high risk, medium risk, and low risk.

To configure FortiSandbox inline scanning in the GUI:

1. Enable FortiSandbox inline scanning globally:
   a. Go to *Security Fabric > Fabric Connectors* and double-click the *Sandbox* card.
   b. In the *Settings* tab, set the *Status* to *Enabled*.
   c. Set the *Type* to *FortiSandbox*.
   d. Enter the server address.
   e. Optionally enter a notifier email address.
   f. Enable *Inline scan*.
   g. Click *OK* to save the changes.
2. Configure the antivirus profile:
   a. Go *to Security Profiles > AntiVirus* and click *Create New*.
   b. Configure the options under *AntiVirus Scan Service*.
   c. Under *Inspection Options*, select *inline* for *Send files to FortiSandbox for inspection*.
   d. Click *OK*.

To configure FortiSandbox inline scanning in the CLI:

1. Enable FortiSandbox inline scanning globally:

```
config system fortisandbox
    set status enable
    set inline-scan enable
    set server "172.18.70.76"
end
```

2. Configure the antivirus profile:

```
config antivirus profile
    edit "Inline_scan_demo"
        config http
            set av-scan block
            set fortisandbox block
        end
        config ftp
            set av-scan block
            set fortisandbox block
        end
        config imap
            set av-scan block
            set fortisandbox block
        end
        config pop3
            set av-scan block
            set fortisandbox block
        end
        config smtp
            set av-scan block
            set fortisandbox block
        end
        config mapi
            set av-scan block
            set fortisandbox block
        end
        config cifs
            set av-scan block
            set fortisandbox block
        end
        config ssh
            set av-scan block
            set fortisandbox block
        end
    next
end
```

To verify that infected files are blocked inline:

1. On a client, open a web browser and download an infected file.
2. The file is held while being scanned by FortiSandbox. Once FortiSandbox determines that file's risk level is not tolerated by the inline block policy, the FortiProxy drops the connection and displays a replacement message that the file cannot be downloaded.
3. In FortiProxy, view the antivirus log.
   - In the GUI, go to *Log & Report* > *Security Events* and click the *AntiVirus* card.
   - In the CLI:

```
# execute log filter category 2
# execute log display
1 logs found.
1 logs returned.

1: date=2022-03-23 time=16:19:37 eventtime=1648077577156255080 tz="-0700"
logid="0210008232" type="utm" subtype="virus" eventtype="fortisandbox" level="warning"
vd="vdom1" policyid=1 poluuid="9170ca3e-aade-51ec-772b-1d31f135fe26" policytype="policy"
msg="Blocked by FortiSandbox." action="blocked" service="HTTP" sessionid=10545
srcip=10.1.100.181 dstip=172.16.200.184 srcport=37046 dstport=80 srccountry="Reserved"
dstcountry="Reserved" srcintf="port1" srcintfrole="undefined" dstintf="port9"
dstintfrole="undefined" srcuuid="5b426c60-aade-51ec-f020-b3d334ba18d3" dstuuid="5b426c60-
aade-51ec-f020-b3d334ba18d3" proto=6 direction="incoming" filename="skip_vm.vXE"
quarskip="File-was-not-quarantined" virus="Trojan" viruscat="Unknown" dtype="fortisandbox"
ref="http://www.fortinet.com/ve?vn=Trojan" virusid=0
url="http://172.16.200.184/sandbox/inline/skip_vm.vXE" profile="Inline_scan_demo"
agent="curl/7.68.0" httpmethod="GET" analyticssubmit="false" fsaaction="deny"
fsaseverity="high-risk" fsaverdict="block" fsafileid=0 fsafiletype="exe" crscore=50
craction=2 crlevel="critical
```

Configuration with FortiSandbox scanning error and timeout actions

In this example, the HTTP protocol settings for `av-scan` and `fortisandbox` in the AV profile are both set to `block`. All files traversing HTTP in this configuration are scanned by the AV engine first, and then by FortiSandbox inline scanning for further file analysis. Based on the FortiSandbox results, FortiProxy will take the appropriate action.

Files can be blocked if they contain a scan error or timeout. The scan timeout is configured in FortiSandbox and set to 50 seconds. If the file scan takes longer than 50 seconds, FortiSandbox returns a timeout to the FortiProxy, and file is dropped with the current configuration. If a user tries to download the same file again, the cached result is provided by FortiSandbox to the FortiProxy based on the previous file scan.

This example assumes FortiSandbox inline scanning has been configured globally. The FortiProxy will block the file if there is an inline scanning error or timeout.

To configure the antivirus profile to block files if there is an inline scanning error or timeout:

```
config antivirus profile
    edit "av"
        set fortisandbox-mode inline
```

```
        config http
            set av-scan block
            set fortisandbox block
        end
        set fortisandbox-error-action block
        set fortisandbox-timeout-action block
    next
end
```

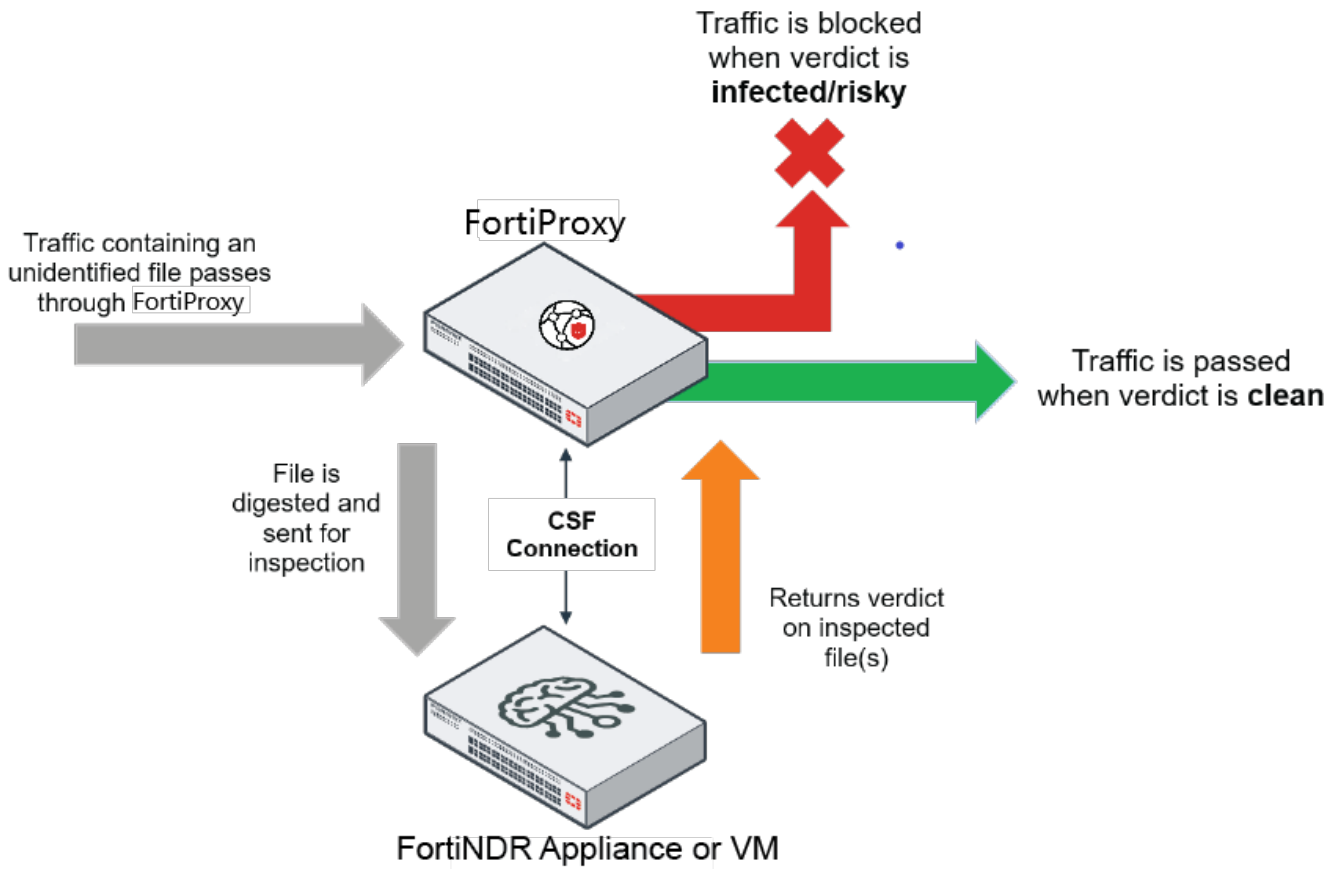
If the administrator decides to take more risk and scan all files traversing HTTP, but log or ignore an inline scanning error or timeout, the profile is modified as follows:

```
config antivirus profile
    edit "av"
        set fortisandbox-error-action {log-only | ignore}
        set fortisandbox-timeout-action {log-only | ignore}
    next
end
```

The AV engine is still used first, followed by FortiSandbox inline scanning. The FortiProxy will log or ignore the file if there is an inline scanning error or timeout, and the file is allowed to pass through.

Using FortiNDR inline scanning with antivirus

FortiNDR (formerly FortiAI) can be used with antivirus profiles in FortiProxy. FortiNDR inspects high-risk files and issues a verdict to the firewall based on how close the file features match those of malware. When enabled, FortiNDR can log, block, ignore, or monitor (allow) the file based on the verdict.



A licensed FortiNDR appliance with version 1.5.1 or later is required to use this feature.

To configure FortiNDR inline inspection with an AV profile:

1. Configure FortiNDR to join a Security Fabric in FortiProxy:
   a. Enable Security Fabric on FortiProxy using the following command:

```
config system csf
       set status enable
       set group-name "fabric-ai"
end
```

   b. Configure the interface to allow other devices to join the FortiProxy Security Fabric:

```
config system interface
    edit "port1"
        set allowaccess ping https ssh http fgfm fabric
    next
end
```

   c. In FortiNDR, configure the device to join the Security Fabric:

```
config system csf
       set status enable
       set upstream-ip 10.6.30.14
       set managment-ip 10.6.30.251
end
```

d. Authorize the FortiNDR in FortiProxy:

```
config system csf
       config trusted-list
               edit "FAIVMSTM21000000"
                       set authorization-type certificate
                       set certificate "********************"
               next
       end
end
```

2. In the FortiProxy CLI, enable inline inspection:

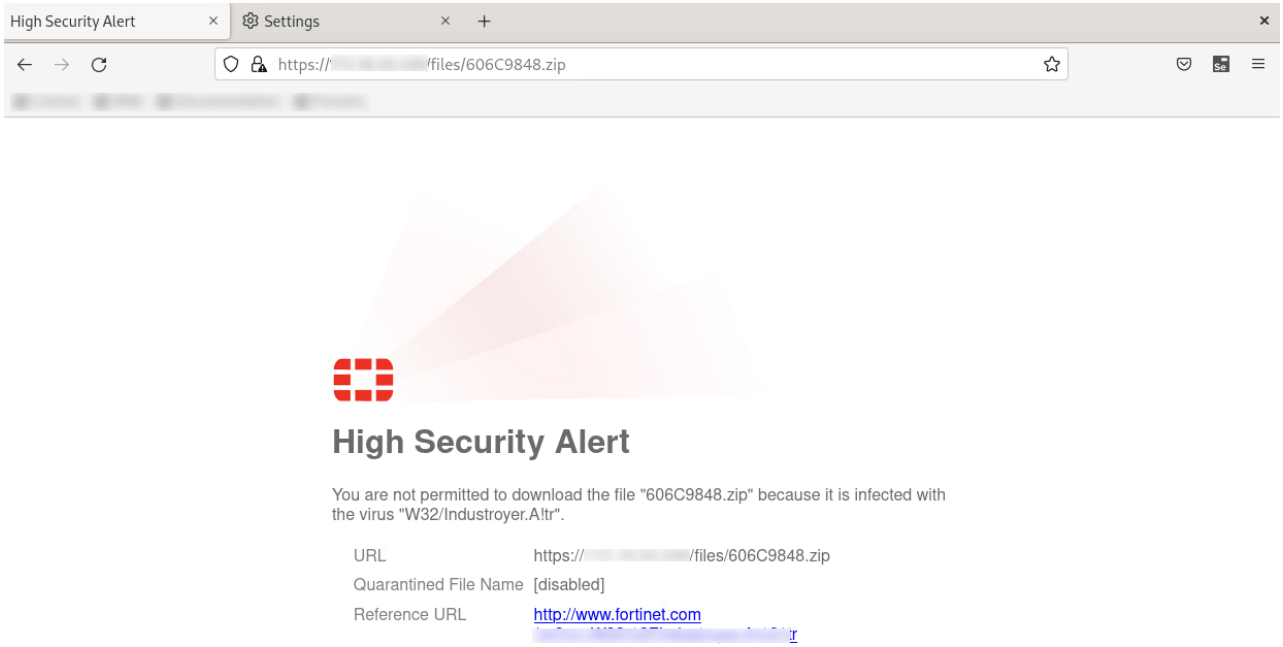
```
config system fortindr
    set status enable
end
```

3. Configure an AV profile in FortiProxy to use inline inspection and block detected infections (see also Create or edit an antivirus profile on page 542):

```
config antivirus profile
    edit "av"
        set feature-set proxy
        config http
            set fortindr block
        end
        config ftp
            set fortindr block
        end
        config imap
            set fortindr block
        end
        config pop3
            set fortindr block
        end
        config smtp
            set fortindr block
        end
        config mapi
            set fortindr block
        end
        config nntp
            set fortindr block
        end
        config cifs
            set fortindr block
```

```
        end
        config ssh
            set fortindr block
        end
    next
end
```

4. To configure the action to take when FortiNDR encounters an error, use the `set fortindr-error-action {log-only | block | ignore}` option of the `config antivirus profile` command. The default is `log-only`.
5. Add the AV profile to a policy. See Create or edit a policy on page 387.
When potential infections are blocked by FortiNDR inline inspection, a replacement message appears. See Replacement Messages on page 944 for more information. An infection blocked over HTTP looks similar to the following:



Sample log

```
4: date=2024-03-03 time=18:46:03 eventtime=1709520363412262227 tz="-0800" logid="0209008220"
type="utm" subtype="virus" eventtype="fortindr" level="warning" vd="v2" policyid=4
poluuid="b5fcdca8-cd37-51ee-0e28-3e96400e4b46" policytype="policy" msg="Blocked by FortiNDR."
action="blocked" service="SSH" subservice="SFTP" sessionid=890734348 srcip=10.40.1.42
dstip=172.18.20.226 srcport=34674 dstport=22 srccountry="Reserved" dstcountry="Reserved"
srcintf="port1" srcintfrole="undefined" dstintf="link11" dstintfrole="undefined" proto=6
direction="incoming" filename="test.pdf" quarskip="Quarantine-disabled" virus="StaticFilter.AI"
viruscat="Generic Trojan" dtype="fortindr" ref=" http://www.fortinet.com/ve?vn=StaticFilter.AI
" virusid=0 profile="ndr" analyticssubmit="false" fndraction="deny" fndrverdict="block"
fndrseverity="low" fndrconfidence="high" fndrfileid=0 fndrfiletype="PDF" crscore=50 craction=2
crlevel="critical"
```

FortiNDR inline inspection with other AV inspection methods

The following inspection logic applies when FortiNDR inline inspection is enabled simultaneously with other AV inspection methods. The AV engine inspection and its verdict always takes precedence because of performance. The actual behavior depends on which inspected protocol is used.

HTTP, FTP, SSH, and CIFS protocols:

1. AV engine scan; AV database and FortiSandbox database (if applicable).
   a. FortiNDR inline inspection occurs simultaneously.
2. AV engine machine learning detection for WinPE PUPs (potentially unwanted programs).
   a. FortiNDR inline inspection occurs simultaneously.
3. Outbreak prevention and external hash list resources.
   a. FortiNDR inline inspection occurs simultaneously.



If any AV inspection method returns an infected verdict, the FortiNDR inspection is aborted.

POP3, IMAP, SMTP, NNTP, and MAPI protocols:

1. AV engine scan; AV database and FortiSandbox database (if applicable).
2. AV engine machine learning detection for WinPE PUPs (potentially unwanted programs).
   a. FortiNDR inline inspection occurs simultaneously.
3. Outbreak prevention and external hash list resources.
   a. FortiNDR inline inspection occurs simultaneously.



In an AV profile, use `set fortindr-error-action {log-only | block | ignore}` to configure the action to take if FortiNDR encounters an error.

Accepted file types

The following file types are sent to FortiNDR for inline inspection:

7Z	HTML	RTF
ARJ	JS	TAR
BZIP	LZH	VBA
BZIP2	LZW	VBS
CAB	MS Office documents (XML and non-XML)	WinPE (EXE)
ELF	PDF	XZ
GZIP	RAR	ZIP

Configuration examples

This section includes the following examples:

- Content disarm and reconstruction on page 561
- Exempt list for files based on individual hash on page 563
- Download quarantined files in archive format on page 564

Content disarm and reconstruction

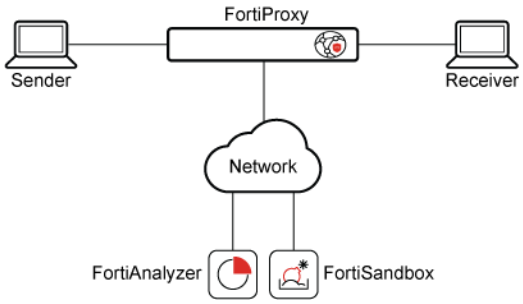
Content disarm and reconstruction (CDR) allows the FortiProxy to sanitize Microsoft Office documents and PDF files (including those that are in ZIP archives) by removing active content, such as hyperlinks, embedded media, JavaScript, macros, and so on from the files (disarm) without affecting the integrity of its textual content (reconstruction). It allows network administrators to protect their users from malicious document files.

CDR is supported on HTTP, SMTP, POP3, and IMAP.

HTTP GET is supported, but not HTTP POST.
SMTP splice and client-comfort mode are not supported.

Example

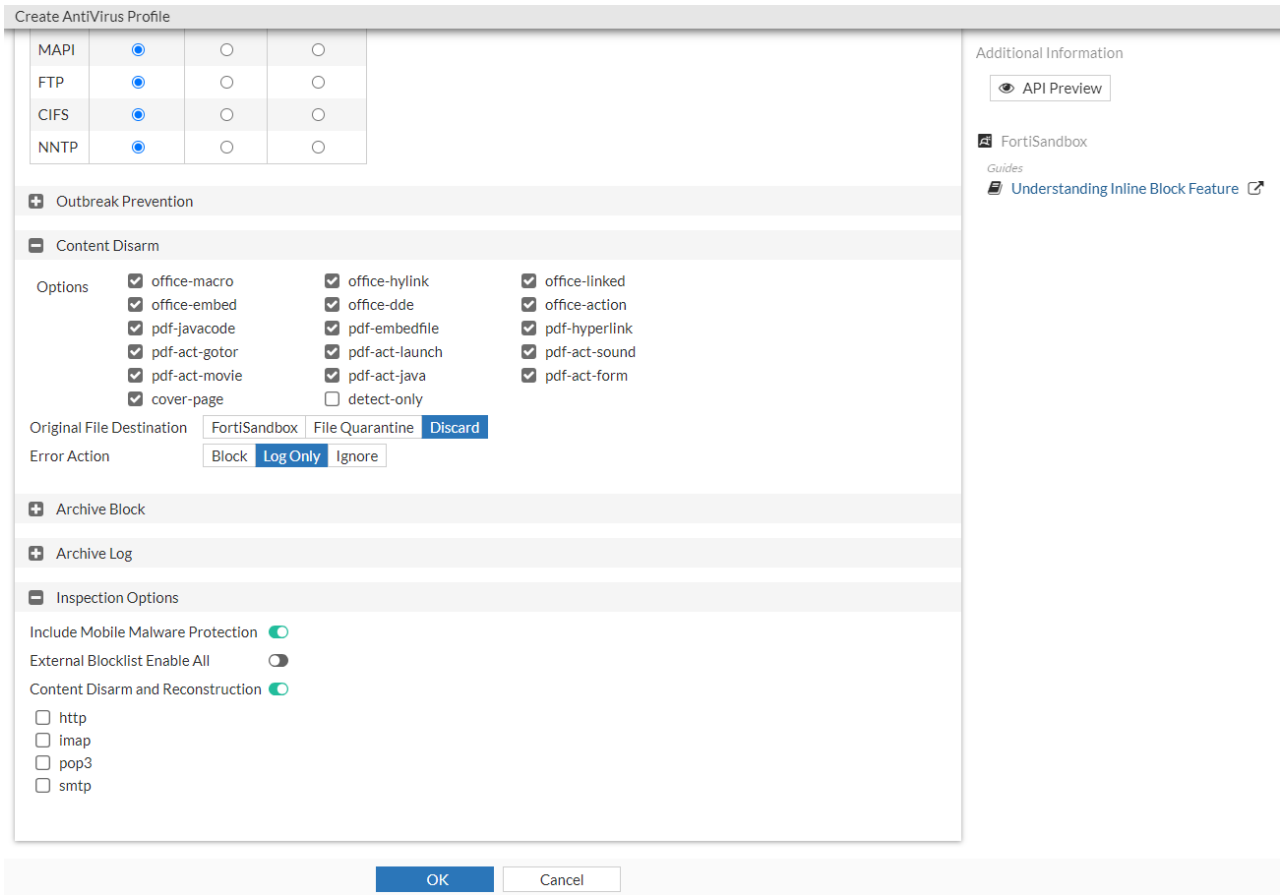
In this example, the a Microsoft Office document with an embedded hyperlink (that redirects to an external website) is sent to the receiver. When the user receives the file, the hyperlink in the document is deactivated.



To configure CDR:

1. Go to *Security Profiles* > *AntiVirus*.
2. Edit an antivirus profile, or create a new one.

3. Under *Inspection Options*, enable *Content Disarm and Reconstruction*.



4. Select a quarantine location from the available options:

FortiSandbox	Saves the original document file to a connected FortiSandbox.
File Quarantine	Saves the original document file to disk (if possible) or a connected FortiAnalyzer based on the FortiProxy log settings (`config log fortianalyzer setting`).
Discard	The default setting, which discards the original document file.

5. Click *OK*.

To edit the CDR detection parameters:

By default, stripping of all active Microsoft Office and PDF content types are enabled. In this example, stripping macros in Microsoft Office documents will be disabled.

```
config antivirus profile
    edit av
        config content-disarm
            set office-macro disable
            set detect-only {enable | disable}
            set cover-page {enable | disable}
        end
```

```
    next
end
```

Where:

detect-only	Only detect disarmable files, do not alter content. Disabled by default.
cover-page	Attach a cover page to the file's content when the file has been processed by CDR. Enabled by default.

Exempt list for files based on individual hash

The antivirus exempt list allows users to exempt known safe files that happen to be incorrectly classified as malicious by the AV signature and AV engine scan. Users can specify file hashes in MD5, SHA1, or SHA256 for matching, which are applied at a per-VDOM level. When matched, the FortiProxy ignores the AV scan verdict so that the corresponding UTM behavior defined in the AV profile is not performed.

```
config antivirus exempt-list
    edit <name>
        set hash-type {md5 | sha1 | sha256}
        set hash <string>
        set status {enable | disable}
    next
end
```



The exempt list does not apply to results from outbreak prevention, machine learning, FortiNDR, or FortiSandbox inline scans.

In this example, an antivirus exempt list is configured for the EICAR anti-malware test file. Although the antivirus profile is configured to block HTTP, the client is able to download the file.

To configure an antivirus exempt list:

1. Configure the antivirus profile:

```
config antivirus profile
    edit "av"
        config http
            set av-scan block
        end
    next
end
```

2. Configure the antivirus exempt list:

```
config antivirus exempt-list
    edit "test-hash"
        set comment "eicar.com"
        set hash-type md5
        set hash "44d88612fea8a8f36de82e1278abb02f"
        set status enable
    next
end
```

3. Get a client to access https://www.eicar.com/ and download the anti-malware test file.
   The FortiProxy exempts the AV scan verdict and bypasses the file. The client can download the file and no replacement message is displayed.

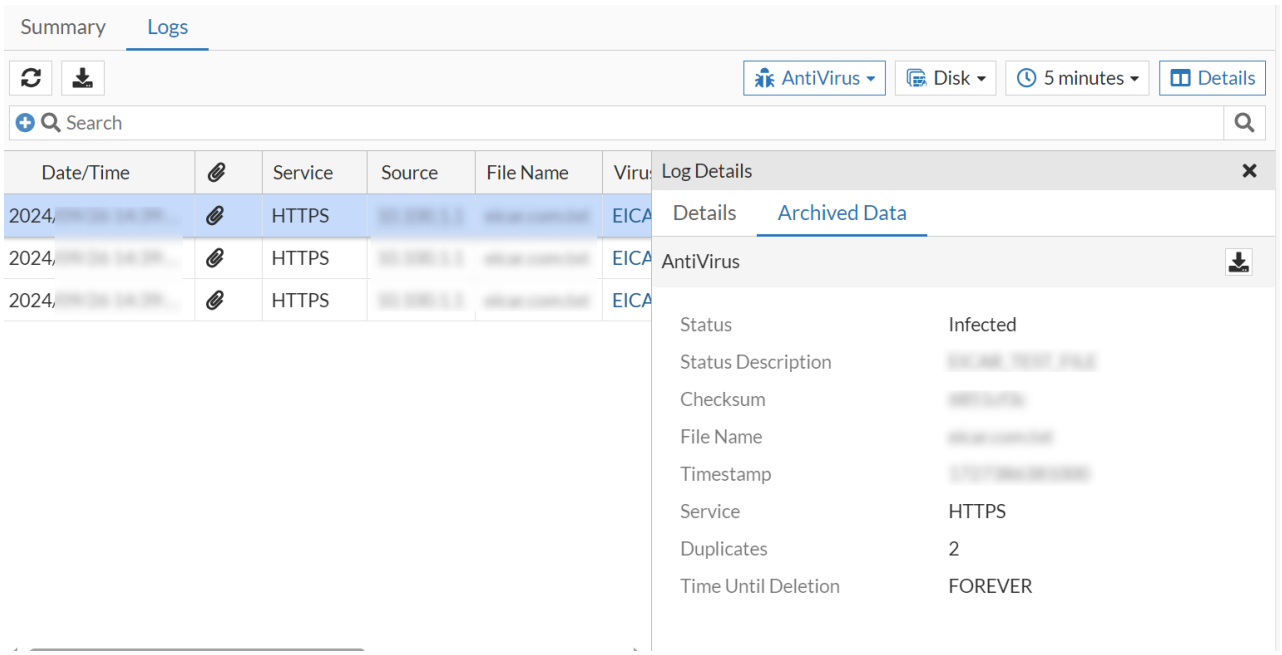
Download quarantined files in archive format

The FortiProxy can download quarantined files in an archive format (.TGZ) instead of the original raw file. This allows for a more detailed analysis of the quarantined files and reduces the risk of malware infection.

The FortiProxy must have a disk logging capacity or be connected to FortiAnalyzer for logging.

To download a quarantined archive file:

1. Ensure that quarantining files is enabled in the AV profile.
   You can use the following commands to enable quarantine for specific protocols in the antivirus profile:
   ```
   config antivirus profile
      edit "default"
         set comment "Scan files and block viruses."
         config http
            set av-scan block
            set quarantine enable
   end
   ```
   Repeat this configuration for other protocols as needed (e.g., ftp, imap, pop3, smtp).
2. Go to *Log & Report > Security Events* and select the *AntiVirus* card.
3. Select a log entry and click *Details*. The *Log Details* pane opens.
4. Select the *Archived Data* tab and click the download icon (in the *AntiVirus* title bar).

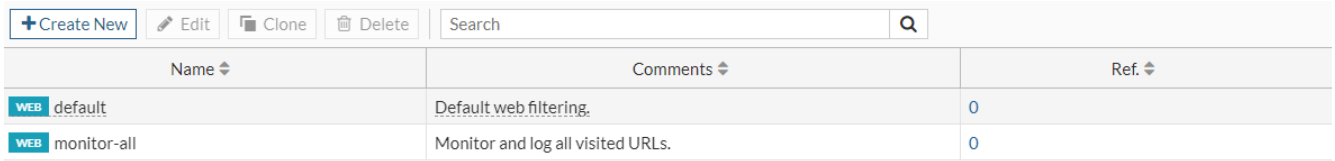


Web Filter

This section describes how to configure web filters for HTTP traffic and configure URL filters to allow or block caching of specific URLs.

After you configure a web filter profile, you can apply it to a policy. A profile is specific information that defines how the traffic within a policy is examined and what action can be taken based on the examination.

To view available web filter profiles, go to *Security Profiles* > *Web Filter*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

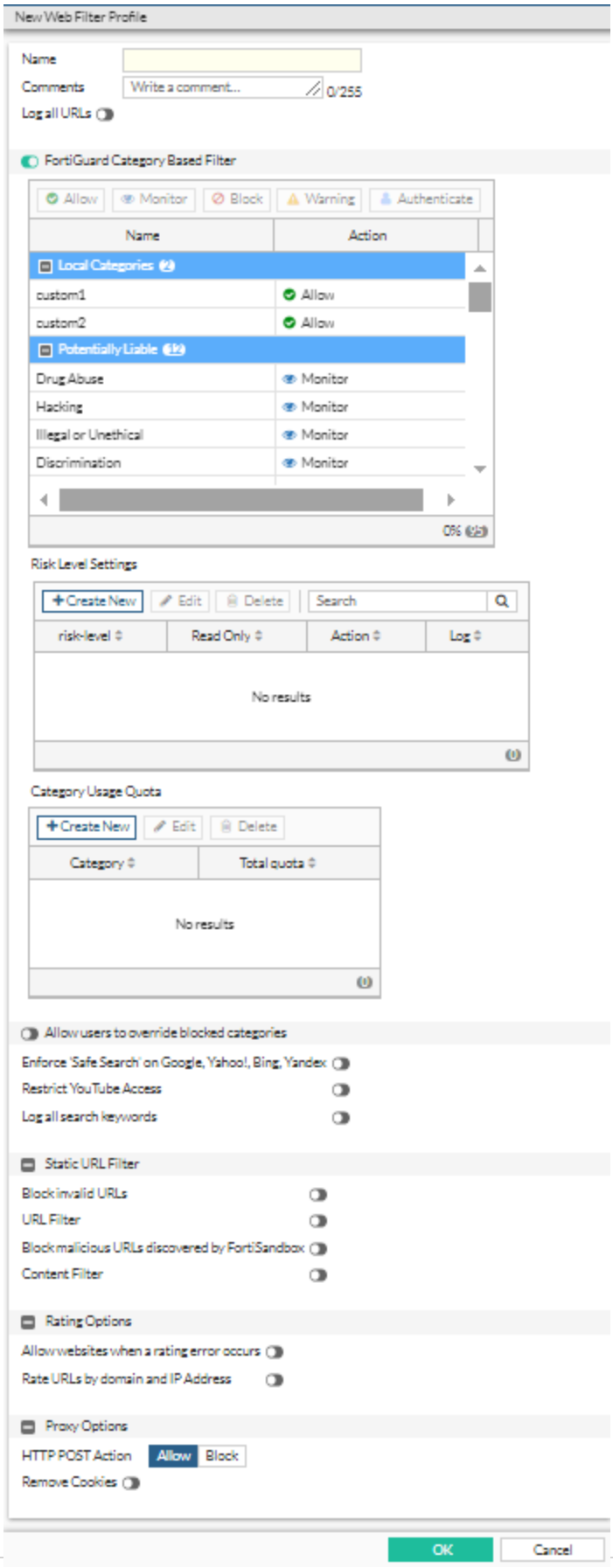
The following options are available:

Create New	Create a web filter profile. See Create or edit a web filter profile on page 566.
Edit	Modify the selected web filter profile. See Create or edit a web filter profile on page 566.

Clone	Make a copy of the selected web filter profile.
Delete	Remove the selected web filter profile.
Search	Enter a search term to find in the web filter profile list.
Name	The name of the web filter profile.
Comments	An optional description of the web filter profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a web filter profile

Click *Create New* to open the *Create Web Filter Profile* window.


New Web Filter Profile
Name
Comments
Write a comment...
0/255
Log all URLs
FortiGuard Category Based Filter
Allow
Monitor
Block
Warning
Authenticate
Name
Action
Local Categories
custom1
Allow
custom2
Allow
Potentially Liable
Drug Abuse
Monitor
Hacking
Monitor
Illegal or Unethical
Monitor
Discrimination
Monitor
0%
Risk Level Settings
Create New
Edit
Delete
Search
risk-level
Read Only
Action
Log
No results
Category Usage Quota
Create New
Edit
Delete
Category
Total quota
No results
Allow users to override blocked categories
Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex
Restrict YouTube Access
Log all search keywords
Static URL Filter
Block invalid URLs
URL Filter
Block malicious URLs discovered by FortiSandbox
Content Filter
Rating Options
Allow websites when a rating error occurs
Rate URLs by domain and IP Address
Proxy Options
HTTP POST Action
Allow
Block
Remove Cookies
OK
Cancel

Select a web filter profile and then click *Edit* to open the *Edit Web Filter Profile* window.

Configure the following settings in the *Create Web Filter Profile* window and then click *OK*:

Name	The name of the web filter profile.
Comments	Optional description of the web filter profile.
Log all URLs	Enable if you want all URLs to be logged.
FortiGuard category based filter	Enable to use FortiGuard categories. If the device is not licensed for the FortiGuard web-filtering service, traffic can be blocked by enabling this option.
Risk Level Settings	Define the web filtering behavior for different risk levels (see Web Filter Risk Level on page 659). You can configure whether to block or monitor URLs for each risk level and whether to allow logging of the activity.
Allow/Monitor/Block/Warning/Authentication	Select the action for each FortiGuard category: *Allow*, *Monitor*, *Block*, *Warning*, or *Authenticate*. You can enter a category to search for.
Allow users to override blocked categories	Enable this option if you want users to be able to override blocked categories.
Groups that can override	Select the user groups that will be able to override blocked categories. This option is available only if *Allow users to override blocked categories* is enabled.
Profile Name	Select which web filter profile to change blocked categories to. This option is available only if *Allow users to override blocked categories* is enabled.
Switch applies to	Select whether the new web filter profile applies to a *User*, *User Groups*, or *IP* or whether to *Ask*. The user or user groups must be specified as the *Source* in firewall policies using this profile. This option is available only if *Allow users to override blocked categories* is enabled.
Switch Duration	Select whether blocked categories can be overridden for a predefined period or to *Ask*. This option is available only if *Allow users to override blocked categories* is enabled.
day(s)/hour(s)/minute(s)	Select how long users can override blocked categories.

	This option is available only if *Allow users to override blocked categories* is enabled and the *Switch Duration* is set to *Predefined*.
Static URL Filter	
Block invalid URLs	Enable to block web sites when their SSL certificate CN field does not contain a valid domain name.
URL Filter	Enable and then create or edit a URL filter. See Create or edit a URL filter on page 573.
Block malicious URLs discovered by FortiSandbox	Enable to block malicious URLs discovered by FortiSandbox.
Content Filter	Enable and then create or edit a content filter to block access to web pages that include the specified patterns. See Create or edit a content filter on page 574.
Rating Options	
Allow websites when a rating error occurs	Enable to allow access to web pages that return a rating error from the web filter service. If your unit is temporarily unable to contact the FortiGuard service, this setting determines what access the unit allows until contact is re-established. If enabled, users will have full unfiltered access to all web sites. If disabled, users will not be allowed access to any web sites.
Rate URLs by domain and IP Address	Enable to have the unit request site ratings by URL and IP address separately, providing additional security against attempts to bypass the FortiGuard Web Filter. FortiGuard Web Filter ratings for IP addresses are not updated as quickly as ratings for URLs. This difference can sometimes cause the unit to allow access to sites that should be blocked or to block sites that should be allowed.
Proxy Options	
HTTP POST Action	Select whether to *Allow* or *Block* HTTP POST traffic. HTTP POST is the command used by your browser when you send information, such as a form you have filled-out or a file you are uploading, to a web server.
Remove Cookies	Enable to filter cookies from web traffic. Web sites using cookies might not function properly with this enabled.

API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Using FortiGuard web filter categories to block child sexual abuse and terrorism

Web filter categories 83 (Child Sexual Abuse, formerly Child Abuse) and 96 (Terrorism) can be used to enforce blocking and logging the Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) lists, respectively.

To create a web filter profile to block the Child Sexual Abuse and Terrorism categories in the GUI:

1. Go to *Security Profiles* > *Web Filter* and click *Create New*.
2. Enter a name for the new filter.
3. Enable *FortiGuard Category Based Filter*.
4. In the category table, in the *Potentially Liable* section, set the *Action* for the *Child Sexual Abuse* and *Terrorism* categories to *Block*.
5. Configure the remaining settings as required.
6. Click *OK*.

To create a web filter profile to block category 83 (Child Sexual Abuse) in the CLI:

```
config webfilter profile
    edit newfilter
        config ftgd-wf
            unset options
            config filters
                ...
                edit 83
                    set category 83
                    set action block
                next
                ...
```

```
            end
        end
    next
end
```

To test the web filter:

1. Use the web filter profile in a policy.
2. On a device that is connected through the FortiProxy unit and that uses the policy, visit the test URLs for each category:
   `http://wfurltest.fortiguard.com/wftest/83.html`
   `http://wfurltest.fortiguard.com/wftest/96.html`
3. Log in to the FortiProxy unit and go to *Log & Report* > *Web filter* to view the logs for the blocked websites.

Configuring user-name-only credential matching

To configure user-name-only credential matching:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            ...
        end
        config antiphish
            set status enable
            set check-username-only enable
            config inspection-entries
                edit "cat34"
                    set fortiguard-category 34
                    set action block
                next
            end
            set domain-controller "win2016"
        end
        set log-all-url enable
    next
end
```

Configuring different custom pattern types for user names and passwords

To configure different custom pattern types for user names and passwords:

```
config webfilter profile
    edit "webfilter"
```

```
        config ftgd-wf
            unset options
            ...
        end
        config antiphish
            set status enable
            config inspection-entries
                edit "cat34"
                    set fortiguard-category 34
                    set action block
                next
            end
            config custom-patterns
                edit "qwer"
                    set type literal
                next
                edit "[0-6]Dat*"
                next
                edit "dauw9"
                    set category password
                    set type literal
                next
                edit "[0-5]foo[1-4]"
                    set category password
                next
            end
            set domain-controller "win2016"
        end
        set log-all-url enable
    next
end
```

In this example, the `qwer` and `dauw9` entries use the literal type, while `[0-6]Dat*` and `[0-5]foo[1-4]` use the default regex type.

Using image-analyzer to categorize images with unknown FortiGuard categories

The image-analyzer (IA) engine can be used to categorize images that had unknown categories from the FortiGuard web filter. The results of an IA scan are cached for twelve hours.

When a URL filter request is received, if the request's URL is in the cache then the cached result is returned. When an image response is received that has an unknown category and IA categorization is enabled, the image is sent to the IA engine for results. The IA engine results are added to the shared memory IA cache.

To enable image-analyzer categorization:

```
config webfilter profile
    edit <name>
```

```
        set ia-categorization enable
    next
end
```

Create or edit a URL filter

You can allow or block access to specific web sites by adding them to the URL filter list. You add the web sites by using patterns containing text and regular expressions. The FortiProxy unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead.



Web site blocking does not block access to other services that users can access with a web browser. For example, web site blocking does not block access to ftp://ftp.example.com. Instead, use firewall policies to deny ftp connections.

When adding a URL to the web site filter list, follow these rules:

- Type a top-level URL or IP address to control access to all pages on a web site. For example, www.example.com or 192.168.144.155 controls access to all pages at these web sites.
- Enter a top-level URL followed by the path and file name to control access to a single page on a web site. For example, www.example.com/monkey.html or 192.168.144.155/monkey.html controls access to the monkey page on this web site.
- To control access to all pages with a URL that ends with example.com, add example.com to the filter list. For example, adding example.com controls access to www.example.com, mail.example.com, www.finance.example.com, and so on.
- Control access to all URLs that match patterns using text and regular expressions (or wildcard characters). For example, example.* matches example.com, example.org, example.net and so on.



URLs with an action set to exempt or pass are not scanned for viruses. If users on the network download files through the FortiProxy unit from a trusted web site, add the URL of this web site to the URL filter list with an action to pass it, so the unit does not scan files downloaded from this URL.

To create a URL filter:

1. Go to *Security Profiles* > *Web Filter*.
2. Click *Create New* or select a web filter profile and then click *Edit*.
3. Enable *URL Filter*.
4. In the *URL Filter* table, click *Create New*. The *New URL Filter* window opens.
5. Enter the URL to filter in the *URL* field. Enter a top-level domain suffix (for example, “com” without the leading period) to block access to all web sites with this suffix.
6. Select the type of pattern to match: *Simple*, *Reg. Expression*, or *Wildcard*.
7. Select the action to take when the pattern is matched:

- *Exempt*: Allow trusted traffic to bypass the antivirus proxy operations.
- *Block*: Block access to any URLs matching the URL pattern and display a replacement message. SeeReplacement Messages on page 944.
- *Allow*: Allow access to any URL that matches the URL pattern.
- *Monitor*: Monitor traffic to and from URLs matching the URL pattern.

8. Enable or disable the status of the filter to make the filter active or inactive.
9. Enter the referrer host name.
10. Click *OK* to save the URL filter.
11. Click *OK* to save the changes to the web filter profile.

To edit a URL filter:

1. Go to *Security Profiles* > *Web Filter*.
2. Click *Create New* or select a web filter profile and then click *Edit*.
3. In the URL Filter table, double-click on a filter or select the filter and then click *Edit* in the toolbar.
4. Edit the filter settings as required.
5. Click *OK* to save your changes to the URL filter.
6. Click *OK* to save the changes to the web filter profile.

Create or edit a content filter

Content filters can be added or edited, as required.

To create a web content filter:

1. Go to *Security Profiles* > *Web Filter*.
2. Click *Create New* or select a web filter profile and then click *Edit*.
3. In the *Static URL Filter* section, enable *Content Filter*.
4. Select *Create New*.
5. Select the *Pattern Type*, either *Wildcard* or *Regular Expression*.
6. Enter the content *Pattern* to match.
7. Select the *Language* from the drop-down menu.
8. Select *Block* or *Exempt*.
9. Enable the *Status*.
10. Click *OK*.

To edit a web content filter:

1. Go to *Security Profiles* > *Web Filter*.
2. Click *Create New* or select a web filter profile and then click *Edit*.
3. In the *Static URL Filter* section, enable *Content Filter*.
4. Select the content filter you want to edit and then click *Edit* from the toolbar. The *Edit Web Content Filter* window opens.
5. Edit the information as required and then click *OK* to apply your changes.

FortiGuard filter

The FortiGuard filter enhances the web filter features by sorting billions of web pages into a wide range of categories that users can allow or block.

The FortiGuard Web Filtering service includes over 45 million individual website ratings that apply to more than two billion pages. When the FortiGuard filter is enabled in a web filter profile and applied to firewall policies, if a request for a web page appears in traffic controlled by one of the firewall policies, the URL is sent to the nearest FortiGuard server. The URL category or rating is returned. If the category is blocked, the FortiProxy shows a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

To use this service, you must have a valid FortiGuard license.

The following actions are available:

FortiGuard web filter action	Description
Allow	Permit access to the sites in the category.
Monitor	Permit and log access to sites in the category. User quotas can be enabled for this option.
Block	Prevent access to the sites in the category. Users trying to access a blocked site see a replacement message indicating the site is blocked.
Warning	Display a message to the user allowing them to continue if they choose.
Authenticate	Require the user to authenticate with the FortiProxy before allowing access to the category or category group.
Disable	Remove the category from the from the web filter profile. This option is only available for local or remote categories from the right-click menu.

FortiGuard web filter categories

FortiGuard has many web filter categories, including two local categories and a special remote category:

- All URL categories—See Web Filter Categories.
- Local categories— See Web Rating Overrides on page 650.
- Remote category

The priority of categories is local category > external category > FortiGuard built-in category. If a URL is configured as a local category, it only follows the behavior of the local category and not the external or FortiGuard built-in category.

Blocking a web category

The following example shows how to block a website based on its category. The Information Technology category (category 52) will be blocked.

To block a category in the GUI:

1. Go to *Security Profiles* > *Web Filter* and click *Create New*, or edit an existing profile.
2. In the *FortiGuard category based filter* section, select *Information Technology*, then click *Block*.
3. Configure the remaining settings as needed.
4. Click *OK*.

To block a category in the CLI:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            config filters
                edit 1
                    set category 52
                    set action block
                next
            end
        end
    next
end
```

To verify that the category is blocked:

1. Go to a website that belongs to the blocked category, such as www.fortinet.com.
   The page should be blocked and display a replacement message.

To view the log of a blocked website in the GUI:

1. Go to *Log & Report* > *Security Events*.
2. Click the *Web Filter* card name.
3. Select an entry with *blocked* in the *Action* column and click *Details*.

To view the log of a blocked website in the CLI:

```
# execute log filter category utm-webfilter
# execute log display

4: date=2023-08-08 time=13:25:31 eventtime=1691526331836645153 tz="-0700" logid="0316013056"
type="utm" subtype="webfilter" eventtype="ftgd_blk" level="warning" vd="root" policyid=1
poluuid="4a4b9d00-e471-51ed-71ec-c1a3bc8f773c" policytype="policy" sessionid=254529 srcip=1.1.1.2
srcport=60836 srccountry="Australia" srcintf="internal7" srcintfrole="lan" srcuuid="45eec070-e471-
```

```
51ed-4b1c-930f37c5d882" dstip=44.240.173.227 dstport=443 dstcountry="United States" dstintf="wan1"
dstintfrole="wan" dstuuid="45eec070-e471-51ed-4b1c-930f37c5d882" proto=6 service="HTTPS"
hostname="www.fortinet.com" profile="default" action="blocked" reqtype="direct"
url="https://www.fortinet.com/" sentbyte=517 rcvdbyte=0 direction="outgoing" msg="URL belongs to a
denied category in policy" ratemethod="domain" cat=52 catdesc="Information Technology"
```

Allowing users to override blocked categories

There is an option to allow users with valid credentials to override blocked categories.

To allow users to override blocked categories in the GUI:

1. Go to *Security Profiles* > *Web Filter* and click *Create New*, or edit an existing profile.
2. Enable *Allow users to override blocked categories*.
3. Enter information in the following fields:
   - *Groups that can override*
   - *Profile name*
   - *Switch applies to*
   - *Switch Duration*
4. Configure the other settings as needed.
5. Click *OK*.

To allow users to override blocked categories in the CLI:

```
config webfilter profile
    edit "webfilter"
        set ovrd-perm bannedword-override urlfilter-override fortiguard-wf-override contenttype-
check-override
        config override
            set ovrd-user-group "radius_group"
            set profile "webfilter"
        end
        config ftgd-wf
            unset options
        end
    next
end
```

Issuing a warning on a web category

The following example shows how to issue a warning when a user visits a website in a specific category (Information Technology, category 52).

To configure a warning for a category in the GUI:

1. Go to *Security Profiles* > *Web Filter* and click *Create New*, or edit an existing profile.
2. In the *FortiGuard category based filter* section, select *Information Technology*, then click *Warning*.
3. Set the *Warning Interval*, then click *OK*.
   The warning interval is the amount of time until the warning appears again after the user proceeds past it.
4. Configure the remaining settings as needed.
5. Click *OK*.

To configure a warning for a category in the CLI:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            config filters
                edit 1
                    set category 52
                    set action warning
                next
            end
        end
    next
end
```

To verify that the warning works:

1. Go to a website that belongs to the category, such as www.fortinet.com.
2. On the warning page, click *Proceed* or *Go Back*.

Authenticating a web category

The following example shows how to authenticate a website based on its category (Information Technology, category 52).

To authenticate a category in the GUI:

1. Go to *Security Profiles* > *Web Filter* and edit or create a new web filter profile.
2. In the *FortiGuard category based filter* section, select *Information Technology*, then click *Authenticate*.

3. Set the *Warning Interval* and select one or more user groups, then click *OK*.
4. Configure the remaining settings as needed.
5. Click *OK*.

To authenticate a category in the CLI:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            config filters
                edit 1
                    set category 52
                    set action authenticate
                    set auth-usr-grp "local_group"
                next
            end
        end
    next
end
```

To verify that you have configured authentication:

1. Go to a website that belongs to the category, such as www.fortinet.com.
2. On the warning page, click *Proceed*.
3. Enter the username and password for the configured user group, then click *Continue*.

Customizing the replacement message page

When the category action is *Block*, *Warning*, or *Authenticate*, you can customize the replacement message page that a user sees.

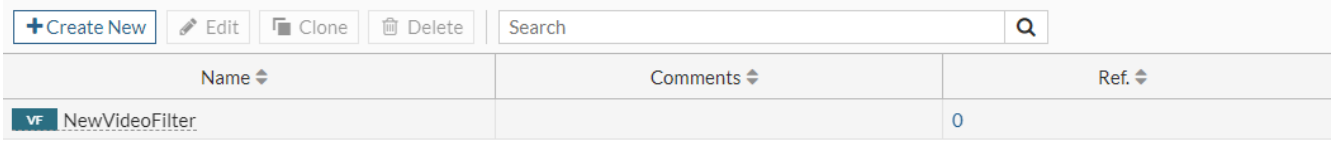
To customize the replacement message page:

1. Go to *Security Profiles* > *Web Filter* and edit or create a new web filter profile.
2. In the *FortiGuard category based filter* section, right-click on a category and select *Customize*.
3. Select a *Replacement Message Group*. See Replacement Message Groups on page 960 for details.
4. Optionally, click *Edit FortiGuard Block Page* or *Edit FortiGuard Warning Page* to make modifications.
5. Click *Save*.
6. Configure the remaining settings as needed.
7. Click *OK*.

Video Filter

With the video filter profile, you can filter YouTube videos by channel ID for a more granular override of a single channel, user, or video. The video filter profile is currently supported in proxy-based policies and requires SSL deep inspection.

To view available video filter profiles, go to *Security Profiles* > *Video Filter*.



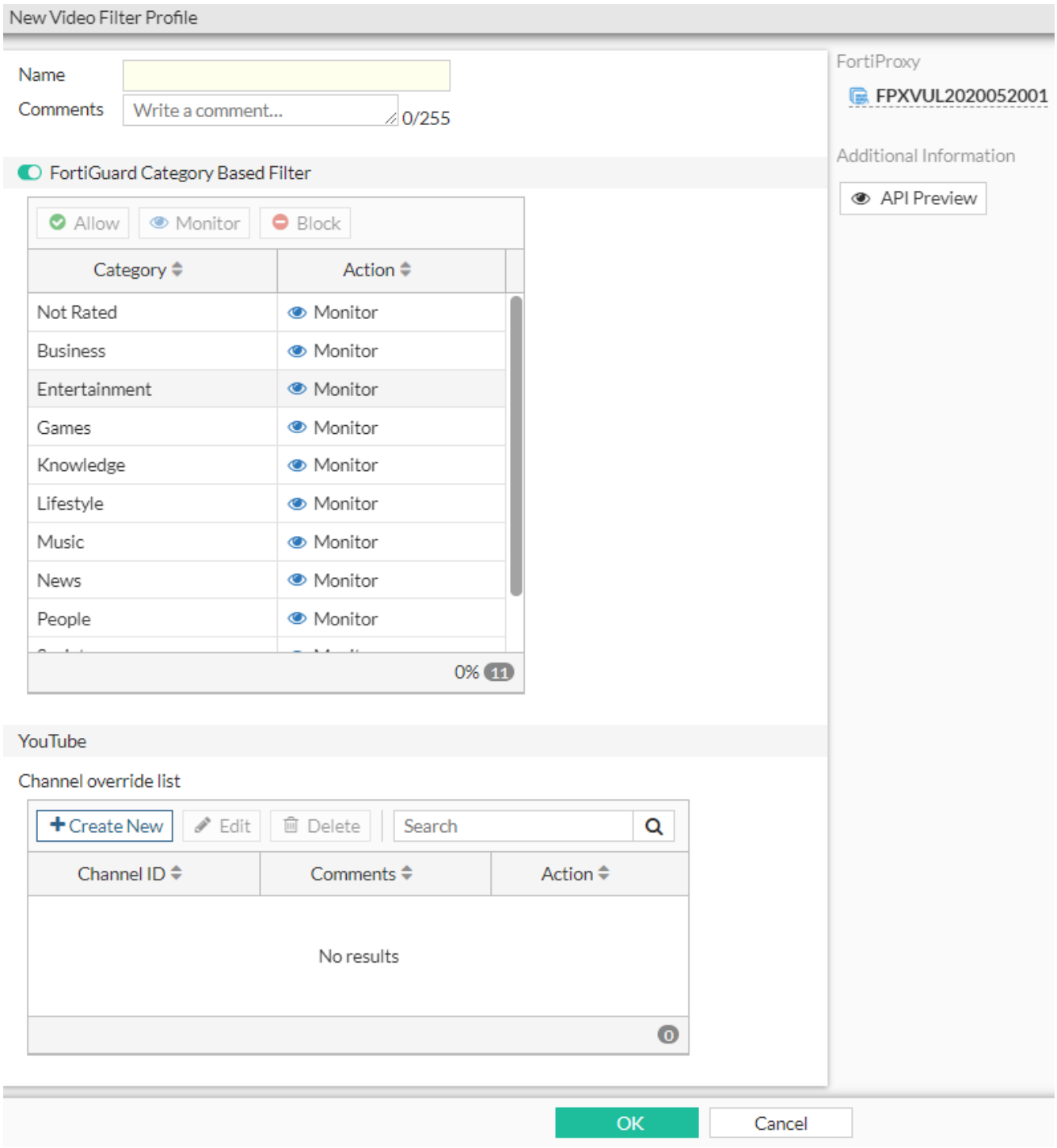
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a video filter profile. See Create or edit a video filter profile on page 580.
Edit	Modify the selected video filter profile. See Create or edit a video filter profile on page 580.
Clone	Make a copy of the selected video filter profile.
Delete	Remove the selected video filter profile.
Search	Enter a search term to find in the video filter profile list.
Name	The name of the video filter profile.
Comments	An optional description of the video filter profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a video filter profile

Click *Create New* to open the *New Video Filter Profile* window.



Select a video filter profile and then click *Edit* to open the *Edit Video Filter Profile* window.

Configure the following settings in the *New Video Filter Profile* window and then click *OK*:

Name	The name of the video filter profile.
Comments	Optional description of thevideo filter profile.

FortiGuard category based filter	Enable to use FortiGuard categories. If the device is not licensed for the FortiGuard web-filtering service, traffic can be blocked by enabling this option.
Allow/Monitor/Block	Select the action for each FortiGuard category: *Allow*, *Monitor*, or *Block*.
YouTube	
Channel override list	Create or edit a YouTube channel override list. See Create or edit a channel override entry on page 583.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

To configure a video filter in the GUI:

```
config videofilter youtube-channel-filter
   edit <identifier>
      set name <string>
      config entries
         edit <identifier>
            set action{allow | monitor | block}
            set channel-id <string>
         next
      end
   next
end
```

For example:

```
config videofilter youtube-channel-filter
   edit 1
      set name "channel_filter"
      config entries
         edit 1
            set action block
            set channel-id "UCJHo4AuVomwMRzgkA5DQEOA"
         next
      end
   next
end
```

Create or edit a channel override entry

You can override the video filter with channel override entries.

To create a channel override entry:

1. Go to *Security Profiles* > *Video Filter*.
2. Click *Create New* or select a video filter profile and then click *Edit*.
3. Click *Create New*. The *New Channel override Entry* window opens.
4. Enter the YouTube channel ID.
5. Enter a description of the YouTube channel.
6. Select the action to take when the pattern is matched:
   - *Allow*: Allow access to the YouTube channel.
   - *Monitor*: Monitor traffic to and from the YouTube channel.
   - *Block*: Block access to the YouTube channel and display a replacement message. SeeReplacement Messages on page 944.
7. Click *OK* to save the channel override entry.
8. Click *OK* to save the changes to the video filter profile.

To edit a channel override entry:

1. Go to *Security Profiles* > *Video Filter*.
2. Click *Create New* or select a video filter profile and then click *Edit*.
3. Select a channel override entry and then click *Edit*.
4. Edit the entry settings as required.
5. Click *OK* to save your changes to the channel override entry.
6. Click *OK* to save the changes to the video filter profile.

Filtering based on title

Video filtering can be configured to filter using keyword-based filters for video titles. When a video's title matches the configured keyword, the video filter will take the corresponding action of allow, monitor, or block. Video filtering is only supported in proxy-based inspection mode, and deep inspection must be enabled in the firewall policy.

The YouTube API key must be configured to use this feature. Otherwise, the title filter will not retrieve the video information and bypass the traffic.

Basic configuration

In this example, videos are blocked that contain the keyword, game. For information about configuring video filter keyword lists, see Example configuration.

To configure the video filter profile in the GUI:

1. Configure the video filter profile:
   a. Go to *Security Profiles* > *Video Filter*, select the *Video Filter Profile* tab, and click *Create new*.
   b. Enter a name (*title-filter-profile*).
   c. In the *Filters* table, click *Create new*.
   d. Configure the filter with the following settings:
      i. Set the *Type* to *Title*.
      ii. Set the *Action* to *Block*.
      iii. Set the *Keyword* to *test-keyword-match-or*.
      iv. Click *OK*.
   e. Click *OK* to save the video filter profile.
2. Apply the video filter in a firewall policy.

To configure the video filter profile in the CLI:

1. Configure the video filter profile:

```
config videofilter profile
    edit "title-filter-profile"
        config filters
            edit 1
                set type title
                set keyword 1
                set action block
                set log enable
            next
        end
    next
end
```

2. Apply the video filter in a firewall policy.

Verifying the configuration

From a client, search for a video in YouTube named "How To Use Python Steam API || Steam game API python". The video is blocked.

Sample log:

```
2: date=2024-09-24 time=14:31:54 eventtime=1727213514461744421 tz="-0700" logid="0350013712"
type="utm" subtype="webfilter" eventtype="videofilter-title" level="warning" vd="root" msg="Video
title is blocked." policyid=2 poluuid="a6ba2400-76a9-51ef-6f17-0f5efd8d28bf" policytype="policy"
sessionid=371964151 srcip=10.40.1.1 dstip=142.251.211.238 srcport=59698 dstport=443
srcintf="port1" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6
httpmethod="GET" service="HTTPS" action="blocked" videoinfosource="Cache" profile="title-filter-
profile" videoid="LaRHkSVvDjI" videotitle="How To Use Python Steam API  || Steam game API python"
hostname="www.youtube.com" agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0)
Gecko/201001" url="https://www.youtube.com/watch?v=LaRHkSVvDjI"
```

Filtering based on description

Video filtering can be configured to filter using keyword-based filters for video descriptions. When a video's description matches the configured keyword, the video filter will take the corresponding action of allow, monitor, or block. The description filter supports the first 100 characters of the video description. Video filtering is only supported in proxy-based inspection mode, and deep inspection must be enabled in the firewall policy.

The YouTube API key must be configured to use this feature. Otherwise, the description filter will not retrieve the video information and bypass the traffic.

Basic configuration

In this example, videos are blocked where the description contains the keyword, API. For information about configuring video filter keyword lists, see Example configuration.

To configure the video filter profile in the GUI:

1. Configure the video filter profile:
   a. Go to *Security Profiles* > *Video Filter*, select the *Video Filter Profile* tab, and click *Create new*.
   b. Enter a name (*test-description-filter*).
   c. In the *Filters* table, click *Create new*.
   d. Configure the filter with the following settings:
      i. Set the *Type* to *Description*.
      ii. Set the *Action* to *Block*.
      iii. Set the *Keyword* to *test-keyword-match-all*.
      iv. Click *OK*.
   e. Click *OK* to save the video filter profile.
2. Apply the video filter in a firewall policy.

To configure the video filter profile in the CLI:

1. Configure the video filter profile:

```
config videofilter profile
    edit "test-description-filter"
        config filters
            edit 1
                set type description
                set keyword 2
                set action block
                set log enable
            next
        end
    next
end
```

2. Apply the video filter in a firewall policy.

Verifying the configuration

From a client, search for a video in YouTube named "Postman Tutorial #7 - HTTP Methods GET and POST in Postman". The description contains the text, "POSTMAN TUTORIAL - Complete API Testing and API Test Automation Course using Postman Tool...", so the video is blocked.

Sample log:

```
4: date=2024-09-24 time=14:48:39 eventtime=1727214519292797544 tz="-0700" logid="0351013728"
type="utm" subtype="webfilter" eventtype="videofilter-description" level="warning" vd="root"
msg="Video description is blocked." policyid=2 poluuid="a6ba2400-76a9-51ef-6f17-0f5efd8d28bf"
policytype="policy" sessionid=371964444 srcip=10.40.1.1 dstip=142.251.215.238 srcport=65259
dstport=443 srcintf="port1" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined"
proto=6 httpmethod="GET" service="HTTPS" action="blocked" videoinfosource="Cache" profile="test-
description-filter" videoid="pUGmhtqVJRk" videodesc="Get all my courses for USD 5.99/Month -
https://bit.ly/all-c..." hostname="www.youtube.com" agent="Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:130.0) Gecko/201001" url="https://www.youtube.com/watch?v=pUGmhtqVJRk"
```

Configuring a video filter keyword list

Users have the ability to filter videos based on the video titles and descriptions by defining a video filter keyword. Multiple keywords can be defined using a wildcard or regular expression, and can be used with AND/OR logic options.



Unicode emoji character code is currently not supported.

Configure the video filter keyword list in the GUI:

1. Go to *Security Profiles* > *Video Filter*, select the *Video Filter Keyword* tab, and click *Create new*.
2. Configure the following:

Name	Enter a name.
Match operator	Select the match operator. • *Any*: match any keyword (OR logic) • *All*: match all keywords (AND logic)

3. Create the keywords:
   a. In the *Keywords* table, click *Create new*.
   b. Configure the following:

Pattern	Enter a regular expression or wildcard pattern string.
Pattern type	Select the pattern type. • *Wildcard*: suitable for basic search

	• *Regular Expression*: suitable for advanced search
Status	Set the status. • *Enable*: consider this keyword • *Disable*: ignore this keyword

   c. Click *OK*.
4. Click *OK* to save the keyword list.

Configure the video filter keyword list in the CLI:

```
config videofilter keyword
    edit <id>
        set name <string>
        set match {or | and}
        config word
           edit <name>
                set pattern-type {wildcard | regex}
                set status {enable | disable}
            next
        end
    next
end
```

Example configuration

In this example, two keywords, API and game, are created with the wildcard and regular expression types, respectively. The match operator is set to *Any*.

Configure the video filter keyword list in the GUI:

1. Go to *Security Profiles* > *Video Filter*, select the *Video Filter Keyword* tab, and click *Create new*.
2. Enter a name (*test-keyword-match-or*) and set *Match operator* to *Any*.
3. In the *Keywords* table, click *Create new*.
4. Configure the API keyword with the following settings:
   a. In the *Pattern* field, enter *API*.
   b. Set the *Pattern type* to *Wildcard*.
   c. Click *OK*.
5. Click *Create new*.
6. Configure the game keyword with the following settings:
   a. In the *Pattern* field, enter *Game*.
   b. Set the *Pattern type* to *Regular Expression*.
   c. Click *OK*.
7. Click *OK* to save the keyword list.

Configure the video filter keyword list in the CLI:

```
config videofilter keyword
    edit 1
        set name "test-keyword-match-or"
        set match or
        config word
           edit "API"
                set pattern-type wildcard
                set status enable
            next
            edit "Game"
                set pattern-type regex
                set status enable
            next
        end
    next
end
```

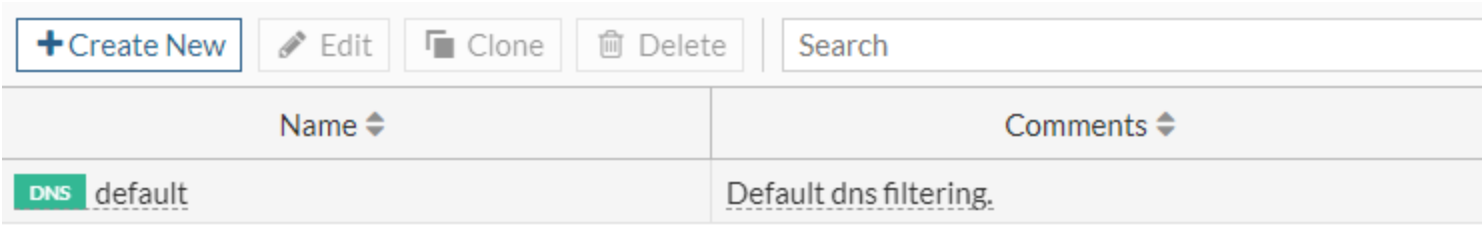
DNS Filter

You can configure DNS filtering to allow, block, or monitor access to web content according to FortiGuard categories. When DNS filtering is enabled, your FortiProxy unit must use the FortiGuard DNS service for DNS lookups. DNS lookup requests sent to the FortiGuard DNS service return with an IP address and a domain rating that includes the FortiGuard category of the web page.

If that FortiGuard category is set to block, the result of the DNS lookup is not returned to the requester. If the category is set to redirect, then the address returned to the requester points at a FortiGuard redirect page.

You can also allow or monitor access based on the FortiGuard category.

To view available DNS filter profiles, go to *Security Profiles* > *DNS Filter*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a DNS filter profile. See Create or edit a DNS filter profile on page 589.
Edit	Modify the selected DNS filter profile. See Create or edit a DNS filter profile on page 589.
Clone	Make a copy of the selected DNS filter profile.
Delete	Remove the selected DNS filter profile.
Search	Enter a search term to find in the DNS filter list.
Name	The name of the DNS filter profile.
Comments	An optional description of the DNS filter profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a DNS filter profile

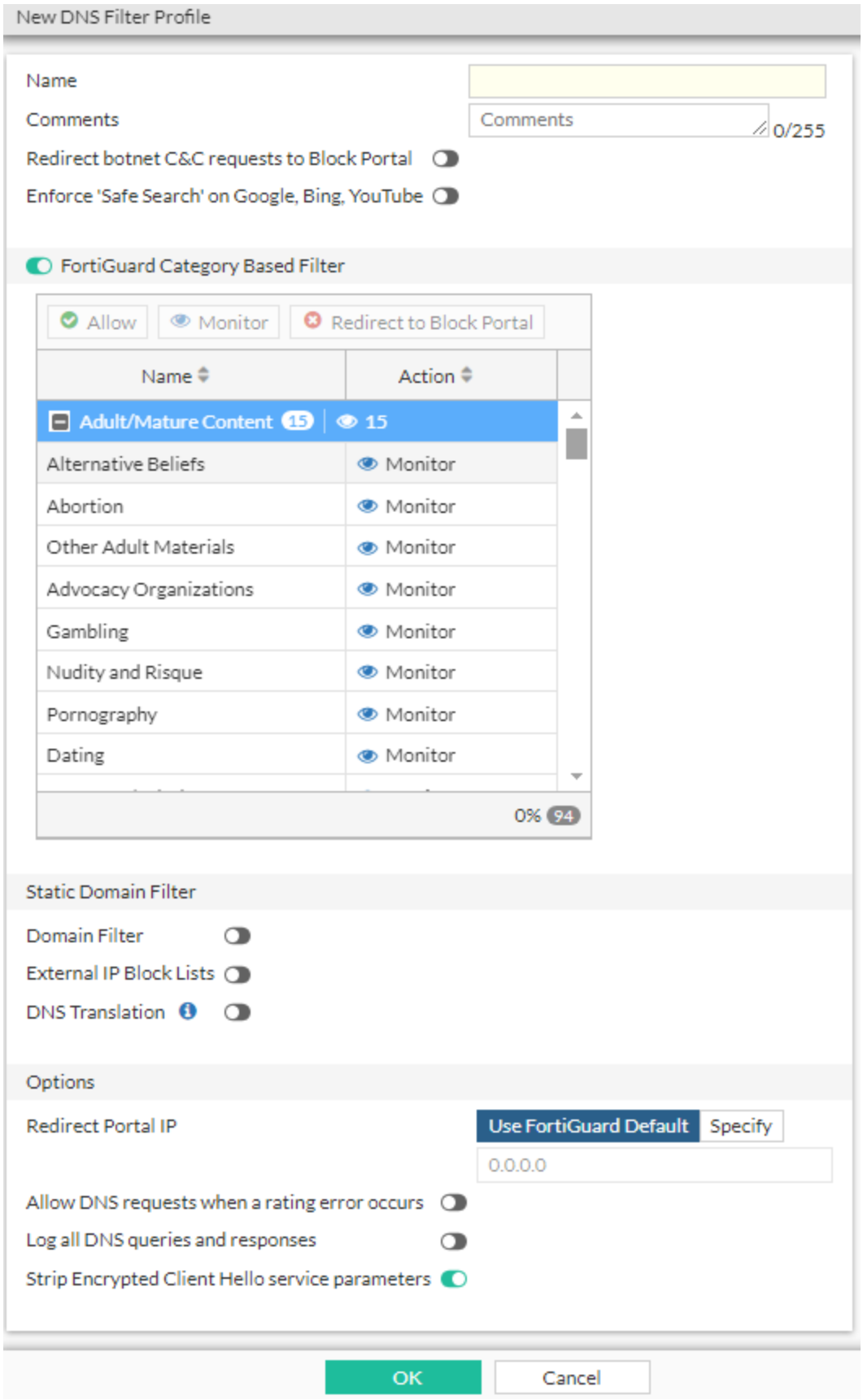
A DNS filter profile contains settings that enable or disable various forms of DNS filtering, including:

- FortiGuard filtering
- Botnet C&C domain blocking
- DNS safe search
- External dynamic category domain filtering
- Local domain filter
- External IP block list
- DNS translation

Once a DNS filter is configured, it can be applied to a policy to scan DNS queries that pass through the FortiProxy or on a FortiProxy DNS server if one is configured.

To configure a DNS filter profile:

1. On the *Security Profiles > DNS Filter* page, click *Create New* to create a new DNS filter profile or select the profile you want to edit in the list and then click *Edit*. The *New/Edit DNS Filter Profile* window opens.


New DNS Filter Profile
Name
Comments
Comments
0/255
Redirect botnet C&C requests to Block Portal
Enforce 'Safe Search' on Google, Bing, YouTube
FortiGuard Category Based Filter
Allow
Monitor
Redirect to Block Portal
Name
Action
Adult/Mature Content 15
15
Alternative Beliefs
Monitor
Abortion
Monitor
Other Adult Materials
Monitor
Advocacy Organizations
Monitor
Gambling
Monitor
Nudity and Risque
Monitor
Pornography
Monitor
Dating
Monitor
0% 94
Static Domain Filter
Domain Filter
External IP Block Lists
DNS Translation
Options
Redirect Portal IP
Use FortiGuard Default
Specify
0.0.0.0
Allow DNS requests when a rating error occurs
Log all DNS queries and responses
Strip Encrypted Client Hello service parameters
OK
Cancel

2. Configure the following settings:

Name	The name of the DNS filter profile.
Comments	Optional description of the DNS filter profile.
Redirect botnet C&C requests to Block Portal	Enable to block botnet website access at the DNS name resolution stage. FortiGuard Service continually updates the botnet C&C domain list. The botnet C&C domain blocking feature can block the botnet website access at the DNS name resolving stage. This provides additional protection for your network.
Enforce 'Safe search' on Google, Bing, YouTube	Enable to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines. The FortiProxy responds with content filtered by the search engine.
Restrict YouTube Access	When *Enforce 'Safe Search' on Google, Bing, YouTube* is enabled, select either *Strict* or *Moderate* to restrict YouTube access by responding to DNS resolutions with CNAME restrict.youtube.com and restrictmoderate.youtube.com respectively.
FortiGuard category based filter	Enable to use the FortiGuard domain rating database to inspect DNS traffic. A FortiGuard Web Filter license is required to use this option. Expand the category groups in the table to view and edit the FortiGuard category settings to *Allow*, *Monitor*, or *Redirect to Block Portal*.
Allow/Monitor/Redirect to Block Portal	Select the action for each FortiGuard category: *Allow*, *Monitor*, or *Redirect to Block Portal*.
Static Domain Filter	
Domain Filter	Enable to define local static domain filters to allow or block specific domains. The local domain filter has a higher priority than the FortiGuard category-based domain filter. Click *Create New* in the table to add a domain filter and configure the following settings. • *Domain*: enter a domain. • *Type*: select *Simple*, *Reg. Expression*, or *Wildcard*. • *Action*: select *Redirect to Block Portal*, *Allow*, or *Monitor*. • *Status*: select *Enable* or *Disable*. See Create or edit a domain filter on page 593.
External IP Block Lists	Enable to create or select a list of external IP addresses to block. See External Connectors on page 1106.
DNS Translation	Enable to translate a DNS resolved IP address to another IP address specified on a per-policy basis. Click *Create New* in the table to add a DNS translation and configure the following settings. • *Type*: select *IPv4* or *IPv6*. • *Original Destination*: enter the address of a host or subnet that

	you want translated. When a resolved address in a DNS response matches this destination, the FortiGate will replace the address with the address in *Translated Destination*. • *Translated Destination*: enter the address of a host or subnet that you want the resolved address to be translated to. • *Network Mask*: enter the netmask for the original and translated destination. If a single host is used for the original and translated destination, set the netmask to *255.255.255.255*. • *Status*: select *Enable* or *Disable*. Enabling DNS translation will override matching DNS responses with translated IPs. See Create or edit a DNS translation entry on page 594.
Options	
Redirect Portal IP	If you want the FortiProxy unit to use the portal IP address to replace the resolved IP address in the DNS response packet, select *Use FortiGuard Default* or *Specify*. If you select *Specify*, enter the portal IP address. When *FortiGuard Category Based Filter* categories are set to *Redirect to Block Portal*, the DNS response will use this IP address in its response to the client. If the client is accessing the domain on a web browser, they will be redirected to the block portal page on this address.
Allow DNS requests when a rating error occurs	Enable to allow access to domains that return a rating error from the web filter service. If your unit is temporarily unable to contact the FortiGuard service, this setting determines what access the unit allows until contact is re-established. If enabled, users will have full unfiltered access to all domains. If disabled, users will not be allowed access to any domains.
Log all DNS queries and responses	Enable if you want DNS queries and responses logged.
Strip Encrypted Client Hello service parameters	Enable to remove the encrypted client hello (ECH) service parameter from supporting DNS RRs. ECH information is stripped from DoH responses, forcing the browser to not use ECH for TLS connections. See Control TLS connections that utilize Encrypted Client Hello on page 635 for more information.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

3. Click *OK*.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create or edit a domain filter

The DNS static domain filter allows you to block, exempt, or monitor DNS requests by using IPS to look inside DNS packets and match the domain being looked up with the domains on the static URL filter list. If there is a match the DNS request can be blocked, exempted, monitored, or allowed.

If blocked, the DNS request is blocked and so the user cannot look up the address and connect to the site.

If exempted, access to the site is allowed even if another method is used to block it.

To create a domain filter:

1. Go to *Security Profiles* > *DNS Filter*.
2. Click *Create New* or select a DNS filter profile and then click *Edit*.
3. Enable *Domain Filter*.
4. In the *Domain Filter* table, select *Create New*. The *Create Domain Filter* window opens.
5. Enter the domain to filter in the *Domain* field. Enter a top-level domain suffix (for example, “com” without the leading period) to block access to all web sites with this suffix.
6. Select the type of pattern to match: *Simple*, *Reg. Expression*, or *Wildcard*.
7. Select the action to take when the pattern is matched:
   - *Redirect to Block Portal*: If a DNS query domain name rating belongs to the block category, the query is blocked and redirected.
   - *Allow*: Allow access to any domain that matches the domain pattern.
   - *Monitor*: Monitor traffic to and from domains matching the domain pattern.
8. Enable or disable the status of the filter to make the filter active or inactive.
9. Click *OK* to save the domain filter.
10. Click *OK* to save the DNS filter profile.

To edit a domain filter:

1. Go to *Security Profiles* > *DNS Filter*.
2. Click *Create New* or select a DNS filter profile and then click *Edit*.
3. Enable *Domain Filter*.
4. In the Domain Filter table, double-click on a filter or select the filter and then click *Edit* in the toolbar.
5. Edit the filter settings as required.

6. Click *OK* to save your changes to the domain filter.
7. Click *OK* to save the DNS filter profile.

Create or edit a DNS translation entry

This setting allows you to translate a DNS resolved IP address to another IP address you specify on a per-policy basis.

For example, website A has a public address of 1.2.3.4. However, when your internal network users visit this website, you want them to connect to the internal host 192.168.3.4. You can use DNS translation to translate the DNS resolved address 1.2.3.4 to 192.168.3.4. Reverse use of DNS translation is also applicable. For example, if you want a public DNS query of your internal server to get a public IP address, then you can translate a DNS resolved private IP to a public IP address.

To create a DNS translation entry:

1. Go to *Security Profiles* > *DNS Filter* and enable *DNS Translation*.
2. In the *DNS Translation* table, select *Create New*. The *New DNS Translation* window opens.
3. Select the type of IP address to translate, either *IPv4* or *IPv6*.
4. In the *Original Destination* field, enter the domain's original IP address.
5. In the *Translation Destination* field, enter the IP address that you want used instead of the original IP address.
6. Enter the network mask.
7. Enable or disable the status.
8. Click *OK* to save the DNS translation entry.
9. Click *OK* to save the DNS filter profile.

To edit a DNS translation entry:

1. Go to *Security Profiles* > *DNS Filter* and enable *DNS Translation*.
2. In the *DNS Translation* table, double-click on an entry or select an entry and then click *Edit* in the toolbar.
3. Edit the settings as required.
4. Click *OK* to save the DNS translation entry.
5. Click *OK* to save the DNS filter profile.

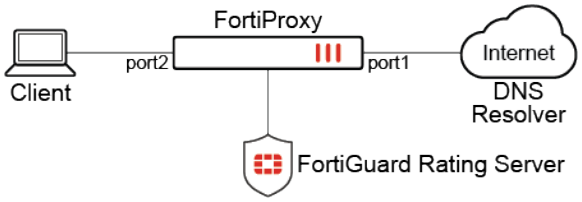
HTTP3 deep inspection, QUIC certificate inspection, DNS over QUIC and DNS over HTTP3 for transparent and local-in DNS modes

The FortiProxy can handle the QUIC/TLS handshake and perform deep inspection for HTTP3 and QUIC traffic, including certificate inspection. This allows for faster and more secure DNS resolution, with improved privacy and reduced latency.

DNS over QUIC (DoQ) and DNS over HTTP3 (DoH3) are also supported in proxy mode inspection for transparent and local-in explicit modes. With DoQ and DoH3, connections can be established faster than with DNS over TLS (DoT) or DNS over HTTPS (DoH).

In transparent mode, the FortiProxy is acting as a proxy, forwarding DNS queries, and not as a DNS server. In local-in DNS mode, the FortiProxy acts as the DNS server and a DNS filter profile is applied in the system DNS server.

DoQ transparent and local-in query can be achieved using tools or applications in Linux, such as the q tiny command line DNS client from Natesales.



DoH3 transparent and local-in query can be achieved in Linux using q or Curl. In Windows, change the client network DNS server to the FortiProxy and treat the FortiProxy as a HTTP3 DNS server listening for DoH3 connections.

To configure DoQ in transparent mode:

1. Enable QUIC in the ssl-ssh-profile:

```
config firewall ssl-ssh-profile
    edit "protocols"
        config dot
            set status deep-inspection
            set quic inspect
        end
    next
end
```

2. Configure a DNS filter profile:

```
config dnsfilter profile
    edit "dnsfilter_fgd"
        config ftgd-dns
            config filters
                edit 1
                    set category 30
                    set action block
                next
            end
        end
    next
end
```

3. Apply the profiles to a proxy firewall policy:

```
config firewall policy
    edit 1
```

```
        set name "dnsfilter"
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "protocols"
        set dnsfilter-profile "dnsfilter_fgd"
        set logtraffic all
        set nat enable
    next
end
```

4. Test the configuration:

   On the client, use q to query a FortiGuard category30 domain with the Adguard DNS server over QUIC. The default redirect block IP address should be returned:

```
pc03:~# q www.sfu.ca @quic://dns.adguard.com --tls-no-verify
2023/08/18 18:53:44 failed to sufficiently increase receive buffer size (was: 208 kiB, wanted:
2048 kiB, got: 416 kiB). See https://github.com/quic-go/quic-go/wiki/UDP-Receive-Buffer-Size
for details.
www.sfu.ca. 1m0s A 208.91.112.55
www.sfu.ca. 1m0s AAAA 2620:101:9000:53::55
```

To configure DoQ in local-in mode:

1. In the FortiProxy DNS server configuration, enable DoQ for a port with the previously configured DNS filter profile applied:

```
config system dns-server
    edit "port2"
        set dnsfilter-profile "dnsfilter_fgd"
        set doq enable
    next
end
```

2. Test the configuration:

   On the client, use q to query a FortiGuard category30 domain with the FortiProxy interface over QUIC. The default redirect block IP address should be returned:

```
pc03:~# q www.mcgill.ca @quic://10.1.100.150 --tls-no-verify
2023/08/18 20:05:53 failed to sufficiently increase receive buffer size (was: 208 kiB, wanted:
2048 kiB, got: 416 kiB). See https://github.com/quic-go/quic-go/wiki/UDP-Receive-Buffer-Size
for details.
www.mcgill.ca. 1m0s A 208.91.112.55
www.mcgill.ca. 1m0s AAAA 2620:101:9000:53::55
```

To configure DoH3 in transparent mode:

1. Enable QUIC in the ssl-ssh-profile:

```
config firewall ssl-ssh-profile
    edit "protocols"
        config https
            set ports 443 8443
            set status deep-inspection
            set quic inspect
        end
    next
end
```

2. Configure a DNS filter profile:

```
config dnsfilter profile
    edit "dnsfilter_fgd"
        config ftgd-dns
            config filters
                edit 1
                    set category 30
                    set action block
                next
            end
        end
    next
end
```

3. Apply the profiles to a proxy firewall policy:

```
config firewall policy
    edit 1
        set name "dnsfilter"
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "protocols"
        set dnsfilter-profile "dnsfilter_fgd"
        set logtraffic all
        set nat enable
    next
end
```

4. Test the configuration:

On the client with HTTP3 support, use q or Curl to query a FortiGuard category30 domain with the Adguard DNS server or Cloudflare DNS server over QUIC. The default redirect block IP address should be returned:

```
[test@localhost q]$ sudo ./q www.mcgill.ca --http3 @https://dns.adguard.com --tls-insecure-skip-verify
www.mcgill.ca. 1m A 208.91.112.55
www.mcgill.ca. 1m AAAA 2620:101:9000:53::55
```

To configure DoH3 in local-in mode:

1. In the FortiProxy DNS server configuration, enable DoH3 for a port with the previously configured DNS filter profile applied:

```
config system dns-server
    edit "port2"
        set dnsfilter-profile "dnsfilter_fgd"
        set doh3 enable
    next
end
```

2. Test the configuration:

   On the client with HTTP3 support, use q or Curl to query a FortiGuard category30 domain with the FortiProxy interface over HTTP3. The default redirect block IP address should be returned:

```
[test@localhost q]$ sudo ./q www.mcgill.ca --http3 @https://10.4.62.160 --tls-insecure-skip-verify
www.mcgill.ca. 1m A 208.91.112.55
www.mcgill.ca. 1m AAAA 2620:101:9000:53::55
```

Application Control

Using the Application Control feature, your FortiProxy unit can detect and take action against network traffic depending on the application generating the traffic. Based on FortiProxy Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the FortiProxy unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses nonstandard ports or protocols. Application control supports detection for traffic using HTTP protocol (versions 1.0, 1.1, and 2.0).

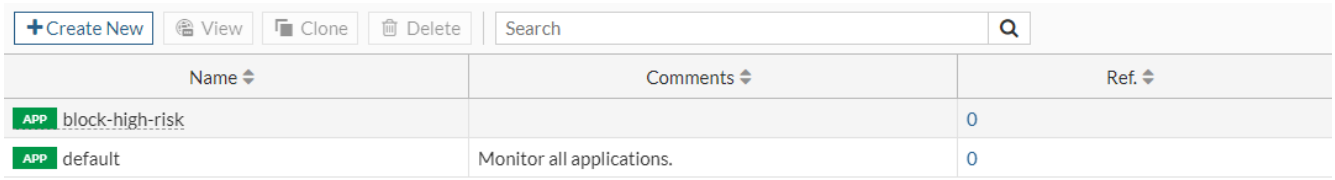
The FortiProxy unit can recognize the network traffic generated by a large number of applications. You can create application control sensors that specify the action to take with the traffic of the applications you need to manage and the network on which they are active, and then add application control sensors to the firewall policies that control the network traffic you need to monitor.

Fortinet is constantly adding to the list of applications detected through maintenance of the FortiGuard Application Control Database. This database is part of the FortiGuard Intrusion Protection

System Database because intrusion protection protocol decoders are used for application control and both of these databases have the same version number.

You can see the complete list of applications supported by FortiGuard Application Control on the FortiGuard site or https://fortiguard.com/appcontrol. This web page lists all of the supported applications. You can select any application name to see details about the application.

To view available application sensors, go to *Security Profiles* > *Application Control*.



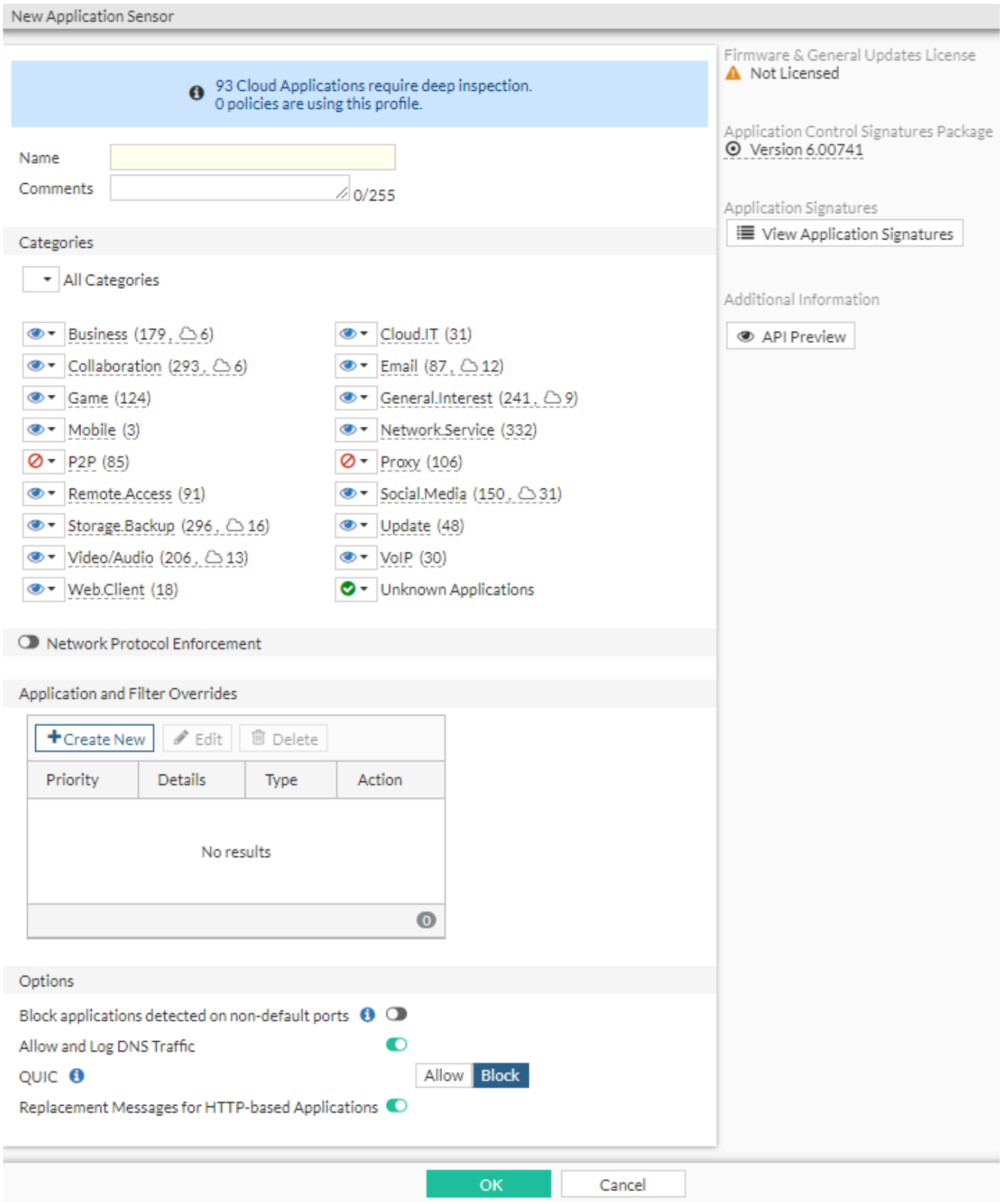
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an application sensor. See Create or edit an application sensor on page 599.
Edit	Modify the selected application sensor. See Create or edit an application sensor on page 599.
Clone	Make a copy of the selected application sensor.
Delete	Remove the selected application sensor.
Search	Enter a search term to search the application sensor list.
Name	The name of the application sensor.
Comments	An optional description of the application sensor.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an application sensor

To create an application sensor, click *Create New*.


New Application Sensor
93 Cloud Applications require deep inspection.
0 policies are using this profile.
Name
Comments
0/255
Categories
All Categories
Business (179, 6)
Collaboration (293, 6)
Game (124)
Mobile (3)
P2P (85)
Remote.Access (91)
Storage.Backup (296, 16)
Video/Audio (206, 13)
Web.Client (18)
Cloud.IT (31)
Email (87, 12)
General.Interest (241, 9)
Network.Service (332)
Proxy (106)
Social.Media (150, 31)
Update (48)
VoIP (30)
Unknown Applications
Network Protocol Enforcement
Application and Filter Overrides
Create New
Edit
Delete
Priority
Details
Type
Action
No results
Options
Block applications detected on non-default ports
Allow and Log DNS Traffic
QUIC
Allow
Block
Replacement Messages for HTTP-based Applications
Firmware & General Updates License
Not Licensed
Application Control Signatures Package
Version 6.00741
Application Signatures
View Application Signatures
Additional Information
API Preview
OK
Cancel

Configure the following settings and then select *OK*:

Name	The name of the application sensor.
Comments	Optional description of the application sensor.
Categories	Select an action for *All Categories* or for each category of applications: • *Monitor*—This action allows the targeted traffic to continue on through the FortiProxy unit but logs the traffic for analysis. • *Allow*—This action allows the targeted traffic to continue on through the FortiProxy unit. • *Block*—This action prevents all traffic from reaching the application and logs all occurrences. • *Quarantine*—This action allows you to quarantine or block access to an application for a specified duration that can be entered in days, hours, and minutes. The default is 5 minutes. You can also select *View Signatures* or *View Cloud Signatures* to see a list of signatures for some categories.
Network Protocol Enforcement	Enable and configure network services on certain ports and determine the violation action. SeeCreate or edit a default network service on page 602. Protocol enforcement allows you to configure networking services (for example, FTP, HTTP, and HTTPS) on known ports (for example, 21, 80, or 43). For protocols that have not been added to the allowlist for certain ports, the IPS engine performs the violation action to block, allow, or monitor that traffic.
Application and Filter Overrides	Application overrides allow you to choose individual applications. To add an application override, see Add or edit an application override on page 603. Filter overrides can be added based on behavior, application category, popularity, protocol, risk, technology, or vendor subtypes. To add a filter override, see Add or edit a filter override on page 603.
Allow and Log DNS Traffic	Enable to allow DNS traffic.
Block applications detected on non-default ports	For monitor and allow actions, applications are blocked if they are detected on nondefault ports (as defined in FortiGuard application signatures). Block actions still block all traffic for the application, regardless of port.
QUIC	Select *Allow* if you want the FortiProxy unit to inspect Google Chrome packets for a QUIC header. Select *Block* to force Google Chrome to use HTTP2/TLS 1.2.
Replacement Messages for HTTP-based Applications	Enable to display replacement messages for HTTP-based applications.

View Application Signatures	Select to see a list of predefined application signatures. To create an application signature, see Create or edit an application signature on page 645.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

To edit an application sensor:

1. From the application sensor list, select the sensor that you need to edit and then click *Edit* from the toolbar or double-click on the sensor name in the list. The *Edit Application Sensor* window opens.
2. Edit the information as required and then select *OK* to save your changes.

Create or edit a default network service

Protocol enforcement allows you to configure networking services (e.g. FTP, HTTP, HTTPS) on known ports (e.g. 21, 80, 443). For protocols that are not allowlisted under select ports, the IPS engine performs the violation action to block, allow, or monitor that traffic.

This feature can be used in the following scenarios:

- When one protocol dissector confirms the service of network traffic, protocol enforcement can check whether the confirmed service is allowlisted under the server port. If it is not allowlisted, the traffic is considered a violation and IPS can take the action specified in the configuration (block or monitor it).
- When there is no confirmed service for the network traffic, the traffic is considered a service violation if IPS dissectors rule out all of the services enforced under its server port.

In an applicable profile, a default-network-service list can be created to associate well known ports with accepted services.

Default network services can be added or edited, as required.

To create a default network service:

1. Go to *Security Profiles* > *Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.

3. Enable *Network Protocol Enforcement*.
4. In the *Network Protocol Enforcement* section, select *Create New*.
5. Enter a port number.
6. Enter one or more protocols to allow on the specified port.
7. Select to block or monitor protocols that are not specified in the *Enforce protocols* field.
8. Click *OK*.

To edit a default network service:

1. Go to *Security Profiles* > *Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. Enable *Network Protocol Enforcement*.
4. Select the default network service that you want to edit and then click *Edit* from the toolbar. The *Edit Default Network Service* window opens.
5. Edit the information as required and then click *OK* to apply your changes.

Add or edit an application override

Application overrides can be added or edited as required.

To add predefined signatures:

1. Go to *Security Profiles* > *Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. In the *Application and Filter Overrides* section, click *Create New*.
4. Select *Application* for the override type.
5. Select the action to take: *Monitor*, *Allow*, *Block*, or *Quarantine*.
6. Use the search field to narrow down the list of possible signatures by a series of attributes.
7. Click *OK*.

To edit a predefined signature:

1. Go to *Security Profiles* > *Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. In the *Application and Filter Overrides* section, select the application override to edit and then click *Edit* from the toolbar.
4. Edit the information as required and then click *OK* to apply your changes.

Add or edit a filter override

Filters overrides can be added or edited as required.

To create a filter override:

1. Go to *Security Profiles* > *Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. In the *Application and Filter Overrides* section, click *Create New*.
4. Select *Filter* for the override type.
5. Select the action to take: *Monitor*, *Allow*, *Block*, or *Quarantine*.
6. Use the search field to narrow down the list of possible filters by a series of attributes.
7. Click *OK*.

To edit a filter override:

1. Go to *Security Profiles* > *Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. In the *Application and Filter Overrides* section, select the filter override to edit and then click *Edit* from the toolbar.
4. Edit the information as required and then click *OK* to apply your changes.

Basic category filters and overrides

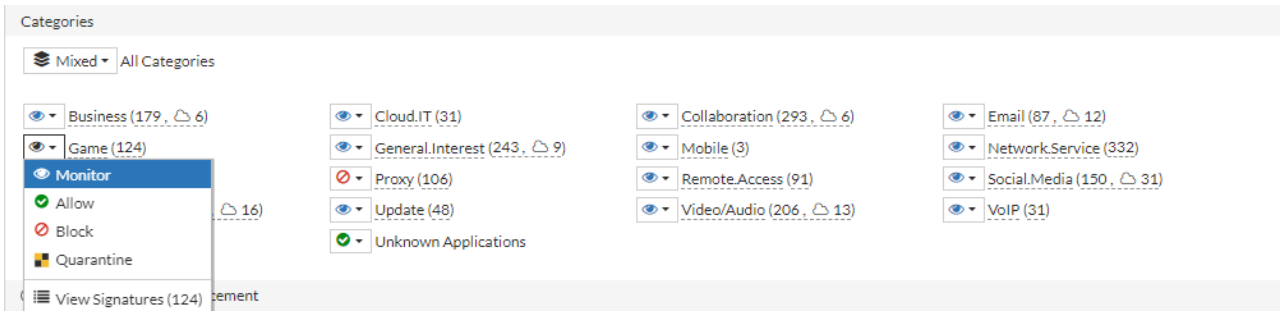
When creating an application sensor, you can define the applications that you want to control. You can add applications and filters using categories, application overrides, and/or filter overrides with designated actions (monitor, allow, block, or quarantine).

Action	Description
Monitor	Passes the traffic and generates a log message.
Allow	Passes the traffic but does not generate a log message.
Block	Drops the detected traffic and generates a log message.
Quarantine	Blocks the traffic from an attacker IP address until the expiration time is reached and generates a log message.

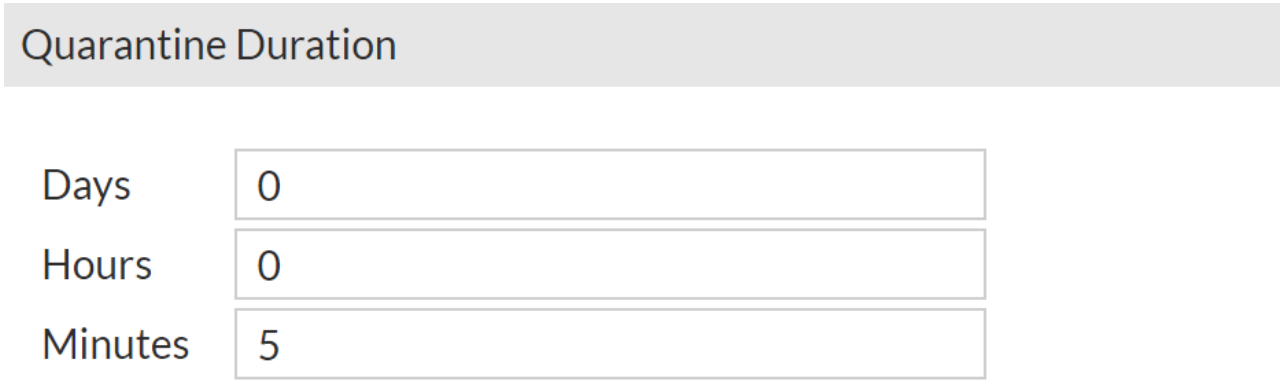
For more information about application control logs, see Security Events on page 1143.

To configure category filters in the GUI:

1. Go to *Security Profiles* > *Application Control* and click *Create New*, or edit an existing sensor.
2. Under *Categories*, click the icon next to the category name to set the action or view the application signatures.



3. If you select the *Quarantine* action, the *Quarantine Duration* pane will open. Enter the duration values and click *OK*.



4. Click *OK*.

To configure category filters in the CLI:

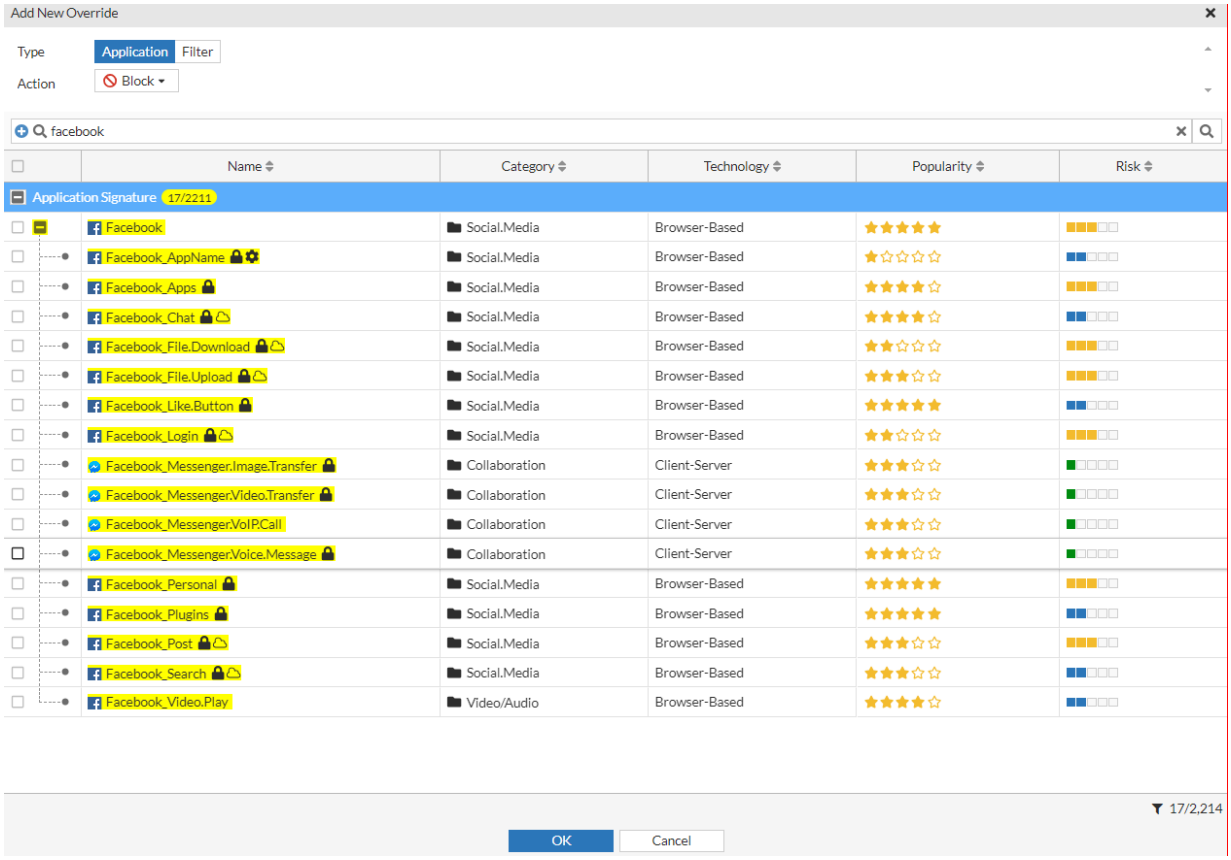
```
config application list
    edit <name>
        config entries
            edit <id>
                set category <id>
                set action {pass | block | reset}
                set quarantine {none | attacker}
                set quarantine-expiry <###d##h##m>
                set log {enable | disable}
            next
        end
    next
end
```

Configuring application and filter overrides

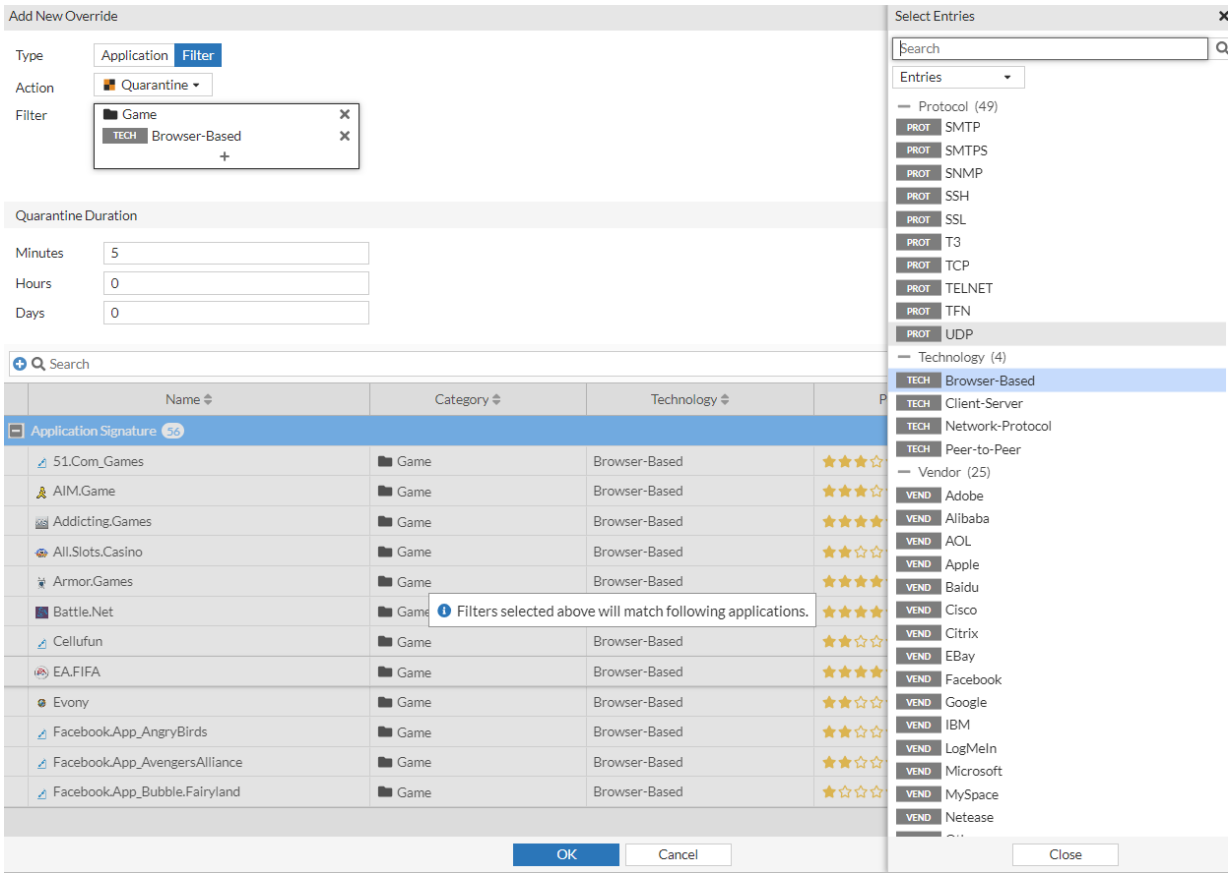
Multiple application signatures can be added for one sensor with a designated action. Filters can be added based on behavior, application category, popularity, protocol, risk, technology, or vendor subtypes.

To configure overrides in the GUI:

1. Go to *Security Profiles* > *Application Control* and click *Create New*, or edit an existing sensor.
2. Add an application:
   a. In the *Application and Filter Overrides* table, click *Create New*.
   b. For *Type*, select *Application*.
   c. Select an *Action* from the dropdown.
   d. In the *Search* box, enter an application name and press Enter, or click the plus icon and configure a search filter.
   e. In the search results, select the required applications (you can select multiple applications).



   f. Click *OK*.
3. Add a filter:
   a. In the *Application and Filter Overrides* table, click *Create New*.
   b. For *Type*, select *Filter*.
   c. Select an *Action* from the dropdown.
      If the action is set to *Quarantine*, set the duration of the quarantine.
   d. In the *Filter* field, click the *+* . The *Select Entries* pane opens, and you can search based on filter subtypes. This example uses Browser-Based (under Technology) and Game (under Category).



e. Click *OK*.

4. Click *OK*.

To configure overrides in the CLI:

```
config application list
    edit <name>
        config entries
            edit <id>
                set protocols <integer>
                set risk <integer>
                set vendor <id>
                set technology <id>
                set behavior <id>
                set popularity <integer>
                set action {pass | block | reset}
                set quarantine {none | attacker}
                set log {enable | disable}
            next
        end
    next
end
```

`protocols <integer>`	Application protocol filter (0 - 47, or all).
`risk <integer>`	Risk or impact of allowing traffic from this application to occur (1 - 5; low (1), elevated (2), medium (3), high (4), and critical (5)).
`vendor <id>`	Application vendor filter (0 - 25, or all).
`technology <id>`	Application technology filter: • all • 0 (network-protocol) • 1 (browser-based) • 2 (client-server) • 4 (peer-to-peer)
`behavior <id>`	Application behavior filter: • all • 2 (botnet) • 3 (evasive) • 5 (excessive bandwidth) • 6 (tunneling) • 9 (cloud)
`popularity <integer>`	Application popularity filter (1 - 5, from least to most popular).
`action {pass | block | reset}`	Pass/block traffic or reset the connection for traffic from this application (default = block).
`quarantine {none | attacker}`	Set the quarantine method: • `none`: Quarantine is disabled. • `attacker`: Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.
`log {enable | disable}`	Enable/disable logging for this application list (default = enable).

For more information, see `config application list` in the FortiProxy CLI reference Guide.

Inline CASB

The inline CASB security profile enables the FortiProxy to perform granular control over SaaS applications directly on policies. The supported controls include:

Control	Description
Privilege control	Specify the action to apply to user activities per application such as upload, download, share, delete, log in, and so on.
Safe search	On SaaS applications that support searching, enable and select the level of safe search.

Control	Description
Tenant control	Allow only users belonging to specific domains to access the SaaS application.
UTM bypass	For each user activity, bypass further UTM scanning any of the following security profiles: • Antivirus • DLP • File filter • Video filter • Web filter

Administrators can customize their own SaaS applications, matching conditions, and custom controls and actions.

Inline CASB can be applied to a policy. The policy must use a deep inspection SSL profile to apply the inline CASB profile and scan the traffic payload.



The Inline-CASB Application Definitions entitlement is licensed under the basic firmware and updates contract. To view the entitlement information, go to *System > FortiGuard* and expand the *Firmware & General Updates* section in the *License Information* table.

Example 1: privilege control

In this example, logging in to Microsoft Outlook is blocked by the privilege control settings in the inline CASB profile.

To configure an inline CASB profile with privilege control in the GUI:

1. Configure the inline CASB profile:
   a. Go to *Security Profiles > Inline-CASB* and click *Create new*.
   b. Enter a *Name*, such as *outlook_test*.
   c. In the *SaaS Applications* table, click *Create new*. The *Create SaaS Application Rules* pane opens.
   d. Set the *Application* to *microsoft-outlook*, then click *Next*.
   e. Enable *Logging*.
   f. In the *Privilege Control* table, select *login* and from the *Set Action* dropdown, select *Block*.
   g. Click *OK*.
2. Configure the firewall policy:
   a. Go to *Policy & Objects > Policy*. Edit an existing policy, or create a new one.
   b. In the *Security Profiles* section, enable *Inline-CASB* and select the *outlook_test* profile.
   c. Set the *SSL Inspection* profile to one that uses deep inspection.
   d. Configure the other settings as needed.
   e. Click *OK*.

To configure an inline CASB profile with privilege control in the CLI:

1. Configure the inline CASB profile:

```
config casb profile
    edit "outlook_test"
        config saas-application
            edit "microsoft-outlook"
                config access-rule
                    edit "microsoft-outlook-login"
                        set action block
                    next
                end
            next
        end
    next
end
```

2. Configure the firewall policy:

```
config firewall policy
    edit 6
        set name "casb_test"
        set srcintf "port1"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "ssl"
        set casb-profile "outlook_test"
        set nat enable
    next
end
```

To test the configuration:

1. Open a browser and attempt to access the Outlook login page.
2. The traffic is blocked by the firewall policy. The browser displays a replacement message: *Blocked by Inline CASB Control*.

Sample log:

```
1: date=2023-08-18 time=16:59:32 eventtime=1692403171962221884 tz="-0700" logid="2500010000"
type="utm" subtype="casb" eventtype="casb" level="warning" vd="vdom1" msg="CASB access was blocked
because it contained banned activity." policyid=6 sessionid=63635 srcip=10.1.100.195
dstip=20.190.190.130 srcport=61013 dstport=443 srcintf="port1" srcintfrole="undefined"
dstintf="port3" dstintfrole="undefined" proto=6 action="block" profile="outlook_test"
```

```
saasapp="microsoft-outlook" useractivity="microsoft-outlook-login" activitycategory="activity-
control"
```

Example 2: safe search

In this example, safe search is configured for Google in the inline CASB profile.

To configure an inline CASB profile with safe search in the GUI:

1. Configure the inline CASB profile:
   a. Go to *Security Profiles* > *Inline-CASB* and click *Create new*.
   b. Enter a *Name*, such as *google_test*.
   c. In the *SaaS Applications* table, click *Create new*. The *Create SaaS Application Rules* pane opens.
   d. Set the *Application* to *google*, then click *Next*.
   e. Enable *Safe search*.
   f. Click *OK*.
2. Configure the firewall policy:
   a. Go to *Policy & Objects* > *Policy*. Edit an existing policy, or create a new one.
   b. In the *Security Profiles* section, enable *Inline-CASB* and select the *google_test* profile.
   c. Set the *SSL Inspection* profile to one that uses deep inspection.
   d. Configure the other settings as needed.
   e. Click *OK*.

To configure an inline CASB profile with safe search in the CLI:

1. Configure the inline CASB profile:

```
config casb profile
    edit "google_test"
        config saas-application
            edit "google"
                set safe-search enable
                set safe-search-control "strict"
            next
        end
    next
end
```

2. Configure the firewall policy:

```
config firewall policy
    edit 7
        set name "casb_test_google"
        set srcintf "port1"
        set dstintf "port3"
```

```
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "ssl"
        set casb-profile "google_test"
        set nat enable
    next
end
```

To test the configuration:

1. Open a browser and attempt to search in Google for content that is considered mature or explicit.
2. The sensitive content is filtered out in the search results.

Sample log:

```
1: date=2023-08-18 time=17:01:36 eventtime=1692403295962385271 tz="-0700" logid="2500010002"
type="utm" subtype="casb" eventtype="casb" level="information" vd="vdom1" msg="CASB access was
monitored because it contained activity." policyid=7 sessionid=63774 srcip=10.1.100.195
dstip=142.250.217.98 srcport=61065 dstport=443 srcintf="port1" srcintfrole="undefined"
dstintf="port3" dstintfrole="undefined" proto=6 action="monitor" profile="google_test"
saasapp="google" useractivity="google-safe-search" activitycategory="safe-search-control"
```

Example 3: tenant control

In this example, tenant control is configured for Microsoft in the inline CASB profile for the fortinet-us.com domain.

To configure an inline CASB profile with tenant control in the GUI:

1. Configure the inline CASB profile:
   a. Go to *Security Profiles* > *Inline-CASB* and click *Create new*.
   b. Enter a *Name*, such as *microsoft_test*.
   c. In the *SaaS Applications* table, click *Create new*. The *Create SaaS Application Rules* pane opens.
   d. Set the *Application* to *microsoft*, then click *Next*.
   e. Enable *Tenant control*. Click the *+* and enter *fortinet-us.com*.
   f. Click *OK*.
2. Configure the firewall policy:
   a. Go to *Policy & Objects* > *Policy*. Edit an existing policy, or create a new one.
   b. In the *Security Profiles* section, enable *Inline-CASB* and select the *microsoft_test* profile.
   c. Set the *SSL Inspection* profile to one that uses deep inspection.

d. Configure the other settings as needed.
e. Click *OK*.

To configure an inline CASB profile with tenant control in the CLI:

1. Configure the inline CASB profile:

```
config casb profile
    edit "microsoft_test"
        config saas-application
            edit "microsoft"
                set tenant-control enable
                set tenant-control-tenants "fortinet-us.com"
            next
        end
    next
end
```

2. Configure the firewall policy:

```
config firewall policy
    edit 8
        set name "casb_test_microsoft"
        set srcintf "port1"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "ssl"
        set casb-profile "microsoft_test"
        set nat enable
    next
end
```

To test the configuration:

1. Open a browser and attempt to log in to Microsoft Office 365 with a fortinet-us.com account.
2. Since the domain is valid, the user can log in successfully.
3. Attempt to log in to Microsoft Office 365 with another account with a different domain.
4. The domain is invalid. The user is unable to log in, and an error message appears: *Your network administrator has blocked access*.

Sample log:

```
1: date=2023-08-18 time=17:09:25 eventtime=1692403765238967943 tz="-0700" logid="2500010002"
type="utm" subtype="casb" eventtype="casb" level="information" vd="vdom1" msg="CASB access was
monitored because it contained activity." policyid=8 sessionid=65108 srcip=10.1.100.195
```

```
dstip=20.189.173.15 srcport=61912 dstport=443 srcintf="port1" srcintfrole="undefined"
dstintf="port3" dstintfrole="undefined" proto=6 action="monitor" profile="microsoft_test"
saasapp="microsoft" useractivity="ms-tenant-control" activitycategory="tenant-control"
```

Example 4: UTM bypass

In this example, UTM bypass is configured for Dropbox file downloading in the inline CASB profile.

To configure an inline CASB profile with UTM bypass in the GUI:

1. Configure the inline CASB profile:
   a. Go to *Security Profiles* > *Inline-CASB* and click *Create new*.
   b. Enter a *Name*, such as *dropbox_test*.
   c. In the *SaaS Applications* table, click *Create new*. The *Create SaaS Application Rules* pane opens.
   d. Set the *Application* to *dropbox*, then click *Next*.
   e. Enable *Logging*.
   f. In the *Privilege Control* table, select *download-file* and from the *Set Action* dropdown, select *Bypass*.
   The *Bypass UTM Profile(s)* pane opens.
   g. Click the *+* and set *Profile(s)* to *File Filter*.
   h. Click *OK* to save the bypass UTM profile.
   i. Click *OK* to save the inline CASB profile
2. Configure the firewall policy:
   a. Go to *Policy & Objects* > *Policy*. Edit an existing policy, or create a new one.
   b. In the *Security Profiles* section, enable *Inline-CASB* and select the *dropbox_test* profile.
   c. Set the *SSL Inspection* profile to one that uses deep inspection.
   d. Configure the other settings as needed.
   e. Click *OK*.

To configure an inline CASB profile with UTM bypass in the CLI:

1. Configure the inline CASB profile:

```
config casb profile
    edit "dropbox_test"
        config saas-application
            edit "dropbox"
                config access-rule
                    edit "dropbox-download-file"
                        set bypass file-filter
                        set action bypass
                    next
                end
            next
```

```
        end
    next
end
```

2. Configure the firewall policy:

```
config firewall policy
    edit 9
        set name "casb_test_dropbox"
        set srcintf "port1"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "ssl"
        set casb-profile "dropbox_test"
        set nat enable
    next
end
```

To test the configuration:

1. Open a browser and log in to Dropbox.
2. Attempt to download a file, such as a PDF. The download is successful.

Sample log:

```
1: date=2023-08-18 time=17:15:29 eventtime=1692404129378193492 tz="-0700" logid="2500010001"
type="utm" subtype="casb" eventtype="casb" level="information" vd="vdom1" msg="CASB access was
allowed although it contained activity." policyid=9 sessionid=65452 srcip=10.1.100.195
dstip=162.125.1.15 srcport=62110 dstport=443 srcintf="port1" srcintfrole="undefined"
dstintf="port3" dstintfrole="undefined" proto=6 action="bypass" profile="dropbox_test"
saasapp="dropbox" useractivity="dropbox-download-file" activitycategory="activity-control"
```

Example 5: customized SaaS application and user activity

In this example, a custom SaaS application is created (pc4) with a custom user action. When a user accesses pc4.qa.fortinet.com/virus, they are redirected to pc4.qa.fortinet.com/testweb/testweb.htm.

To configure a customized inline CASB profile in the GUI:

1. Configure the inline CASB profile:
   a. Go to *Security Profiles* > *Inline-CASB* and click *Create new*.
   b. Enter a *Name*, such as *custom_test*.

c. In the *SaaS Applications* table, click *Create new*. The *Create SaaS Application Rules* pane opens.
d. In the *Application* dropdown, click the *+* to create a custom entry. The *Create Inline-CASB SaaS Application* pane opens.
e. Enter the *Name* (*pc4*) and *Domains* (*pc4.qa.fortinet.com*), then click *OK*.
f. Select *pc4* and click *Next*.
g. Configure the custom control and action:
   i. In the *Custom Controls* table, *Create new*. The *Create Custom Control* pane opens.
   ii. Enter a *Name*, such as *pc4-virus_test_replace*.
   iii. Set *Apply when HTTP packet matches* to *All of the following*.
   iv. Enable *URL path* and enter */virus*.
   v. In the *Application-Defined Controls* table, *Create new*. The *Create Custom Control Action* pane opens.
   vi. Enter a *Name*, such as *virus_replace_operation*.
   vii. Set the *Control Type* to *Edit URL path*.
   viii. Set the *Action* to *Replace path with value*.
   ix. Set the *Path* to */virus*.
   x. Set the *Value* to */testweb/testweb.html*.
   xi. Click *OK* to save the custom action.
   xii. Click *OK* to save the custom control.
h. Click *OK* to save the application rule.
i. Click *OK* to save the inline CASB profile.

2. Configure the firewall policy:
   a. Go to *Policy & Objects > Policy*. Edit an existing policy, or create a new one.
   b. In the *Security Profiles* section, enable *Inline-CASB* and select the *custom_test* profile.
   c. Set the *SSL Inspection* profile to one that uses deep inspection.
   d. Configure the other settings as needed.
   e. Click *OK*.

To configure a customized inline CASB profile in the CLI:

1. Configure the CASB SaaS application:

```
config casb saas-application
    edit "pc4"
        set domains "pc4.qa.fortinet.com"
    next
end
```

2. Configure the CASB user activity:

```
config casb user-activity
    edit "pc4-virus_test_replace"
        set application "pc4"
        set category other
        config match
```

```
            edit 1
                config rules
                    edit 1
                        set type path
                        set match-value "/virus"
                    next
                end
            next
        end
        config control-options
            edit "virus_replace_operation"
                config operations
                    edit "virus_replace_operation"
                        set target path
                        set action replace
                        set search-key "/virus"
                        set values "/testweb/testweb.html"
                    next
                end
            next
        end
    next
end
```

3. Configure the inline CASB profile:

```
config casb profile
    edit "custom_test"
        config saas-application
            edit "pc4"
                config custom-control
                    edit "pc4-virus_test_replace"
                        config option
                            edit "virus_replace_operation"
                            next
                        end
                    next
                end
            next
        end
    next
end
```

4. Configure the firewall policy:

```
config firewall policy
    edit 10
        set name "casb_test_custom"
        set srcintf "port1"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
```

```
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "ssl"
        set casb-profile "custom_test"
        set nat enable
    next
end
```

To test the configuration:

1. Open a browser and go to pc4.qa.fortinet.com/virus.
2. Access is redirected to pc4.qa.fortinet.com/testweb/testweb.htm.

Sample log:

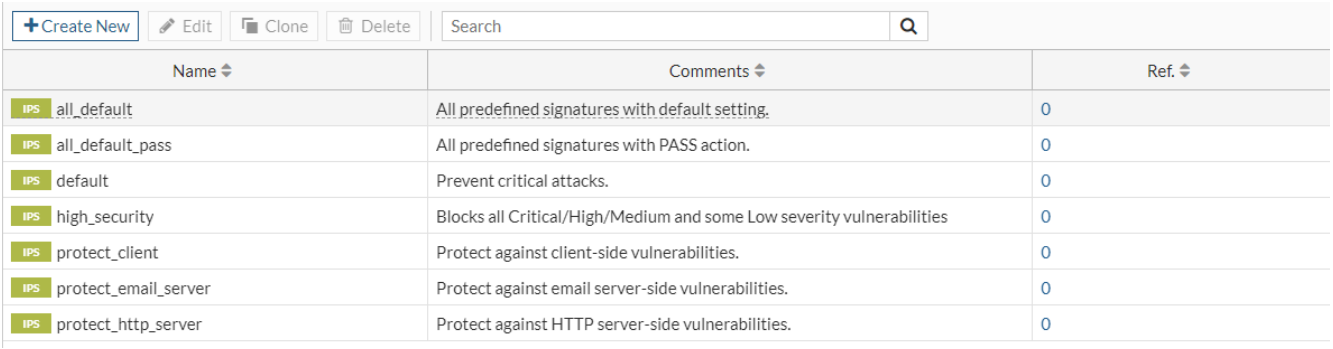
```
1: date=2023-08-21 time=08:31:06 eventtime=1692631866382806917 tz="-0700" logid="2500010001"
type="utm" subtype="casb" eventtype="casb" level="information" vd="vdom1" msg="CASB access was
allowed although it contained activity." policyid=10 sessionid=3139 srcip=10.1.100.195
dstip=172.16.200.44 srcport=56774 dstport=80 srcintf="port1" srcintfrole="undefined"
dstintf="port3" dstintfrole="undefined" proto=6
url="http://pc4.qa.fortinet.com/testweb/testweb.html" action="bypass" profile="custom_test"
saasapp="pc4" useractivity="pc4-virus_test_replace" activitycategory="other"
```

Intrusion Prevention

The Intrusion Prevention System (IPS) combines signature detection and prevention with low latency and excellent reliability. With intrusion protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to any security policy.

This section describes how to configure the Intrusion Prevention settings.

To view available IPS sensors, go to *Security Profiles* > *Intrusion Prevention*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

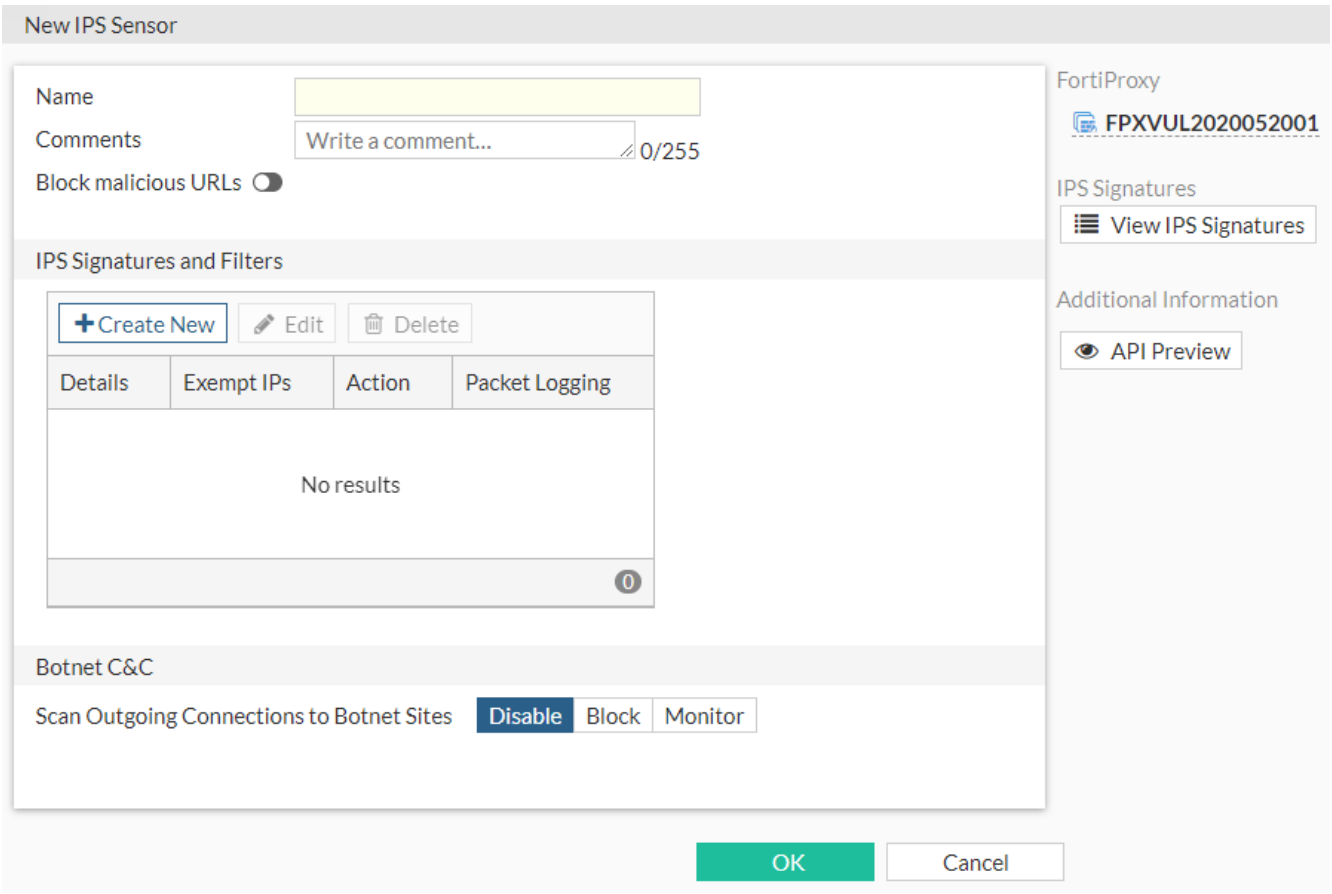
Create New	Create an IPS sensor. See Create or edit an IPS sensor on page 619.
Edit	Modify the selected IPS sensor. See Create or edit an IPS sensor on page 619.
Clone	Make a copy of the selected IPS sensor.
Delete	Remove the selected IPS sensor.
Search	Enter a search term to find in the IPS sensor list.
Name	The name of the IPS sensor.
Comments	An optional description of the IPS sensor.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an IPS sensor

The Intrusion Prevention System (IPS) combines signature detection and prevention with low latency and excellent reliability. With intrusion protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to any security policy.

IPS sensors can be added, edited, cloned, and deleted as required.

To create an IPS sensor, go to *Security Profiles* > *Intrusion Prevention* and click *Create New*.



Configure the following settings and then select *OK* to save your changes:

Name	The name of the IPS sensor.
Comments	Optional description of the IPS sensor.
Block malicious URLs	Enable this setting to block malicious URLs that FortiSandbox finds. Your FortiProxy unit must be connected to a registered FortiSandbox.
IPS Signatures and Filters	Add or edit an IPS signature or filter. See Add or edit an IPS signature or filter on page 621. While individual signatures can be added to a sensor, a filter allows you to add multiple signatures to a sensor by specifying the characteristics of the signatures to be added.
Scan Outgoing Connections to Botnet Sites	Select *Block* or *Monitor* to enable botnet blocking across all traffic that matches the policy.
View IPS Signatures	Select to see a list of predefined IPS signatures. To create an IPS signature, see Create or edit an IPS signature on page 649.

API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

To edit an IPS sensor:

1. From the IPS sensor list, select the sensor that you need to edit and then click *Edit* from the toolbar or double-click on the sensor name in the list. The *Edit IPS Sensor* window opens.
2. Edit the information as required and then select *OK* to save your changes.

Add or edit an IPS signature or filter

You can add or edit IPS signatures and filters.

To create a filter:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. In the *IPS Signatures and Filters* section, select *Create New*.
3. In the *Add Signatures* window, select *Filter*.
4. For the action, select *Allow*, *Monitor*, *Block*, *Reset*, *Default*, or *Quarantine*.
5. Enable or disable packet logging.
6. Enable the status to make the filter active.
7. Use the *Filter* field to select filters.
8. Use the search field to narrow down the list of possible signatures by a series of attributes.
9. Click *OK*.

To create a signature:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. In the *IPS Signatures and Filters* section, select *Create New*.
3. In the *Add Signatures* window, select *Signature*.
4. For the action, select *Allow*, *Monitor*, *Block*, *Reset*, *Default*, or *Quarantine*.
5. Enable or disable packet logging.
6. Enable the status to make the filter active.

7. Select *Default* or *Specify* for the rate-based settings. If you select *Specify*, enter the number of incidents per minute in the *Threshold* field, enter the number of seconds after which the block will be removed in the *Duration (seconds)* field, and select whether the rate-based settings use the source IP address, the destination IP address, or any IP address.
8. If you want to exempt certain IP addresses from the signature, click *Edit IP Exemptions* and add the source IP address and netmask and the destination IP address and netmask.
9. Use the search field to narrow down the list of possible signatures by a series of attributes.
10. Click *OK*.

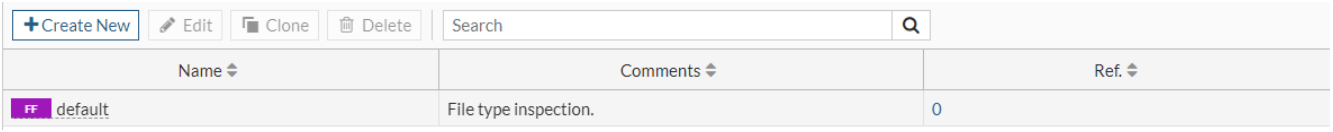
To edit a filter or signature:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. In the *IPS Filters* section, select the filter or signature that you want to edit and then click *Edit* from the toolbar.
3. Edit the information as required and then select *OK* to apply your changes.

File Filter

The file filter allows the FortiProxy unit to block files passing through based on file type based on the file's metadata only and not on file size or file content. A DLP sensor must be configured to block files based on size or content, such as SSN numbers, credit card numbers, or regular expression pattern. The file filter can be applied directly to firewall policies.

To view available file filter profiles, go to *Security Profiles* > *File Filter*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

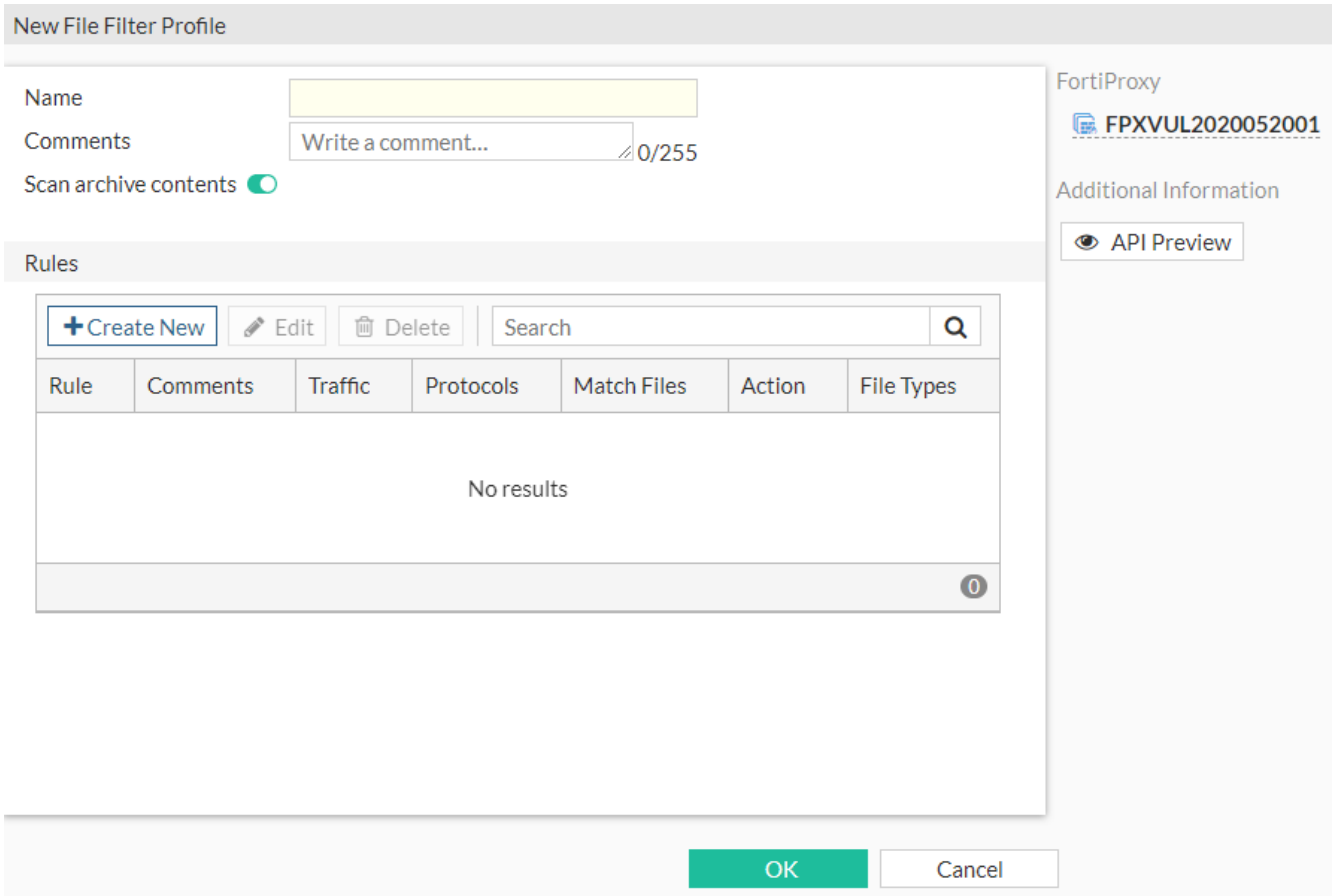
The following options are available:

Create New	Create a file filter profile. See Create or edit a file filter profile on page 623.
Edit	Modify the selected file filter profile. See Create or edit a file filter profile on page 623.
Clone	Make a copy of the selected file filter profile.
Delete	Remove the selected file filter profile.
Search	Enter a search term to find in the file filter profile list.
Name	The name of the file filter profile.

Comments	An optional description of the file filter profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.
Scan Archive Contents	Whether the scanning of archive contents has been enabled or disabled.

Create or edit a file filter profile

Click *Create New* to open the *New File Filter Profile* window.



Select a file filter profile and then click *Edit* to open the *Edit File Filter Profile* window.

Configure the following settings in the *New File Filter Profile* window and then click *OK*:

Name	The name of the file filter profile.
Comments	Optional description of the file filter profile.

Scan archive contents	Enable if you want the archive contents to be scanned.
Rules	Create or edit file filter rules. See Create or edit a file filter rule on page 624.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create or edit a file filter rule

You can create or edit rules for the file filter profile.

To create a file filter rule:

1. Go to *Security Profiles* > *File Filter*.
2. Click *Create New* or select a file filter profile and then click *Edit*.
3. In the *Rules* table, select *Create New*. The *Create New File Filter Rule* window opens.
4. Enter the name of the file filter rule.
5. Enter an optional description of the file filter rule.
6. Select one or more protocols.
7. Select *Incoming*, *Outgoing*, or *Both*.
8. Enable *Password-protected only* if you want to just match password-protected files.
9. Select the file types to match.
10. Select the action to take when the rule is matched:
    - *Block*: Block access to any file that matches the rule.
    - *Monitor*: Monitor traffic to and from files matching the rule.
11. Click *OK* to save the file filter rule.
12. Click *OK* to save the file filter profile.

To edit a file filter rule:

1. Go to *Security Profiles* > *File Filter*.
2. Click *Create New* or select a file filter profile and then click *Edit*.
3. In the *Rules* table, double-click on a rule or select the rule and then click *Edit* in the toolbar.

4. Edit the rule settings as required.
5. Click *OK* to save your changes to the file filter rule.
6. Click *OK* to save the file filter profile.

SSL/SSH Inspection

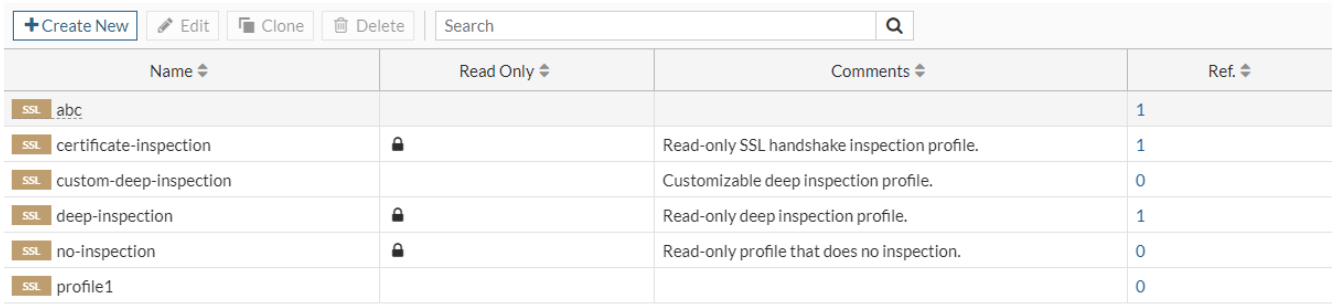
Secure sockets layer (SSL) content scanning and inspection allows you to apply antivirus scanning, web filtering, and email filtering to encrypted traffic. You can apply SSL inspection profiles to firewall policies.

Deep inspection (also known as SSL/SSH inspection) is typically applied to outbound policies where destinations are unknown. Depending on your policy requirements, you can configure the following:

- Which CA certificate will be used to decrypt the SSL encrypted traffic
- Which SSL protocols will be inspected
- Which ports will be associated with which SSL protocols for inspection
- Whether or not to allow invalid SSL certificates
- Whether or not SSH traffic will be inspected
- Which addresses or web category allowlists can bypass SSL inspection

SSL/SSH inspection profile

To view the available SSL/SSH inspection profiles, go to *Security Profiles* > *SSL/SSH Inspection*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an SSL/SSH inspection profile. See Create or edit an SSL/SSH inspection profile on page 626.
Edit	Modify the selected SSL/SSH inspection profile. See Create or edit an SSL/SSH inspection profile on page 626.

Clone	Make a copy of the selected SSL/SSH inspection profile.
Delete	Remove the selected SSL/SSH inspection profile.
Search	Enter a search term to find in the SSL/SSH inspection profile list.
Name	The name of the SSL/SSH inspection profile.
Read Only	The `certificate-inspection`, `deep-inspection`, and `no-inspection` profiles are read only and cannot be edited.
Comments	An optional description of the SSL/SSH inspection profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

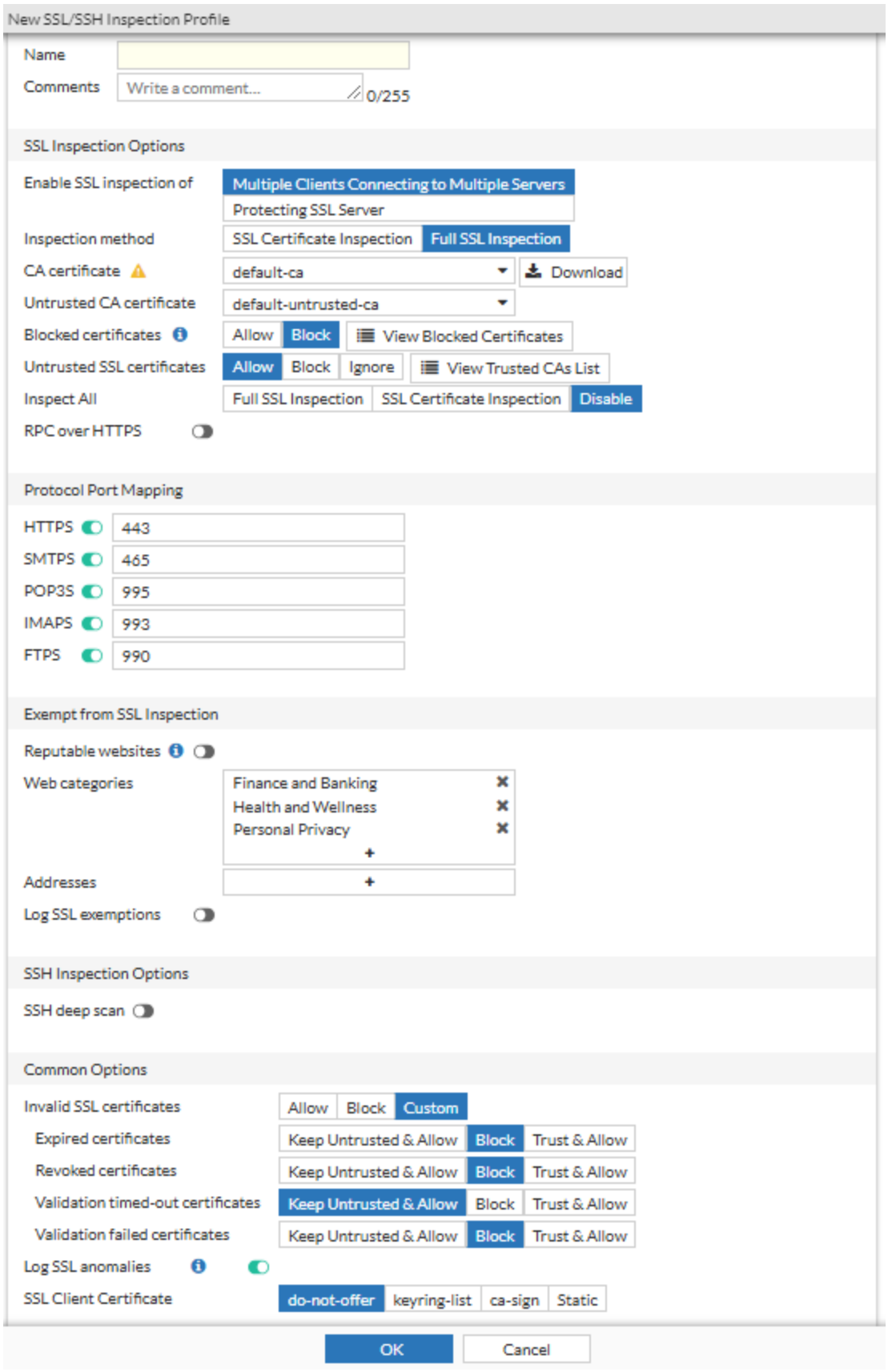
Create or edit an SSL/SSH inspection profile

The FortiProxy unit includes four preloaded SSL/SSH inspection profiles, three of which are read-only and can be cloned:

- `certificate-inspection`
- `deep-inspection`
- `no-inspection`

The `custom-deep-inspection` profile can be edited, or you can create your own SSL/SSH inspection profiles.

To create an SSL/SSH inspection profile, go to *Security Profiles* > *SSL/SSH Inspection* and click *Create New*.


New SSL/SSH Inspection Profile
Name
Comments
Write a comment...
0/255
SSL Inspection Options
Enable SSL inspection of
Multiple Clients Connecting to Multiple Servers
Protecting SSL Server
Inspection method
SSL Certificate Inspection
Full SSL Inspection
CA certificate
default-ca
Download
Untrusted CA certificate
default-untrusted-ca
Blocked certificates
Allow
Block
View Blocked Certificates
Untrusted SSL certificates
Allow
Block
Ignore
View Trusted CAs List
Inspect All
Full SSL Inspection
SSL Certificate Inspection
Disable
RPC over HTTPS
Protocol Port Mapping
HTTPS
443
SMTPS
465
POP3S
995
IMAPS
993
FTPS
990
Exempt from SSL Inspection
Reputable websites
Web categories
Finance and Banking
Health and Wellness
Personal Privacy
Addresses
Log SSL exemptions
SSH Inspection Options
SSH deep scan
Common Options
Invalid SSL certificates
Allow
Block
Custom
Expired certificates
Keep Untrusted & Allow
Block
Trust & Allow
Revoked certificates
Keep Untrusted & Allow
Block
Trust & Allow
Validation timed-out certificates
Keep Untrusted & Allow
Block
Trust & Allow
Validation failed certificates
Keep Untrusted & Allow
Block
Trust & Allow
Log SSL anomalies
SSL Client Certificate
do-not-offer
keyring-list
ca-sign
Static
OK
Cancel

Configure the following settings and then click *OK* to save your changes:

Name	Give the profile an easily identifiable name that references its intent.
Comments	Enter any additional information that might be needed by administrators, as a reminder of the profile's purpose and scope. This setting is optional.
SSL Inspection Options	
Enable SSL Inspection of	• *Multiple Clients Connecting to Multiple Servers*—Select this option for generic policies where the destination is unknown. This is normally used when inspecting outbound internet traffic. Other SSL Inspection Options become available to configure if this option is selected. • *Protecting SSL Server*—Select this option when setting up a profile customized for a specific SSL server with a specific certificate.
Server certificate	Click + and select a certificate or click *Create* to import a certificate. This option is available only when *Protecting SSL Server* is selected.
Inspection Method	Define the inspection method: • *SSL Certificate Inspection*—Only inspects the certificate, by way of the headers up to the SSL/TLS layer, and not the contents of the traffic. • *Full SSL Inspection*—Inspects the SSL/TLS encrypted traffic payload.
CA Certificate	Select a CA certificate from the drop-down menu or select *Download Certificate*.You need to have the certificate installed in your browser, or you might see certificate warnings.
Untrusted CA certificate	Select the CA certificate to use when a CA certificate is not issued by a trusted root CA server.
Blocked certificates	Block or allow potentially malicious certificates. The FortiProxy unit receives Botnet C&C SSL connections from FortiGuard that contain SHA1 fingerprints of malicious certificates. By default, these certificates are blocked. Click *View Blocked Certificates* for a detailed list of blocked certificates, including the listing reason and date.
Untrusted SSL certificates	Configure the action to take when a server certificate is not issued by a trusted CA. • *Allow*: Allow the untrusted server certificate. This is the default value. • *Block*: Block the session. • *Ignore*: This option is for Full SSL inspection only. It re-signs the server certificate as trusted. When configured in the GUI for certificate inspection, it has no effect, and the setting is not saved.

	Click *View Trusted CAs List* to see a list of the factory bundled and user imported CAs that are trusted by the FortiProxy unit.
RPC over HTTPS	Enable/disable inspection of Remote Procedure Calls (RPC) over HTTPS traffic. This option is available only if *Full SSL Inspection* is selected.
Protocol Port Mapping	To optimize the resources of the unit, enable or disable the mapping and inspection of protocols. The default port numbers are automatically filled in, but you can change them.
Encrypted Client Hello	Configure whether to block or allow TLS connections that use Encrypted Client Hello (ECH) in certificate inspection mode. This option is available only when *SSL Certificate Inspection* is selected. See Control TLS connections that utilize Encrypted Client Hello on page 635 for more information.
Exempt from SSL Inspection	These options are for *Full SSL inspection* only. Use the menus in this section to specify any reputable websites, FortiGuard Web Categories, or addresses that will be exempt from SSL inspection:
Reputable Websites	Enable this option to exempt any websites identified by FortiGuard as reputable. You can view the list of reputable websites under *System > Reputable Websites on page 967*.
Web Categories	By default, the categories of *Finance and Banking*, *Health and Wellness*, and *Personal Privacy* have been added because they are most likely to require a specific certificate. Click + to add web categories to be exempt from SSL inspection.
Addresses	Click + to add web addresses to be exempt from SSL inspection.
Log SSL exemptions	Enable this option to log all SSL exemptions.
SSH Inspection Options	
SSH Deep Scan	Enable to perform SSH deep scan and then enter the SSH port to use for the SSH deep scan.
Common Options	This section is available only when *Multiple Clients Connecting to Multiple Servers* is selected.
Invalid SSL Certificates	• Select *Allow* to allow traffic with invalid certificate. • Select *Block* to block traffic with an invalid certificate. • Select *Custom* to display more options.
Expired certificates	Select the action to take when the server certificate is expired. The default action is block. This option is available only when *Custom* is selected.
Revoked certificates	Select the action to take when the server certificate is revoked. The default action is block. This option is available only when *Custom* is selected.

Validation timed-out certificates	Select the action to take when the server certificate validation times out. For certificate inspection, the default action is *Allow*. For deep inspection, the default action is *Keep Untrusted & Allow*. This option is available only when *Custom* is selected.
Validation failed certificates	Select the action to take when the server certificate validation fails. The default action is block. This option is available only when *Custom* is selected.
Log SSL anomalies	Enable this feature to record and log traffic sessions containing invalid certificates. By default, SSL anomalies logging is enabled. Logs are generated in the UTM log type under the SSL subtype when invalid certificates are detected.
SSL Client Certificate	Configure SSL client certificate status.

Option	Description
do-not-offer	Do not offer SSL client certificate.
keyring-list	For authenticated users, offer matching SSL client certificate from keyring list.
ca-sign	For authenticated users, offer SSL client certificate signed by configured CA.
Static	Offer static SSL client certificate for mTLS authentication on behalf of all users. When this option is selected, you can further select the client certificate to use.

API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.



SSL options can be configured in SSL/SSH profiles even when the protocol is disabled.

HTTP/2 support in SSL inspection

Security profiles can perform SSL inspection on HTTP/2 traffic that is secured by TLS 1.2 or 1.3 using the Application-Layer Protocol Negotiation (ALPN) extension.

To set the ALPN support:

```
config firewall ssl-ssh-profile
   edit <profile>
      set supported-alpn {all | http1-1 | http2 | none}
   next
end
```

Multiple certificates can be defined in an SSL profile in replace mode

Multiple certificates can be defined in an SSL inspection profile in replace mode (*Protecting SSL Server*). This allows multiple sites to be deployed on the same protected server IP address, and inspection based on matching the SNI in the certificate.

When the FortiProxy unit receives the client and server hello messages, it will compare the SNI and CN with the certificate list in the SSL profile, and use the matched certificate as a replacement. If there is no matched server certificate in the list, the first server certificate in the list is used as a replacement.

To configure an SSL profile in replace mode with multiple certificates:

```
config firewall ssl-ssh-profile
    edit "multi-cert"
        set server-cert-mode replace
        set server-cert "bbb" "aaa"
    next
end
```

To configure a policy that uses the SSL profile:

```
config firewall policy
    edit 1
        set name "multi-cert"
        set srcintf "port6"
        set dstintf "port11"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "multi-cert"
        set av-profile "default"
```

```
        set webfilter-profile "default"
        set logtraffic all
    next
end
```

Results

If the Server Name Identification (SNI) matches the Common Name (CN) in the certificate list in the SSL profile, then the FortiProxy unit uses the matched server certificate.

If the Server Name Identification (SNI) does not match the Common Name (CN) in the certificate list in the SSL profile, then the FortiProxy unit uses the first server certificate in the list.

DNS inspection with DoT and DoH

DNS over TLS (DoT) and DNS over HTTPS (DoH) are supported in DNS inspection. The WAD is able to handle DoT and DoH and redirect DNS queries to the DNS proxy for further inspection.

To configure DNS inspection of DoT and DoH queries in the CLI:

1. Configure the SSL-SSH profile:

```
config firewall ssl-ssh-profile
    edit "ssl"
        config dot
            set status deep-inspection
            set client-certificate bypass
            set unsupported-ssl-version block
            set unsupported-ssl-cipher allow
            set unsupported-ssl-negotiation allow
            set expired-server-cert block
            set revoked-server-cert block
            set untrusted-server-cert allow
            set cert-validation-timeout allow
            set cert-validation-failure block
        end
    next
end
```

2. Configure the DNS filter profile:

```
config dnsfilter profile
    edit "dnsfilter"
        config ftgd-dns
            config filters
                edit 1
                    set category 30
                    set action block
                next
            end
```

```
        end
        set block-botnet enable
    next
end
```

3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port1"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "ssl"
        set webfilter-profile "webfilter"
        set dnsfilter-profile "dnsfilter"
    next
end
```

Client authentication with an SSL client certificate for the Original Content Server

FortiProxy can provide a client certificate for authentication to the Original Content Server on behalf of a user.

To use the SSL client certificate for server authentication:

- Set the client certificate to `inspect` under the `config https` command.
- Set the status of the SSL client certificate to `keyring-list` or `ca-sign`.
  - The `keyring-list` setting matches the user name to the Common Name of the SSL client certificate in the keyring list for authenticated users. See SSL Keyring on page 179.
  - The `ca-sign` setting provides an SSL client certificate signed by a configured CA for authenticated users. The signed client certificate has the Common Name set to the authenticated user's user name.

  By default, the status of the SSL client certificate is set to `do-not-offer`, which means that the SSL client certificate is not provided.

To provide an SSL client certificate from the keyring list:

```
config firewall ssl-ssh-profile
   edit <profile_name>
      config https
         set client-certificate inspect
      end
      config ssl-client-certificate
         set status keyring-list
```

```
        set keyring-list <keyring_list_used_to_find_client_certificate>
    end
  next
end
```

To provide an SSL client certificate signed by a CA:

```
config firewall ssl-ssh-profile
  edit <profile_name>
    config https
      set client-certificate inspect
    end
    config ssl-client-certificate
      set status ca-sign
      set caname <CA_certficate_used_to_sign_client_certificate>
    end
  next
end
```

Use the FortiProxy CLI to specify which keyring list to use for the SSL client certificate. The universally unique identifiers (UUIDs) are automatically assigned. See SSL Keyring on page 179 for information about uploading keyring lists.

To specify the keyring list to use for the SSL client certificate:

```
config firewall ssl keyring-list
  edit <keyring_list_used_to_find_client_certificate>
  next
end
```

Disable IP-based URL rating

You can disable IP-based URL rating for SSL-exemption and proxy-address objects. By default, IP -based URL rating is enabled.

To configure IP-based URL rating in an SSL/SSH inspection profile:

```
config firewall ssl-ssh-profile
    edit <name>
        set ssl-exemption-ip-rating {enable | disable}
    next
end
```

To configure IP-based URL rating in web proxy settings:

```
config firewall profile-protocol-options
    edit <protocol>
        config http
            set address-ip-rating {enable | disable}
        end
```

```
    next
end
```

Control TLS connections that utilize Encrypted Client Hello

TLS connections that use Encrypted Client Hello (ECH) can be blocked or allowed, and the client can be forced to switch to a non-ECH TLS connection by modifying the DNS over HTTPS (DoH) responses. This increases control and flexibility when managing TLS connections.

If the FortiProxy is performing deep inspection, it always strips the ECH extension from an ECH, effectively forcing the client browser to use a non-ECH TLS connection.

To configure ECH in the CLI:

```
config firewall ssl-ssh-profile
    edit <name>
        config https
            set status certificate-inspection
            set encrypted-client-hello {block | allow}
        end
        config ech-outer-sni
            edit <name>
                set sni <string>
            next
        end
    next
end
```

`encrypted-client-hello {block | allow}`	Block/allow session based on existence of encrypted-client-hello.
`ech-outer-sni`	ClientHelloOuter Server Name Indications (SNIs) to be blocked.
`sni <string>`	ClientHelloOuter SNI to be blocked.

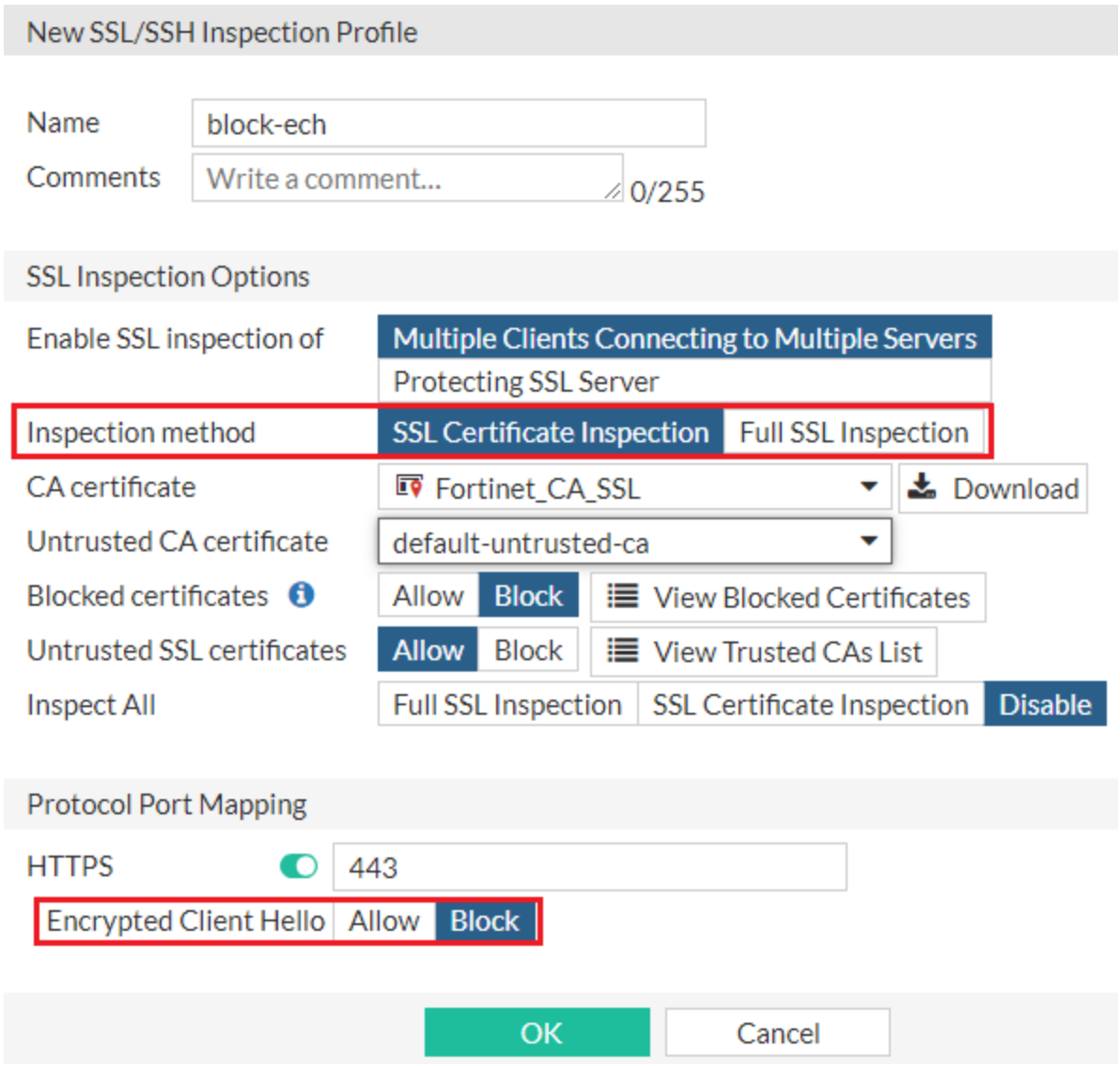
To configure stripping ECH information in the CLI:

```
config dnsfilter profile
    edit <name>
        set strip-ech {enable | disable}
    next
end
```

`strip-ech {enable | disable}`	Enable/disable removal of the ECH service parameter from supporting DNS RRs.

To configure ECH in the GUI:

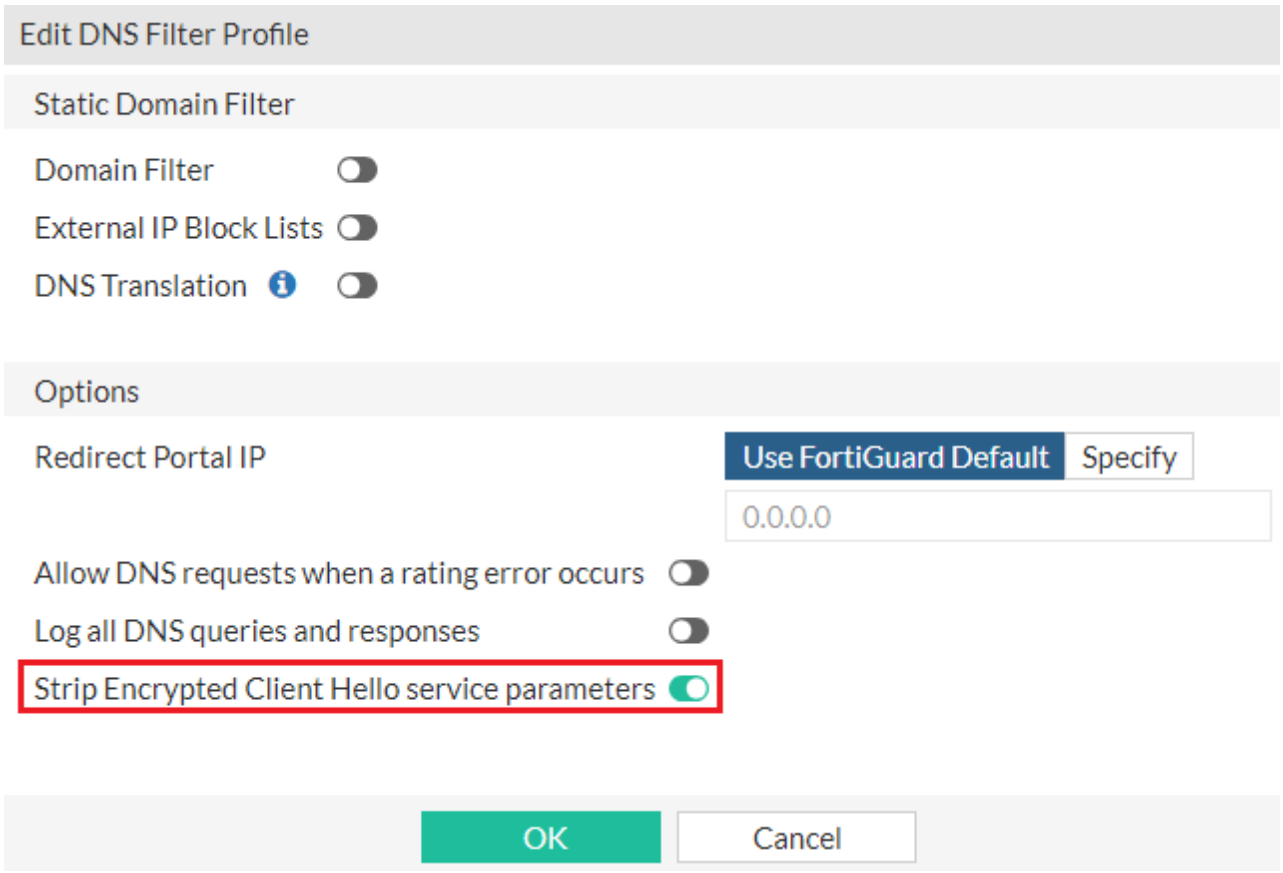
1. Go to *Security Profiles* > *SSL/SSH Inspection* and edit an existing profile or click *Create New*.
2. Set *Inspection method* to *SSL Certificate Inspection*.
3. Set *Encrypted Client Hello* to *Block*.



4. Click *OK*.
   SNIs cannot be configured in the GUI.

To configure stripping ECH information in the GUI:

1. Go to *Security Profiles* > *DNS Filter* and edit an existing profile or click *Create New*.
2. Enable *Strip Encrypted Client Hello service parameters*.



3. Click *OK*.

Blocking TLS connections with certificate inspection when ECH is used in the TLS handshake through the FortiProxy

In this example, an SSL/SSH inspection profile is configured to block TLS connections from some SNIs when ECH is used in the TLS handshake.

To configure blocking a TLS connection that uses ECH:

1. Configure an SSL/SSH inspection profile to block ECH and set the SNIs to match the outer SNI in the ECH message during the TLS handshake:

```
config firewall ssl-ssh-profile
    edit "block-ech"
        config https
            set status certificate-inspection
            set encrypted-client-hello block
        end
        config ech-outer-sni
            edit "cloudflare"
                set sni "cloudflare-ech.com"
            next
```

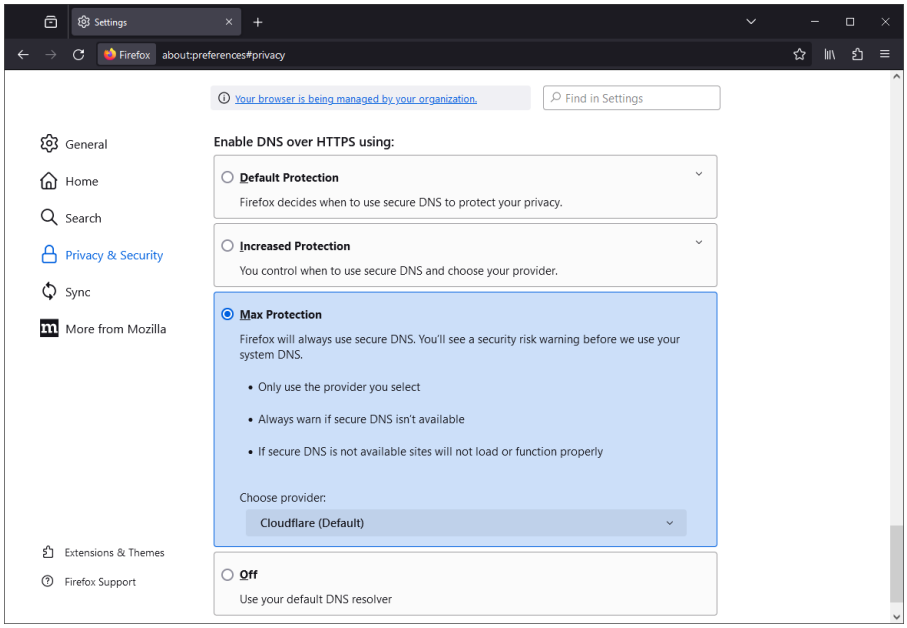
```
            edit "tls-ech"
                set sni "public.tls-ech.dev"
            next
            edit "defo.ie"
                set sni "cover.defo.ie"
            next
        end
    next
end
```

2. Apply the profile in a firewall policy:

```
config firewall policy
    edit 1
        set ssl-ssh-profile "block-ech"
    next
end
```

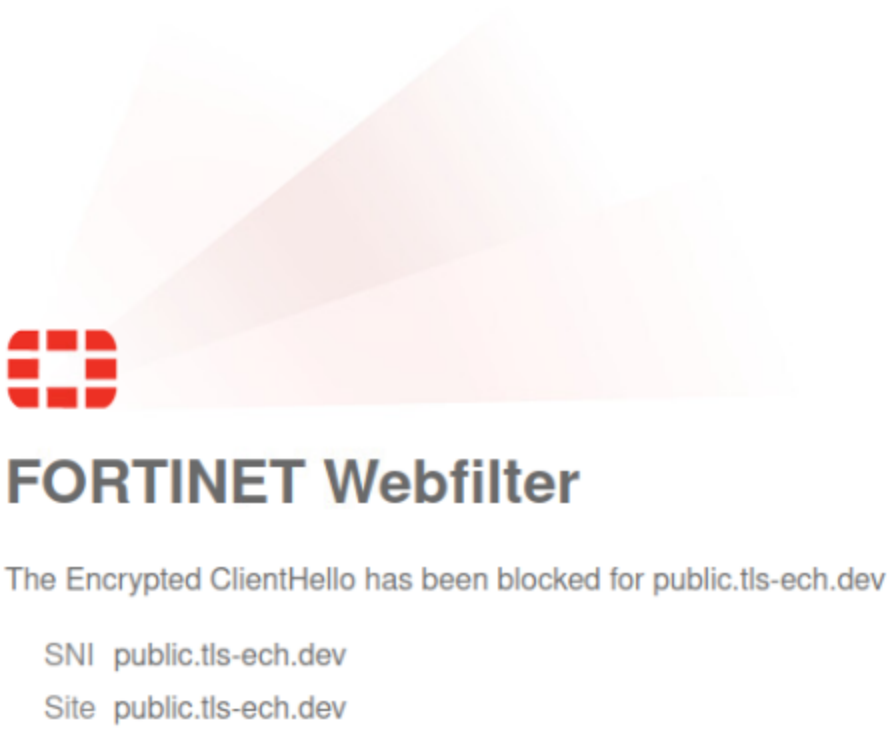
To check the results:

1. In a browser, enable DNS over HTTPS. For example, in Firefox go to *Settings* > *Privacy & Security* and under *DNS over HTTPS* enable *Max Protection*.



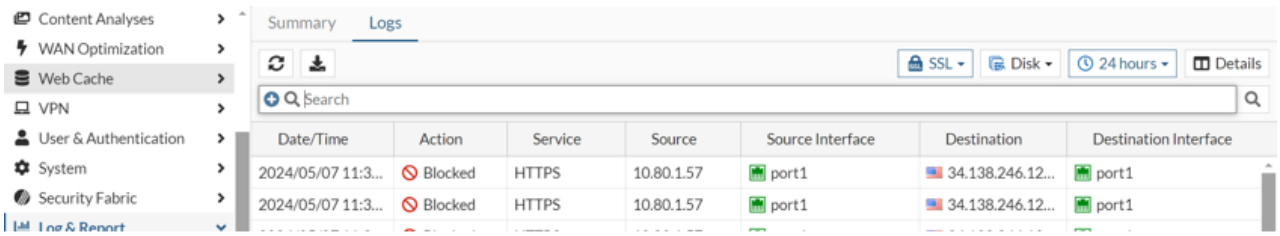
2. Visit a website, such as *https://public.tls-ech.dev*.

   Because ECH is blocked and the outer SNI matches one of the configured SNIs, the ECH initiated by the browser is blocked. In this case, the browser shows a replacement message:

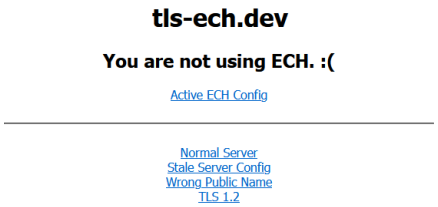


3. An SSL log shows the blocked connection:

```
1: date=2024-05-07 time=11:39:04 eventtime=1715107144327933775 tz="-0700" logid="1702062101"
type="utm" subtype="s
sl" eventtype="ssl-negotiation" level="warning" vd="root" action="blocked" policyid=1
poluuid="f6848eb2-dc73-51ec-
165d-e6fe7f98c611" policytype="policy" sessionid=1546437816 service="HTTPS" profile="block-
ech" srcip=10.80.1.57 s
rcport=33204 srccountry="Reserved" dstip=34.138.246.121 dstport=443 dstcountry="United States"
srcintf="port1" src
intfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6 eventsubtype="encrypted-
client-hello" hostnam
e="public.tls-ech.dev" msg="SSL connection is blocked."
```



4. Try to visit a different website, such as *tls-ech.dev*, that does not match a default SNI to be blocked. The browser will initial try to establish an ECH-enabled TLS connection to *public.tls-ech.dev*, but that will be blocked, forcing the browser to connect to the actual website without ECH and, in this case, the browser will load the actual website and not the replacement message:

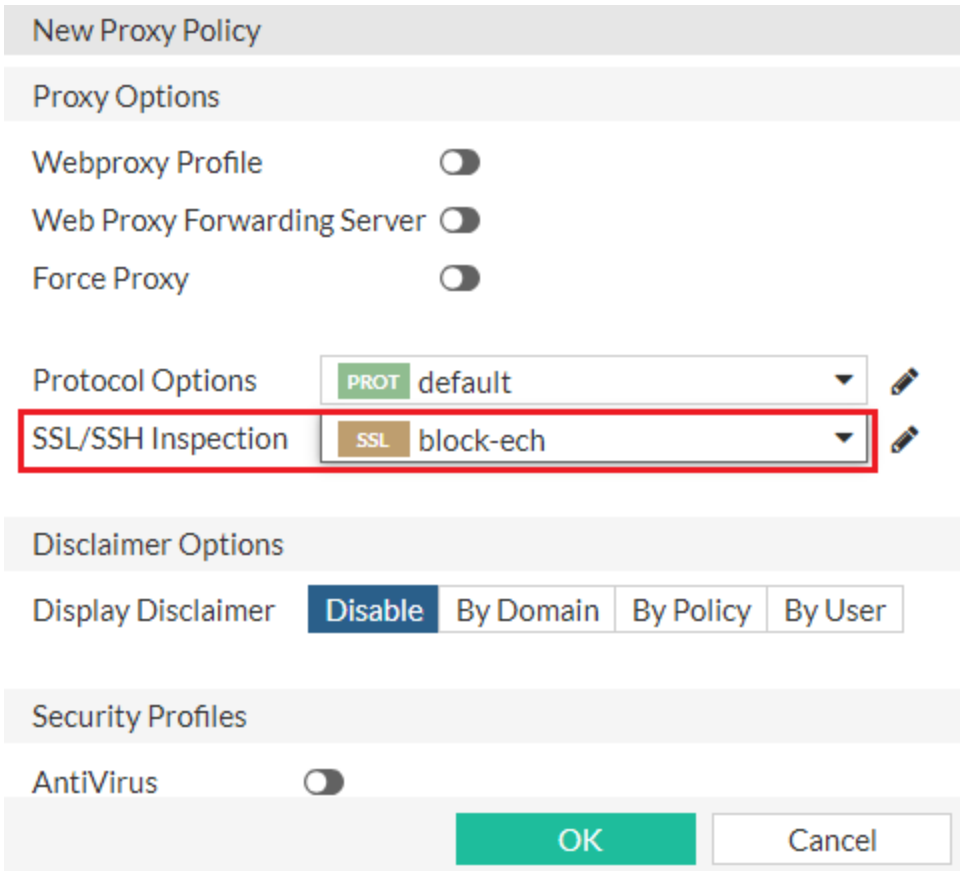


Allowing TLS connections with certificate inspection when ECH is used in the TLS handshake through the FortiGate

In this example, an SSL/SSH inspection profile is configured to allow TLS connections when ECH is used in the TLS handshake.

To configure allowing a TLS connection that uses ECH in the GUI:

1. Go to *Security Profiles* > *SSL/SSH Inspection* and edit an existing profile or click *Create New*.
2. Set *Inspection method* to *SSL Certificate Inspection*.
3. Set *Encrypted Client Hello* to *Allow*.
4. Click *OK*.
5. Go to *Policy & Objects* > *Policy* and edit an existing policy or click *Create New*.
6. Set *SSL inspection* to the SSL/SSH Inspection profile.



7. Click *OK*.

To configure allowing a TLS connection that uses ECH in the CLI:

1. Configure an SSL/SSH inspection profile to block ECH and set the SNIs to match the outer SNI in the ECH message during the TLS handshake:

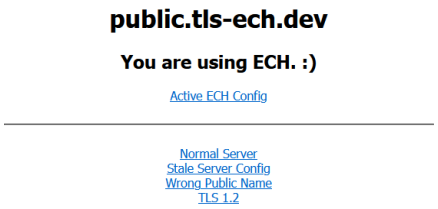
```
config firewall ssl-ssh-profile
    edit "allow-ech"
        config https
            set status certificate-inspection
            set encrypted-client-hello allow
        end
    next
end
```

2. Apply the profile in a firewall policy:

```
config firewall policy
    edit 1
        set ssl-ssh-profile "allow-ech"
    next
end
```

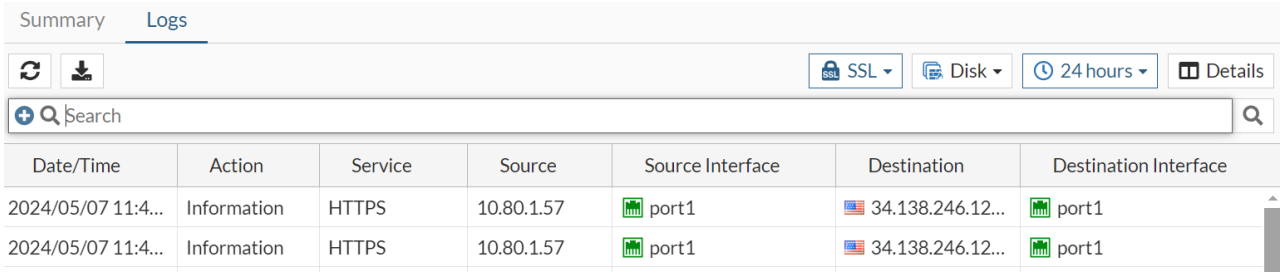
To check the results:

1. In a browser, enable DNS over HTTPS. For example, in Firefox go to *Settings* > *Privacy & Security* and under *DNS over HTTPS* enable *Max Protection*.
2. Visit a website, such as *https://public.tls-ech.dev*.
   The ECH-enabled TLS connection is allowed through the firewall policy and the website opens:



3. An SSL log shows the allowed connection:

```
5: date=2024-05-07 time=11:36:43 eventtime=1715107003423643625 tz="-0700" logid="1702062103"
type="utm" subtype="s
sl" eventtype="ssl-negotiation" level="information" vd="root" action="info" policyid=1
poluuid="f6848eb2-dc73-51ec
-165d-e6fe7f98c611" policytype="policy" sessionid=1546437808 service="HTTPS" profile="allow-
ech" srcip=10.80.1.57
srcport=34902 srccountry="Reserved" dstip=34.138.246.121 dstport=443 dstcountry="United
States" srcintf="port1" sr
cintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6 eventsubtype="encrypted-
client-hello" hostna
me="public.tls-ech.dev"
```



Stripping ECH information from DoH responses

DNS filters are used to strip ECH information from DoH responses, and force the browser to not use ECH for TLS connections. The browser relies on the ECH information from DoH for ECH-enabled TLS connections.

In this example, policy 3 performs deep inspection on DoH traffic between the browser and the DoH server (mozilla.cloudflare-dns.com). A DNS filter profile is applied that strips the ECH information from the DoH response, forcing the browser to use a non-ECH TLS connection. The browser then establishes a TLS connection through policy 1. Although policy 1 has an SSL/SSH inspection profile applied that allows ECH, ECH is not used because the ECH information from the DoH response was stripped by policy 3.

To configure and test stripping ECH information from DoH responses:

1. Configure the DNS filter profile that removes the ECH information:

```
config dnsfilter profile
    edit "strip-ech-enable"
        set strip-ech enable
    next
end
```

2. Configure a firewall address:

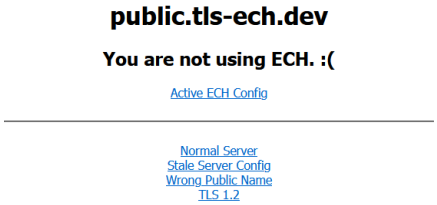
```
config firewall address
    edit "mozilla.cloudflare-dns.com"
        set type fqdn
        set fqdn "mozilla.cloudflare-dns.com."
    next
end
```

3. Configure the policies:

```
config firewall policy
    edit 3
        set uuid f6848eb2-dc73-51ec-165d-e6fe7f98c611
        set srcintf "any"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "mozilla.cloudflare-dns.com"
        set action accept
```

```
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set logtraffic all
        set log-http-transaction all
        set extended-log enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "default"
        set dnsfilter-profile "strip-ech-enable"
    next
    edit 1
        set uuid 0dae0342-e058-51ec-3eef-00878727409c
        set srcintf "any"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set logtraffic all
        set log-http-transaction all
        set extended-log enable
        set ssl-ssh-profile "allow-ech"
        set av-profile "default"
    next
end
```

4. In a browser, go to *https://public.tls-ech.dev* to see that ECH is not being used:

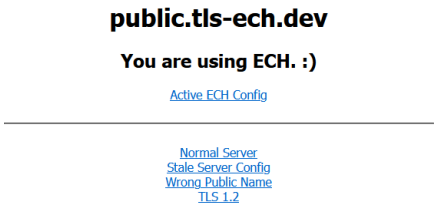


5. The debug log will show that the ECH service parameter was removed:

```
# diagnose debug application dnsproxy -1
...
[worker 0] dns_secure_filter_ech()-2166: Found ECH key=5
...
[worker 0] dns_secure_filter_ech()-2203: Removed ECH service parameter
```

6. If the DNS filter profile is changed to disable stripping the ECH information, then the website will show that ECH is being used:

```
config dnsfilter profile
    edit "strip-ech-enable"
        set strip-ech disable
    next
end
```



Application Signatures

The FortiProxy predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.

You can create custom IPS signatures and custom application signatures to further extend protection. For example, you can use custom IPS signatures to protect unusual or specialized applications or even custom platforms from known and unknown attacks.

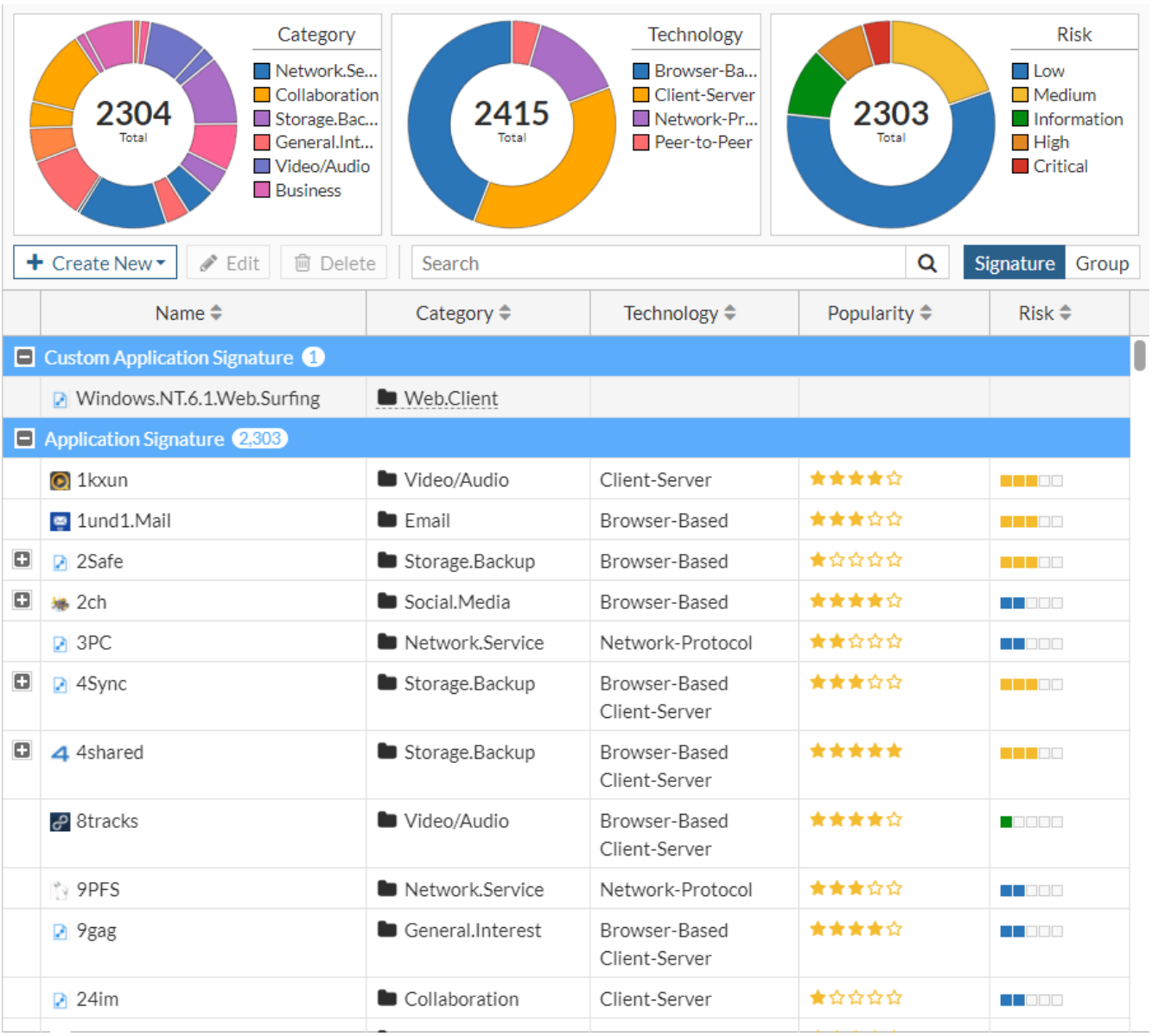
All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.

A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [( )]. The keyword and value pairs are separated by a semicolon (;) and consist of a keyword and a value separated by a space. The following is the basic format of a definition:

```
HEADER (KEYWORD VALUE;)
```

You can use as many keyword/value pairs as required within the 512-character limit.

To view the available custom application signatures, go to *Security Profiles > Application Signatures* and click *Signature*. Custom application signatures are listed under a separate heading in the table. To create a custom application signature, see Create or edit an application signature on page 645.



To view the available custom application groups, go to *Security Profiles* > *Application Signatures* and click *Group*.To create a custom application group, see Create or edit an application group on page 646.

Create or edit an application signature

If you have to detect an application that is not already in the application list, you can create an application signature:

1. Go to *Security Profiles* > *Application Signatures* and select *Create New* > *Custom Application Signature*. You can also go to *Security Profiles* > *Application Control*, click *Create New*, click *View Application Signatures*, and select *Create New* > *Custom Application Signature*.
2. Enter a name (no spaces) for the application signature in the *Name* field.

3. Enter a brief description in the *Comments* field.
4. Enter the text for the signature in the *Signature* field. The syntax for signatures is described in Valid syntax on page 646.
5. Click *OK*.

You can edit application signatures that you have created. Select the application signature and then click *Edit*.

Valid syntax

The following table shows the valid characters and basic structure. For details about each keyword and its associated values, see Custom signature keywords on page 1175.

Field	Valid Characters	Usage
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.
KEYWORD	Each keyword must start with a pair of dashes (--) and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword identifies a parameter.
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. **NOTE:** If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.

Create or edit an application group

When creating an application group, you can now define the application group by protocols, risk, vendor, technology, behavior, popularity, and category.

To create an application group in the CLI:

```
config application group
   edit <name>
      set comment <string>
      set type {application | filter}
      set application <application_ID>
      set category <2 | 3 | 5-8 | 12 | 15 | 17 | 21-23 | 25 | 26 | 28-32>
      set risk <1-5>
```

```
      set protocols <0-47 | all>
      set vendor <0-25 | all>
      set technology <all | 0-4>
      set behavior <all | 2 | 5 | 6 | 9>
      set popularity <1-6>
   next
end
```

To create an application group:

1. Go to *Security Profiles* > *Application Signatures*.
2. Select *Create New* > *Application Group*.
3. Enter a group name.
4. Select the group type, either *Application* or *Filter*.
5. Click + to add members to the group.
6. Enter an optional description of the group.
7. Click *OK*.

To edit an application group:

1. Go to *Security Profiles* > *Application Signatures*.
2. Select *Group*.
3. Select a group name and click *Edit*.
4. Make your changes.
5. Click *OK*.

IPS Signatures

The FortiProxy predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.

You can create custom IPS signatures and custom application signatures to further extend protection. For example, you can use custom IPS signatures to protect unusual or specialized applications or even custom platforms from known and unknown attacks.

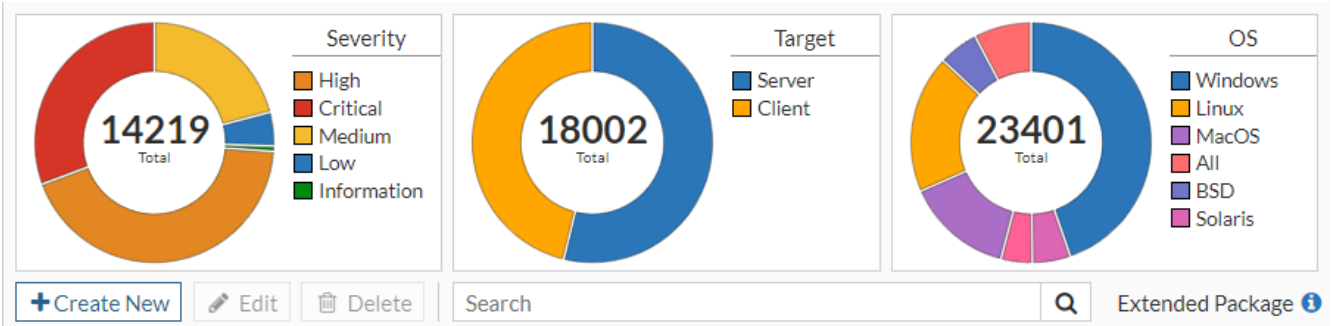
All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.

A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [( )]. The keyword and value pairs are separated by a semicolon (;) and consist of a keyword and a value separated by a space. The following is the basic format of a definition:

```
HEADER (KEYWORD VALUE;)
```

You can use as many keyword/value pairs as required within the 512-character limit.

To view the available custom IPS signatures, go to *Security Profiles* > *IPS Signatures*. Custom IPS signatures are listed under a separate heading inthe table.



+Create New | Edit | Delete | Search | Extended Package

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 14,219					
2Wire.Wireless.Router.XSRF.Password...		Server Client	Linux	Block	CVE-2007-4387
3CX.Phone.System.VAD_Deploy.Arbitr...		Server	Windows	Block	
3Com.3CDaemon.FTP.Server.Buffer.O...		Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Informati...		Client	Windows	Block	CVE-2005-0278
3Com.Intelligent.Management.Center.I...		Server	Windows	Block	
3Com.OfficeConnect.ADSL.Wireless.Fi...		Server	Linux	Block	
3Com.OfficeConnect.Utility.CGI.Remo...		Server	Linux	Block	
3D.Life.Player.WebPlayer.ActiveX.Cont...		Client	Windows	Block	
3S-Pocketnet.VMS.ActiveX.Control.Bu...		Client	Windows	Block	CVE-2014-9263
3ivx.MPEG4.File.Processing.Buffer.Ov...		Client	Windows	Block	CVE-2007-6401
4D.WebStar.FTP.Command.Buffer.Ove...		Server	Windows	Block	CVE-2004-0695
4D.WebStar.Tomcat.Plugin.Remote.Buf...		Server	Windows	Block	CVE-2005-1507
7-Zip.RAR.Solid.Compression.Remote....		Server Client	Windows	Block	CVE-2018-10115
74CMS.Config.Controller.Remote.Cod...		Server	Windows Linux	Block	CVE-2019-10684

To create a custom IPS signature, see Create or edit an IPS signature on page 649.

Highlight of on-hold IPS signatures

IPS signatures that are on hold (administrator-added delay for activation time) are highlighted in the GUI as follows:

- On-hold signatures are grayed out with an hourglass icon beside the signature name.
- The signature tooltip displays the on hold expiry time.

- Users can still use on-hold signatures in an IPS sensor profile; however, the profile will not block matching traffic. It will monitor it instead (logging in effect) until the on hold time expires.

After a hold time is configured in the CLI, go to *Security Profiles > IPS Signatures*. Hover over the grayed-out entry to view the tooltip, which includes the action and hold time expiry.

The same tooltip is available on the *Edit IPS Sensor* (*Security Profiles > Intrusion Prevention*) page when creating or editing the IPS signatures. In the *Add Signatures* pane when the *Type* is *Signature*, on-hold signatures are only displayed as on hold if `override-signature-hold-by-id` is enabled.

Create or edit an IPS signature

You can create an IPS signature.

To create an IPS signature:

1. Go to *Security Profiles > IPS Signatures* and click *Create New*. You can also go to *Security Profiles > Intrusion Prevention*, click *Create New*, click *View IPS Signatures*, and click *Create New*.
2. Enter a name (no spaces) for the IPS signature in the *Name* field.
3. Enter a brief description in the *Comments* field
4. Enter the text for the signature in the *Signature* field. The syntax for signatures is described in Valid syntax on page 649.
5. Click *OK*.

You can also edit IPS signatures that you have created. Select the IPS signature and then click *Edit*.

Valid syntax

The following table shows the valid characters and basic structure. For details about each keyword and its associated values, see Custom signature keywords on page 1175.

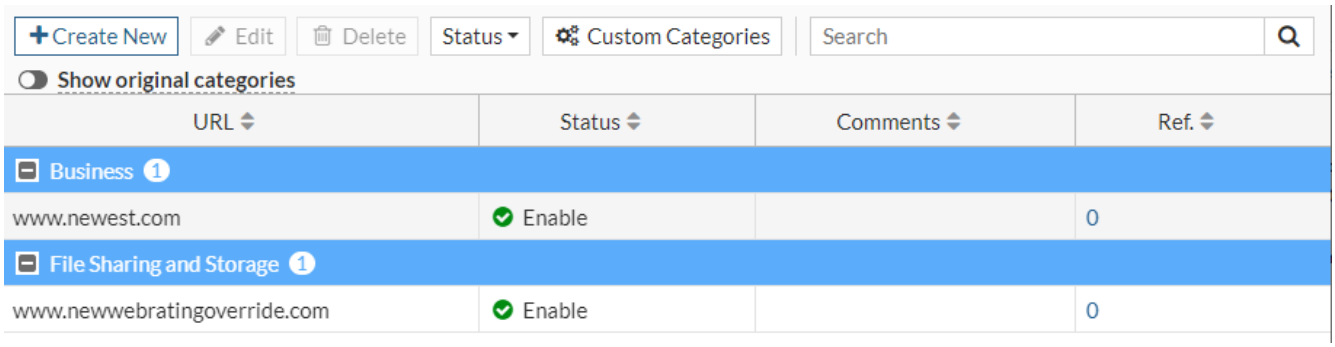
Field	Valid Characters	Usage
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.
KEYWORD	Each keyword must start with a pair of dashes (--) and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword identifies a parameter.
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive.	The value is set specifically for a parameter identified by a keyword.

Field	Valid Characters	Usage
	NOTE: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	

Web Rating Overrides

This feature allows you to override the FortiGuard web filtering. You can change the rating for a web site and control access to the site without affecting the rest of the sites in the original category.

To override the FortiGuard web rating, go to *Security Profiles* > *Web Rating Overrides*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

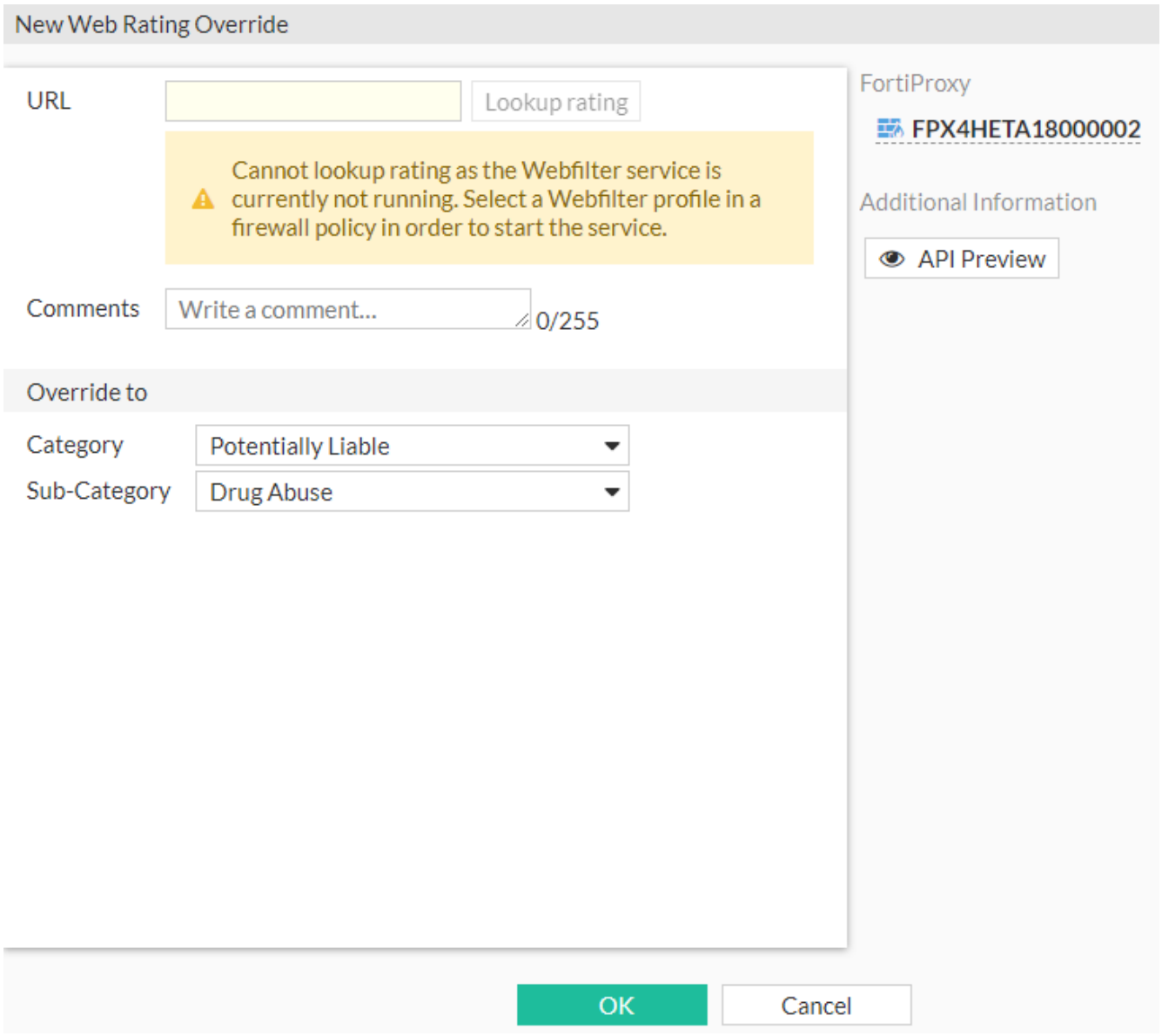
The following options are available:

Create New	Create a web rating override. See Create or edit a web rating override on page 651.
Edit	Modify the selected web rating override. See Create or edit a web rating override on page 651.
Delete	Remove the selected web rating override.
Status	Select *Enable* or *Disable* to make the override active or inactive.
Custom Categories	Select to create a custom category for groups of URLs. See Create or edit a custom category on page 653.
Search	Enter a search term to find in the web rating override list.
Show original categories	Enable to add the *Original Category* column, which shows the categories that are being overridden.
URL	The URL of a web site.
Status	Whether the override is enabled or disabled.

Comments	An optional description of the web rating override
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.
Override Category	The new category for the web site.
Original Category	The category that the web site originally belonged to.

Create or edit a web rating override

Click *Create New* to open the *New Web Rating Override* window.



To open the *Edit Web Rating Override* window, select a web rating override from the list and then click *Edit*.

Configure the following settings and then click *OK* to save your changes:

URL	Enter the URL of a website.
Lookup Rating	Click to find the FortiGuard rating if it exists for the URL you entered.
Comments	Enter an optional description of the web rating override.
Category	Select the new category for the website.
Sub-Category	Select a more narrowly defined option within the category that you selected for the website.
API Preview	The API Preview allows you to view all REST API requests being used

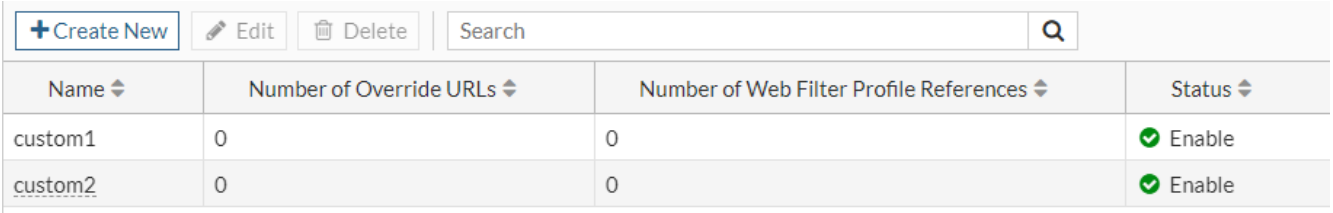
by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Create or edit a custom category

Click *Custom Categories* to open the *Custom Categories* window.



To create a category for a group of web sites:

1. Go to *Security Profiles* > *Web Rating Overrides*.
2. Click *Custom Categories*. The *Custom Categories* window opens.
3. Click *Create New*.
4. Enter the name of the custom category.
5. Click *Enable* to make the custom category active.
6. Click *OK*.

To use the new category, select the *Custom Categories* category in the *New Web Rating Override* window or the *Edit Web Rating Override* window. The new categories are listed in the *Sub-Category* drop-down menu.

To edit a custom category, select a category from the list and then click *Edit*.

Web Risk Overrides

You can use risk level as a parameter for policy matching and web filtering. The policy or web filter action applies when the risk score of the URL is within the score range of the specified risk level (see

Web Filter Risk Level on page 659). FortiProxy provides the following predefined risk levels (read-only):

Risk level	Score range	Description
high	91-100	Strong confidence of malicious intent.
suspicious	71-90	Medium confidence of malicious intent.
moderate	51-70	Generally benign with a potential risk of attack.
low	21-50	Low predictive risk of attack.
trustworthy	1-20	Very low predictive risk of attack.
unrated	0	The URL does not exist in FortiGuard DB or the risk score of the URL is unknown.

To define the risk score of a website in the GUI:

1. Go to *Security Profiles* > *Web Risk Overrides*.
2. Click *Create New* or select an existing entry and click *Edit*.
3. specify the URL of the website.
4. Specify a desired risk score for the website.
5. Click *OK*.

To define the risk score of a specific website in the CLI:

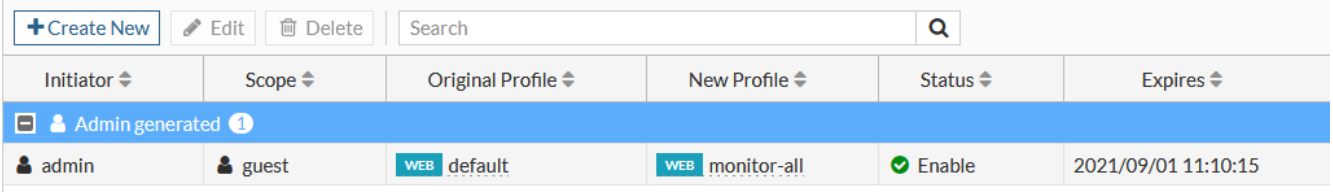
```
config webfilter ftgd-local-risk
   edit "www.ubc.ca"
      set risk-score 22
   next
end
```

Web Profile Overrides

Administrators can grant temporary access to sites that are otherwise blocked by a web filter profile. You can grant temporary access to a user, user group, or source IP address. You can set the time limit by selecting a date and time. The default is 15 minutes.

When the administrative web profile override is enabled, a blocked access page or replacement message does not appear, and authentication is not required.

To override the web filter profile, go to *Security Profiles* > *Web Profile Overrides*.



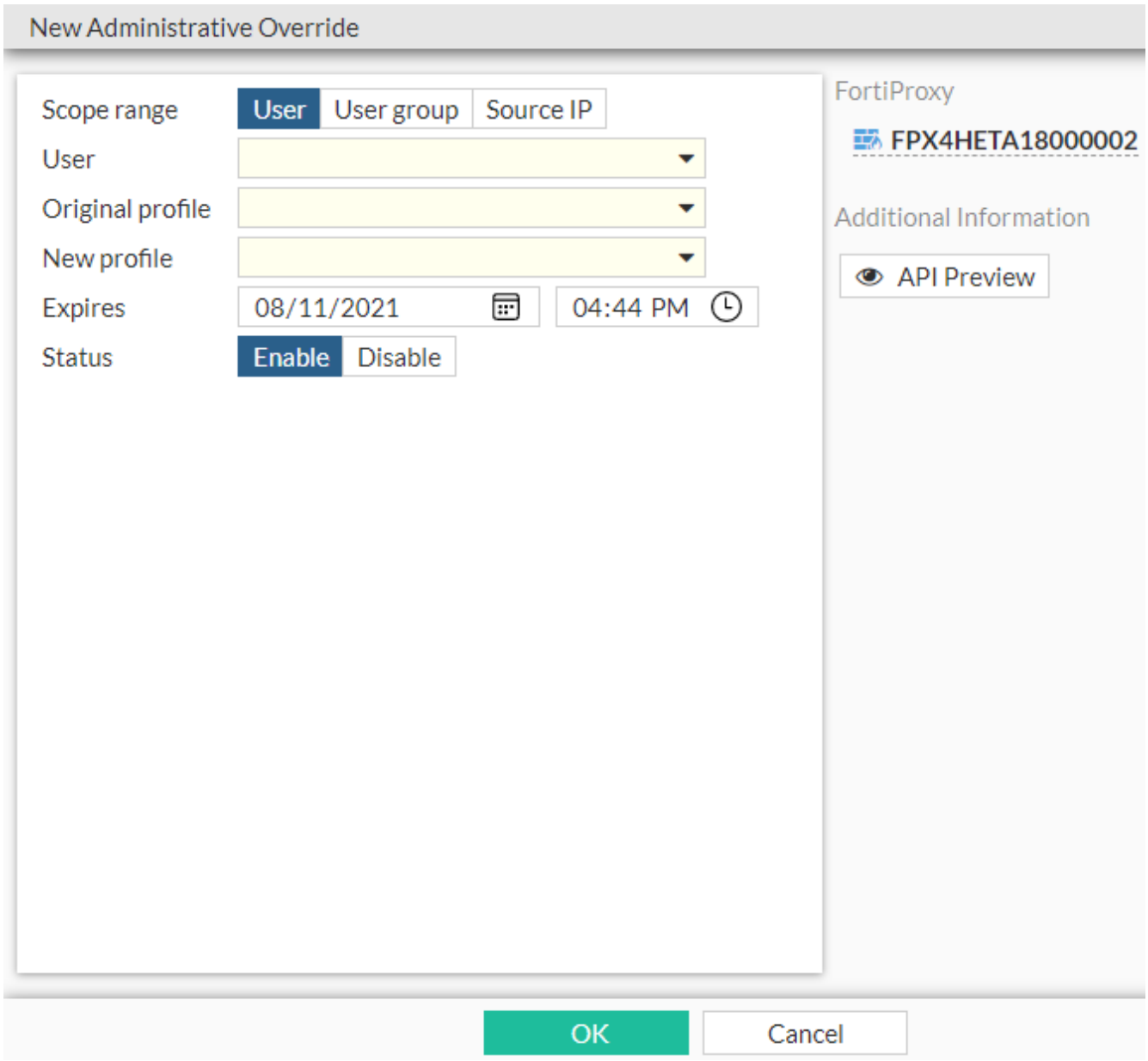
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a web profile override. See Create or edit a web profile override on page 655.
Edit	Modify the selected web profile override. See Create or edit a web profile override on page 655.
Delete	Remove the selected web profile override.
Search	Enter a search term to find in the web profile override list.
Initiator	The user who created the web profile override.
Scope	The scope is a user, a user group, or a source IP address.
Original Profile	The web filter profile that is being overridden.
New Profile	The web filter profile that is overriding the original web filter profile.
Status	Whether the override is enabled or disabled.
Expires	The day and time when the override ends.

Create or edit a web profile override

Click *Create New* to open the *New Administrative Override* window.



To open the *Edit Administrative Override* window, select a web profile override from the list and then click *Edit*.

Configure the following settings and then click *OK* to save your changes:

Scope range	Select one of the following scope ranges: • *User*: Authentication for permission to override is based on whether or not the user is using a specific user account. • *User group*: Authentication for permission to override is based on whether or not the user account supplied as a credential is a member of the specified user group. • *Source IP*: Authentication for permission to override is based on the IP address of the computer that was used to authenticate.

	This would be used for computers that have multiple users. For example, if a user logs on to the computer, engages the override by using their credentials, and then logs off, anyone who logs on with an account on that computer would be using the alternate override web filter profile.
User	If you selected *User* for the scope range, select or create the user. See Creating or editing a user on page 798.
User group	If you selected *User group* for the scope range, select or create the user group. See Create or edit a user group on page 809.
Source IP	If you selected *Source IP* for the scope range, enter the source IP address.
Original profile	Select or create a web filter profile to override. See Create or edit a web filter profile on page 566.
New profile	Select or create a web filter profile that will override the original web filter profile. See Create or edit a web filter profile on page 566.
Expires	Select the date and time when the override ends.
Status	Enable to make the override active.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.
References	Click to open the object usage page to show which other configuration are referencing the object.
Edit in CLI	Click to open a CLI console window to view and edit the setting in the CLI. If there are multiple CLI settings on the page, the CLI console shows the first setting.

To use the API Preview:

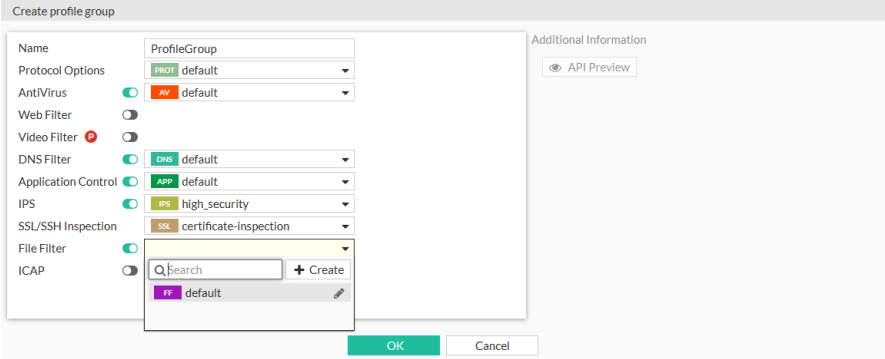
1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Profile Groups

Profile groups are used to group security profiles of different types together, and can be used in policies instead of individual profiles.

To create a profile group in the GUI:

1. Go to *Security Profiles* > *Profile Groups* and click *Create New*.
2. Enter a name for the group.
3. Select the *Protocol Options* from the drop-down list.
4. Enable the required profile types and select a profile for each.



5. Click *OK*.

To create a profile group in the CLI:

```
config firewall profile-group
    edit <name>
        set profile-protocol-options <options>
        set ssl-ssh-profile {certificate-inspection | custom-deep-inspection | deep-inspection |
no-inspection}
        set av-profile <profile>
        set ia-profile <profile>
        set webfilter-profile <profile>
        set dnsfilter-profile <profile>
        set emailfilter-profile <profile>
        set dlp-sensor <sensor>
        set file-filter-profile <profile>
        set ips-sensor <sensor>
        set application-list <list>
        set icap-profile <profile>
        set cifs-profile <profile>
        set videofilter-profile <profile>
        set ssh-filter-profile <profile>
    next
end
```

To use a profile group in a policy:

```
config firewall policy
    edit <policy>
        set profile-type group
        set profile-group <group>
    next
end
```

Web Filter Risk Level

You can use risk level as a parameter for policy matching and web filtering. The policy or web filter action applies when the risk score of the URL (see Web Risk Overrides on page 653) is within the score range of the specified risk level. FortiProxy provides the following predefined risk levels (read-only):

Risk level	Score range	Description
high	91-100	Strong confidence of malicious intent.
low	21-50	Low predictive risk of attack.
moderate	51-70	Generally benign with a potential risk of attack.
suspicious	71-90	Medium confidence of malicious intent.
trustworthy	1-20	Very low predictive risk of attack.
unrated	0	The URL does not exist in FortiGuard DB or the risk score of the URL is unknown.

To define a custom risk level with a desired score range in the GUI:

1. Go to the *Security Profiles* > *Web Filter Risk Level* page.
2. Click *Create New* to create a new entry or select an existing custom risk level and click *Edit*.
3. Specify the name of the risk level.
4. Specify the low and high scores for the risk level.
5. Click *OK*.

To add a custom risk level with a desired score range in the CLI:

```
config webfilter ftgd-risk-level
   edit "Good"
      set high 30
      set low 10
   next
end
```

You can then select the risk level in the risk level dropdown list when you Create or edit a policy on page 387 or Create or edit a web filter profile on page 566.

For example, you can create a risk level *Good* with a score range of 10-30 and use it in a policy. FortiProxy will then apply the policy for URLs with a risk score between 10-30.

Data Loss Prevention

The FortiProxy data loss prevention (DLP) system prevents sensitive data from leaving or entering your network by scanning for various patterns while inspecting traffic passing through the FortiProxy. Data that matches defined sensitive data patterns is blocked, logged, allowed, or quarantined, or archived when it passes through the FortiProxy.

The DLP system is configured based on the following components. You can configure DLP in both the CLI and the GUI.

Component	Description
Data type	Define the type of pattern that DLP is trying to match. For example, this can be a pre-defined type such as credit card, hex, keyword, mip-label, regex, and US social security number (SSN). You can also create custom data types.
Dictionary	A collection of data type entries. When selecting a data type such as keyword, regex or hex, define the pattern that you are looking for.
EDM template	An exact data match (EDM)template pairs the data from an external file, such as a data threat feed file, with pre-defined FortiProxy data types. The external file can be in text (TXT)or comma-separated value (CSV) format. The EDM template can link to file on an external server to support dynamic updates, or the file can be uploaded to the EDM template.
Sensor	Define which dictionaries to check. You can match any dictionary, all dictionaries, or a special logical combination of the dictionaries. It can also count the number of dictionary matches to trigger the sensor.
File pattern	Define groups of file patterns based on pre-defined file types, or define your own pattern to match the file name.
DLP profile	Define rules for matching a sensor based on a file type or a message, and the type of protocol being used. It also allows you to choose the action to allow, log, block, or quarantine the address.

A DLP profile selects one or more sensors, and applies the sensor's pattern matching against the file type or message that is passing through selected protocols. The profile can be applied to a policy where the traffic will be inspected.

In the backend, DLP uses Hyperscan to perform a one-parse algorithm for scanning multiple patterns. This allows DLP to scale up without any performance downgrade.

Protocol support for DLP inspection

FortiProxy DLP inspection supports the following protocols:

- HTTP
- FTP
- IMAP
- POP3
- SMTP
- NNTP
- MAPI
- CIFS
- SFTP/SCP

Archiving

DLP can archive some or all of the content that passes through the DLP system. There are two forms of DLP archiving.

- Summary only: a summary of all the activity detected by the profile is recorded. For example, when an email message is detected, the sender, recipient, message subject, and total size are recorded. When a user accesses a web browser, every URL that they visit is recorded.
- Full: detailed records of all the activity detected by the profile is recorded. For example, when an email message is detected, the message itself, including any attachments, is recorded. When a user accesses a web browser, every page that they visit is archived.

You can configure the type of archiving per protocol.

Logging and blocking files by file name

Sometimes, file names are not accurately recorded in DLP logs, even though the files are blocked correctly based on the DLP profile. This is particularly apparent on cloud-based services, such as Google Drive or SharePoint.

For HTTP file uploads, some cloud services use proprietary encodings and APIs to transfer files and exchange metadata, instead of standard HTTP mechanisms, requiring custom handling of the proprietary API. If a cloud service changes the API without notice, the custom handling becomes outdated and file names might not be logged properly. Due to this, special consideration must be taken when using DLP to block files by file pattern. To block a specific file type, it is better to block by file type, and not by file name pattern.

The following topics provide information about DLP:

- DLP techniques on page 662
- Basic DLP settings on page 663
- Advanced DLP configurations on page 669
- DLP fingerprinting on page 672

- Sensitivity labels on page 676
- Exact data matching on page 680
- DLP examples on page 689

DLP techniques

The security of sensitive data is a top priority for organizations. A range of techniques and tools are used to maintain the confidentiality and accessibility of data.

The following table describes some of the industry standard techniques that are used for data loss protection, and if they can be configured in the GUI or CLI.

Technique	Description	GUI	CLI
Indexed Document Matching (IDM)	IDM creates unique fingerprints for your organization's crucial documents that hold sensitive information. This process involves analyzing the content of these documents and generating a checksum for each one. See DLP fingerprinting on page 672 for more information.		✓
Exact Data Matching (EDM)	EDM identifies particular data values within an indexed data source that require safeguarding. See Exact data matching on page 680 for more information.	✓	✓
Described Content Matching (DCM)	DCM scans through data to identify the presence of specific patterns using regular expressions (Regex). See DLP data type on page 669 for more information.	✓	✓
Optical Character Recognition (OCR)	OCR scans and analyzes the content embedded within images for sensitive information, extending data protection to image-based content. You can enable OCR and configure the OCR activation threshold when configuring an image analysis profile in the GUI or CLI.	✓	✓
Predefined data patterns	Default DLP patterns that classify private and confidential data that should be regulated in accordance with regulatory compliance requirements. See DLP data type on page 669 for more information.	✓	✓
Custom data classification tags (data pattern)	FortiProxy allows you to create patterns for your custom data type. See Custom DLP data type on page 669 for more information.	✓	✓
True file type filtering	Identify a file by the data type in its meta data. See DLP file pattern on page 671 for more information.	✓	✓
File size filtering	Identify a file based on its size. See Block HTTPS downloads of EXE files and log HTTPS downloads of files larger than 500 KB on page 695 for an example.		✓

Technique	Description	GUI	CLI
Microsoft Purview sensitivity labels	Sensitivity labels provide a mechanism to categorize and safeguard your data. They function as identifiers and highlight the significance of the data that they are attached to. See Sensitivity labels on page 676 for more information.	✓	✓
FortiGuard DLP service	A database of predefined DLP patterns, such as data types, dictionaries, and sensors, that are dynamically managed by FortiGuard. A valid DLP license is required.	✓	✓

Basic DLP settings

DLP settings can be configured for data types, dictionaries, EDM templates, sensors, file patterns, and profiles. This topic includes three examples that incorporate several DLP settings. DLP can be configured in both the CLI and the GUI.

The *Security Profiles* > *Data Loss Prevention* page includes the *Profiles*, *Sensors*, *Dictionaries*, and *EDM templates* tabs for configuring those DLP settings. DLP profiles can be added to policies from the GUI.

This section breaks down the DLP configuration into a sequence of steps:

1. Configure the DLP dictionary and/or EDM template:
   - A DLP dictionary is a collection of data type entries. See DLP data type on page 669 for more information.
   - An EDM template pairs pairs the data from an external file, such as a data threat feed file, with pre-defined FortiProxy data types. See Exact data matching on page 680 for more information.
2. Configure the DLP sensor:
   - A DLP sensor defines which dictionary to check. It counts the number of dictionary and/or EDM template to check. It counts the number of matches to trigger the sensor.
3. Configure the DLP profile:
   - A DLP profile allows for filtering by size and file type. See DLP file pattern on page 671 for custom file type.
4. Add the DLP profile to a policy.



All the steps mentioned above should be configured in the exact order given for ease of configuration.

Configuring DLP from the GUI

Use the following steps to configure DLP from the GUI.

To configure a DLP dictionary:

1. Go to *Security Profiles > Data Loss Prevention*.
2. Select the *Dictionaries* tab and click *Create New*.
3. Enter a name.
4. In the *Dictionary Entries* section, click *Create New*.
5. Set the *Type* and click *OK*.
6. Click *OK* to save the dictionary.

To configure an EDM template:

1. Go to *Security Profiles > Data Loss Prevention*.
2. Select the *EDM Templates* tab and click *Create New*.
3. Enter a name.
4. In the *Resource settings* section, select one of the following:
   Each column in the external file represents a pre-defined data type.

File upload	Select to upload an external file of data to use with pre-defined data types. The external file can be in text (TXT) or comma-separated value (CSV) format.
External feed	Select to provide the URL to a file of data on an external server to use with pre-defined data types. The external file must be in comma-separated value (CSV) format. FortiProxy will periodically fetch entries from the external file using HTTPS.
External feed URL	Specify the URL to the data file in CSV format on the external server.
HTTP basic authentication	Enable to use basic HTTP authentication when accessing the feed file on the external server. Specify the username and password for the external server.
Refresh rate	Specify the time interval to refresh the external resource (minutes).

5. Set the *Match criteria* section:
   The patterns in the data file must be valid. If the patterns are invalid, FortiProxy cannot use them, and no warning is displayed.

+All of these fields	Click to pair each column in the external data file with a DLP data type. All of the specified data in this section must match for FortiProxy to take an action.
Column index	Specify the column number in the external file that contains the data.
Column data type	Indicate which DLP data type pairs with the column index. Choose from: • credit-card

	• edm-keyword • mip-label • ssn-us
+Any of these fields	Click to pair the column in the external data file with a DLP data type, and to specify how many of these pairs must match for FortiProxy to take an action.
Minimum number of fields matched	Specify how many of the fields in the *Any of these fields* section must match for FortiProxy to take an action.
Column index	Specify the column number in the external file that contains the data.
Column data type	Indicate which DLP data type pairs with the column index. Choose from: • credit-card • edm-keyword • mip-label • ssn-us • fg-edm-can-natl_is-sin  The data type *fg-edm-can-natl_id-sin*, which represents the Canadian Social Insurance Number (SIN), is dynamically managed by FortiGuard. It is available for use as one of the data types in EDM templates, provided the user has a valid FortiGuard DLP service license.

6. Click *OK* to save the EDM template.

To configure a DLP sensor:

1. Go to *Security Profiles > Data Loss Prevention*.
2. Select the *Sensors* tab and click *Create New*.
3. Enter a name.
4. In the *Sensors Entries* section, click *Create New*.
5. In the *Sensor entry* list, select a dictionary and/or EDM template and click *OK*.
6. Click *OK* to save the sensor.

To configure a DLP profile:

1. Go to *Security Profiles > Data Loss Prevention*.
2. Select the *Profiles* tab and click *Create New*.
3. Enter a name.
4. In the *Rules* section, click *Create New*.
5. Configure the following settings:

Name	Filter name.
Data source type	Specify what type of data source to use: • *Sensor*: Use DLP sensors, such as dictionaries or EDM templates to match content. • *MIP label*: Use MIP label dictionaries to match content.
Sensors	Select DLP sensors or MIP labels: • *Sensor*: Select one or more DLP sensors when *Data source type* is set to *Sensor*. • *MIP label*: Select one or more MIP label dictionaries when *Data source type* is set to *MIP label*.
Severity	Select the severity or threat level that matches this filter.
Action	Action to take with content that this DLP profile matches.
Type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).
File type	Select the number of a DLP file pattern table to match.
Protocol	Check messages or files over one or more of these protocols.

6. Click *OK*.
7. Click *OK* to save the profile.

To add the DLP profile to a policy:

1. Go to *Policy & Objects* > *Policy*.
2. Click *Create New*.
3. Set the *Type* to any except *SSH Tunnel* which does not support DLP.
4. In the *Security Profiles* section, enable *DLP Profile* and select the desired profile.
5. Configure the other settings as needed.
6. Click *OK*.

Configuring DLP from the CLI

Use the following steps to configure DLP from the CLI.

To configure a DLP dictionary:

```
config dlp dictionary
    edit <name>
        config entries
            edit 1
                set type {credit-card | hex | keyword | mip-label | regex | ssn-us}
                set pattern <string>
                set repeat {enable | disable}
                set status {enable | disable}
```

```
            next
        end
    next
end
```

To configure an EDM template:

When configuring an EDM template from the CLI, you must link to a data file in CSV format on an external server.

1. Add the URL for the data threat feed file to FortiProxy.

   In this example, an external resource named `customer data EDM` is created, and it defines the location of the data threat feed file in CSV format on an external server.

```
config system external-resource
       edit "customer data EDM"
        set uuid 3cadb9be-f639-51ee-df8d-ea94d069c9cf
        set type data
        set resource "http://172.16.200.175/customer_data.csv"
```

```
 end
 next
end
```

2. Configure the EDM template.

   In this example, an exact data-match template named `Customer SSN EDM` is created for the external resource named `customer data EDM`. The matching record must contain the pattern for the data type from column index 1 (`g-ssn-us`) and at least one pattern for the data type from column index 3 (`g-edm-keyword`) or 9 (`g-edm-keyword`).

```
config dlp exact-data-match
       edit "Customer SSN EDM"
               set optional 1
               set data "customer data EDM"
                       config columns
                               edit 1
                               set type {credit-card | edm-keyword | mip-label | ssn-us | fg-edm-can-natl_i
                       next
               end
       next
end
```



The data type `fg-edm-can-natl_id-sin`, which represents the Canadian Social Insurance Number (SIN), is dynamically managed by FortiGuard. It is available for use as one of the data types in EDM templates, provided the user has a valid FortiGuard DLP service license.

To configure a DLP sensor:

```
config dlp sensor
    edit <name>
        set match-type {match-all | match-any | match-eval}
        set eval <string>
        config entries
            edit <id>
                set dictionary <dlp_dictionary or EDM template>
                set count <integer>
                set status {enable | disable}
            next
        end
    next
end
```

See Evaluation by Logical relationship on page 671 for more information about `match-eval`.

To configure a DLP profile:

```
config dlp profile
    edit <name>
        set feature-set {flow | proxy}
        config rule
            edit <id>
                set proto <protocol> <protocol> ...
                set sensor <dlp_sensor>
                set action {allow | log-only | block | quarantine-ip}
            next
        end
    next
end
```

To add the DLP profile to a policy:

```
config firewall policy
    edit <id>
        set srcintf <interface>
        set dstintf <interface>
        set action accept
        set srcaddr <address>
        set dstaddr <address>
        set schedule "always"
        set service "ALL"
        set utm-status enable
       set dlp-profile <string>
    next
end
```

See DLP examples on page 689 for sample configurations.

Advanced DLP configurations

The following topic provides information on advanced DLP configurations.

DLP data type

This configuration includes pre-defined data types to match for credit card, hex, keyword, mip-label, regex, and US social security number (SSN). Custom data types can be added.

```
config dlp data-type
    edit "keyword"
        set pattern "built-in"
    next
    edit "regex"
        set pattern "built-in"
    next
    edit "hex"
        set pattern "built-in"
    next
    edit "mip-label"
        set pattern "^[[:xdigit:]]{8}-[[:xdigit:]]{4}-[[:xdigit:]]{4}-[[:xdigit:]]{4}-[[:xdigit:]]
{12}$"
        set transform "built-in"
    next
    edit "credit-card"
        set pattern "\\b([2-6]{1}\\d{3})[- ]?(\\d{4})[- ]?(\\d{2})[- ]?(\\d{2})[- ]?(\\d{2,4})\\b"
        set verify "built-in"
        set look-back 20
        set transform "\\b\\1[- ]?\\2[- ]?\\3[- ]?\\4[- ]?\\5\\b"
    next
    edit "ssn-us"
        set pattern "\\b(\\d{3})-(\\d{2})-(\\d{4})\\b"
        set verify "(?<!-)\\b(?!666|000|9\\d{2})\\d{3}-(?!00)\\d{2}-(?!0{4})\\d{4}\\b(?!-)"
        set look-back 12
        set transform "\\b\\1-\\2-\\3\\b"
    next
end
```

Custom DLP data type

Custom data types can be added. See Custom data classification tags (data pattern) on page 662 for more information.

Custom DLP data type allows for both the proximity keyword check and data validation check within the same data type. The data type simultaneously supports two verification checks and one proximity match check to significantly lower the occurrence of false positives, enhancing the precision and dependability of the search.

To configure a custom DLP data type:

```
config dlp data-type
    edit <name>
       set verify <string>
       set verify2 <string>
       set look-ahead <integer>
       set look-back <integer>
       set match-around <string>
       set match-ahead <integer>
       set match-back <integer>
       set pattern <string>
    next
end
```

`config dlp data-type`	Configure predefined data type used by DLP scans.
`edit <name>`	Specify the name of the table containing the data type.
`set pattern`	Regular expression pattern string without look around
`set verify <string>`	Specify the regular expression pattern string used to verify the data type.
`set verify2 <string>`	Specify the extra regular expression pattern string used to verify the data type.
`set look-ahead <integer>`	Specify the number of character to obtain in advance for verification. (1 to 255, default = 1).
`set look-back <integer>`	Specify the number of characters required to save for verification. (1 to 255, default = 1).
`set match-around <string>`	Dictionary to check whether it has a match around (Only support match-any and basic types, no repeat supported).
`set match-back <integer>`	Specify the number of characters in front for `match-around` (1 to 4096, default = 1).
`set match-ahead <integer>`	Specify the number of characters behind for `match-around` (1 to 4096, default = 1).



The `set pattern` command can be used to define a regular expression for use with Hyperscan. However, Hyperscan does not fully support Perl Compatible Regular Expressions (PCRE), such as `look-ahead` and `look-behind`. To use advanced features supported by PCRE, you can use the `set verify` or `set verify2` commands.



To use "?" in a regex pattern, see CLI basics on page 41. This method only supports direct console connection and SSH. It does not support the CLI console in the GUI.

See Proximity search on page 709 for a sample configuration.

DLP file pattern

A DLP file pattern can block, allow, log, or quarantine a file based on the specified file type in the file filter list. Refer to Create or edit a DLP file pattern on page 718 for instructions about configuring a DLP file pattern.

To configure a DLP file pattern in CLI:

```
config dlp filepattern
    edit <id>
        set name <name>
        config entries
            edit <name>
                set filter-type {type | pattern}
                set file-type <file_type>
            next
        end
    next
end
```

Evaluation by Logical relationship

Evaluation by Logical relationship is a powerful tool used to combine multiple dictionary entries to define an accurate DLP sensor using logical expression.

Syntax example:

1. `set eval "dict(1) == 2"`
   Match DLP sensor only when dictionary one match count is two.
2. `set eval "(dict(1) + dict(2)) == 3"`
   Match DLP sensor only when dictionary one and dictionary two combined match count is three.
3. `set eval "(dict(1) == 2) && (dict(2) == 1)"`
   Match DLP sensor only when dictionary one match count is equal to two and dictionary two match count is equal to one.
4. `set eval "(dict(1) == 2) || (dict(2) == 1)"`
   Match DLP sensor only when dictionary one match count is equal to two or dictionary two match count is equal to one.
5. `set eval "dict(1) > dict(2)"`
   Match DLP sensor only when dictionary one match count is greater than dictionary two match count.

See Block HTTPS upload traffic that includes Visa or Mastercard information using evaluation via logical expression on page 697.

DLP fingerprinting

DLP fingerprinting employs Indexed Document Matching (IDM) to detect sensitive data. See Indexed Document Matching (IDM) on page 662 for more information. The file that the DLP profile filters is uploaded and the FortiProxy generates and stores a checksum fingerprint. The FortiProxy generates a fingerprint for all the files that are detected in network traffic, and compares all the checksums stored in its database. If a match is found, the configured action is taken. Any type of file can be detected by DLP fingerprinting, and fingerprints can be saved for each revision of a file as it is updated.

Using fingerprinting requires:

1. Creating a DLP fingerprint database by allowing the FortiProxy to access a file server containing files from which to create fingerprints.
2. Adding fingerprinting filters to DLP profiles.
3. Adding the profiles to policies that accept traffic that the fingerprinting will be applied on.

See Fingerprinting example on page 673 for a sample configuration.



The document fingerprint feature requires a FortiProxy that has internal storage.

To configure a DLP fingerprint document:

```
config dlp fp-doc-source
    edit <name>
        set server <string>
        set username <string>
        set password <password>
        set file-path <string>
        set sensitivity <Critical | Private | Warning>
    next
end
```

Command	Description
`server <string>`	Enter the IPv4 or IPv6 address of the file server.
`username <string>`	Enter the user name required to log into the file server.
`password <password>`	Enter the password required to log into the file server.
`file-path <string>`	Enter the path on the server to the fingerprint files.
`sensitivity <Critical | Private | Warning>`	Set the sensitivity or threat level for matches with this fingerprint database.

See `config dlp fp-doc-source` in the FortiProxy CLI Reference for a comprehensive list of commands.



A file server is required for the user to upload files. Each uploaded file will have a fingerprint generated by FortiProxy, and will be stored locally as a checksum. Currently, only servers that are using the Samba (SMB) protocol are compatible.

To configure a DLP fingerprint profile:

```
config dlp profile
    edit <name>
        config rule
            edit <id>
                set severity {info | low | medium | high | critical}
                set proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi | ssh | cifs}
                set filter-by fingerprint
                set sensitivity {Critical | Private | Warning}
                set action {allow | log-only | block | ban | quarantine-ip}
            next
        end
       set full-archive-proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi | ssh |
cifs}
```

```
    next
end
```

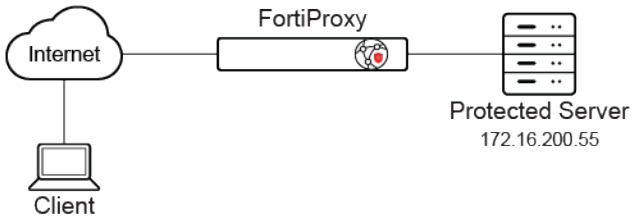
Command	Description
`severity {info | low | medium | high | critical}`	Set the severity or threat level that matches this filter.
`proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi | ssh | cifs}`	Set the protocol to inspect.
`filter-by fingerprint`	Set to match against a fingerprint sensitivity.
`sensitivity {Critical | Private | Warning}`	Set the DLP file pattern sensitivity to match.
`action {allow | log-only | block | ban | quarantine-ip}`	Set the action to take with content that matches the DLP profile.
`full-archive-proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi | ssh | cifs}`	Set the protocols to always content archive.

Fingerprinting example

This configuration will block HTTPS download traffic that matches the checksums that are stored in the FortiProxy fingerprint database.

When utilizing commonly-used SSL-encrypted protocols, such as HTTPS, SMTPS, POP3S, IMAPS, and FTPS, SSL inspection must be set to Deep Inspection. See Create or edit an SSL/SSH inspection profile on page 626 for more information.

The client machine must also have the corresponding deep inspection Certificate Authority (CA) certificate installed.



In this example, a text document with sensitive data is being downloaded by the client using the HTTP GET method. The term *Protected Server* refers to the Samba file server that stores the fingerprint files. It is assumed that you already have a configured Samba file server.

The FortiProxy intercepts the traffic using deep inspection and blocks the traffic as it matches the DLP profile configured on this FortiProxy. See Sample log on page 676 for a log sample.

To block network traffic that matches the checksums stored in the FortiProxy fingerprint database:

1. Configure the DLP fingerprint database:

```
config dlp fp-doc-source
    edit "test"
        set server "172.16.200.55"
        set username "kiki"
        set password *****
        set file-path "/Users/"
        set sensitivity "Warning"
    next
end
```

   This step can only be configured in the CLI.

2. Configure the DLP profile:

```
config dlp profile
    edit "fingerprint"
        config rule
            edit 1
                set proto http-get
                set filter-by fingerprint
                set sensitivity "Critical"
                set action block
            next
        end
    next
end
```

   DLP profiles that filter by fingerprint can only be configured in the CLI.

3. Add the DLP profile to a policy:

```
config firewall policy
    edit 1
        set type explicit-web
        set name "ExplicitPROXY"
        set uuid c0a2e814-7ff8-51ee-1815-054bdf34bd03
```

```
        set dstintf "any"
        set srcaddr "LAB-SUBNET"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "webproxy"
        set explicit-web-proxy "web-proxy"
        set utm-status enable
        set logtraffic all
        set log-http-transaction all
        set ssl-ssh-profile "test"
        set dlp-profile "fingerprint"
    next
end
```

This can also be configured in the GUI. See Create or edit a policy on page 387.

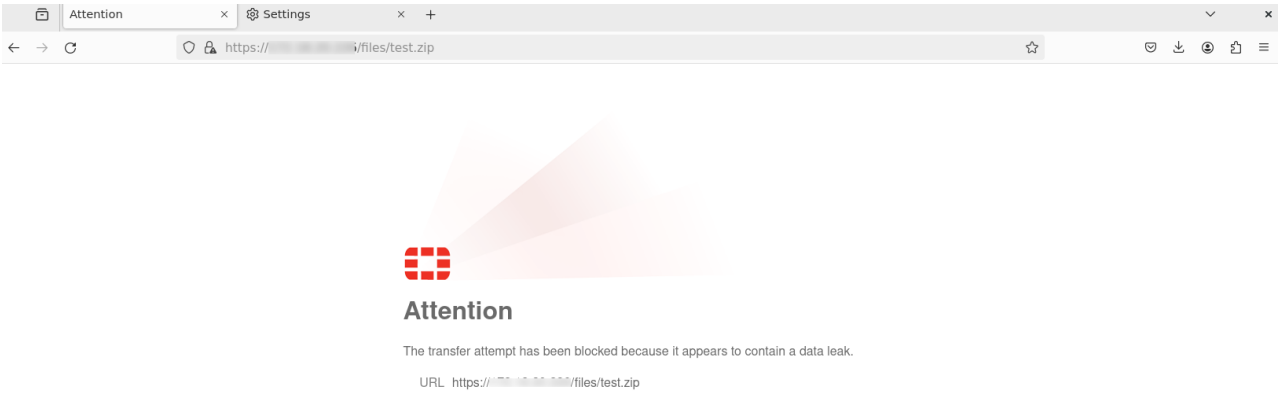
To verify the results:

1. Verify that the DLP fingerprint database is present on the FortiProxy:

```
# diagnose te app dlpfingerprint 3
File DB:
----------------------------------------
id,     filename,       vdom,   archive,        deleted,        scanTime,       docSourceSrvr,
 sensitivity,    chunkCnt,       reviseCnt,
1,      /Users/test.pdf,        root,   0,      0,      1709852459,     fp1,    3,      190,
 0,
2,      /Users/test.zip,        root,   0,      0,      1710201502,     fp1,    3,      1,
 0
```

2. Verify HTTP GET traffic that matches the checksums stored in the FortiProxy fingerprint database is being blocked:

   download attempt of a zip file from a linux device was made using Firefox. This zip file is the same as the one located on the protected server and its fingerprint is saved in the FortiProxy fingerprint database.



Sample log

To view the sample log:

1. Go to *Log & Report > Security Events* and select *Data Loss Prevention*.
2. View the log details in the GUI, or download the log file:

```
date=2024-03-12 time=17:14:24 eventtime=1710288863581501560 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" ruleid=1
dlpextra="Critical, Private, Warning" filtertype="fingerprint" filtercat="file" severity="low"
policyid=1 poluuid="c0a2e814-7ff8-51ee-1815-054bdf34bd03" policytype="policy"
sessionid=1710678066 epoch=1845053153 eventid=0 srcip=10.40.1.1 srcport=46572
srccountry="Reserved" srcintf="port1" srcintfrole="undefined" srcuuid="7f1725e0-7ff8-51ee-
fbe1-b5ff0424dfda" dstip=172.18.20.226 dstport=443 dstcountry="Reserved" dstintf="port1"
dstintfrole="undefined" proto=6 service="HTTPS" filetype="zip" direction="incoming"
action="block" hostname="172.18.20.226" url="
https://172.18.20.226/files/test.zip"
agent="Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0"
httpmethod="GET" filename="test.zip" filesize=501 profile="fingerprint"
```

Sensitivity labels

In order to safeguard your organization's data, labels can be employed as markers for sensitive information. Microsoft provides sensitivity labels, which act as identifiers emphasizing the importance of the data they're associated with, thereby enhancing the security measures in place. See Protect your sensitive data with Microsoft Purview (formerly MIP) for more information.

Any data traffic that includes a sensitivity label can be effectively managed using FortiProxy. This is made possible through the utilization of a pre-defined data type, *mip-label*, specifically designed for MIP in the Data Loss Prevention (DLP) dictionary. See Microsoft Purview sensitivity labels on page 663for more information.

Example

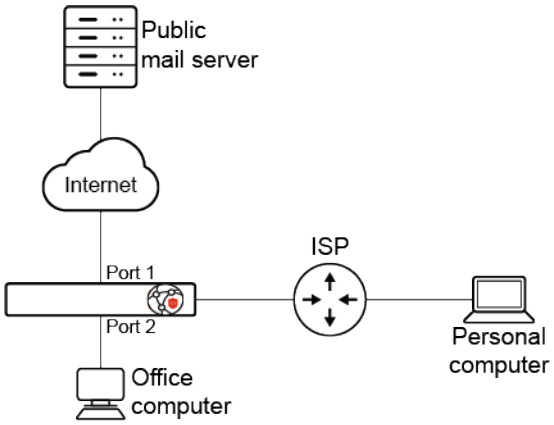
This configuration will block HTTPS upload traffic that matches the DLP profile.



When utilizing commonly-used SSL-encrypted protocols such as HTTPS, SMTPS, POP3S, IMAPS, and FTPS, SSL inspection must be set to Deep Inspection. See Create or edit an SSL/SSH inspection profile on page 626 for more information.

Additionally, the client machine must have the corresponding deep inspection Certificate Authority (CA) certificate installed.

Sample topology



In this example, a Microsoft Office document that is marked with a sensitivity label is being attached to an email in the Chrome browser using Office Desktop. See Learn about sensitivity labels for more information. The FortiProxy intercepts this traffic using deep inspection and blocks the attachment of the file because it matches the DLP profile that has been set up on this FortiProxy.

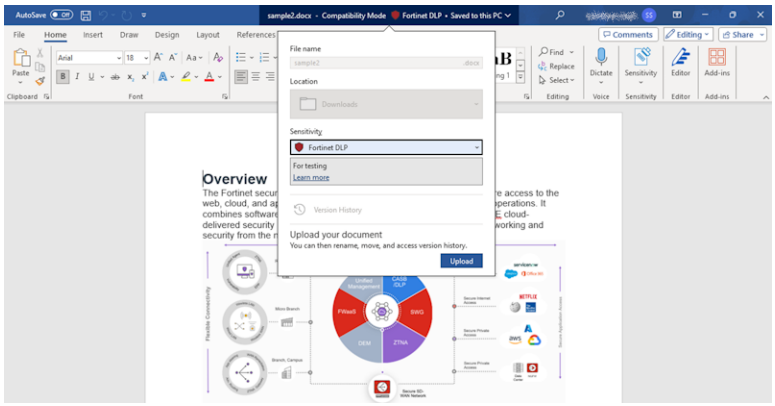
When a sensitivity label is included in HTTPS upload traffic, the file is blocked and a DLP log is generated. See Sample log on page 679 for a log sample.

Prerequisites

Before configuring FortiProxy, complete the following steps:

1. Create and configure sensitivity labels and their policies. See Create sensitivity labels for more information.
2. Apply a sensitivity label to content. See Apply sensitivity labels to your files and email for more information.

   Once the sensitivity label is applied on a file, you'll see it displayed on the sensitivity bar.



3. Obtain Globally Unique Identifier (GUID) for your sensitivity labels. See Search for documents by sensitivity label for more information.

   Sample GUID:

```
PS C:\Windows\system32> Get-Label |Ft Name, Guid

Name                                Guid
----                                ----
Fortinet DLP                        ca51e4ff-0733-4744-bebb-d3e1eb6383f4
```

FortiProxy uses the GUID for label matching. The *Pattern* for *mip-label* is configured to correspond to the label's GUID.

To block HTTPS upload traffic that includes MIP labels in the GUI:

1. Configure the DLP dictionary:
   a. Go to *Security Profiles* > *Data Loss Prevention*, select the *Dictionaries* tab, and click *Create New*.
   b. Set *Name* to *dic-case5*.
   c. In the *Dictionary Entries* table click *Create New*:
      i. Set *Type* to *mip-label*.
      ii. Set *Pattern* to *ca51e4ff-0733-4744-bebb-d3e1eb6383f4*.

      The pattern set here corresponds to the GUID of a specific sensitivity label. Please use your own GUID in this step. See step 3 of Prerequisites on page 677 for how to obtain your label GUID.

      iii. Click *OK*.
   d. Click *OK*.
2. DLP profiles that filter by MIP can only be configured in the CLI. See Configure the DLP profile.
3. Add the DLP profile to a firewall policy:
   a. Go to *Policy & Objects* > *Policy* and click *Create New*.
   b. In the *Security Profiles* section, enable *DLP Profile* and select *profile-case5*.
   c. Set *SSL Inspection* to *deep-inspection*.
   d. Configure the other settings as needed.
   e. Click *OK*.

To block HTTPS upload traffic that includes MIP labels in the CLI:

1. Configure the DLP dictionary:

```
config dlp dictionary
    edit "dic-case5"
        config entries
            edit 1
                set type "mip-label"
                set pattern "ca51e4ff-0733-4744-bebb-d3e1eb6383f4"
            next
        end
    next
end
```



The `set pattern` is set to the GUID of a specific sensitivity label. Please use your own GUID in this step. See step 3 of Prerequisites on page 677 for how to obtain your label GUID.

2. Configure the DLP profile:

```
config dlp profile
    edit "profile-case5"
        set feature-set proxy
        config rule
            edit 1
                set name "mip-label"
                set severity critical
                set proto smtp pop3 imap http-get http-post ftp nntp mapi ssh cifs
                set filter-by mip
                set file-type 1
                set label "dic-case5"
                set action block
            next
        end
    next
end
```

3. Add the DLP profile to a policy:

```
config firewall policy
    edit 1
        set type explicit-web
        set name "ExplicitPROXY"
        set uuid c0a2e814-7ff8-51ee-1815-054bdf34bd03
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set explicit-web-proxy "web-proxy"
        set utm-status enable
        set logtraffic all
        set log-http-transaction all
        set ssl-ssh-profile "deep-inspection"
        set dlp-profile "profile-case5"
    next
end
```

Sample log

An attempt was made to send an email from a Windows device using Gmail's webmail service. The email was intended to include an attachment with a MIP label, but the attachment failed to upload, resulting in the generation of a sample log.

```
date=2024-03-11 time=15:53:35 eventtime=1710197614776880630 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" ruleid=1 rulename="1"
filtertype="mip" filtercat="file" severity="critical" policyid=1 poluuid="c0a2e814-7ff8-51ee-1815-
054bdf34bd03" policytype="policy" sessionid=150411423 epoch=1589476180 eventid=0 srcip=10.40.1.226
srcport=39830 srccountry="Reserved" srcintf="port1" srcintfrole="undefined" srcuuid="7f1725e0-
7ff8-51ee-fbe1-b5ff0424dfda" dstip=142.251.211.229 dstport=443 dstcountry="Reserved"
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS" filetype="msoffice"
direction="outgoing" action="block" hostname="mail.google.com" url="
https://mail.google.com/_/upload?authuser=0&dcp=asu-n&upload_id=ABPtcPoZPYAkCzE-FaGZS_QUNjml-
0vPOGdjf7nk02kKLLnoTmg-wqsAbeWfuzerDACV0b8dZ6v0bkUZnB57Is1QdvjFBE2r90bT&upload_protocol=resumable"
agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/118.0.0.0 Safari/537.36" httpmethod="POST" referralurl=" https://mail.google.com/mail/u/0/"
filename="doc.doc" filesize=53248 profile="profile-case5"
```

Exact data matching

Exact Data Matching (EDM) identifies particular data values within an indexed data source that require safeguarding. It offers precise detection and handling of sensitive data based on user-defined criteria. This enhances security and improves efficiency by reducing false-positive detections.

Administrators can define a dataset in a CSV or TXT file on a server, upload file directly on FortiProxy or point FortiProxy to the external resource. See EDM template on page 680 for more information.

CSV file example:

Jason	Valentino	120 Jefferson St.	Riverside	CA	92504
Marry	Baxter	415 W Willow Grove Ave	Philadelphia	PA	19118
David	Solace	555 Pierce Street APT #123	Albany	CA	94706
Thomas	Jefferson	1600 Pennsylvania Avenue NW	Washington	DC	20500

TXT file example:

```
213321,john,doe
201111,karen,smith
322122,rick,wong
```

A CSV or TXT file can have a maximum of 32 columns. Each indexed column in the external file represents data (or patterns) for a built-in data type that you want to match using EDM template.

EDM template

The EDM template is used to specify the URL location of the data threat feed file or upload the file directly on to the FortiProxy. Once the data is imported it can be utilized with an EDM template to maps individual columns of data (or patterns) from a file to built-in data types to match credit card, keyword, mip label, social insurance number (SIN), and social security number (SSN) data. When the data passing through FortiProxy matches with the EDM template, FortiProxy responds according to the preset rules.



A CSV or TXT file can be uploaded directly to FortiProxy using the File Upload option. However, this option is exclusively available through the GUI. It's important to note that file upload is only possible if your FortiProxy unit is equipped with a hard disk. In the absence of a hard disk, the File Upload option will be grayed out.

Please note that if the CSV or TXT file is uploaded using the File Upload option, it will not be dynamically synchronized nor periodically updated. This means that any changes made to the file will not be imported by FortiProxy. Therefore, users are required to manually update the file again on the FortiProxy using the Update file option. This option is located under Resource Type and is only visible if the file was previously uploaded via the File Upload option.

The sequence of steps for configuring EDM is consistent with other DLP configurations. See Basic DLP settings on page 663 for more information.

Data threat feed

A data threat feed is a dynamic list that contains data. The data is patterns for DLP data types. The dynamic list is stored in a text (TXT) or comma-separated value (CSV) file format on an external server and periodically updated. After FortiProxy can access the file, the patterns can be used with an EDM template.

```
config system external-resource
    edit <name>
        set type data
        set resource <string>
        set refresh-rate <integer>
    next
end
```

`set type {category | domain | malware | address | mac-address | data}`	Specify the type of user resource. • data: Specify a data file as the user source.
`set resource <string>`	Specify the URL of the external resource.
`set refresh-rate <integer>`	Time interval to refresh the external resource (minutes).

The size of the Data Threat Feed file varies depending on the device model. The maximum file size limit for each model is as follows:

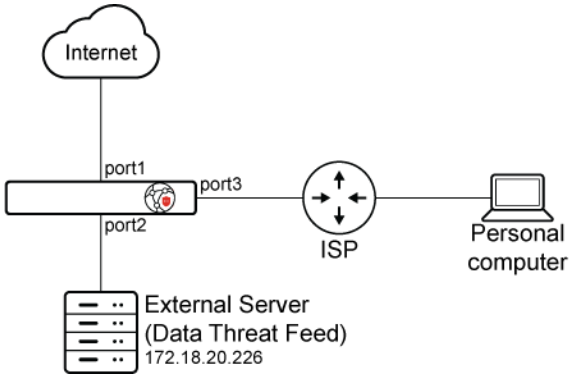
- 128 MB for High-End (Data Center) models
- 64 MB for Mid-Range (Campus) models
- 32 MB for Entry-Level (Branch) models.

Example

This configuration will block HTTPS upload traffic that matches the DLP profile.

When utilizing commonly-used SSL-encrypted protocols such as HTTPS, SMTPS, POP3S, IMAPS, and FTPS, SSL inspection must be set to Deep Inspection. See Deep inspection for more information.

Additionally, the client machine must have the corresponding deep inspection Certificate Authority (CA) certificate installed.



In this example, an EDM template named Customer SSN EDM is created on the FortiProxy. During this process, a CSV file (`customer_data.csv`) located on an external server is imported using the data thread feed.

Sample CSV file:

SSN	Last Name	First Name	Address	City	State	ZIP	Phone	Email	CCN
172-32-1176	Doe	John	10932 Big Rd	Malibu	CA	94025	408-497-7223	jdoe@domain.com	5270-4267-6450-5516
514-14-8905	Bard	Ashley	4469 Sher St	Golf	KS	66428	785-939-6046	abard@domain.com	5370-4638-8881-302

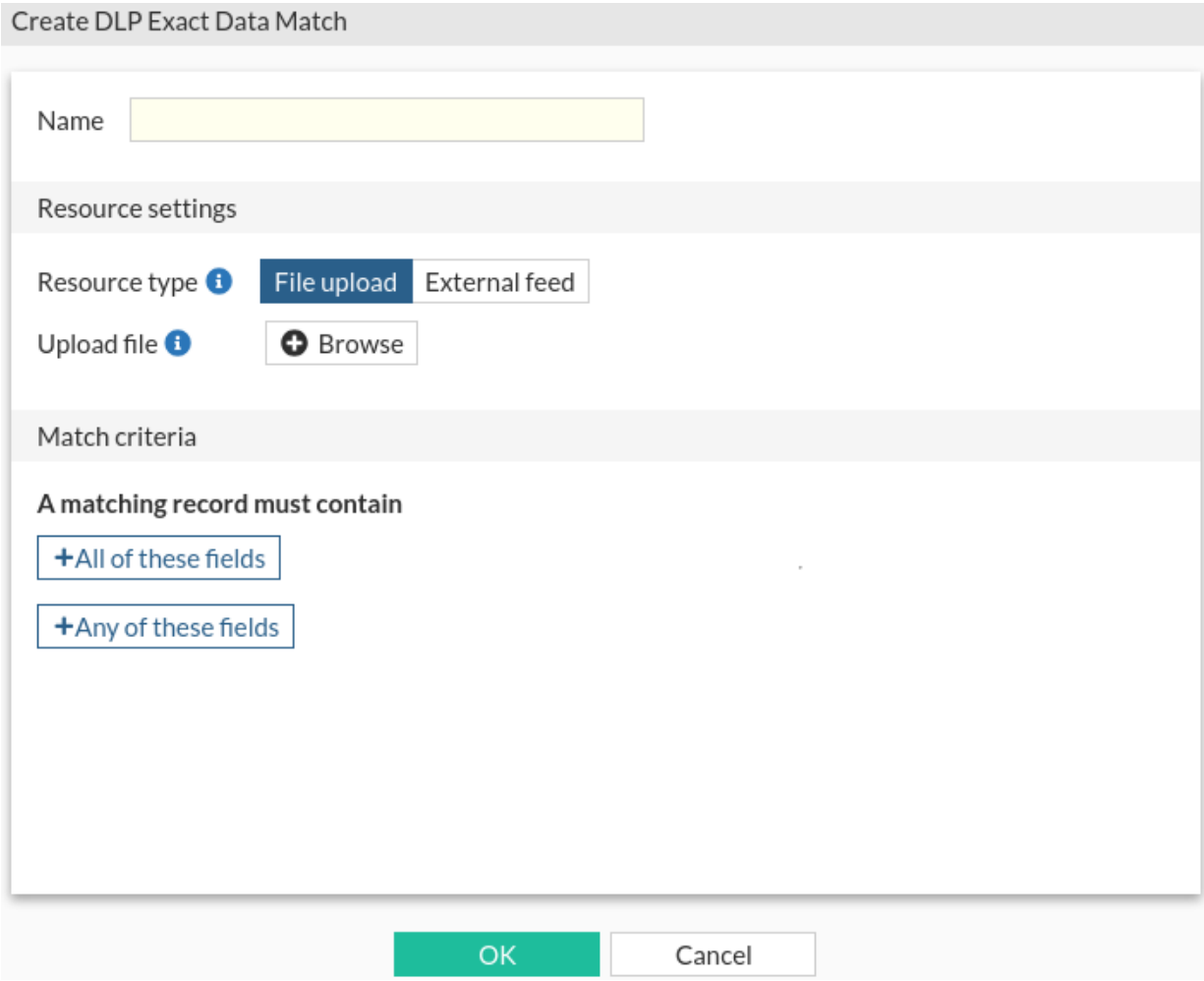
In this example, the EDM template specifies:

- Column index 1 in the external data threat feed file contains patterns for the `g-ssn-us` data type.
- Column index 3 and 9 contain patterns for the `g-edm-keyword` data type.
- The patterns from column index 1 must match for FortiProxy to take an action.
- The pattern from either column index 3 or 9 must match for FortiProxy to take an action.

Based on the aforementioned template, the DLP profile will match any traffic containing data that corresponds to the SSN in column 1, and either the First Name in column 3 or the Email in column 9. For instance, if the HTTPS upload traffic sent from personal computer contains '172-32-1176' AND 'John', or '172-32-1176' AND 'jdoe@domain.com', the traffic will be blocked and a DLP log is generated. See Sample log for a log sample.

To configure EDM for DLP in the GUI:

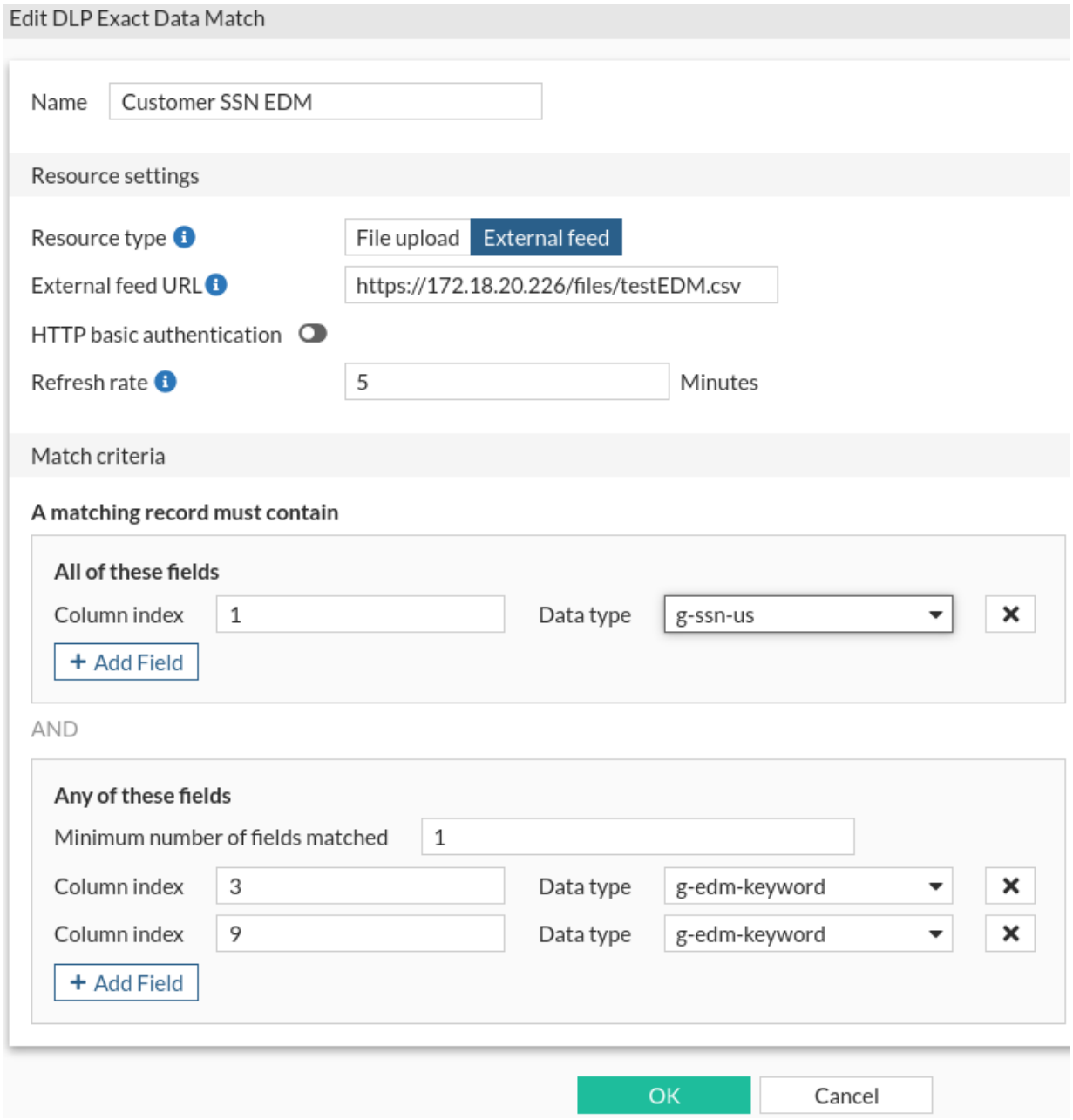
1. Create an EDM template with matching criteria:
   a. Go to *Security Profiles* > *Data Loss Prevention* > *EDM Templates*, and click *Create New*.



   b. Specify a name for the template, such as *Customer SSN EDM*.
   c. Set *Resource type* to *External feed*, and set *External feed URL* to the location of the file on the external server, such as *https://172.18.20.226/customer_data.csv*.
   d. Click *+All of these fields* to pair the column index of patterns with a DLP data type. All of the specified data in this section must match for FortiProxy to take an action.

      In this example, column 1 in the external resource file contains the patterns for the *g-ssn-us* data type.
   e. Click *+Any of these fields* to pair the column index of patterns with a DLP data type, and to specify how many of these pairs must match for FortiProxy to take an action.

      In this example, columns 3 and 9 in the external resource file contains the patterns for the *g-edm-keyword* data type. Only one pattern from the two columns must match.

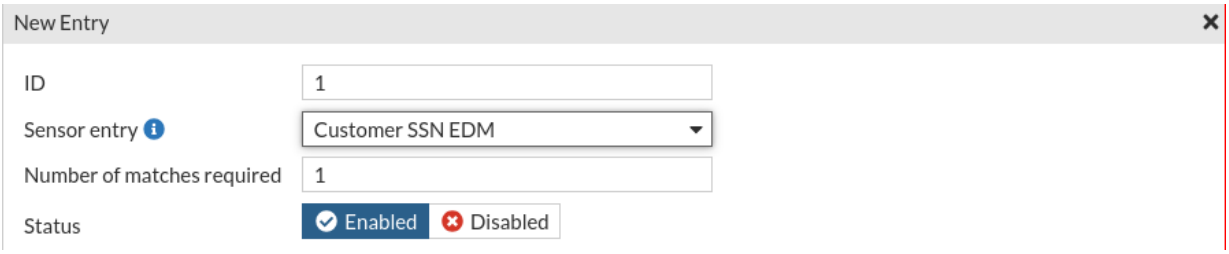


f. Click *OK*.

g. Edit the DLP EDM template and click *View Entries* to view the data entries in the field.

When viewing EDM entries, the GUI currently does not validate the entries and displays all entries as Valid. However, a Valid entry must have all values matching the data-type of the specific column. If one value does not match, the entry is invalid and will not be used for pattern matching.

2. Configure a DLP sensor for the EDM template.
   a. In *Security Profiles* > *Data Loss Prevention*, click *Sensors* > *Create New*.
   b. Specify a name for the DLP sensor, such as *Sensor SSN EDM*.
   c. Click *Create New*. The *New Entry* pane is displayed.
   d. From the *Sensor entry* list, select *Customer SSN EDM*, and click *OK*.



   The *New DLP Sensor* pane is displayed
   e. Click *OK*.
3. Create a DLP profile and select the DLP sensor for the EDM template.
   a. In *Security Profiles* > *Data Loss Prevention*, click *Profiles* > *Create New*.
   b. Specify a name for the DLP profile, such as *Profile SSN EDM*.
   c. Click *Create New*. The *New Rule* pane is displayed.
   d. Specify a name for the rule, such as *Rule SSN EDM*.
   e. Set *Data source type* to *Sensor*, and select *Sensor SSN EDM*.
   f. Set *Action* to *Block*.
   g. Set *Match type* to *Message*.
   h. Select *HTTP-POST* protocol.
   i. Click *OK*. The *New DLP Profile* pane is displayed.
   j. Click *OK* to save the profile.
4. Add the DLP profile to a policy:
   a. Go to *Policy & Objects* > *Policy*.
   b. Click *Create New*.
   c. In the *Security Profiles* section, enable *DLP Profile* and select *Profile SSN EDM*.
   d. Set *SSL/SSH Inspection* to *deep-inspection*.
   e. Configure the other settings as needed.
   f. Click *OK*.

To configure EDM for DLP in the CLI:

1. Add the URL for the data threat feed file to FortiProxy.
   In this example, an external resource named `customer data EDM` is created, and it defines the location of the data threat feed file in CSV format on an external server.

```
config system external-resource
    edit "customer data EDM"
        set type data
        set resource "https://172.18.20.226/customer_data.csv"
        end
```

```
    next
end
```

2. Configure the EDM template.

   In this example, an exact data-match template named `Customer SSN EDM` is created for the external resource named `customer data EDM`. The matching record must contain the pattern for the data type from column index 1 (`g-ssn-us`) and at least one pattern for the data type from column index 3 (`g-edm-keyword`) or 9 (`g-edm-keyword`).

```
config dlp exact-data-match
    edit "Customer SSN EDM"
        set optional 1
        set data "customer data EDM"
        config columns
            edit 1
                set type "g-ssn-us"
            next
            edit 3
                set type "g-edm-keyword"
                set optional enable
            next
            edit 9
                set type "g-edm-keyword"
                set optional enable
            next
        end
    next
end
```

3. Add the EDM template to a DLP sensor.

```
config dlp sensor
    edit "Sensor SSN EDM"
        config entries
            edit 1
                set dictionary "Customer SSN EDM"
            next
        end
    next
end
```

4. Configure a DLP profile to use the DLP sensor.

```
config dlp profile
    edit "Profile SSN EDM"
        set feature-set proxy
        config rule
            edit 1
                set name "Rule SSN EDM"
                set type message
                set proto http-post
                set filter-by sensor
```

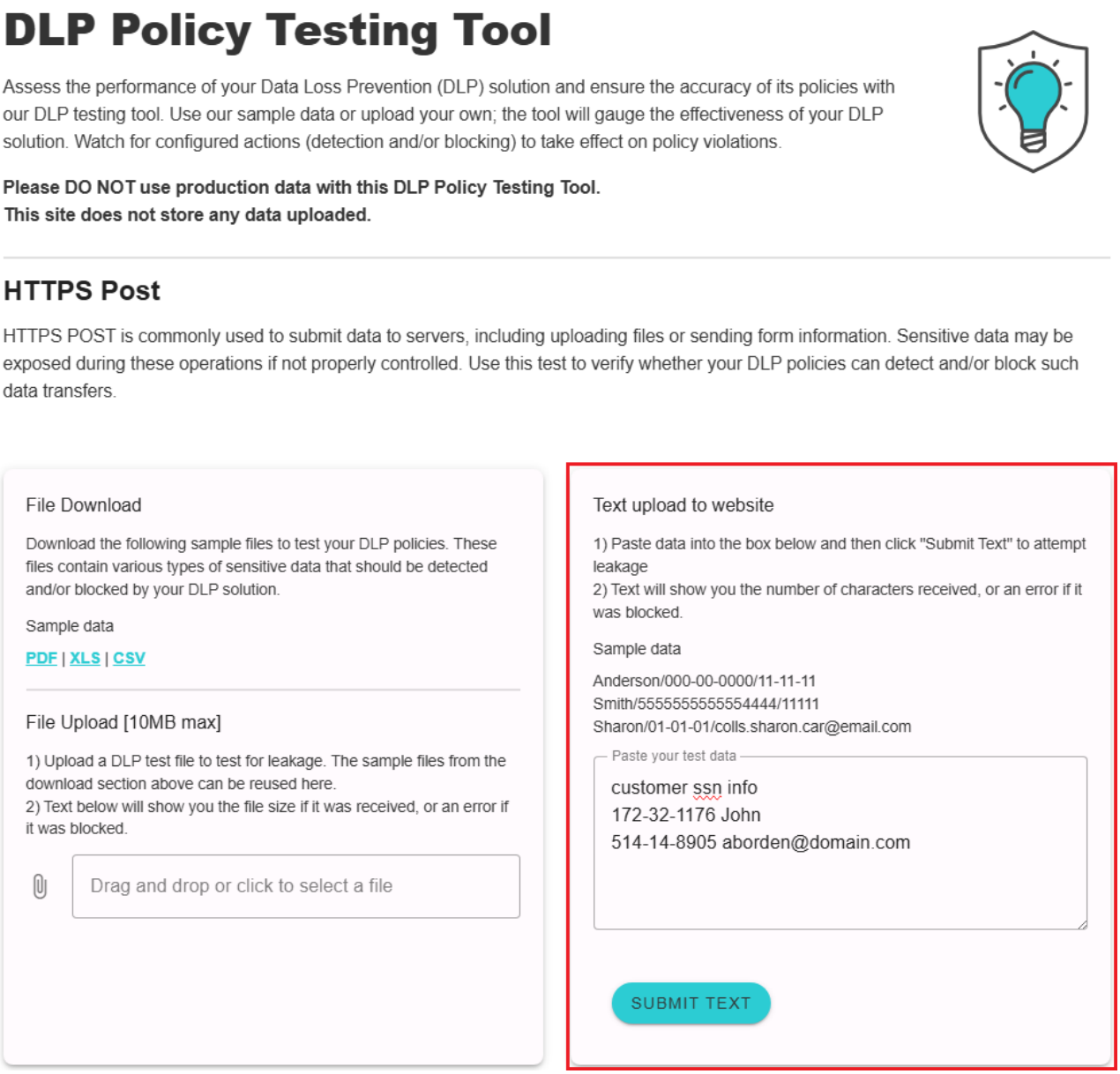
```
                set sensor “Sensor SSN EDM”
                set action block
            next
        end
    next
end
```

5. Add the DLP profile to a policy.

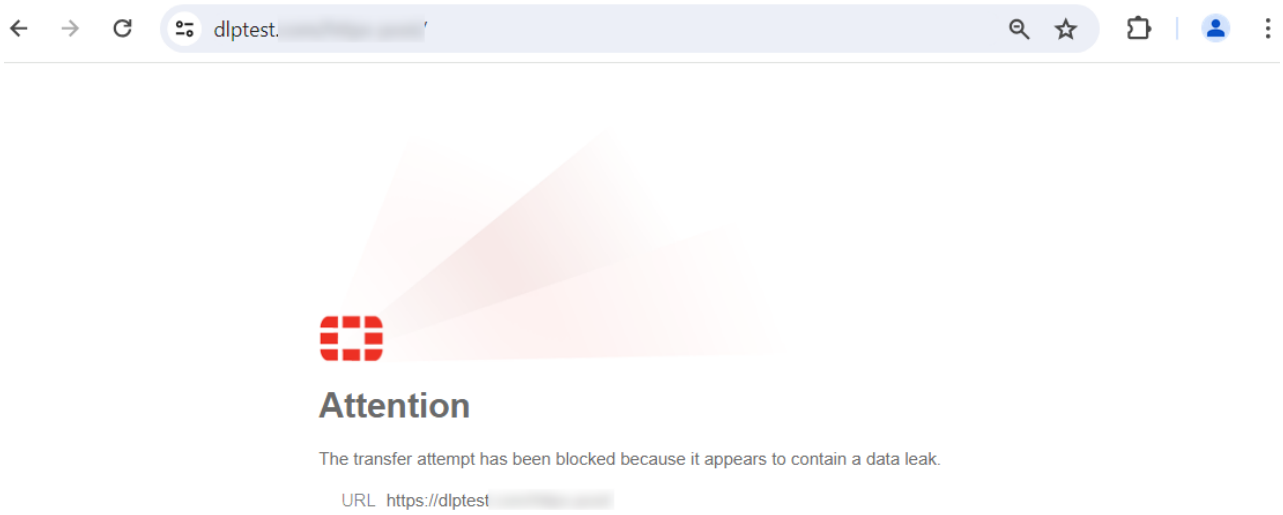
```
config firewall policy
    edit 1
        set name "Internet"
        set srcintf "port3"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set dlp-profile "Profile SSN EDM"
    next
end
```

To verify:

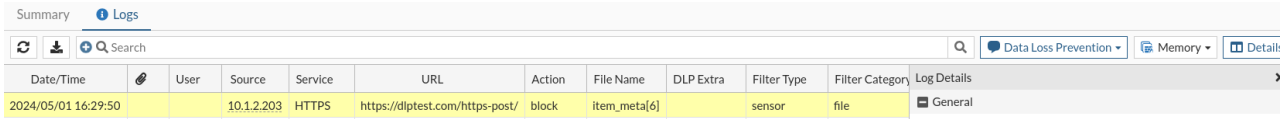
1. A user attempts to post a sensitive message through HTTPS to dlptest.ai, and the message content matches the EDM template.



2. FortiProxy blocks the user's attempt and displays a replacement message:



3. FortiProxy generates a DLP log:




```
1: date=2024-08-23 time=18:02:00 eventtime=1724461319796558635 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" ruleid=1 rulename="Rule SSN
EDM" filtertype="sensor" filtercat="message" severity="medium" policyid=113 poluuid="65885ef4-
5131-51ef-cf0f-2f757f2e9aeb" policytype="policy" sessionid=1845688663 epoch=412739369
eventid=1 srcip=10.40.1.1 srcport=60850 srccountry="Reserved" srcintf="port1"
srcintfrole="undefined" dstip=35.209.95.242 dstport=443 dstcountry="United States"
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS" filetype="N/A"
direction="outgoing" action="block" hostname="dlptest.ai" url="https://dlptest.ai"
agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0"
httpmethod="POST" referralurl="https://dlptest.ai" profile="Profile SSN EDM"
```

DLP examples

The following topics provide examples of DLP:

- Block HTTPS upload traffic that includes credit card information on page 690
- Log FTP upload traffic with a specific pattern on page 692
- Block HTTPS downloads of EXE files and log HTTPS downloads of files larger than 500 KB on page 695
- Block HTTPS upload traffic that includes Visa or Mastercard information using evaluation via logical expression on page 697
- Block access to LLM applications using keywords and FQDN on page 701
- Proximity search on page 709
- Assign confidence levels in FortiGuard managed DLP dictionaries on page 713

Block HTTPS upload traffic that includes credit card information

This configuration will block HTTPS upload traffic that includes credit card information. The pre-defined data type for credit card is used in the dictionary.

To block HTTPS upload traffic that includes credit card information in the GUI:

1. Configure the DLP dictionary:
   a. Go to *Security Profiles* > *Data Loss Prevention*, select the *Dictionaries* tab, and click *Create New*.
   b. Enter a name (*dic-case1*).
   c. In the *Dictionary Entries* section, click *Create New*.
   d. Set the *Type* to *credit-card* and click *OK*.
   e. Click *OK* to save the dictionary.
2. Configure the DLP sensor:
   a. Go to *Security Profiles* > *Data Loss Prevention*, select the *Sensors* tab, and click *Create New*.
   b. Enter a name (*sensor-case1*).
   c. In the *Sensor Entries* section, click *Create New*.
   d. Set the *Dictionary* to *dic-case1* and click *OK*.
   e. Click *OK* to save the sensor.
3. Configure the DLP profile:
   a. Go to *Security Profiles* > *Data Loss Prevention*, select the *Profiles* tab, and click *Create New*.
   b. Enter a name (*profile-case1*).
   c. In the *Rules* section, click *Create New*.
   d. Configure the following settings:

Name	*1*
Sensors	*sensor-case1*
Severity	*Medium*
Action	*Block*
Type	*File*
File type	*builtin-patterns*
Protocol	*HTTP-POST*, *HTTP-GET*

   e. Click *OK*.
   f. Click *OK* to save the profile.
4. Add the DLP profile to a policy:
   a. Go to *Policy & Objects* > *Policy* and click *Create New*.
   b. Set the *Type* to any except *SSH Tunnel* which does not support DLP.
   c. In the *Security Profiles* section, enable *DLP Profile* and select *profile-case1*.
   d. Configure the other settings as needed.
   e. Click *OK*.

When a credit card is included in HTTP POST traffic, the file is blocked and a DLP log is generated.

To block HTTPS upload traffic that includes credit card information in the CLI:

1. Configure the DLP dictionary:

```
config dlp dictionary
    edit "dic-case1"
        config entries
            edit 1
                set type "credit-card"
            next
        end
    next
end
```

2. Configure the DLP sensor:

```
config dlp sensor
    edit "sensor-case1"
        config entries
            edit 1
                set dictionary "dic-case1"
            next
        end
    next
end
```

3. Configure the DLP profile:

```
config dlp profile
    edit "profile-case1"
        set feature-set proxy
        config rule
            edit 1
                set name "1"
                set proto http-get http-post
                set filter-by sensor
                set file-type 1
                set sensor "sensor-case1"
                set action block
            next
        end
    next
end
```

4. Add the DLP profile to a policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
```

```
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set dlp-profile "profile-case1"
    next
end
```

When a credit card is included in HTTP POST traffic, a replacement message appears because it is blocked. A DLP log is generated.

Sample log

From Windows, the following command can be used to generate a sample log, using the cURL tool to post data, which contains a sample credit card number. See sample data at https://dlptest.ai/ for sample credit card numbers.

```
# curl –k -F "file=@C:\Users\test\Desktop\demo.doc https://172.16.200.55/card.doc -o NUL

1: date=2022-10-26 time=11:25:01 eventtime=1666808700281057923 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" filteridx=1 filtername="1"
dlpextra="builtin-patterns;sensor-case1" filtertype="sensor" filtercat="file" severity="medium"
policyid=1 poluuid="891a526a-51cd-51ed-577a-6505bec88af9" policytype="policy" sessionid=3905
epoch=2143297701 eventid=0 srcip=10.1.100.11 srcport=40370 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="502d2c8e-51cd-51ed-a24e-a091f4ff6fed" dstip=172.16.200.55
dstport=443 dstcountry="Reserved" dstintf="port1" dstintfrole="undefined" dstuuid="502d2c8e-51cd-
51ed-a24e-a091f4ff6fed" proto=6 service="HTTPS" filetype="msoffice" direction="outgoing"
action="block" hostname="172.16.200.55" url="https://172.16.200.55/card.doc" agent="curl/7.83.1"
httpmethod="POST" filename="card.doc" filesize=108 profile="profile-case1"
```

Log FTP upload traffic with a specific pattern

This configuration will log FTP upload traffic with the following patterns:

- keyword = demo
- regex = demo(regex){1,5}
- hex = e6b58be8af95

The dictionary entries have repeat match enabled. The DLP sensor is set so this is repeated five times.

To log FTP upload traffic that has specific keyword, regex, and hex patterns repeated for five times in the GUI:

1. Configure the DLP dictionary with three entries:
   a. Go to *Security Profiles > Data Loss Prevention*, select the *Dictionaries* tab, and click *Create New*.
   b. Enter a name (*dic-case2*).
   c. In the *Dictionary Entries* section, click *Create New*.
   d. Set the *Type* to *keyword* and the *Pattern* to *demo*.
   e. Enable *Repeats* and click *OK*.
   f. Repeat these steps to add dictionary entries for the following (with *Repeats* enabled):
      i. Set the *Type* to *regex* and the *Pattern* to *demo(regex){1,5}*.
      ii. Set the *Type* to *hex* and the *Pattern* to *e6b58be8af95*.
   g. Click *OK* to save the dictionary.
2. Configure the DLP sensor:
   a. Go to *Security Profiles > Data Loss Prevention*, select the *Sensors* tab, and click *Create New*.
   b. Enter a name (*sensor-case2*).
   c. In the *Sensor Entries* section, click *Create New*.
   d. Set the *Dictionary* to *dic-case2*, set the *Count* to *5*, and click *OK*.
   e. Click *OK* to save the sensor.
3. Configure the DLP profile:
   a. Go to *Security Profiles > Data Loss Prevention*, select the *Profiles* tab, and click *Create New*.
   b. Enter a name (*profile-case2*).
   c. In the *Rules* section, click *Create New*.
   d. Configure the following settings:

Name	*1*
Sensors	*sensor-case2*
Severity	*Medium*
Action	*Block*
Type	*File*
File type	*builtin-patterns*
Protocol	*FTP*

   e. Click *OK*.
   f. Click *OK* to save the profile.
4. Add the DLP profile to a policy:
   a. Go to *Policy & Objects > Policy* and click *Create New*.
   b. Set the *Type* to any except *SSH Tunnel* which does not support DLP.
   c. In the *Security Profiles* section, enable *DLP Profile* and select *profile-case2*.
   d. Configure the other settings as needed.
   e. Click *OK*.

5. Upload a Word document that contains "demo, demo, demo, demoregexregex," using FTP.
   A DLP log is generated after the FTP traffic passes.

To log FTP upload traffic that has specific keyword, regex, and hex patterns repeated for five times in the CLI:

1. Configure the DLP dictionary:

```
config dlp dictionary
    edit "dic-case2"
        config entries
            edit 1
                set type "keyword"
                set pattern "demo"
                set repeat enable
            next
            edit 2
                set type "regex"
                set pattern "demo(regex){1,5}"
                set repeat enable
            next
            edit 3
                set type "hex"
                set pattern "e6b58be8af95"
                set repeat enable
            next
        end
    next
end
```

2. Configure the DLP sensor:

```
config dlp sensor
    edit "sensor-case2"
        config entries
            edit 1
                set dictionary "dic-case2"
                set count 5
            next
        end
    next
end
```

3. Configure the DLP profile:

```
config dlp profile
    edit "profile-case2"
        set feature-set proxy
        config rule
            edit 1
                set proto ftp
                set filter-by sensor
```

```
                set file-type 1
                set sensor "sensor-case2"
                set action block
            next
        end
    next
end
```

4. Add the DLP profile to a policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "protocols"
        set dlp-profile "profile-case2"
    next
end
```

5. Upload a Word document that contains "demo, demo, demo, demoregexregex," using FTP. A DLP log is generated after the FTP traffic passes.

Sample log

```
1: date=2022-10-26 time=12:37:57 eventtime=1666813077679725858 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" filteridx=1 filtername="1"
dlpextra="builtin-patterns;sensor-case2" filtertype="sensor" filtercat="file"
severity="medium" policyid=1 poluuid="891a526a-51cd-51ed-577a-6505bec88af9"
policytype="policy" sessionid=6267 epoch=909159520 eventid=0 srcip=10.1.100.11 srcport=52858
srccountry="Reserved" srcintf="port2" srcintfrole="undefined" srcuuid="502d2c8e-51cd-51ed-
a24e-a091f4ff6fed" dstip=172.16.200.55 dstport=43411 dstcountry="Reserved" dstintf="port1"
dstintfrole="undefined" dstuuid="502d2c8e-51cd-51ed-a24e-a091f4ff6fed" proto=6 service="FTP"
filetype="msoffice" direction="outgoing" action="block" filename="realizedDoc.doc"
filesize=26624 profile="profile-case2"
```

Block HTTPS downloads of EXE files and log HTTPS downloads of files larger than 500 KB

This configuration will block HTTPS downloads of EXE files and log HTTPS downloads of files larger than 500 KB.

To block HTTPS download of EXE files and log downloads larger than 500 KB:

1. Configure the DLP file pattern:

```
config dlp filepattern
    edit 3
        set name "case3-exe"
        config entries
            edit "exe"
                set filter-type type
                set file-type exe
            next
        end
    next
end
```

2. Configure the DLP profile:

```
config dlp profile
    edit "profile-case3-type-size"
        config rule
            edit 1
                set proto http-get
                set filter-by none
                set file-type 3
                set action block
            next
            edit 2
                set proto http-get
                set filter-by none
                set file-size 500
                set action log-only
            next
        end
    next
end
```

3. Add the DLP profile to a policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "custom-deep-inspection"
        set dlp-profile "profile-case3-type-size"
```

```
        set logtraffic all
    next
end
```

4. Download an EXE file using HTTPS. The download is blocked, a replacement message appears, and a DLP log is generated.

Sample log

```
1: date=2022-02-15 time=11:54:29 eventtime=1644954869682887856 tz="-0800" logid="0954024577"
type="utm" subtype="dlp" eventtype="dlp" level="notice" vd="root" filteridx=2 dlpextra="500
kB" filtertype="none" filtercat="file" severity="medium" policyid=1 poluuid="905fb604-7ed4-
51ec-0853-79e498591bf8" policytype="policy" sessionid=12082 epoch=901683674 eventid=0
srcip=10.1.100.18 srcport=59520 srccountry="Reserved" srcintf="port2" srcintfrole="undefined"
srcuuid="358d0f56-7ed4-51ec-50f7-a5e4525a641d" dstip=51.81.186.201 dstport=443
dstcountry="United States" dstintf="port1" dstintfrole="undefined" dstuuid="358d0f56-7ed4-
51ec-50f7-a5e4525a641d" proto=6 service="HTTPS" direction="incoming" action="log-only"
hostname="2.na.dl.wireshark.org" url="https://2.na.dl.wireshark.org/win64/Wireshark-win64-
3.6.2.exe" agent="curl/7.61.1" filename="Wireshark-win64-3.6.2.exe" filesize=10502090
profile="profile-case3-type-size"
```

Block HTTPS upload traffic that includes Visa or Mastercard information using evaluation via logical expression

This example will allow users to create a subset of the existing DLP data type, *credit-card*. It can be very beneficial for an organization that wants to prevent only certain types of credit cards and not all.

This configuration will block HTTPS traffic that includes Visa or Mastercard information. Two dictionary entries with DLP data-type regex are created with custom patterns to match Visa and Mastercard numbers respectively, and a third dictionary entry is created with pre-defined data type *credit-card*. All three entries are used in the sensor using evaluation via logical expression to further supplement the detection.

In the CLI, evaluation via logical expression can be defined using the command `match-eval`. It is a tool used to combine multiple entries to define an accurate DLP sensor.

In this example, a Microsoft Office document with Visa credit card information is sent securely to the receiver using the HTTP POST method. The FortiProxy intercepts the traffic using deep inspection and blocks the traffic as it matches the DLP profile configured on this FortiProxy.

To block HTTPS upload traffic that includes Visa or Mastercard credit card information in the GUI:

1. Configure the DLP dictionary:
   a. Go to *Security Profiles* > *Data Loss Prevention*, select the *Dictionaries* tab, and click *Create New*.
   b. Create an entry for Visa:
      i. Enter a name (*Finance_Credit_Card_Visa*).
      ii. In the *Dictionary Entries* section, click *Create New*.
      iii. Set the *Type* to *regex*.

iv. Set *Pattern* to *4[0-9]{12}(?:[0-9]{3})* and click *OK*.
v. Click *OK* to save the dictionary.

c. Create an entry for Mastercard:
i. Enter a name (*Finance_Credit_Card_Mastercard*).
ii. In the *Dictionary Entries* section, click *Create New*.
iii. Set the *Type* to *regex*.
iv. Set *Pattern* to *(?:5[1-5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-9]{2}|27[01][0-9]|2720)[0-9]{12}* and click *OK*.
v. Click *OK* to save the dictionary.

d. Create an entry for Credit Card:
i. Enter a name (*CC_Number*).
ii. In the *Dictionary Entries* section, click *Create New*.
iii. Set the *Type* to *credit-card* and click *OK*.
iv. Click *OK* to save the dictionary.

2. Configure the DLP sensor:
a. Go to *Security Profiles > Data Loss Prevention*, select the *Sensors* tab, and click *Create New*.
b. Enter a name (*Finance_Credit_Card_High*).
c. In the *Sensor Entries* section, click *Create New*.
d. Set the *Dictionary* to *Finance_Credit_Card_Visa* and click *OK*.
e. Repeat the previous step twice to add *Finance_Credit_Card_Mastercard* and *CC_Number* in this order.
f. Click *OK* to save the sensor.
g. Edit the newly created sensor.
h. Set the *Logical relationship* to *Evaluate*.
i. In the *Evaluated by* field, enter *(dict(1) > 0 && dict(3) > 0) || (dict(2) > 0 && dict(3) > 0)*.
j. Click *OK* to save the sensor.



For the DLP sensor with the *Logical relationship* set to *Evaluate*, *Count* and *Status* of any sensor entry will be ignored.

3. Configure the DLP profile:
a. Go to *Security Profiles > Data Loss Prevention*, select the *Profiles* tab, and click *Create New*.
b. Enter a name (*cc-block*).
c. In the *Rules* section, click *Create New*.
d. Configure the following settings:

Name	*1*
Sensors	*Finance Credit Card High*
Severity	*Critical*
Action	*Block*
Type	*File*

File type	*builtin-patterns*
Protocol	*HTTP-POST*, *HTTP-GET*

e. Click *OK*.
f. Click *OK* to save the profile.

4. Add the DLP profile to a policy:
   a. Go to *Policy & Objects* > *Policy* and click *Create New*.
   b. Set the *Type* to any except *SSH Tunnel* which does not support DLP.
   c. In the *Security Profiles* section, enable *DLP Profile* and select *cc-block*.
   d. Set *SSL/SSH Inspection* to *deep-inspection* to inspect HTTPS traffic.
   e. Configure the other settings as needed.
   f. Click *OK*.

When a Visa or Mastercard credit card is included in HTTP GET or POST traffic, the file is blocked and a DLP log is generated. See the Sample log on page 701 for details on how to test this configuration.

To block HTTPS upload traffic that includes Visa or Mastercard credit card information in the CLI:

1. Configure the DLP dictionary:

```
config dlp dictionary
    edit "Finance_Credit_Card_Visa"
        config entries
            edit 1
                set type "regex"
                set pattern "4[0-9]{12}(?:[0-9]{3})"
                set repeat enable
                set comment "Visa"
            next
        end
    next
    edit "Finance_Credit_Card_Mastercard"
        config entries
            edit 1
                set type "regex"
                set pattern "(?:5[1-5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-9]{2}|27[01][0-
9]|2720)[0-9]{12}"
                set repeat enable
                set comment "Mastercard"
            next
        end
    next
    edit "CC_Number"
        config entries
            edit 1
                set type "credit-card"
            next
        end
    next
end
```

2. Configure the DLP sensor:

```
config dlp sensor
    edit "Finance_Credit_Card_High"
        config entries
            edit 1
                   set dictionary "Finance_Credit_Card_Visa"
            next
            edit 2
                set dictionary "Finance_Credit_Card_Mastercard"
            next
            edit 3
                set dictionary "CC_Number"
            next
        end
        set match-type match-eval
        set eval "(dict(1) > 0 && dict(3) > 0) || (dict(2) > 0 && dict(3) > 0)"
    next
end
```

3. Configure the DLP profile:

```
config dlp profile
    edit "cc_block"
        set feature-set proxy
        config rule
            edit 1
                set name "1"
                set severity critical
                set proto http-get http-post
                set filter-by sensor
                set file-type 1
                set sensor "Finance_Credit_Card_High"
                set action block
            next
        end
    next
end
```

4. Add the DLP profile to a policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set dlp-profile "cc_block"
```

```
    next
end
```

When a Visa or Mastercard credit card is included in HTTP GET or POST traffic, a replacement message appears because it is blocked. A DLP log is generated. See the Sample log on page 701 for details on how to test this configuration.

Sample log

From Windows, the following command can be used to generate a sample log via HTTP POST traffic, using the cURL tool to post data, which contains a sample Visa credit card number. See sample data at https://dlptest.ai/ for sample credit card numbers.

```
# curl -k -d 4024007149133315 https://192.168.10.13/cc.doc -o?

1: date=2023-03-17 time=15:37:41 eventtime=1679092660998869199 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" filteridx=1 filtername="1"
dlpextra="builtin-patterns;Finance_Credit_Card_High" filtertype="sensor" filtercat="file"
severity="critical" policyid=1 poluuid="26540ed0-ae54-51ed-80eb-89af8af4d53f" policytype="policy"
sessionid=14854 epoch=570215534 eventid=0 srcip=172.20.120.13 srcport=58012 srccountry="Reserved"
srcintf="port2" srcintfrole="undefined" srcuuid="3342cb44-9140-51ed-5dbe-8e0787bedeec"
dstip=192.168.10.13 dstport=443 dstcountry="Reserved" dstintf="port3" dstintfrole="wan"
dstuuid="3342cb44-9140-51ed-5dbe-8e0787bedeec" proto=6 service="HTTPS" filetype="msoffice"
direction="incoming" action="block" hostname="192.168.10.13" url="https://192.168.10.13/cc.doc"
agent="curl/7.83.1" httpmethod="POST" filename="cc.doc" filesize=12288 profile="cc-block"
```

Block access to LLM applications using keywords and FQDN

Large language models (LLMs), such as GPT, are a type of Generative AI (GenAI) and are widely used in applications like chatbots. This configuration will block HTTPS upload traffic to LLM applications that include sensitive keywords. The pre-defined data type, keyword, is used in the Data Loss Prevention (DLP) dictionary.



Web-based chatbot implementations are dynamic and and can exhibit a wide range of variations. To maximize the effectiveness of blocking unwanted keywords, it is advised to add both a message and a file-based DLP rule. While this method enhances detection, it may not be entirely infallible. For optimal protection, it is recommended to restrict access to LLM applications.

To entirely prevent access to LLM applications, use a web filter profile with the FortiGuard *Artificial Intelligence Technology* category set to block.

To confirm that the URL of the LLM application that you need to block is in the *Artificial Intelligence Technology* category. The URL category can be verified using the FortiGuard Web Filter Lookup.



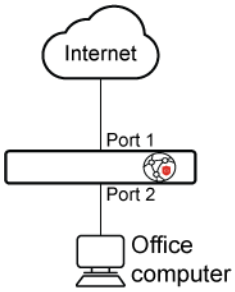
When utilizing commonly-used SSL-encrypted protocols such as HTTPS, SMTPS, POP3S, IMAPS, and FTPS, SSL inspection must be set to Deep Inspection. See SSL/SSH Inspection on page 625 for more information.

Additionally, the client machine must have the corresponding deep inspection Certificate Authority (CA) certificate installed.

Example

In this example, a user is conducting a search on an LLM application in the Chrome browser on an office computer, using a sensitive keyword that has been configured in the DLP dictionary. The FortiProxy intercepts this traffic using deep inspection and prevents the search that contains sensitive keywords because it matches the DLP profile that has been set up on this FortiProxy.

When a sensitive keyword is included in HTTPS upload traffic, the request is blocked and a DLP log is generated.



To block HTTPS upload traffic that includes sensitive keywords in the GUI:

1. Configure the DLP dictionary:
   a. Go to *Security Profiles* > *Data Loss Prevention*, select the *Dictionary* tab, then click *Create New*.
   b. Set *Name* to *llmapps*.
   c. In the *Dictionary Entries* table click *Create New*:
      i. Set *Type* to *keyword*.
      ii. Set *Pattern* to *fortinet*.
      iii. Enable *Case sensitive*.
      iv. Click *OK*.
   d. Repeat step c and set *Pattern* to *source code*.
   e. Click *OK*.
2. Configure the DLP sensor:
   a. Go to *Security Profiles* > *Data Loss Prevention*, select the *Sensor* tab, then click *Create New*.
   b. Set *Name* to *llmapps*.
   c. In the *Sensor Entries* section, click *Add*. The *Select Entries* pane is displayed.
   d. Select *Managed Locally* from the dropdown menu.
   e. Select *llmapps* and click *Apply*.
   f. Click *OK*.
3. Configure the DLP profile:
   a. Go to *Security Profiles* > *Data Loss Prevention*, select the *Profile* tab, then click *Create New*.
   b. Set *Name* to *llmapps*.
   c. In the *Rules* section, click *Create New*:

i. Configure the following settings:

Name	llmapps1
Sensors	llmapps
Severity	Critical
Action	Block
Type	File
File type	builtin-patterns
Protocol	HTTP-POST

ii. Click *OK*.

d. In the *Rules* section, click *Create New* again:

i. Configure the following settings:

Name	llmapps2
Sensors	llmapps
Severity	Critical
Action	Block
Type	Message
Protocol	HTTP-POST

ii. Click *OK*.

e. Click *OK* to save the profile.

f. Unset the file type option to enable filtering of all file types, including unknown ones:

```
config dlp profile
    edit "llmapps"
        config rule
            edit 1
                unset file-type
            next
        end
    next
end
```

4. Configure the firewall address for the LLM application:

a. Go to *Policy & Objects* > *Addresses*, select the *Standard* tab, then click *Create New*.

b. Set the following:

Name	<name>
Type	FQDN
FQDN	See FQDN on page 706 for the FQDN on the specific LLM application.

c. Click *OK*.

5. Add the firewall address to a group:
   a. Go to *Policy & Objects* > *Addresses*, select the *Address Group* tab, then click *Create New*.
   b. Set the following:

Group name	llmapps
Members	ChatGpt, Gemini, DeepSeek

6. Add the DLP profile and the address group to a policy:
   a. Go to *Policy & Objects* > *Policy* and click *Create New*.
   b. Set the *Destination* to *llmapps*.
   c. In the *Security Profiles* section:
      i. Enable *Application control* and select the profile that *QUIC* is blocked in. In this example, the *default* profile is selected.
      ii. Enable *DLP Profile* and select *llmapps*.
   d. Set *SSL Inspection* to *deep-inspection*.
   e. Configure the other settings as needed.
   f. Click *OK*.

To block HTTPS upload traffic that includes sensitive keywords in the CLI:

1. Configure the DLP dictionary:

```
config dlp dictionary
    edit "llmapps"
        config entries
            edit 1
                set type "keyword"
                set pattern "source code"
                set ignore-case enable
            next
            edit 2
                set type "keyword"
                set pattern "fortinet"
                set ignore-case enable
            next
        end
    next
end
```

2. Configure the DLP sensor:

```
config dlp sensor
    edit "llmapps"
        config entries
            edit 1
                set dictionary "llmapps"
            next
        end
```

```
    next
end
```

3. Configure the DLP profile:

```
config dlp profile
    edit "llmapps"
        set feature-set proxy
        config rule
            edit 1
                set name "llmapps1"
                set severity critical
                set proto http-post
                set filter-by sensor
                set sensor "llmapps"
                set action block
            next
            edit 2
                set name "llmapps2"
                set type message
                set proto http-post
                set filter-by sensor
                set sensor "llmapps"
                set action block
            next
        end
    next
end
```

4. Configure the firewall address for the LLM application:

```
config firewall address
    edit <name>
        set type fqdn
        set fqdn <string>
    next
end
```

See FQDN on page 706 for the FQDN on the specific LLM application.

5. Add the firewall addresses to a group:

```
config firewall addrgrp
    edit "llmapps"
        set member "ChatGpt" "Gemini" "DeepSeek"
    next
end
```

6. Add the DLP profile and the FQDN address to a firewall policy:

```
config firewall policy
    edit 1
        set name "llmapps "
```

```
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "llmapps"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "deep-inspection"
        set dlp-profile "llmapps"
        set application-list "default"
        set nat enable
    next
end
```

FQDN

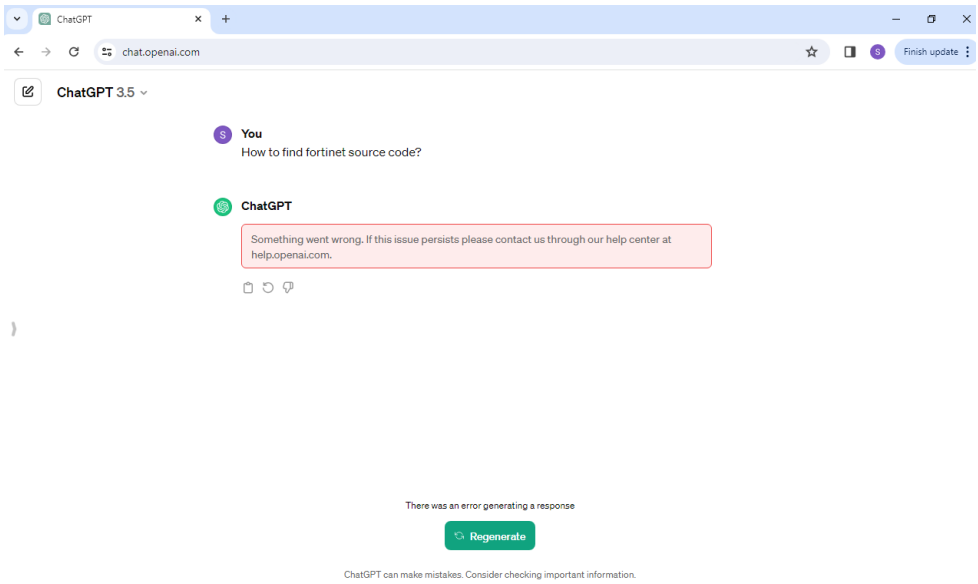
A firewall address should be created for each LLM application:

LLM application	FQDN
ChatGPT	*chat.openai.com*
Gemini	*gemini.google.com*
DeepSeek	*chat.deepseek.com*

Verification

ChatGPT:

1. Visit https://chat.openai.com.
2. Search for any phrase that includes keywords set up in the DLP dictionary.

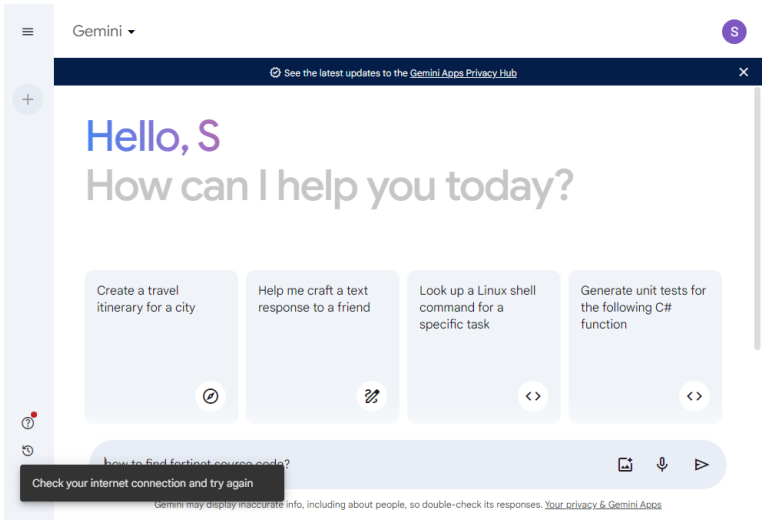


3. Verify that the request failed and an error was generated.
4. Review the log that was generated when the attempt was made to send an HTTP POST request containing sensitive keywords:

```
1: date=2024-03-15 time=09:59:35 eventtime=1710453575538415503 tz="+1200" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" ruleid=1
rulename="llmapps1" dlpextra="Sensor 'llmapps' matching any: ('llmapps'=1) >= 1; match."
filtertype="sensor" filtercat="file" severity="critical" policyid=1 poluuid="eea32b46-db4e-
51ee-92a9-b46e5580db33" policytype="policy" sessionid=69254 epoch=424445846 eventid=1
srcip=13.13.13.13 srcport=56747 srccountry="United States" srcintf="port2"
srcintfrole="undefined" srcuuid="d2f06fda-15e7-51ee-0d22-faaf5170dad2" dstip=104.18.37.228
dstport=443 dstcountry="United States" dstintf="port1" dstintfrole="undefined"
```

Gemini:

1. Visit https://gemini.google.com .
2. Search for any phrase that includes keywords set up in the DLP dictionary.

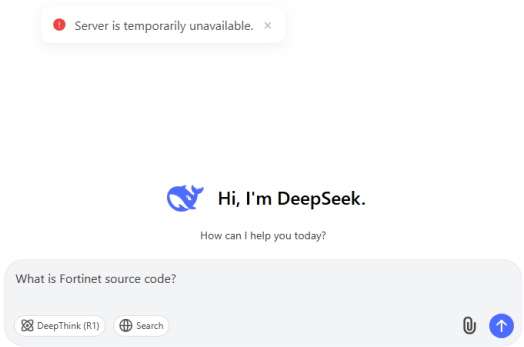


3. Verify that the request failed and an error was generated.
4. Review the log that was generated when the attempt was made to send an HTTP POST request containing sensitive keywords:

```
1: date=2024-03-15 time=12:46:08 eventtime=1710463568053453203 tz="+1200" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" ruleid=1
rulename="llmapps1" dlpextra="Sensor 'llmapps' matching any: ('llmapps'=1) >= 1; match."
filtertype="sensor" filtercat="file" severity="critical" policyid=1 poluuid="eea32b46-db4e-
51ee-92a9-b46e5580db33" policytype="policy" sessionid=77832 epoch=424449372 eventid=1
srcip=13.13.13.13 srcport=58137 srccountry="United States" srcintf="port2"
srcintfrole="undefined" srcuuid="d2f06fda-15e7-51ee-0d22-faaf5170dad2" dstip=142.251.33.110
dstport=443 dstcountry="United States" dstintf="port1" dstintfrole="undefined"
dstuuid="d2f06fda-15e7-51ee-0d22-faaf5170dad2" proto=6 service="HTTPS" filetype="unknown"
direction="outgoing" action="block" hostname="gemini.google.com"
url="https://gemini.google.com/_
/BardChatUi/data/assistant.lamda.BardFrontendService/StreamGenerate?bl=boq_assistant-bard-web-
server_20240313.09_p0&f.sid=2103257702826212605&hl=en&_reqid=1474614&rt=c" agent="Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0
Safari/537.36" httpmethod="POST" referralurl="https://gemini.google.com/"
filename="StreamGenerate" filesize=2211 profile="llmapps"
```

DeepSeek:

1. Visit https://chat.deepseek.com.
2. Search for any phrase that includes keywords set up in the DLP dictionary.



3. Verify that the request failed and an error was generated.
4. Review the log that was generated when the attempt was made to send an HTTP POST request containing sensitive keywords:

```
1: date=2025-03-13 time=05:42:35 eventtime=1741797755180776410 tz="+1200" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" ruleid=1
rulename="llmapps1" dlpextra="Sensor 'lmapps' matching any: ('llmapps'=2) >= 1; match."
filtertype="sensor" filtercat="file" severity="critical" policyid=3 poluuid="27681982-ff5c-
51ef-61f2-c3db5a98100c" policytype="policy" sessionid=22163 epoch=1199369450 eventid=1
srcip=10.10.10.13 srcport=65353 srccountry="Reserved" srcintf="port2" srcintfrole="undefined"
srcuuid="d2f06fda-15e7-51ee-0d22-faaf5170dad2" dstip=104.18.27.90 dstport=443
dstcountry="United States" dstintf="port1" dstintfrole="undefined" dstuuid="bb60c556-ff59-
51ef-216d-86ad81ccf871" proto=6 service="HTTPS" filetype="unknown" direction="outgoing"
action="block" hostname="chat.deepseek.com"
```

```
url="https://chat.deepseek.com/api/v0/chat/completion" agent="Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
httpmethod="POST" referralurl="https://chat.deepseek.com/a/chat/s/fcd6fce1-bdd8-4999-b49f-
c27eacb1f960" filename="completion" filesize=187 profile="llmapps"
```

Proximity search

In this example, any HTTPS upload traffic containing both a keyword and a username within a specified proximity can be identified. The FortiProxy intercepts this traffic through deep inspection. When HTTPS upload traffic includes both a keyword and a username, which match the criteria defined on the data loss prevention (DLP) profile configured on the FortiProxy, the traffic is blocked. This action subsequently generates a DLP log. See Verification on page 712 for a log sample.

To block HTTPS upload traffic that match the DLP profile in the GUI:

1. Configure the DLP dictionary:
   a. Go to *Security Profiles* > *Data Loss Prevention* and select the *Dictionaries* tab.
   b. Select *Create New*.
   c. Set *Name* to: *matcharound*.
   d. In the *Dictionary Entries* table, click *Create New*:
      i. Set *Type* to *keyword*
      ii. Set *Pattern* to *user*
      iii. Enable *Case sensitive*
      iv. Click *OK*.
   e. Click *OK*.
   f. Select the newly created dictionary and click *Edit*.
   g. Select *Edit in CLI* and enter the following command:
   ```
   #set match-around enable
   end
   ```
   h. Close the CLI Console and click *Cancel*.



DLP data types can only be configured in the CLI. See step 2 of To block HTTPS upload traffic that match the DLP profile in the CLI: on page 710.

2. Configure the DLP dictionary:
   a. Go to *Security Profiles* > *Data Loss Prevention* and select the *Dictionaries* tab.
   b. Click *Create New*.
   c. Set *Name* to *username*.
   d. In the *Dictionary Entries* table, click *Create New*:
      i. Set *Type* to *user*
      ii. Click *OK*.
   e. Click *OK*.
3. Configure the DLP sensor:

a. Go to *Security Profiles > Data Loss Prevention* and select the *Sensors* tab.
b. Click *Create New*.
c. Enter a name *(user)*.
d. In the *Sensor Entries* section, click *Create New*.
e. Set the *sensor entry* to *username* and click *OK*.
f. Click *OK* to save the sensor.

4. Configure the DLP profile:
   a. Go to *Security Profiles > Data Loss Prevention* and select the *Profiles* tab.
   b. Click *Create New*.
   c. Enter a name *(keyword)*.
   d. In the *Rules* section, click *Create New*.
   e. Configure the following settings:

Name	*keyword*
Data source type	*Sensor*
Sensors	*user*
Severity	*Critical*
Action	*Block*
Match Type	*Message*
Protocol	*HTTP-POST*

   f. Click *OK*.
   g. Click *OK* to save the profile.
5. Add the DLP profile to a policy:
   a. Go to *Policy & Objects > Policy* and click *Create New*.
   b. In the *Security Profiles* section, enable *DLP Profile* and select *keyword*.
   c. Set *SSL/SSH Inspection* to *deep-inspection* to inspect HTTPS traffic.
   d. Configure the other settings, as needed.
   e. Click *OK*.

To block HTTPS upload traffic that match the DLP profile in the CLI:

1. Configure the DLP dictionary:

```
config dlp dictionary
       edit "matcharound"
       set match-around enable
               config entries
                       edit 1
                               set type "keyword"
                               set pattern "user"
                               set ignore-case enable
                       next
               end
```

```
        next
end
```

2. Configure the DLP data type:

```
config dlp data-type
        edit "user"
                set pattern "\\b[a-zA-Z]{6,12}\\b"
                set verify "(?<=@)\\w+"
                set match-around "matcharound"
                set look-back 13
                set match-back 15
        next
end
```



The pattern specified using the `set pattern` command, is designed to match any word, irrespective of case sensitivity, that contains between 6 and 12 characters. On the other hand, the pattern specified using the `set verify` command employs a positive lookbehind assertion. This assertion checks for the presence of the @ symbol preceding the word, without including it in the match. This is a feature supported in PCRE but not in Hyperscan. For a match to occur, the content must satisfy all parameters defined in the DLP Data type.

3. Configure the DLP dictionary:

```
config dlp dictionary
        edit "username"
                config entries
                        edit 1
                                set type "user"
                        next
                end
        next
end
```

4. Configure the DLP sensor:

```
config dlp sensor
        edit "user"
                config entries
                        edit 1
                        set dictionary "username"
                next
        end
 next
end
```

5. Configure the DLP profile:

```
config dlp profile
       edit "keyword"
               config rule
               edit 1
                       set name "keyword"
                       set severity critical
                       set type message
                       set proto http-post
                       set filter-by sensor
                       set sensor "user"
                       set action block
               next
       end
 next
end
```

6. Add the DLP profile to a policy:

```
config firewall policy
       edit 1
               set name "keyword"
               set srcintf "port2"
               set dstintf "port1"
               set action accept
               set srcaddr "all"
               set dstaddr "all"
               set schedule "always"
               set service "ALL"
               set utm-status enable
               set ssl-ssh-profile "deep-inspection"
               set dlp-profile "keyword"
               set logtraffic all
               set nat enable
       next
end
```

Verification

1. Visit https://dlptest.ai.
2. Enter any phrase that will match the DLP profile configured on the FortiProxy and click *Submit*.
   Example:
   user: @kikinaynay
3. Verify that the replacement message indicates the transfer attempt has been blocked.
4. Review the log that was generated when the attempt was made to send an HTTP POST request containing sensitive keywords:
   `1: date=2024-06-11 time=11:53:10 eventtime=1718131990428533349 tz="-0700" logid="0954024576" type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root"`

```
ruleid=1 rulename="keyword" filtertype="sensor" filtercat="message" severity="critical"
policyid=1 poluuid="c0a2e814-7ff8-51ee-1815-054bdf34bd03" policytype="policy"
sessionid=486254337 epoch=1186366517 eventid=1 srcip=10.40.1.1 srcport=65112
srccountry="Reserved" srcintf="port1" srcintfrole="undefined" srcuuid="0e3359c4-5fa7-51ed-
6fd1-9862a5c10176" dstip=35.209.95.242 dstport=443 dstcountry="United States"
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS" filetype="N/A"
direction="outgoing" action="block" hostname="dlptest.ai" url=" https://dlptest.ai"
agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0"
httpmethod="POST" referralurl=" https://dlptest.ai" profile="keyword"
```

Assign confidence levels in FortiGuard managed DLP dictionaries

Users can select a FortiGuard dictionary with varying confidence levels based on their specific requirements.

- The high level provides maximum precision to minimize false positives.
- The medium level balances match quantity and precision.
- The low level captures the most matches, but may result in more false positives.



A valid DLP license is required to obtain the latest package.

When applying a FortiGuard built-in dictionary to a custom sensor, the dictionary with the highest confidence level is selected by default.

Use case examples

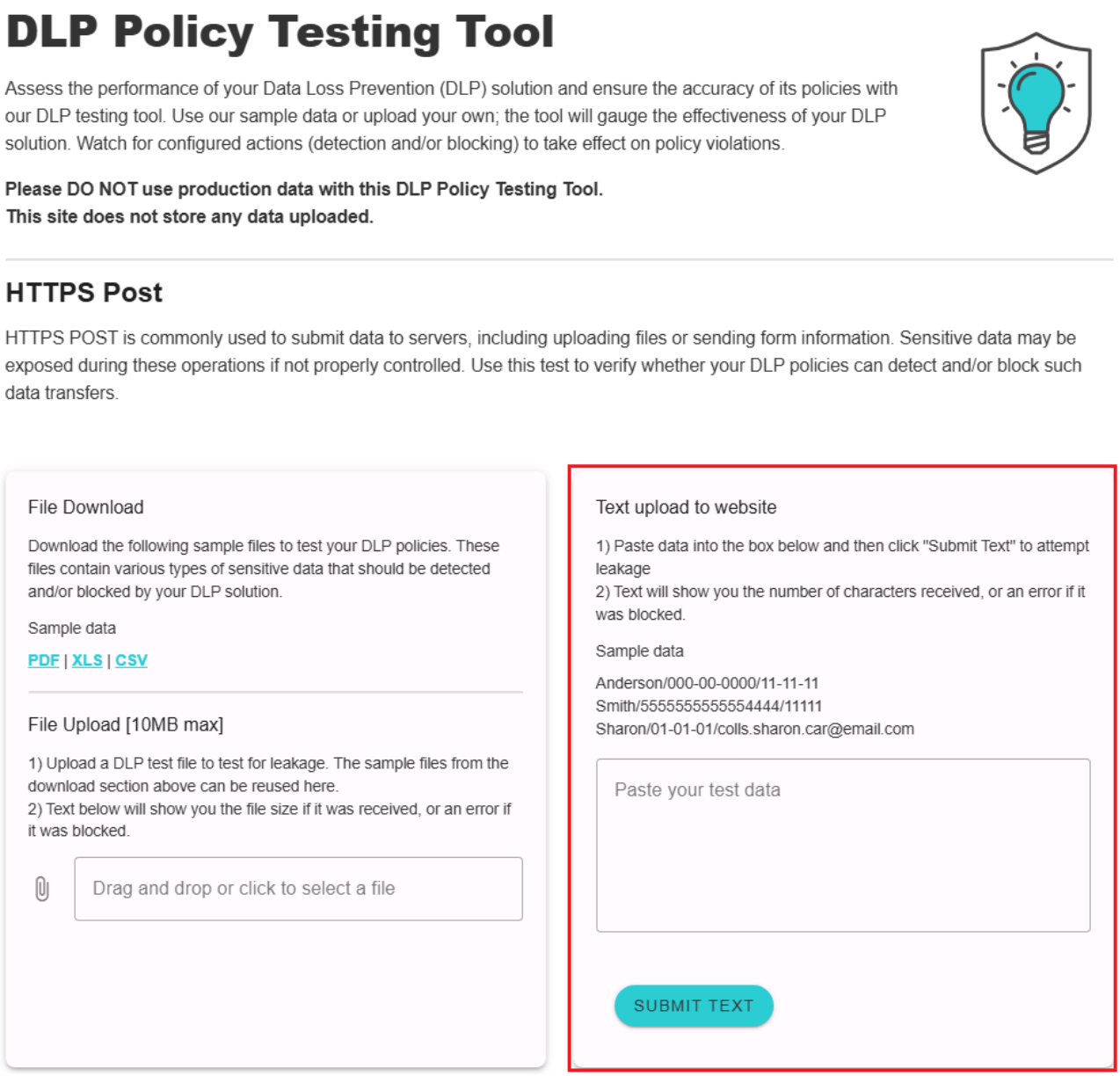
In these use case examples, various Canadian Social Insurance Number (SIN) formats are tested at different confidence levels using different protocols.

SIN format	Low Confidence Matching criteria: regular expression, data validation	Medium Confidence Matching criteria: regular expression, data validation SIN format validation	High Confidence Matching criteria: regular expression, data validation, SIN format validation, Match-around data
815489034	match	does not match	does not match
193849270	match	match	does not match
sin# 193849270	match	match	match

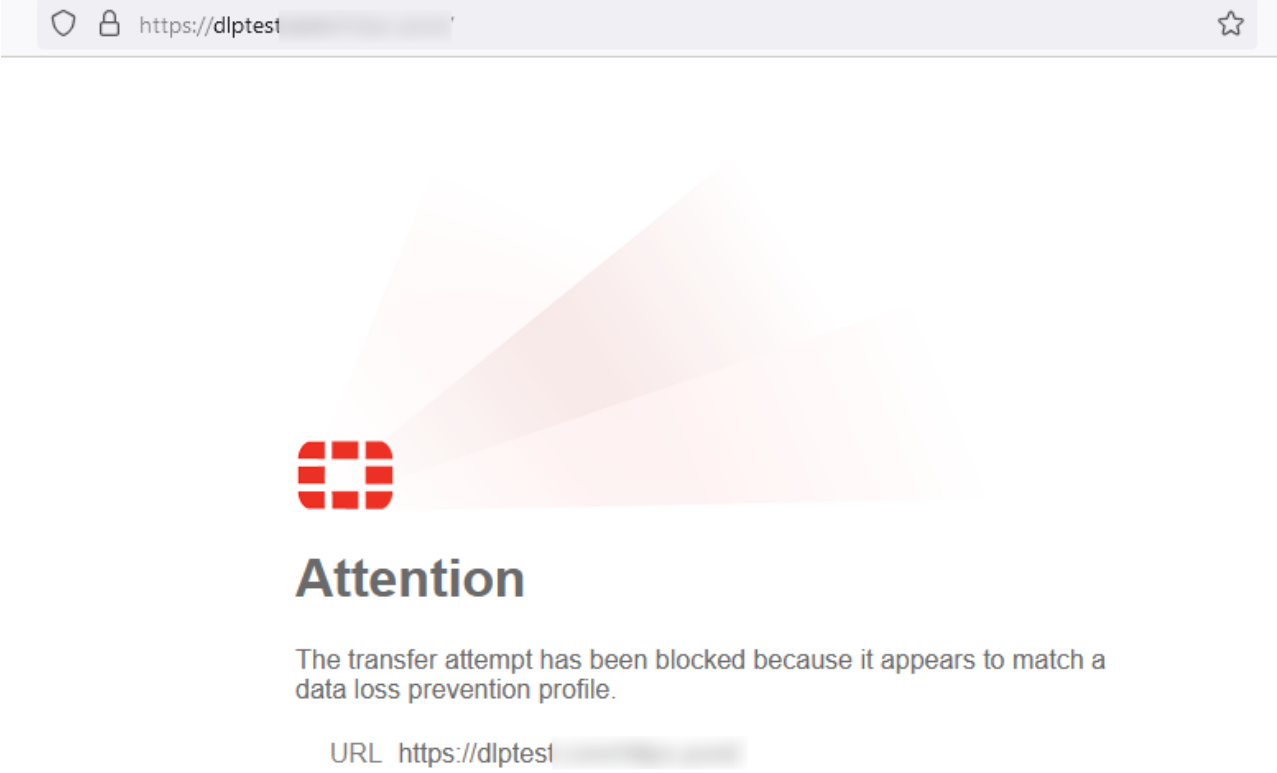
To verify that a FortiGuard dictionary with the low confidence level will block matching message through an HTTPS post:

1. Configure a DLP profile with a DLP sensor that uses the Canadian SIN card dictionary (`fg-can-natl_id-sin-dict`) DLP dictionary with the *Confidence level* set to *Low* and then use the profile in a policy.

2. Test that an HTTPS message containing a SIN is blocked. DLP Test can be used to send a test message:



The message is blocked:

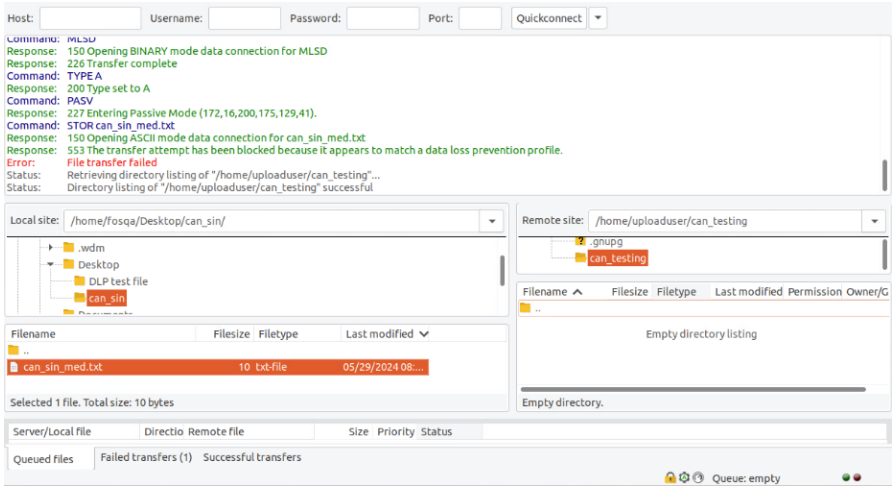


3. Go to *Log & Report* > *Security Events* and view the *Data Loss Prevention* logs matching the *can-natl_id-sin-dict-low* dictionary.
4. Check the raw logs:

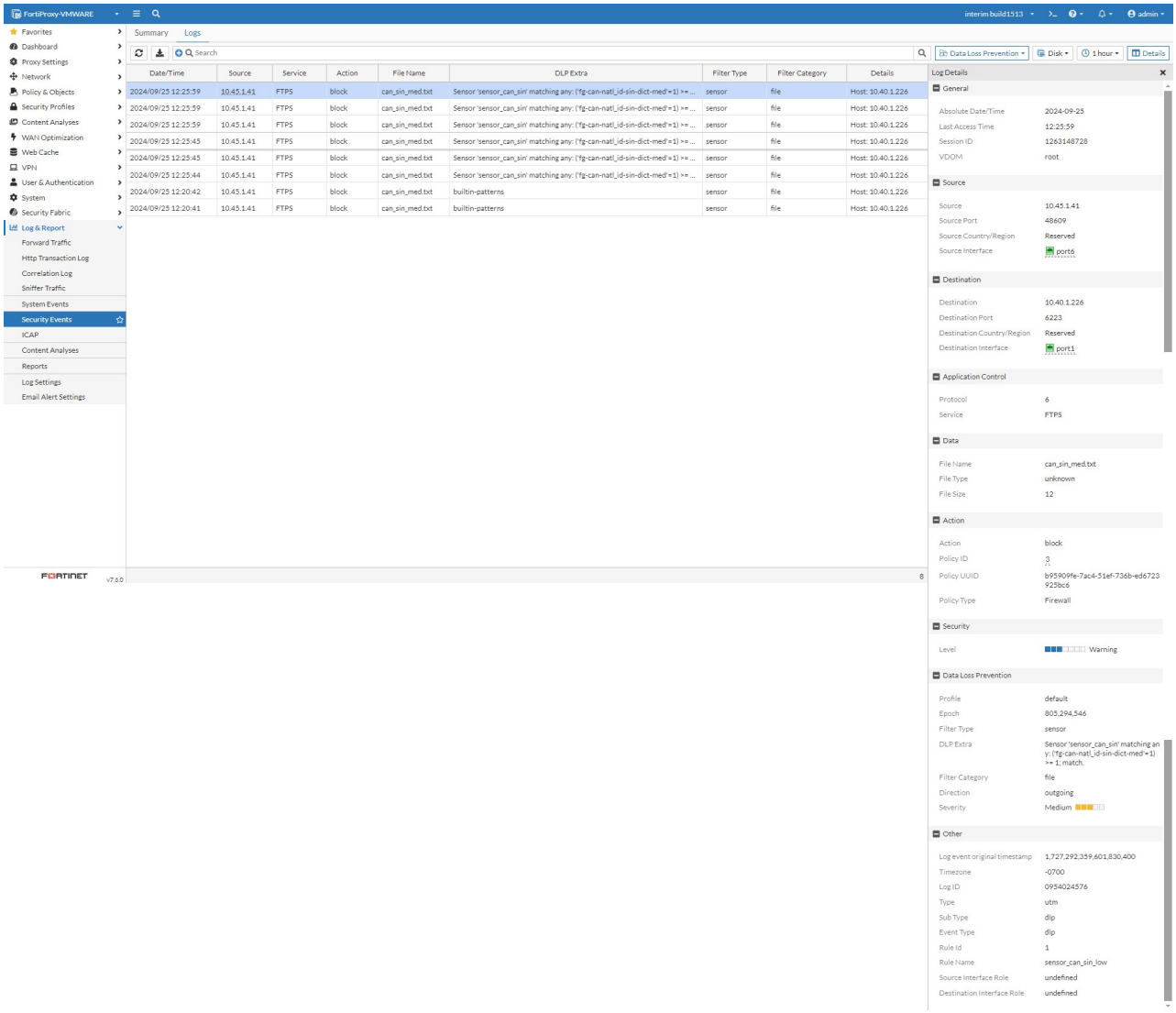
```
1: date=2024-05-29 time=16:55:27 eventtime=1717026926501493215 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="vdom1" ruleid=1 rulename="sensor_
can_sin_low" dlpextra="Sensor 'sensor_can_sin_low' matching any: ('g-fg-can-natl_id-sin-dict-
low'=1) >= 1; match." filtertype="sensor" filtercat="message" severity="medium" policyid=1
poluuid="a084e3dc-1d48-51ef-5286-940d89557186" policytype="policy" sessionid=64304
epoch=2100732550 eventid=1 srcip=10.1.100.241 srcport=34184 srccountry="Reserved"
srcintf="port2" srcintfrole="undefined" srcuuid="5a9d01f6-1d48-51ef-1c5f-c5a49f106988"
dstip=35.209.95.242 dstport=443 dstcountry="United States" dstintf="port1"
dstintfrole="undefined" dstuuid="5a9d01f6-1d48-51ef-1c5f-c5a49f106988" proto=6 service="HTTPS"
filetype="N/A" direction="outgoing" action="block" hostname="dlptest.ai"
url="https://dlptest.ai" agent="Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.0.0 Safari/537.36" httpmethod="POST" referralurl="https://dlptest.ai"
profile="customer_can_sin"
```

To verify that a FortiGuard dictionary with medium confidence level will block matching message through a FTPS post:

1. Configure a DLP profile with a DLP sensor that uses the Canadian SIN card dictionary (`fg-can-natl_id-sin-dict`) DLP dictionary with the *Confidence level* set to *Medium* and then use the profile in a policy.
2. Test that posting a file that contains `193849270` is blocked.



3. Go to *Log & Report > Security Events* and view the *Data Loss Prevention* logs matching the *can-natl_id-sin-dict-med* dictionary.



4. Check the raw logs:

```
1: date=2024-09-25 time=12:25:59 eventtime=1727292359601830454 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" ruleid=1 rulename="sensor_
can_sin_med" dlpextra="Sensor 'sensor_can_sin' matching any: ('fg-can-natl_id-sin-dict-med'=1)
>= 1; match." filtertype="sensor" filtercat="file" severity="medium" policyid=3
poluuid="b95909fe-7ac4-51ef-736b-ed6723925bc6" policytype="policy" sessionid=1263148728
epoch=805294546 eventid=0 srcip=10.45.1.41 srcport=48609 srccountry="Reserved" srcintf="port6"
srcintfrole="undefined" dstip=10.40.1.226 dstport=6223 dstcountry="Reserved" dstintf="port1"
dstintfrole="undefined" proto=6 service="FTPS" filetype="unknown" direction="outgoing"
action="block" filename="can_sin_med.txt" filesize=12 profile="default"
```

To verify that the FortiGuard dictionary with a high confidence level will block matching message through an SMTP post:

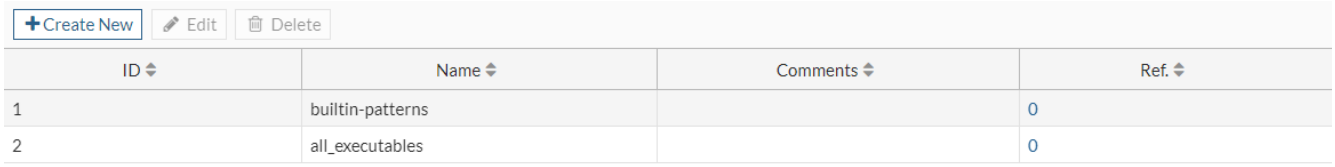
1. Configure a DLP profile with a DLP sensor that uses the Canadian SIN card dictionary (`fg-can-natl_id-sin-dict`) DLP dictionary with the *Confidence level* set to *High* and then use the profile in a policy.
2. Test that sending email with an attached file that contains `sin# 193849270` is blocked.
3. Go to *Log & Report* > *Security Events* and view the *Data Loss Prevention* logs matching the *can-natl_id-sin-dict-high* dictionary.
4. Check the raw logs:

```
1: date=2024-09-25 time=13:11:00 eventtime=1727295059589158625 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="root" ruleid=1 rulename="sensor_
can_sin_high" dlpextra="Sensor 'sensor_can_sin' matching any: ('fg-can-natl_id-sin-dict-
high'=1) >= 1; match." filtertype="sensor" filtercat="file" severity="medium" policyid=3
sessionid=168480999 epoch=1488425925 eventid=2 srcip=10.40.1.229 srcport=0
srccountry="Reserved" srcintf="unknown-0" srcintfrole="undefined" dstip=52.96.166.82
dstport=587 dstcountry="United States" dstintf="unknown-0" dstintfrole="undefined" proto=6
service="SMTPS" filetype="unknown" direction="outgoing" action="block"
from="annasundayhi@outlook.com" to="annasundayhi@outlook.com"
sender="annasundayhi@outlook.com" recipient="annasundayhi@outlook.com" subject="718485"
attachment="yes" filename="can_sin_high.txt" filesize=15 profile="default"
```

DLP File Pattern

DLP file patterns match selected file types and file patterns. They are used as DLP filter rules in DLP sensors.

To view available DLP file patterns, go to *Security Profiles* > *DLP File Pattern*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a DLP file pattern. See Create or edit a DLP file pattern on page 718.
Edit	Modify the selected DLP file pattern. See Create or edit a DLP file pattern on page 718.
Delete	Remove the selected DLP file pattern.
ID	Identifier for the DLP file pattern.
Name	The name of the DLP file pattern.
Comments	An optional description of the DLP file pattern.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a DLP file pattern

You can create or edit DLP file patterns.

To create a DLP file pattern:

1. Go to *Security Profiles* > *DLP File Pattern*.
2. Click *Create New*. The *Create DLP File Pattern* window opens.
3. Enter an identifier for the DLP file pattern.
4. Enter a name for the DLP file pattern.
5. Enter an optional description of the DLP file pattern.
6. Select one or more file types.
7. Enter one or more file patterns.
8. Click *OK* to save the DLP file pattern.

To edit a DLP file pattern:

1. Go to *Security Profiles* > *DLP File Pattern*.
2. Select a DLP file pattern and then click *Edit*.
3. Edit the settings as required.
4. Click *OK* to save your changes to the DLP file pattern.

Content Analyses

Content Analysis Service is an automated computer vision AI that detects visual threats including pornography, extremism, and graphic violence. Content Analysis empowers your application with AI content moderation that recognizes threats in images of the following types:

- BMP
- JPEG
- PNG
- TIFF

Internet Content Adaptation Protocol (ICAP) allows for the offloading of certain processes to a separate server so that your FortiProxy firewall can optimize its resources and maintain the best level of performance possible.

This section covers the following topics:



By default, ICAP-related tabs are not visible in the tree menu in the GUI. To make them visible, go to *System > Feature Visibility* and enable *ICAP*. See Feature Visibility on page 970 for more information.

- Image Analysis on page 719
- ICAP Profile on page 724
- ICAP Remote Server on page 729
- ICAP Load Balancing on page 731
- ICAP Local Server on page 732
- ICAP scanning with FTP on page 736

Image Analysis

Content Analysis is a licensed feature, powered by AI that detects visual threats including pornography, extremism, graphic violence, and other inappropriate Not Safe for Work (NSFW) visual content in images of the following types:

- BMP
- JPEG
- PNG
- TIFF

This service is a real-time analysis of the content passing through the FortiProxy unit. The Content Analysis Service uses advanced artificial intelligence that delivers unparalleled accuracy with near zero false positives, all in a matter of milliseconds. After inappropriate NSFW content is detected, such content can be optionally blocked or reported. Unlike early heuristic-based technologies the AI-

powered Content Analysis Service has been extensively trained and developed, and more NSFW-relevant Threat Categories are being added as they become available.

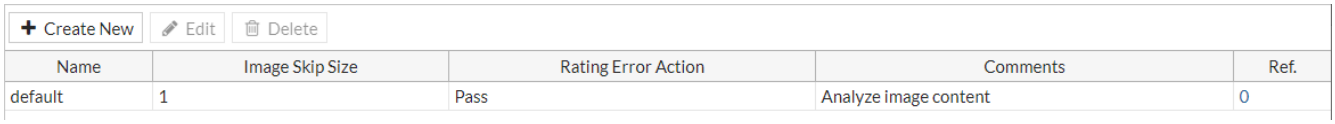
In general, the procedure is similar to the HTTP antivirus scanning procedure.

When a client HTTP requests an image, the HTTP header content-type determines the image type. Then the WAD process holds the image content from the server for scanning before sending it to the client.

If the scan results are larger than the configurable threshold, the requested image is blocked, and the client receives a replacement image. This replacement image keeps the same image type and size if you enable the option to re-size images. The FortiProxy unit stores the results to improve performance for future requests.

The default settings provide a good balance, but they might require some adjustment in some instances.

To use Content Analysis, you need to set up at least one profile and apply it to a policy. Content Analysis profiles are configured under *Content Analyses* > *Image Analyses*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a Content Analysis profile. See Create or edit an Image Analysis profile on page 721.
Edit	Modify the selected Content Analysis profile. See Create or edit an Image Analysis profile on page 721.
Delete	Remove the selected Content Analysis profile.
Name	The name of the Content Analysis profile.
Image Skip Size	Enter a value between 0 and 2,048. This value represents the size of image that will be skipped by the image scan unit, in kilobytes. Images that are too small are difficult to scan and are more likely to be rated incorrectly by the image scan engine. The default value is 1.
Action	Set to either *Pass* or *Block* the image when it exceeds the rating threshold. The default is *Pass*.
Comments	An optional description of the Content Analysis profile.
Ref.	Displays the number of times the object is referenced to other objects.

	To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Validating Content Analysis

You can use the following debug commands to validate the service licensing and image cache:

`get system fortiguard`—Display licensing information.

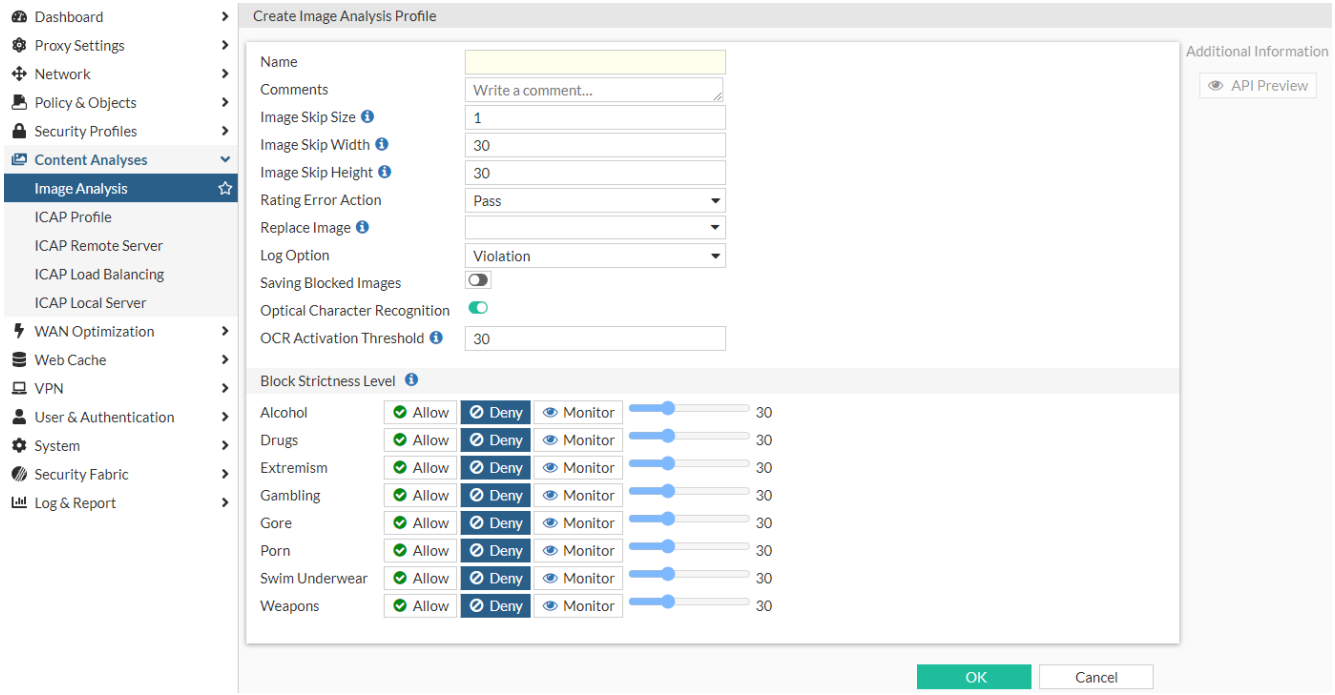
`diagnose test application wad 143`—Display image cache.

`diagnose test application wad 144`—Clear image cache.

You need a license to display and clear the image cache; otherwise, these commands are not available.

Create or edit an Image Analysis profile

Select *Create New* to open the *Create Image Analysis Profile* window.



To open the *Edit Image Analysis Profile* window, select a profile and then click *Edit*.

Configure the following settings and then click *OK*:

Name	Enter a name for this profile.
Comments	Optional description of the profile.

Image Skip Size	Enter a value between 0 and 2,048. This value represents the image size that will be skipped by the image scan unit, in kilobytes. Images that are too small are difficult to scan and are more likely to be rated incorrectly by the image scan engine. The default value is 1.
Image Skip Width	This value represents the image width that will be skipped by the image scan unit, in pixels. Images that are too small are difficult to scan and are more likely to be rated incorrectly by the image scan engine. The default value is 30 pixels; the minimum value is 5 pixels.
Image Skip Height	This value represents the image height that will be skipped by the image scan unit, in pixels. Images that are too small are difficult to scan and are more likely to be rated incorrectly by the image scan engine. The default value is 30 pixels; the minimum value is 5 pixels.
Rating Error Action	Set to either *Pass* or *Block* the image when it exceeds the rating threshold. The default is *Pass*.
Replace Image	Select a replacement image in the following formats: • JPEG • GIF • TIFF • PNG Other image types are not supported. To specify the replacement image, go to *System* > *Replacement Messages* and select *Manage Images*.
Log Option	Select *All* to log all content or *Violation* to log content that exceeds any of the strictness levels.
Saving Blocked Images	Enable to save blocked images.
Optical Character Recognition	Enable or disable optical character recognition which detects and extracts text in images with a score greater than the configured OCR threshold and takes action accordingly as defined in the DLP profile.  This option takes effect only if the policy meets the following requirements: • *Content Analysis* is enabled with this image analysis profile selected. • *DLP Profile* is enabled with a profile configured and selected.

OCR Activation Threshold		When *Optical Character Recognition* is enabled, configure the threshold to activate optical character recognition. The value range is 0 - 100, where 0 means bypassing all images without DLP and 100 means processing all images with DLP that triggers OCR. The default is 30.
Block Strictness Level		For each category, select to *Allow*, *Deny*, or *Monitor* content that exceeds the strictness level, and set the level between 0 and 100. The higher the image score, the more chance of the image being explicit. The challenge with this setting is that if you set it too high, it will block legitimate images. If you set it too low, it will allow explicit images through. If the image score is above this setting, the *Rating Error Action* is taken. The default value is 30.
	Alcohol	The alcohol category is designed to identify images containing alcoholic brands and beverages, people drinking alcohol, frat parties, keg stands, bars and nightclubs, party aftermaths, shots, beer pong, kegs, and plastic cups associated with drinking.
	Drugs	The drugs category is designed to identify images containing illegal and legal drugs, drug use, drug paraphernalia, and plants and symbols relating to drugs.
	Extremism	The extremism category is designed to identify images containing terrorist militants, beheadings, executions, propaganda, acts of terrorism, KKK rallies, Hitler, insignia related to Nazism, KKK, ISIS, and white supremacy icons.
	Gambling	The gambling category is designed to identify images containing gambling.
	Gore	The gore or graphic violence category is designed to identify images containing gore, graphic violence, self-harm, suicide, horrific imagery, bloody wounds, accident victims, shooting victims, beatings, mutilation, decapitation, and images that contain blood and guts.
	Porn	The pornography category is designed to identify images and videos containing commercial pornography, amateur pornography, sexting selfies, nudity, sex acts, grayscale pornographic images, sexually explicit cartoons, and manga.
	Swim Underwear	The swim and underwear, or risqué, category is designed to identify images containing people wearing swimwear or beachwear, underwear, and lingerie.
	Weapons	The weapons category is designed to identify images containing rifles, machine guns, handguns, grenade launchers, swords, knives, and people holding handheld weapons.

Alternatively, use the `config image-analyzer profile` command to configure an image analysis profile in the CLI.

ICAP Profile

Internet Content Adaptation Protocol (ICAP) is an application layer protocol that is used to offload tasks from the firewall to separate, specialized servers. For more information see RFC 3507.

If you enable ICAP in a policy, HTTP and HTTPS (if HTTPS inspection is supported) traffic that is intercepted by the policy is transferred to the ICAP server specified by the selected ICAP profile. Responses from the ICAP server are returned to the FortiProxy, and then forwarded to their destination

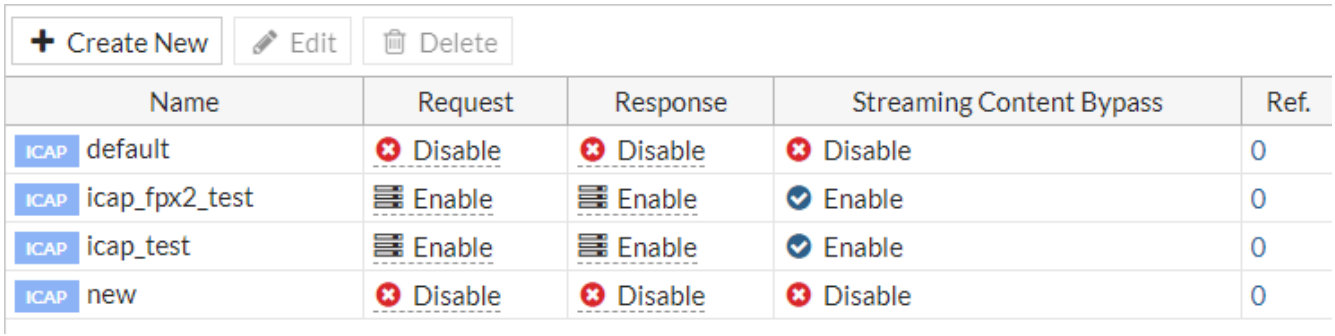


By default, ICAP is not visible in the tree menu in the GUI. To make it visible, go to *System > Feature Visibility* and enable it. See Feature Visibility on page 970 for more information.

The ICAP Profile page allows you to view and configure ICAP profiles, which you can then apply to a policy.

If you enable ICAP in a security policy, HTTP traffic intercepted by the policy is transferred to the ICAP servers in the ICAP profile added to the policy. The FortiProxy unit acts as the surrogate and carries the ICAP responses from the ICAP server to the ICAP client. The ICAP client then responds back, and the FortiProxy unit determines the action that should be taken with these ICAP responses and requests.

You can configure ICAP profiles under *Content Analyses > ICAP Profile*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

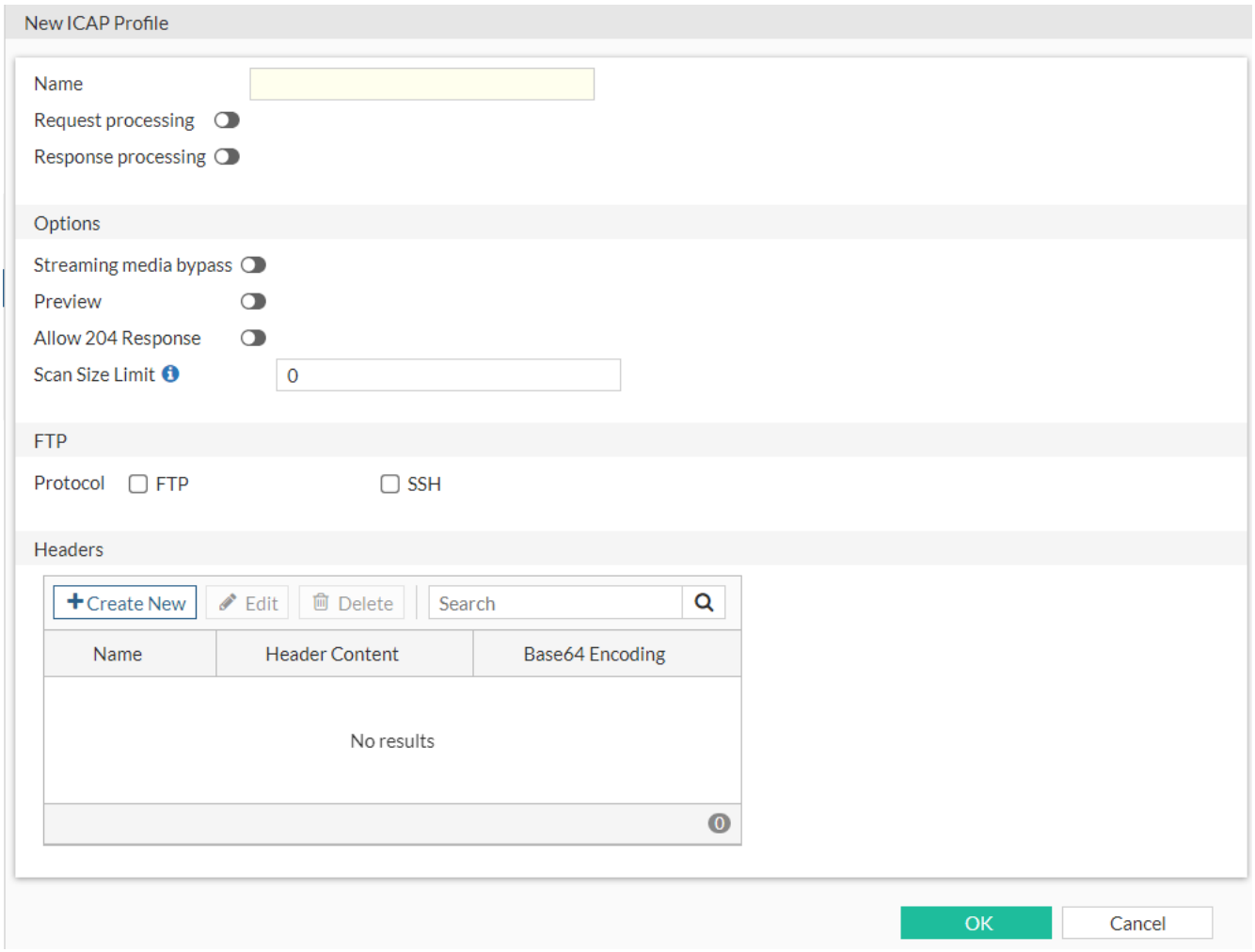
The following options are available:

Create New	Create an ICAP profile. See Create or edit an ICAP profile on page 725.
Edit	Edit an ICAP profile. See Create or edit an ICAP profile on page 725.
Delete	Delete a profile or profiles.
Name	The name of the ICAP profile.

Request	Whether request processing is enabled or disabled.
Response	Whether response processing is enabled or disabled.
Streaming Content Bypass	Whether streaming media is allowed (enabled) to ignore offloading to the ICAP server.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an ICAP profile

Select *Create New* to open the *New ICAP Profile* window.



To open the *Edit ICAP Profile* window, select an ICAP profile and then click *Edit*.

Configure the following settings in the *New ICAP Profile* window or *Edit ICAP Profile* window and then click *OK*:

Name	Specify a name for the ICAP profile. After you create an ICAP profile, you cannot change the name.

Request Processing	Enable or disable request processing.
	When enabled, you can further configure the following options:
	• **Server**—Select an existing server from the list or create a new server.
	• **Path**—Path to the processing component on the server, such as `/proprietary_code/content-filter/`.
	• **Method**—Allowed HTTP methods that will be sent to ICAP server for further processing. Click the *Add* button to add more methods to the list. Click the *Delete* button on the right of a method to delete it from the list.
	• **On failure**—Action to take if the ICAP server cannot be contacted when processing an HTTP request.
	  • *Error*—HTTP or FTP traffic reports an error and is blocked when the ICAP server is down.
	  • *Bypass*—HTTP or FTP traffic can still pass through when the ICAP server is down.

Response Processing	Enable or disable response processing.
	When enabled, you can further configure the following options:
	• **Server**—Select an existing server from the list or create a new server.
	• **Path**—Path to the processing component on the server, such as `/proprietary_code/content-filter/`.
	• **On failure**—Action to take if the ICAP server cannot be contacted when processing an HTTP response.
	  • *Error*—HTTP or FTP traffic reports an error and is blocked when the ICAP server is down.
	  • *Bypass*—HTTP or FTP traffic can still pass through when the ICAP server is down.

Streaming Media Bypass	Specify whether to bypass offloading of streaming media to the ICAP server. When enabled, streaming media is not offloaded to the ICAP server.
Preview	Enable preview of data to the ICAP server. When enabled, you can further configure the *Preview Data Length*, which is the preview data length to be sent to the ICAP server.
Allow 204 Response	Specify whether to allow 204 response. When enabled, you can further configure the *204 Size Limit*.
Scan Size Limit	Specify the ICAP server scan size limit for a single request within the range of 0-4096 (MB). The default is 0 MB, which means unlimited.
Protocol	Select the FTP protocol: FTP or SSH. You can select both.

	When a protocol is enabled, you can further configure the following options:
	• **Server**—Select an existing server from the list or create a new server.
	• **On failure**—Action to take if the FTP server cannot be contacted when processing an FTP request.
	  • *Error*—FTP traffic reports an error and is blocked when the FTP server is down.
	  • *Bypass*—FTP traffic can still pass through when the FTP server is down.
	• **Path**—Path to the processing component on the server, such as `/proprietary_code/content-filter/`.

Headers	View existing ICAP headers or create a new ICAP header using the *Create New* button. When creating a new ICAP header, specify the following options in the *Create Header* window: • **Name**—Name of the HTTP forwarded header. • **Header Content**—HTTP header content. • **Base64 Encoding**—Enable or disable base64 encoding of HTTP content.

TCP connection pool for connections to ICAP server

A TCP connection pool can maintain local-out TCP connections to the external ICAP server due to a backend update in the FortiProxy unit. TCP connections will not be terminated once data has been exchanged with the ICAP server, but instead are reused in the next ICAP session to maximize efficiency.

Use case

In this scenario, an ICAP profile is used as a UTM profile in an explicit web proxy policy, and a client visits web servers through this proxy policy.

After the WAD is initialized, when a HTTP request is sent from the client to the server through the FortiProxy unit with an ICAP profile applied to the matched proxy policy, a TCP connection is established between the FortiProxy unit and the ICAP server to exchange data.

When an ICAP session is finished, the TCP connection is kept in the WAD connection pool. When another ICAP session needs to be established, the WAD will check if there are any idle connections available in the connection pool. If an idle connection is available, it will be reused; otherwise, a new TCP connection is established for the ICAP session. This process can be checked in the WAD debug log.

ICAP server response extension headers

ICAP server responses can be configured to include X-Virus-ID, X-Infection-Found, and X-Violation-Found extension headers.

```
config icap local-server
    edit 1
        config icap-service
            edit 1
                set extension-headers {X-Virus-id X-Infection-Found X-Violation-Found}
            next
        end
    next
end
```

X-Virus-id	Enable X-Virus-ID ICAP extension header.
X-Infection-Found	Enable X-Infection-Found ICAP extension header.
X-Violation-Found	Enable X-Violation-Found ICAP extension header.

X-Scan-Progress-Interval header in the FortiProxy ICAP client

You can specify that the X-Scan-Progress-Interval header is used in the FortiProxy ICAP client and specify the scan progress interval value:

```
config icap profile
    edit <profile_name>
        set response {enable | disable}
        set response-server <name_of_ICAP_server>
        set response-path <HTTP_response_processing_service>
        set extension-feature scan-progress
        set scan-progress-interval <5-30 seconds (default = 10)>
    next
end
```

Timeout configuration for the FortiProxy ICAP client

You can configure the number of seconds that the ICAP client waits for a response from the ICAP server:

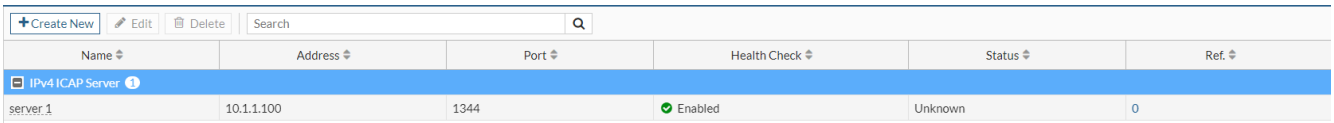
```
config icap profile
    edit <profile_name>
        set timeout <30-3600 seconds (default = 30)>
    next
end
```

ICAP Remote Server

To view the list of ICAP remote servers, go to *Content Analyses* > *ICAP Remote Servers*.



By default, ICAP is not visible in the tree menu in the GUI. To make it visible, go to *System* > *Feature Visibility* and enable it. See Feature Visibility on page 970 for more information.



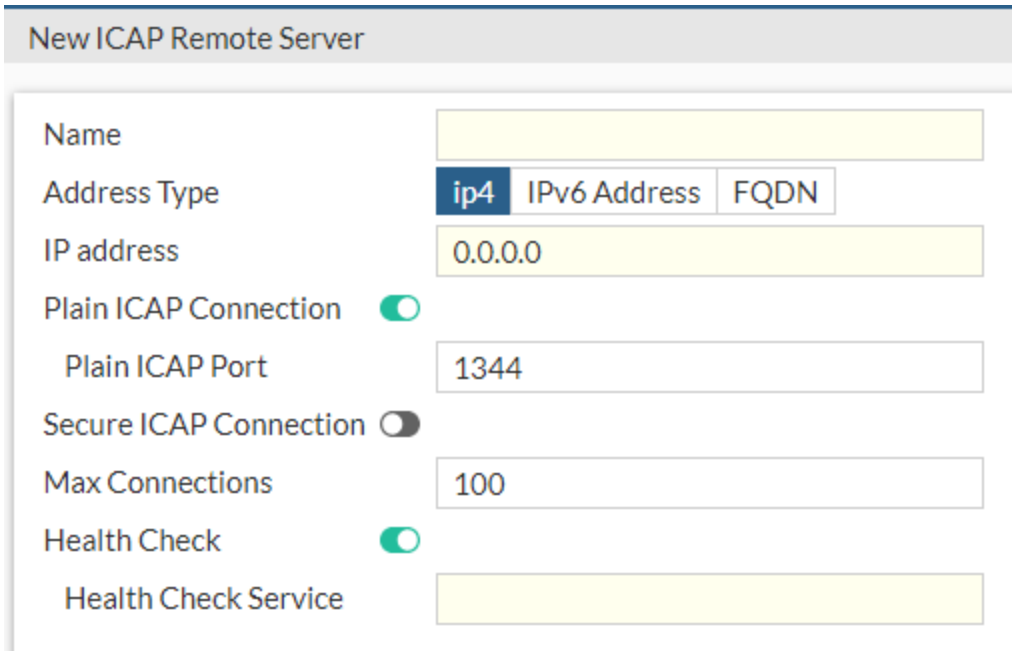
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an ICAP remote server. See Create or edit an ICAP remote server on page 729.
Edit	Edit an ICAP remote server. See Create or edit an ICAP remote server on page 729.
Delete	Delete an ICAP remote server or servers.
Name	The name of the ICAP remote server.
Address	The IP address of the ICAP remote server.
Port	The port number that the ICAP remote server is using.
Health Check	Indicates whether health check is enabled or disabled for the ICAP remote server.
Status	Health status of the ICAP remote server, which can be *Online*, *Offline*, or *Unknown*.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an ICAP remote server

Select *Create New* to open the *New ICAP Remote Server* window.



To open the *Edit ICAP Remote Server* window, select a server and then click *Edit*.

Configure the following settings in the *New ICAP Remote Server* window or *Edit ICAP Remote Server* window and then click *OK*:

Name	Enter a name for the ICAP remote server. After you create an ICAP remote server, you cannot change the name.
Address Type	Select *IPv4* or *IPv6 Address* or *FQDN*.
IP Address/IPv6 Address/FQDN	Enter the IPv4 or IPv6 address or the Fully Qualified Domain Name (FQDN) for the ICAP remote server.
Plain ICAP Connection	Enable or disable unsecure connection from the FortiProxy unit to the remote ICAP server.
Secure ICAP Connection	Enable or disable secure SSL connection from the FortiProxy unit to the remote ICAP server.
Plain/Secure ICAP Port	Enter the TCP port number used by the ICAP remote server, from 1 to 65,535. The default is 1344.
Certificate	Select the CA certificate. This option is available only if you enable *Secure ICAP Connection*.
Max Connections	Enter the maximum number of concurrent connections to the ICAP remote server. Must not be less than wad-workercount. The default is 100. The valid value range is 0-4294967295.

Health Check	Enable or disable ICAP remote server health checking. When enabled, FortiProxy attempts to connect to the remote ICAP server to verify that the server is operating normally and generates an event log each time the ICAP server health check fails or goes back online. The default is disabled.
Health Check Service	Enter the ICAP service name to use for health checks.

To configure an ICAP remote server via CLI:

```
config icap remote-server
   edit <server_name>
      set addr-type [ip4|ip6|fqdn]
      set ip-address {ipv4-address-any}
      set ip6-address {ipv6-address}
      set fqdn {string}
      set port {integer}
      set max-connections {integer}
      set secure [disable|enable]
      set ssl-cert {string}
      set healthcheck [disable|enable]
      set healthcheck-service {string}
   next
end
```

ICAP Load Balancing

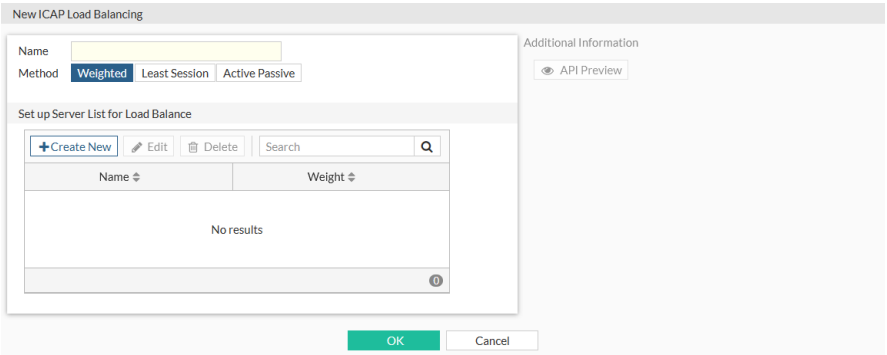
ICAP load balancing can be configure the balance the traffic load to ICAP servers based on assigned weights, send new sessions to the ICAP server with the lowest session count, or send new sessions to the active ICAP server with the highest weight.



By default, ICAP is not visible in the tree menu in the GUI. To make it visible, go to *System > Feature Visibility* and enable it. See Feature Visibility on page 970 for more information.

To configure an ICAP load balancing in the GUI:

1. Go to *Content Analyses* > *ICAP Load Balancing* and click *Create New*.



2. Enter a name for the ICAP load-balancing configuration.
3. Select the load-balancing method:
   - *Weighted*: Balance the traffic load to ICAP servers based on the assigned weights.
   - *Least Session*: Send new sessions to the ICAP server with the lowest session count.
   - *Active Passive*: Send new sessions to the active ICAP server with the highest weight.
4. To create a server list for load balancing:
   a. Click *Create New* in the *Set up Server List for Load Balance* table.
   b. Select or create a remote server. See ICAP Remote Server on page 729 for information.
   c. Enter a weight for the remote server.
   d. Click *OK*.
   e. Add more servers as required.
5. Click *OK*.

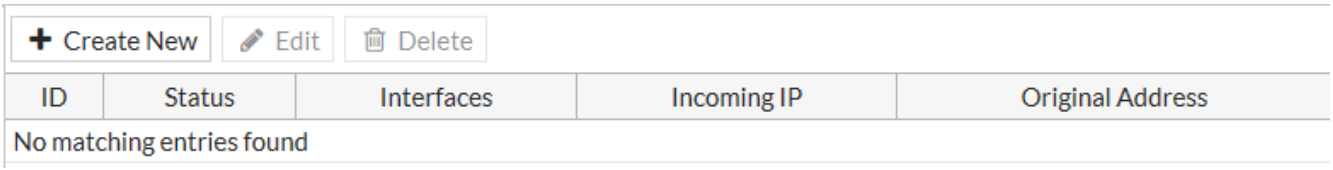
To configure an ICAP load balancing in the CLI:

```
config icap remote-server-group
    edit <name>
        set ldb-method {weighted | least-session | active-passive}
        config server-list
            edit <ICAP_remote_server>
                set weight <integer>
            next
        end
    next
end
```

ICAP Local Server

To view the list of ICAP local servers, go to *Content Analyses> ICAP Local Server*.

By default, ICAP is not visible in the tree menu in the GUI. To make it visible, go to *System* > *Feature Visibility* and enable it. See Feature Visibility on page 970 for more information.



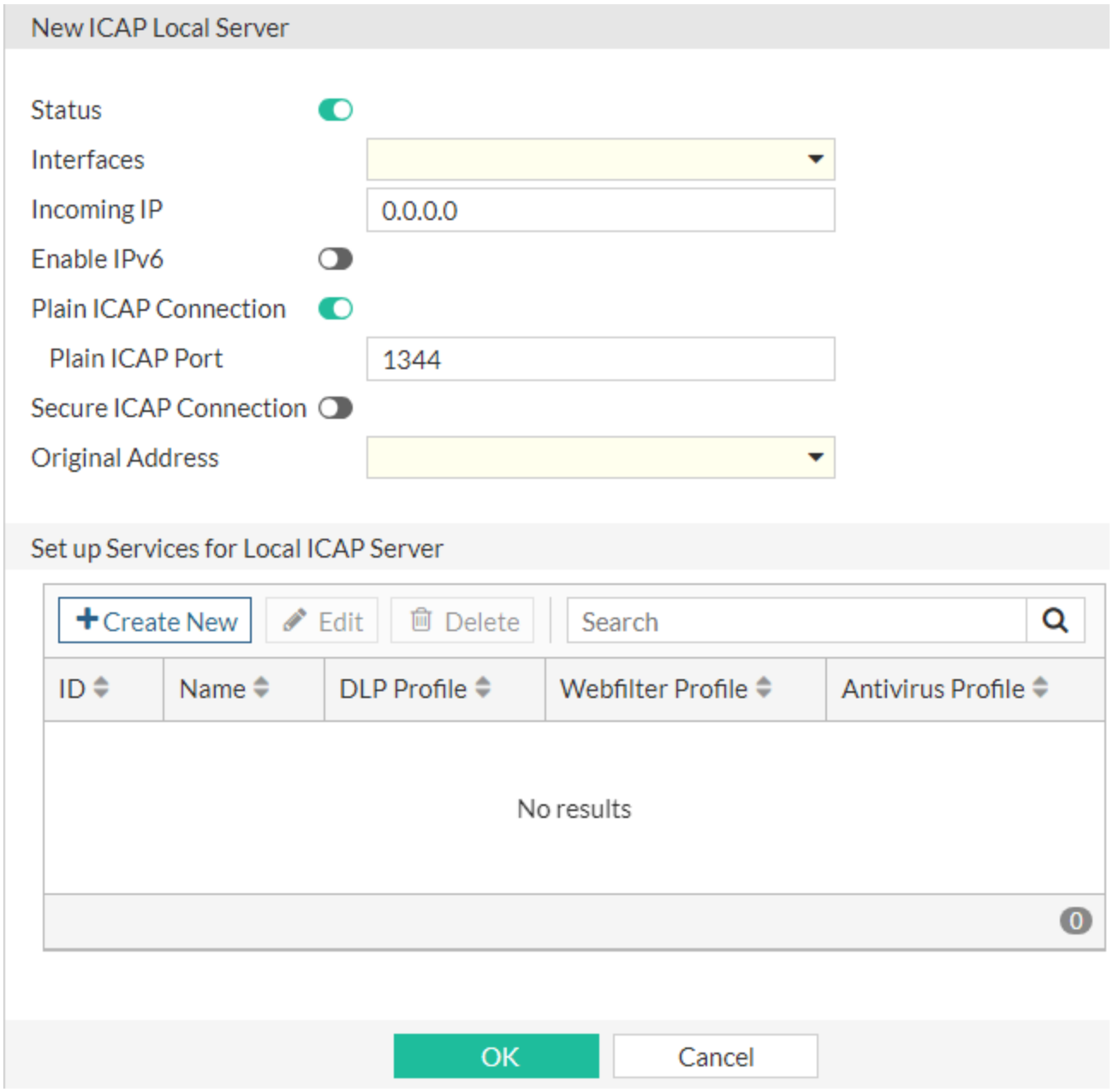
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an ICAP local server. See Create or edit an ICAP local server on page 733.
Edit	Edit an ICAP local server. See Create or edit an ICAP local server on page 733.
Delete	Delete an ICAP local server or servers.
ID	The identifier for the ICAP local server.
Status	Whether the server is active.
Interfaces	The interface that the ICAP local server will use.
Incoming IP	The IP address that the ICAP local server will use.
Original Address	The original address.

Create or edit an ICAP local server

Select *Create New* to open the *New ICAP Local Server* window.



To open the *Edit ICAP Local Server* window, select a server and then click *Edit*.

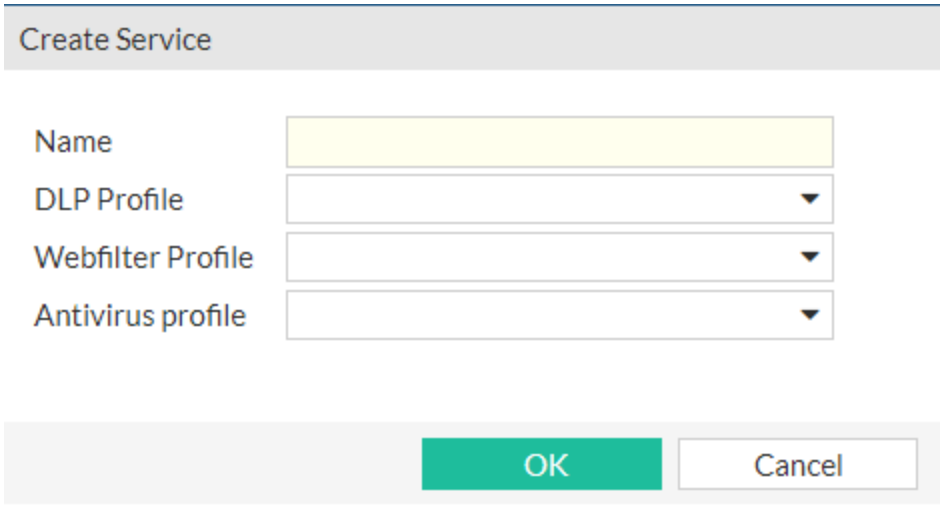
Configure the following settings in the *New ICAP Local Server* window or *Edit ICAP Local Server* window and then click *OK*:

Status	Enable or disable this ICAP local server.
Interfaces	Select an interface for the ICAP local server to use.
Incoming IP	Enter an IP address for the ICAP local server to use.
Original Address	Select the original address.

Create New	Create an ICAP service. See Create or edit an ICAP service on page 735.
Edit	Edit an ICAP service. See Create or edit an ICAP service on page 735.
Delete	Delete an ICAP service.
ID	The identifier for the ICAP service.
Name	The name of the ICAP service.
DLP Profile	The DLP profile used by the ICAP service. See Basic DLP settings on page 663.
Webfilter Profile	The web filter profile used by the ICAP service. See Create or edit a web filter profile on page 566.
AV Profile	The antivirus profile used by the ICAP service. See Create or edit an antivirus profile on page 542.

Create or edit an ICAP service

Select *Create New* to open the *Create Service* window.



To open the *Edit Service* window, select an ICAP service and then click *Edit*.

Configure the following settings in the *Create Service* window or *Edit Service* window and then click *OK*:

Name	Enter the name of the ICAP service.
DLP Profile	Select the DLP profile that the ICAP service will use. See Basic DLP settings on page 663.
Webfilter Profile	Select the web filter profile that the ICAP service will use. See Create or edit a web filter profile on page 566.

AV Profile	Select the antivirus profile that the ICAP service will use. See Create or edit an antivirus profile on page 542.

ICAP scanning with FTP

Transferred files can be forwarded to the ICAP server for further processing using FTP.

To configure ICAP scanning with FTP in the GUI:

1. Configure an ICAP remote server.
2. Create an ICAP profile that references the server.



- Select *FTP* in *Protocol*.
- Select the server you created in step 1 in *Server*.

3. Enable and configure explicit FTP Proxy on page 169.
4. Create an explicit FTP proxy policythat uses the ICAP profile.



- Select *FTP* under *Type* for an explicit FTP proxy policy.
- Select *ACCEPT* for *Action* to enable the *Security Profiles* options. You can then enable *ICAP* and select the ICAP profile you configured in step 2 from the dropdown list.

To configure ICAP scanning with FTP in the CLI:

1. Configure an ICAP remote server:

```
config icap remote-server
    edit "icap1"
        set ip-address 172.18.20.43
    next
end
```

See config icap remote-server in the CLI guide for more details.

2. Create an ICAP profile that references the server:

```
config icap profile
    edit "icapFTP"
        set file-transfer ftp
        set file-transfer-server "icap1"
        set file-transfer-failure error
        set file-transfer-path "ftpicap"
    next
end
```

See config icap profile in the CLI guide for more details.

3. Enable and configure explicit FTP Proxy:

```
config ftp-proxy explicit
    set status [enable|disable]
    set incoming-port {user}
    set incoming-ip {ipv4-address-any}
    set outgoing-ip {ipv4-address-any}
    set sec-default-action [accept|deny]
    set server-data-mode [client|passive]
    set ssl [enable|disable]
    set ssl-cert {string}
    set ssl-dh-bits [768|1024|...]
    set ssl-algorithm [high|medium|...]
end
```

See config ftp-proxy explicit in the CLI guide for more details.

4. Create an explicit FTP proxy policy that uses the ICAP profile:

```
config firewall policy
    edit 1
        set type explicit-ftp
        set name "test"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set ssl-ssh-profile "certificate-inspection"
        set utm-status enable
        set icap-profile "icapFTP"
    next
end
```

See config firewall policy in the CLI guide for more details.

WAN Optimization

You can add WAN optimization to improve traffic performance and efficiency as it crosses the WAN. For more information about WAN optimization, see WAN optimization on page 73.

The WAD traffic dispatcher now allows incoming traffic to be directly distributed to the workers. This enhancement also allows source addresses to be exempt from proxy affinity, which allows traffic from the same source and different server to be distributed to workers in a round-robin configuration. A maximum of 255 workers is now supported.

This section describes the following:

- Profiles on page 738
- Peers on page 742
- Authentication Groups on page 744

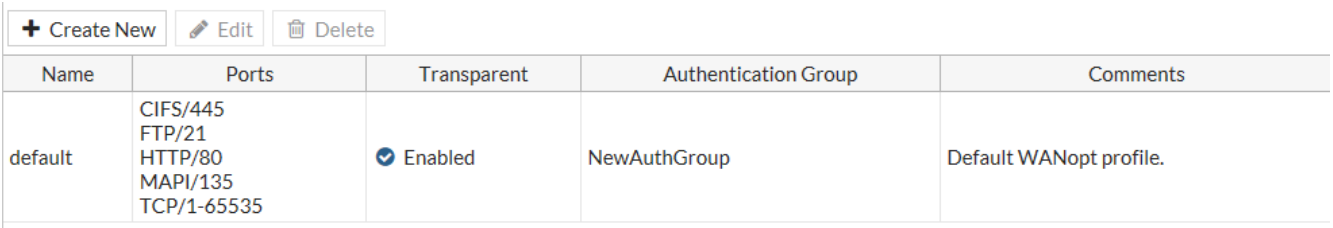
Profiles

FortiProxy WAN optimization consists of a number of techniques that you can apply to improve the efficiency of communication across your WAN. These techniques include the following:

- Protocol optimization—Protocol optimization can improve the efficiency of traffic that uses the CIFS, FTP, HTTP, or MAPI protocol, as well as general TCP traffic.
- Byte caching—Byte caching caches files and other data on FortiProxy units to reduce the amount of data transmitted across the WAN.
- Web caching—Web caching stores web pages on FortiProxy units to reduce latency and delays between the WAN and web servers.
- SSL offloading—SSL offloading offloads SSL decryption and encryption from web servers onto FortiProxy SSL acceleration hardware.
- Secure tunneling—Secure tunneling secures traffic as it crosses the WAN.

You can apply different combinations of these WAN optimization techniques to a single traffic stream depending on the traffic type. For example, you can apply byte caching and secure tunneling to any TCP traffic. For HTTP and HTTPS traffic, you can also apply protocol optimization and web caching.

You can view the list of WAN optimization profiles by going to *WAN Optimization* > *Profiles* and selecting the List icon (the farthest right of the three icons in the upper right of the window; it resembles a page with some lines on it) in the *Edit WAN Optimization Profile* page toolbar.



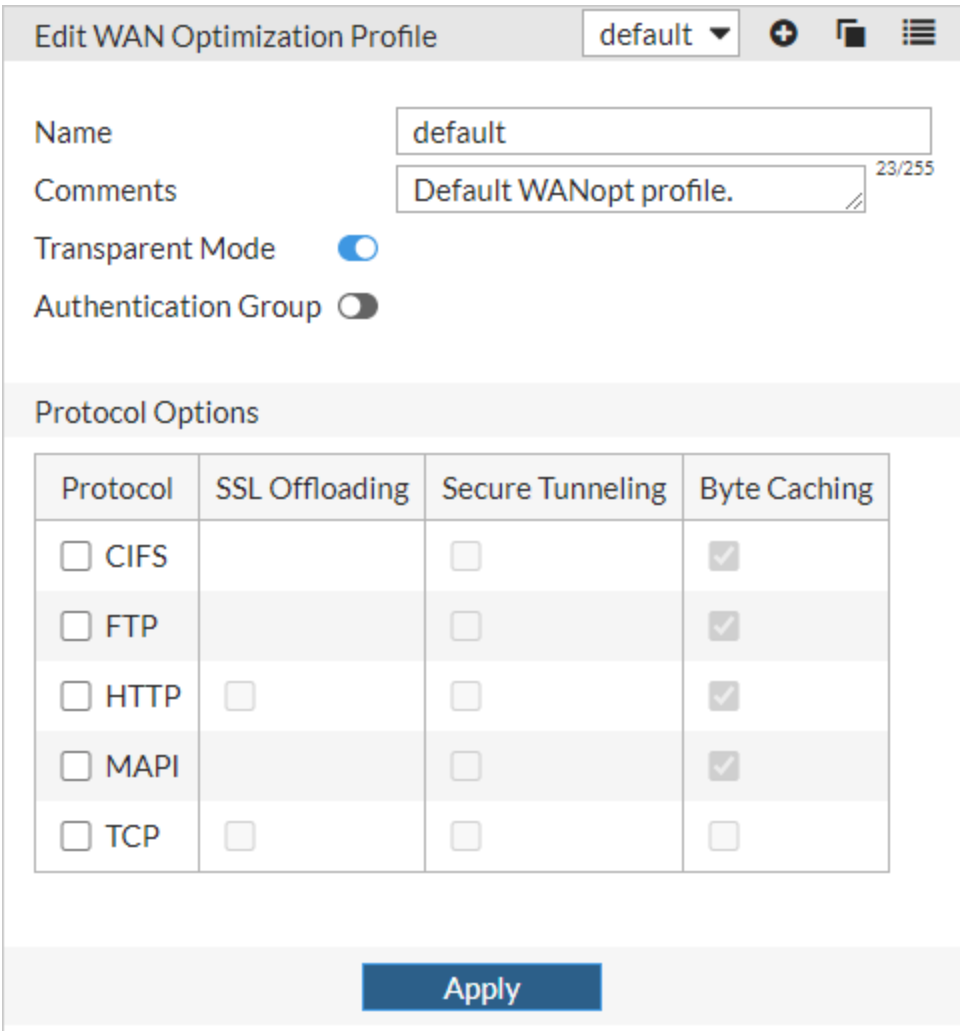
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a WAN optimization profile. See Create or edit a WAN optimization profile on page 739.
Edit	Modify the profile. See Create or edit a WAN optimization profile on page 739.
Delete	Remove the profile.
Name	The name of the WAN optimization profile.
Ports	The ports used by the profile.
Transparent	Whether the WAN optimization transparent mode is enabled. For more information about the WAN optimization transparent mode, see WAN optimization transparent mode on page 74.
Authentication Group	The authentication group used by the profile, if any. See Authentication Groups on page 744.
Comments	Optional description of the WAN optimization profile.

Create or edit a WAN optimization profile

To configure WAN optimization profiles, go to *WAN Optimization* > *Profiles*. The *Edit WAN Optimization Profile* page is displayed.



Configure the following settings and then select *Apply* to save your changes:

drop-down list	Select a profile to edit from the drop-down list. See To create a WAN optimization profile: on page 741.
Create New icon	Create a WAN optimization profile. See To edit a WAN optimization profile: on page 741.
Clone icon	Clone the current profile. See To clone a WAN optimization profile: on page 742.
List icon	View the WAN optimization profile list. See Profiles on page 738.
Name	Enter a name for the WAN optimization profile.
Comments	Optionally, enter a description of the profile.
Transparent Mode	Enable or disable transparent mode. For more information about the WAN optimization transparent mode, see WAN optimization transparent mode on page 74.

Authentication Group	Enable to select the authentication group from the drop-down list that will be applied to the WAN optimization profile. To create an authentication group, see Create or edit an authentication group on page 745.
Protocol	Select the protocols that are enabled for this profile: *CIFS*, *FTP*, *HTTP*, *MAPI*, and *TCP*. **NOTE:** The FortiProxy unit supports WAN optimization for SMBv1, SMBv2 and SMBv3 (unencrypted only) protocols.
SSL Offloading	Select to enable SSL offloading. SSL offloading offloads SSL decryption and encryption from web servers onto FortiProxy SSL acceleration hardware. It is only available for HTTP and TCP protocols.
Secure Tunneling	Select to enable secure tunneling. To use secure tunneling, it must be enabled for a protocol, and an authentication group must be added. The authentication group specifies the certificate or pre-shared key used to set up the secure tunnel. The *Peer Acceptance* setting of the authentication group does not affect secure tunneling. The FortiProxy units at each end of the secure tunnel must have the same authentication group with the same name and the same configuration, including the same pre-shared key or certificate.
Byte Caching	Select to enable byte caching. Byte caching breaks large units of application data (for example, a file being downloaded from a web page) into small chunks of data, labeling each chunk of data with a hash of the chunk and storing those chunks and their hashes in a database. The database is stored on a WAN optimization storage device.

You can add, edit, clone, and delete WAN optimization profiles.

To create a WAN optimization profile:

1. From either the *Edit WAN Optimization Profile* page or the WAN optimization profile list, select *Create New*.
2. Enter the required information and then click *OK* to create the new WAN optimization profile.

To edit a WAN optimization profile:

1. From the *Edit WAN Optimization Profile* page, select the profile you need to edit from the profile drop-down list.

   Alternatively, from the profile list, either select the profile you want to edit and then click *Edit* from the toolbar or double-click on the profile name in the list. The *Edit WAN Optimization Profile* page opens.
2. Edit the information as required and then select *Apply* to apply your changes.

To clone a WAN optimization profile:

1. From the *Edit WAN Optimization Profile* page, select the profile you need to clone from the profile drop-down list.
2. Select *Clone* from the toolbar.
3. Enter a name for the profile in the dialog box and then click *OK*.
4. Edit the clone as required.

To delete a profile or profiles:

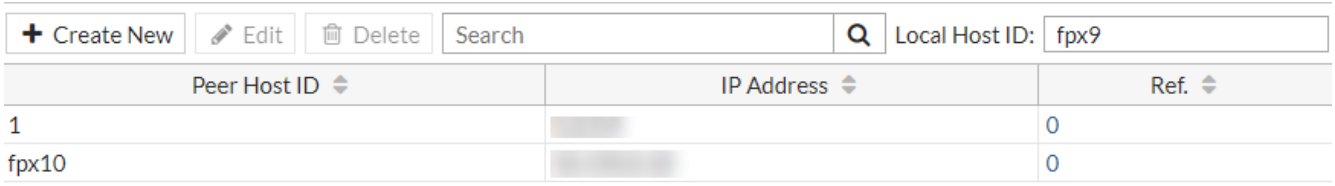
1. From the profile list, select the profile or profiles that you want to delete.
2. Click *Delete* from the toolbar.
3. Click *OK* in the confirmation dialog box to delete the selected profile or profiles.

Peers

The client-side and server-side FortiProxy units are called WAN optimization peers because all of the FortiProxy units in a WAN optimization network have the same peer relationship with each other. The client and server roles relate to how a session is started. Any FortiProxy unit configured for WAN optimization can be both a client-side and a server-side FortiProxy unit at the same time, depending on the direction of the traffic. Client-side FortiProxy units initiate WAN optimization sessions, and server-side FortiProxy units respond to the session requests. Any FortiProxy unit can be a client-side FortiProxy unit for some sessions and a server-side FortiProxy unit for others.

To identify all of the WAN optimization peers that a FortiProxy unit can perform WAN optimization with, host IDs and IP addresses of all of the peers are added to the FortiProxy unit configuration. The peer IP address is actually the IP address of the peer unit interface that communicates with the FortiProxy unit.

Go to *WAN Optimization* > *Peer Settings* to view the WAN optimization peer list.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

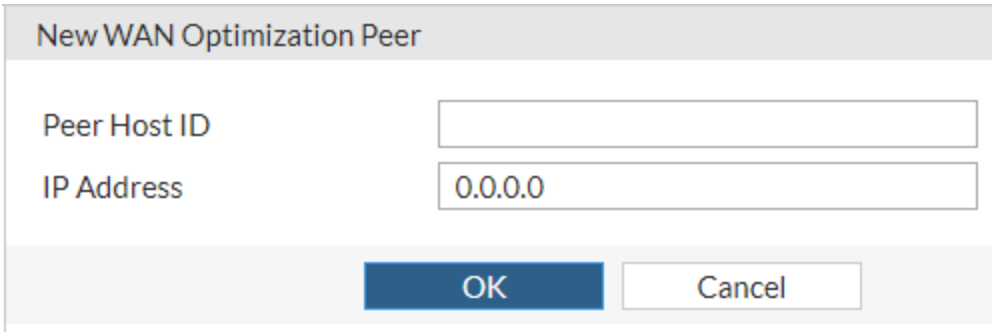
Create New	Create a WAN optimization peer. See To create a WAN optimization peer: on page 743.

Edit	Edit a WAN optimization peer. See To create a WAN optimization peer: on page 743.
Delete	Delete a WAN optimization peer or peers.
Search	Enter a search term to search for in the peer list.
Local Host ID	The local host identifier. Enter an identifier and then select *Apply* to apply the identifier.
Peer Host ID	The peer host identifier of the WAN optimization peer.
IP Address	The IP address of the peer.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a WAN optimization peer

To create a WAN optimization peer:

1. From the peer list, select *Create New* in the toolbar.
   The *New WAN Optimization Peer* window opens.



2. Enter the *Peer Host ID* and *IP Address*.
3. Click *OK* to create the new peer.

To edit a WAN optimization peer:

1. Select the peer that you want to edit in the peer list and then click *Edit* from the toolbar or double-click on the peer in the peer list. The *Edit WAN Optimization Peer* window opens.
2. Edit the peer as required and click *OK* to apply your changes.

To delete a WAN optimization peer or peers:

1. Select the peer or peers that you want to delete in the peer list.
2. Click *Delete* from the toolbar.

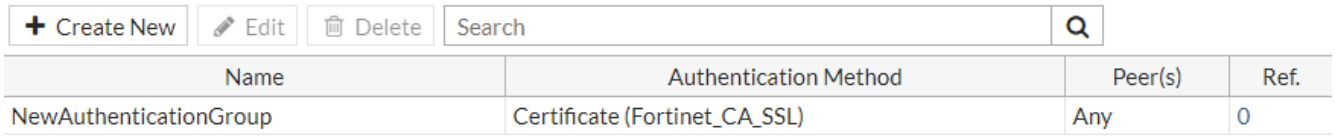
3. Click *OK* in the confirmation dialog box to delete the selected peer or peers.

Authentication Groups

You need to add authentication groups to support authentication and secure tunneling between WAN optimization peers.

To perform authentication, WAN optimization peers use a certificate or a pre-shared key added to an authentication group, so they can identify each other before forming a WAN optimization tunnel. Both peers must have an authentication group with the same name and settings. The authentication group is added to a peer-to-peer or active rule on the client-side FortiProxy unit. When the server-side FortiProxy unit receives a tunnel start request that includes an authentication group from the client-side unit, the server-side unit finds an authentication group in its configuration with the same name. If both authentication groups have the same certificate or pre-shared key, the peers can authenticate and set up the tunnel.

Go to *WAN Optimization* > *Authentication* to manage the authentication groups.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

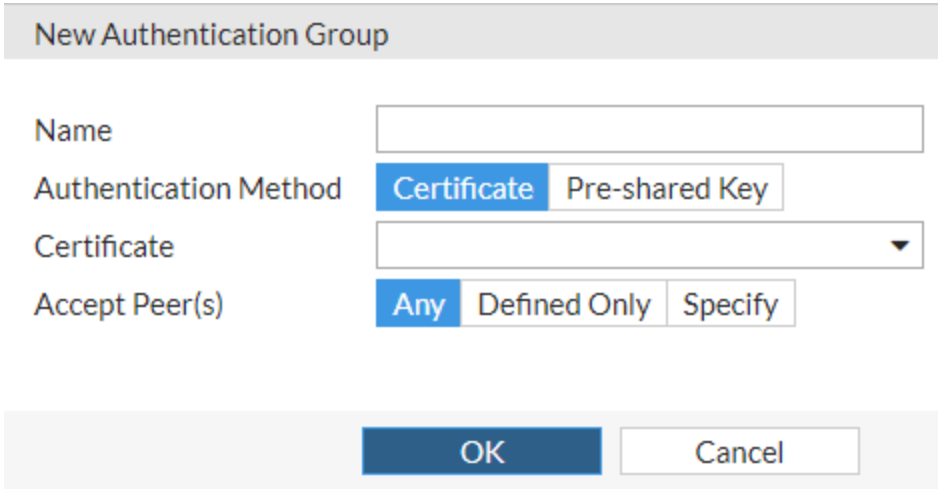
The following options are available:

Create New	Create an authentication group. See Create or edit an authentication group on page 745.
Edit	Edit an authentication group. See Create or edit an authentication group on page 745.
Delete	Delete an authentication group or groups.
Search	Enter a search term to search for in the group list.
Name	The name of the authentication group.
Authentication Method	The authentication used by the group, either *Certificate* or *Pre-shared key*.
Peer(s)	The peer or peers in the authentication group.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an authentication group

To create an authentication group:

1. Go to *WAN Optimization* > *Authentication*.
2. Select *Create New* from the toolbar.
   The *New Authentication Group* window opens.



3. Enter the following information:

Name	Enter a name for the authentication group.
Authentication Method	Select the authentication method to use. • *Certificate*: Use a certificate to authenticate and encrypt WAN optimization tunnels. Then select a local certificate that has been added to this FortiProxy unit from the drop-down list. • *Pre-shared Key*: Use a pre-shared key or password to authenticate and encrypt WAN optimization tunnels. Then enter the password (or pre-shared key) in the *Password* field. Other FortiProxy units that participate in WAN optimization tunnels with this unit must have an authentication group with the same name and password. The password must contain at least 6 printable characters and should be known only by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 alphanumeric characters.
Certificate	Select a local certificate from the drop-down list.
Pre-shared Key	Enter the pre-shared key.
Accept Peer(s)	Select the peer acceptance method for the authentication group. • *Any*: If you do not know the peer host IDs or IP addresses of the peers that will use this authentication group. This setting is most often used for WAN optimization with

	FortiProxy units that do not have static IP addresses, such as units that use DHCP. • *Defined Only*: Authenticate with peers that have added to the peer list only. • *Specify*: Select a peer from the drop-down list to authenticate with the selected peer only. Select *Create New* from the drop-down list to create a peer; see Create or edit a WAN optimization peer on page 743.

4. Click *OK* to create the new authentication group.
   The authentication group can now be added to WAN optimization profiles to apply the authentication settings in the authentication group to the profile. See Create or edit a WAN optimization profile on page 739.

To edit an authentication group:

1. Go to *WAN Optimization > Authentication*.
2. Select the group you want to edit and then click *Edit* from the toolbar or double-click on the group in the authentication group list.
   The *Edit Authentication Group* window opens.
3. Edit the group information as required and click *OK* to apply your changes.

To delete an authentication group or groups:

1. Go to *WAN Optimization > Authentication*.
2. Select the group or groups that you want to delete.
3. Click *Delete* from the toolbar.
4. Click *OK* in the confirmation dialog box to delete the selected group or groups.

Web Cache

You can use web caching to cache web pages from any web server. All traffic between a client network and one or more web servers is then intercepted by a web cache policy. This policy causes the FortiProxy unit to cache pages from the web servers on the FortiProxy unit and makes the cached pages available to users on the client network. Web caching can be configured for standard and reverse web caching.

In a standard web caching configuration, the FortiProxy unit caches pages for users on a client network. A router sends HTTP traffic to be cached to the FortiProxy unit.

You can also create a reverse proxy web caching configuration where the FortiProxy unit is dedicated to providing web caching for a single web server or server farm. In this second configuration, one or more FortiProxy units can be installed between the server network, and the WAN or Internet or traffic to be cached can be routed to the FortiProxy units.

This section describes the following:

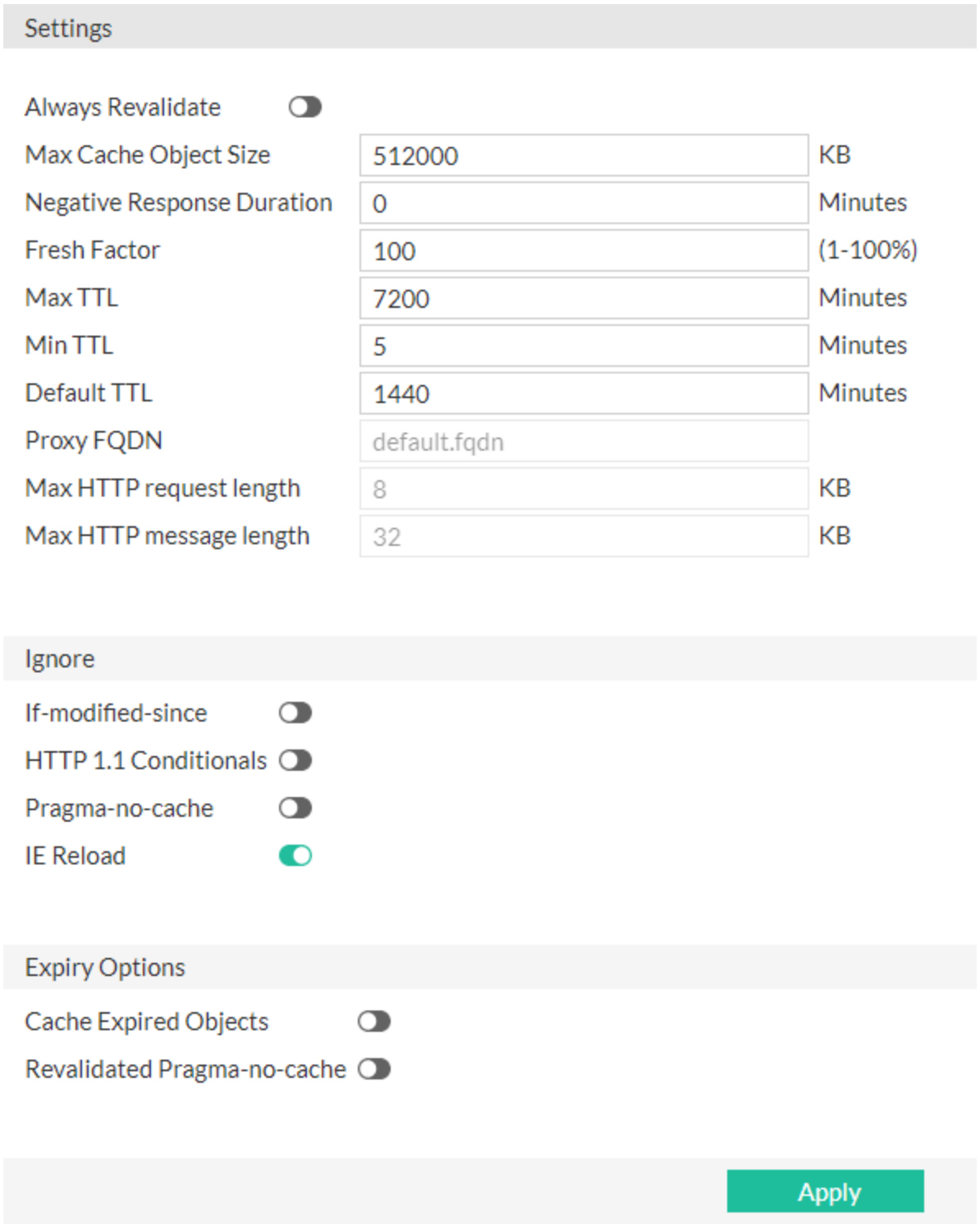
- Settings on page 747
- Prefetch URLs on page 751
- Reverse Cache Server on page 753
- Prefetch File on page 755
- WCCP Settings on page 758
- User Agent on page 766

Settings

You can optimize web cache settings to improve performance and exempt specific URL patterns from caching and/or forward them to a web proxy server.

In most cases, the default settings for the WAN optimization web cache are acceptable. However, you might want to change them to improve performance or optimize the cache for your configuration.

Go to *Web Cache* > *Settings* to configure web cache settings.



Configure the following settings and then select *Apply* to save your changes:

Always Revalidate	Always re-validate requested cached objects with content on the server before serving them to the client.

Max Cache Object Size	The maximum size of objects (files) that are cached (the default is 512,000 KB). Objects that are larger than this size are still delivered to the client but are not stored in the FortiProxy web cache.
Negative Response Duration	The amount of time, in minutes, that the FortiProxy unit caches error responses from web servers (default is 0 minutes). The content server might send a client error code (4xx HTTP response) or a server error code (5xx HTTP response) as a response to some requests. If the web cache is configured to cache these negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes, regardless of the actual object status.
Fresh Factor	For cached objects that do not have an expiry time, the web cache periodically checks the server to see if the objects have expired. The higher the fresh factor, the less often the checks occur (default is 100%). For example, if you set *Max TTL* and *Default TTL* to 7,200 minutes (5 days) and set *Fresh Factor* to 20, the web cache checks the cached objects 5 times before they expire, but, if you set the *Fresh Factor* to 100, the web cache will only check once.
Max TTL	The maximum amount of time (Time to Live), in minutes, an object can stay in the web cache without the cache checking to see if it has expired on the server. From 1 to 5,256,000 minutes (one year) (default is 7,200 minutes).
Min TTL	The minimum amount of time an object can stay in the web cache before the web cache checks to see if it has expired on the server. From 1 to 5,256,000 minutes (default is 5 minutes).
Default TTL	The default expiry time for objects that do not have an expiry time set by the web server. From 1 to 5,256,000 minutes (default is 1,440 minutes).
Proxy FQDN	This setting cannot be changed from the default: *default.fqdn*.
Max HTTP request length	This setting cannot be changed from the default: *4KB*.
Max HTTP message length	This setting cannot be changed from the default: *32KB*.
Ignore	
If-modified-since	If the time specified by the if-modified-since (IMS) header in the client's conditional request is greater than the last modified time of the object in the cache, it is a strong indication that the copy in the cache is stale. If so, HTTP does a conditional GET to the original content source, based on the last modified time of the cached object. Enable ignoring if-modified-since to override this behavior.

HTTP 1.1 Conditionals	HTTP 1.1 provides additional controls to the client for the behavior of caches toward stale objects. Depending on various cache-control headers, the FortiProxy unit can be forced to consult the OCS before serving the object from the cache. For more information about the behavior of cache-control header values, see RFC 2616. Enable ignoring HTTP 1.1 conditionals to override this behavior.
Pragma-no-cache	Typically, if a client sends an HTTP GET request with a pragma no-cache (PNC) or cache-control no-cache header, a cache must consult the OCS before serving the content. This behavior means that the unit always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh. Because of this behavior, PNC requests can degrade performance and increase server-side bandwidth use. Enable ignoring Pragma-no-cache so that the PNC header from the client request is ignored. The FortiProxy unit treats the request as if the PNC header is not present.
IE Reload	Some versions of Internet Explorer issue Accept / header instead of Pragma no-cache header when you select *Refresh*. When an Accept header has only the / value, the FortiProxy unit treats it as a PNC header if it is a type-N object. Enable ignoring IE reload to cause the FortiProxy unit to ignore the PNC interpretation of the Accept / header.
Expiry Options	
Cache Expired Objects	Enable to cache expired type-1 objects (if all other conditions make the object cacheable).
Revalidated Pragma-no-cache	The PNC header in a request can affect how efficiently the device uses bandwidth. If you do not want to completely ignore PNC in client requests by selecting *Ignore > Pragma-no-cache*, you can lower the impact on bandwidth usage with this option. When selected, a client's nonconditional PNC-GET request results in a conditional GET request sent to the OCS if the object is already in the cache. This gives the OCS a chance to return the *304 Not Modified* response, which consumes less server-side bandwidth because the OCS has not been forced to return full content. By default, *Revalidate Pragma-no-cache* is disabled and is not affected by changes in the top-level profile. When the Substitute Get for PNC configuration is enabled, the revalidate PNC configuration has no effect. Most download managers make byte-range requests with a PNC header. To serve such requests from the cache, you need to also configure byte-range support when you configure the *Revalidate pragma-no-cache* option.

HTTP traffic caching reports

Another way to review traffic caching is to generate top-entry reports with the following CLI commands:

```
config system global
   set http-view {enable | disable}
end
```

After enabling top-entry reports, you can execute and generate six different kinds of reports, depending upon what statistics you are interested in. Enter the following command:

```
execute http-view report {00 | 01 | 02 | 03 | 04 | 05}
```

Enter the two-digit value for the report that you want generated:

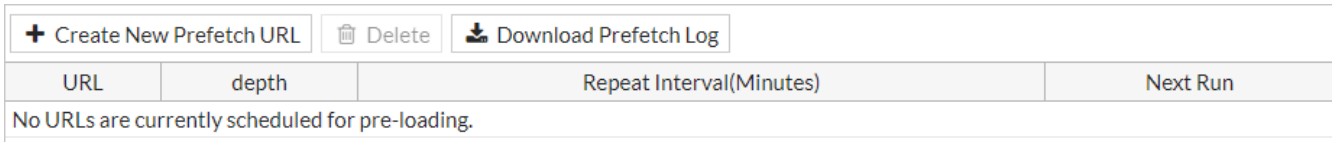
- **00:** Top entries by total HTTP requests
- **01:** Top entries by bandwidth consumed
- **02:** Top entries by cacheable percent of total requests
- **03:** Top entries by cache hit percent of total requests
- **04:** Top entries by cache hit percent of cacheable requests
- **05:** Top entries by bandwidth saved with cache hits

Each generated report shows the appropriate domain traffic within the last hour.

Prefetch URLs

To improve the speed of your system, you can specify URLs to preload.

To see the list of prefetch files of URLs to preload, go to *Web Cache* > *Prefetch URLs*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

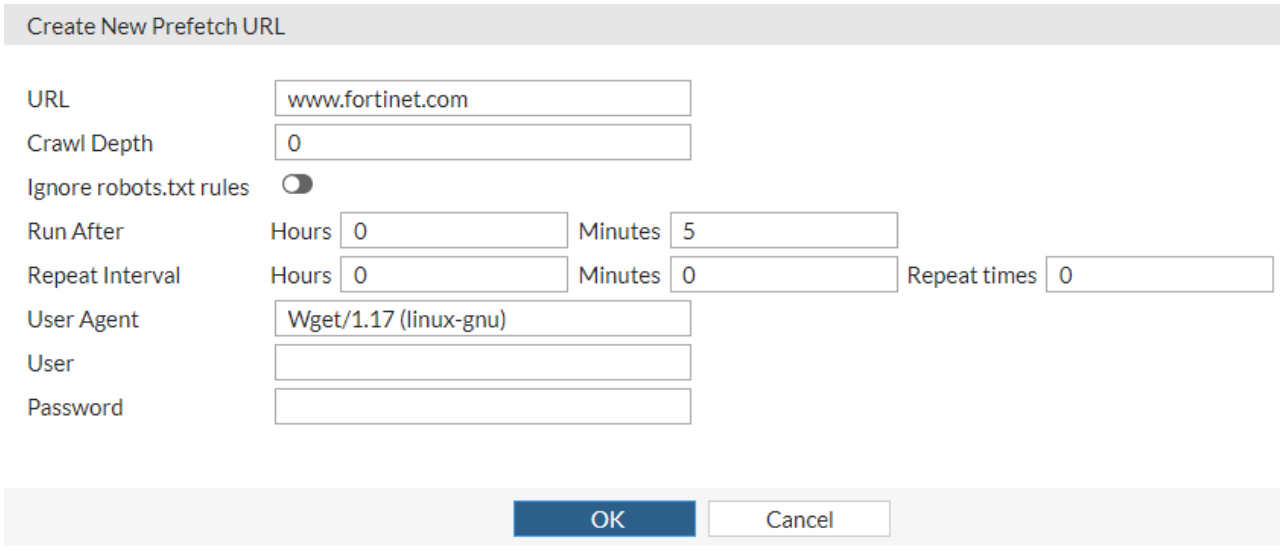
The following options are available:

Create New Prefetch URL	Add a new prefetch file. See To create a prefetch file: on page 752.
Edit	Edit the selected prefetch file. See To edit a prefetch file: on page 753.
Delete	Delete the selected prefetch file. See To delete a prefetch file or files: on page 753.
Download Prefetch Log	Select to download the prefetch log.

URL	The URLs to preload.
Depth	How many levels deep to preload.
Repeat Interval (Minutes)	How often, in minutes, to preload the URLs.
Next Run	When the URLs will be preloaded next.

To create a prefetch file:

1. Go to *Web Cache > Prefetch URLs* and select *Create New Prefetch URL* from the toolbar. The *Create New Prefetch URL* window opens.



2. Configure the following settings:

URL	Enter the URLs to preload. Separate multiple URLS with a semicolon.
Crawl Depth	Enter how many levels deep to preload the URLs.
Ignore robots.txt rules	Enable to ignore the rules found in the `robots.txt` file.
Run After	Select when the URL is preloaded the first time.
Repeat Interval	Enter how often to preload the URLs and how many times to preload the URLs.
User Agent	The name of the computer program to use to preload the URLs.
User	The user name for the user agent.
Password	The password for the user agent.

3. Click *OK* to create the new prefetch file.

To edit a prefetch file:

1. Go to *Web Cache* > *Prefetch URLs*.
2. Select the file that you want to edit and then click *Edit* from the toolbar or double-click on the file in the table. The *Edit Reverse Cache Prefetch* window opens.
3. Edit the information as required, then click *OK* to apply your changes.

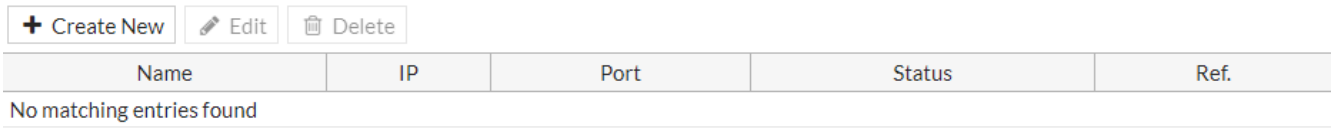
To delete a prefetch file or files:

1. Go to *Web Cache* > *Prefetch URLs*.
2. Select the file or files that you want to delete.
3. Click *Delete* from the toolbar.
4. Click *OK* in the confirmation dialog box to delete the selected file or files.

Reverse Cache Server

If you want to use reverse proxy web-caching, you need to configure a reverse cache server. For more information about reverse proxy web caching, see Web-caching topologies on page 80.

To see the list of reverse cache servers, go to *Web Cache* > *Reverse Cache Server*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

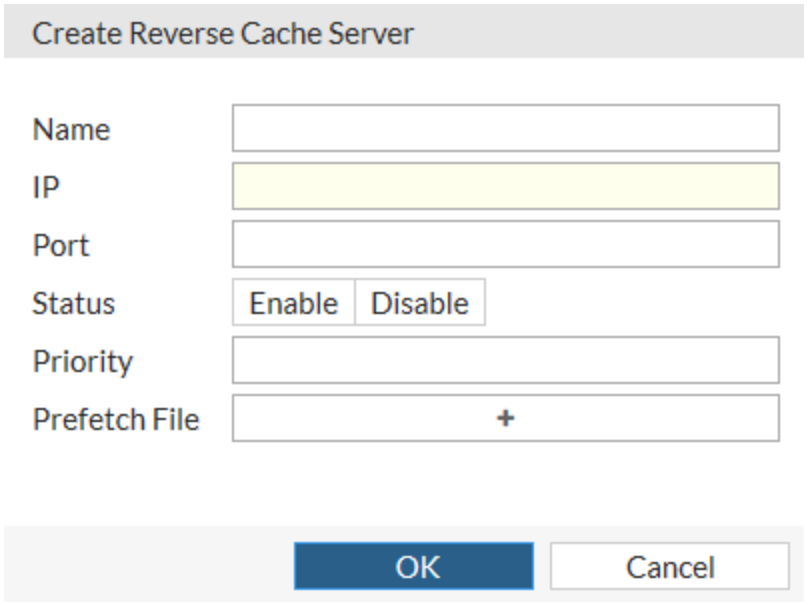
Create New	Add a new reverse cache server. See Create or edit a reverse cache server on page 754.
Edit	Edit the selected reverse cache server. See Create or edit a reverse cache server on page 754.
Delete	Delete the selected reverse cache server.
Name	The name of the reverse cache server.
IP	The IP address of the reverse cache server.
Port	The port number that the reverse cache server is using.
Status	The status is *Enabled* or *Disabled*.
Ref.	Displays the number of times the object is referenced to other objects.

	To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a reverse cache server

To create a reverse cache server:

1. Go to *Web Cache* > *Reverse Cache Server* and select *Create New* from the toolbar. The *Create Reverse Cache Server* window opens.



2. Configure the following settings:

Name	Enter a name for the reverse cache server.
IP	Enter the IP address of the reverse cache server.
Port	Enter the port number that the reverse cache server will use.
Status	Enable or disable the reverse cache server.
Priority	Enter a number to indicate the priority of the reverse cache server.
Prefetch File	If you created a prefetch file of URLs that you want preloaded, select + to open the Select Entries window and then select the prefetch file. To create a prefetch file, see Prefetch URLs on page 751.

3. Click *OK* to create the reverse cache server.

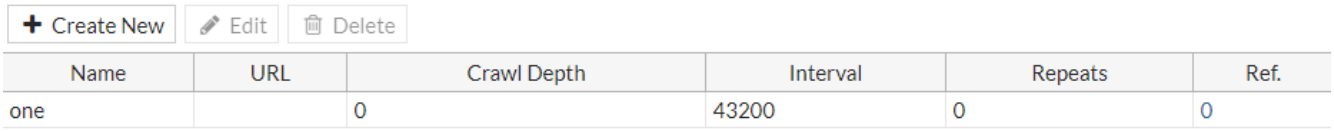
To edit a reverse cache server:

1. Go to *Web Cache* > *Reverse Cache Server*.
2. Select the server you want to edit and then click *Edit* from the toolbar or double-click on the server in the table. The *Edit Reverse Cache Server* window opens.
3. Edit the information as required and then click *OK* to apply your changes.

Prefetch File

Use the prefetch file to specify which URLs to preload.

To see the list of prefetch files, go to *Web Cache* > *Prefetch File*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

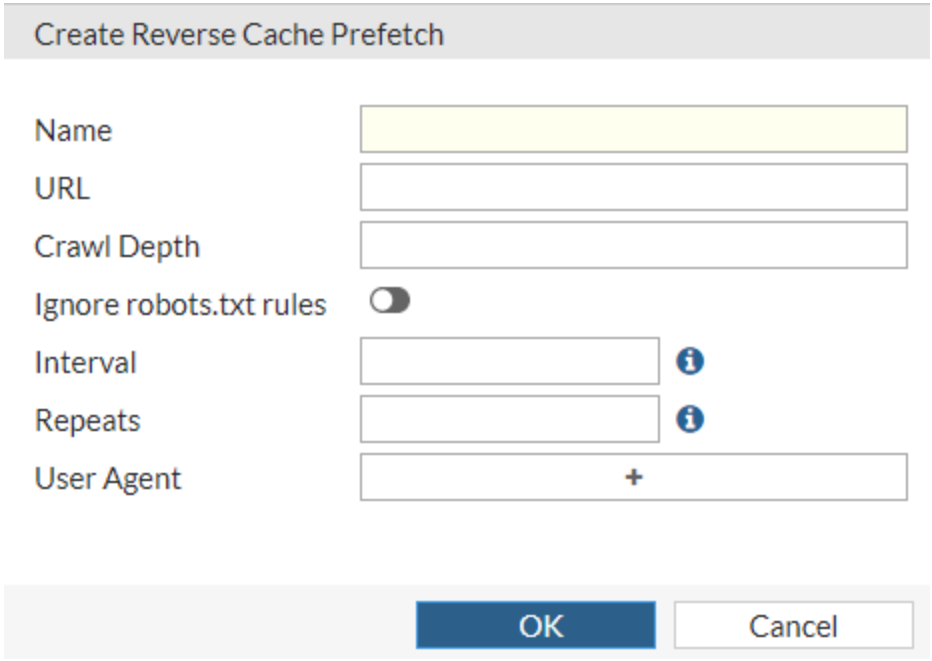
The following options are available:

Create New	Add a new prefetch file. See Create or edit a prefetch file on page 756.
Edit	Edit the selected prefetch file. See Create or edit a prefetch file on page 756.
Delete	Delete the selected reverse cache prefetch file.
Name	The name of the reverse cache prefetch file.
URL	The URLs to preload.
Crawl Depth	How many levels deep to preload.
Interval	How often, in seconds, to preload the URLs.
Repeats	How many times to preload the URLs. The value range is 0-4,200,000,000.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a prefetch file

To create a prefetch file:

1. Go to *Web Cache* > *Prefetch File* and select *Create New* from the toolbar.
   The *Create Reverse Cache Prefetch* window opens.



2. Configure the following settings:

Name	Enter a name for the reverse cache prefetch file.
URL	Enter the URLs to preload. Separate multiple URLS with a semicolon.
Crawl Depth	Enter how many levels deep to preload the URLs.
Ignore robots.txt rules	Enable to ignore the rules found in the `robots.txt` file.
Interval	Enter how often, in seconds, to preload the URLs.
Repeats	Enter how many times to preload the URLs. The value range is 0-4,200,000,000.
User Agent	The name of the computer program to use to preload the URLs. To create a user agent, see Create or edit a user agent on page 767.

3. Click *OK* to create the new reverse cache prefetch file.

To edit a prefetch file:

1. Go to *Web Cache* > *Prefetch File*.
2. Select the file that you want to edit and then click *Edit* from the toolbar or double-click on the file in the table.

The *Edit Reverse Cache Prefetch* window opens.

3. Edit the information as required, then click *OK* to apply your changes.

WCCP Settings

WCCP can be used to provide web caching with load balancing and fault tolerance. In a WCCP configuration, a WCCP server receives HTTP requests from users' web browsers and redirects the requests to one or more WCCP clients. The clients either return cached content or request new content from the destination web servers, before caching it and returning it to the server. The server then returns the content to the original requester. If a WCCP configuration includes multiple WCCP clients, the WCCP server balances traffic among the clients and can detect when a client fails and redirects traffic to still operating clients. WCCP is described by the Web Cache Communication Protocol internet draft.



You can purge specific cached content with a CLI command. See Purging specific cached content for details.

FortiProxy units operate as WCCP clients and support WCCPv2. FortiProxy units use UDP port 2048 for WCCP communication, with user traffic encapsulated in GRE-mode or L2-mode.

This section describes the following:

- WCCP service groups, numbers, IDs, and well-known services on page 758
- WCCP configuration overview on page 759
- Example: Caching HTTP sessions on page 760
- WCCP packet flow on page 763
- Configure forward and return methods and adding authentication on page 763
- WCCP messages on page 764
- Troubleshooting WCCP on page 765

WCCP service groups, numbers, IDs, and well-known services

A FortiProxy unit configured as a WCCP client can include multiple client configurations. Each of these configurations is called a WCCP service group. A service group consists of one or more FortiProxy units configured as WCCP servers (or routers) and one or more FortiProxy WCCP clients working together to cache a specific type of traffic. The service group configuration includes information about the type of traffic to be cached, the addresses of the WCCP clients and servers, and other information about the service.

A service group is identified with a numeric WCCP service ID (or service number) in the range 0 to 255. All of the servers and clients in the same WCCP service group must have service group configurations with the same WCCP service ID.

The value of the service ID provides some information about the type of traffic to be cached by the service group. Service IDs in the range 0 to 50 are reserved for well-known services. A well-known service is any service that is defined by the WCCP standard as being well known. Because the service is well known, you just need to specify the service ID to identify the traffic to be cached.

Even though the well-known service ID range is 0 to 50, only one well known service has been defined. Its service ID is 0, which is used for caching HTTP (web) traffic.

To configure WCCP to cache HTTP sessions, you can add a service group to the FortiProxy WCCP router and FortiProxy WCCP clients with a service ID of 0. No other information about the type of traffic to cache needs to be added to the service group.

Because service IDs 1 to 50 are reserved for well-known services and because these services are not defined yet, you should not add service groups with IDs in the range 1 to 50.



FortiProxy allows you to add service groups with IDs between 1 and 50. However, because these service groups have not been assigned as well-known services, they will not cache any sessions. Service groups with IDs 51 to 255 allow you to set the port numbers and protocol number of the traffic to be cached. So you can use service groups with IDs 51 to 255 to cache different kinds of traffic based on port numbers and protocol number of the traffic. Service groups 1 to 50 however, do not allow you to set port or protocol numbers, so they cannot be used to cache any traffic.

To cache traffic other than HTTP traffic you must add service groups with IDs in the range 51 to 255. These service group configurations must include the port numbers and protocol number of the traffic to be cached. It is the port and protocol number configuration in the service group that determines what traffic will be cached by WCCP.

WCCP configuration overview

To configure WCCP, you must create a service group that includes FortiProxy units configured as WCCP servers and FortiProxy units configured as WCCP clients. WCCP servers intercept sessions to be cached (for example, sessions from users browsing the web from a private network). To intercept sessions to be cached, the WCCP server must include a firewall policy that accepts sessions to be cached, and WCCP must be enabled in this firewall policy.

The server must have an interface configured for WCCP communication with WCCP clients. That interface sends and receives encapsulated GRE or L2 traffic to and from WCCP clients. The server must also include a WCCP service group that includes a service ID and the addresses of the WCCP clients, as well as other WCCP configuration options.

To use a FortiProxy unit as a WCCP client, you must configure an interface on the unit for WCCP communication. The client sends and receives encapsulated GRE traffic to and from the WCCP server using this interface.

The client must also include a WCCP service group with a service ID that matches a service ID on the server. The client service group also includes the IP address of the servers in the service group and specifies the port numbers and protocol number of the sessions that will be cached on the FortiProxy unit.

When the client receives sessions from the server on its WCCP interface, it either returns cached content over the WCCP interface or connects to the destination web servers using the appropriate interface, based on the client routing configuration. Content received from web servers is then cached by the client and returned to the WCCP server over the WCCP link. The server then returns the received content to the initial requesting user's web browser.

Finally, you might also need to configure routing on the FortiProxy server unit and FortiProxy client units, and you might need to add additional firewall policies to the server to accept sessions not cached by WCCP.

Example: Caching HTTP sessions

In this example configuration, a FortiProxy unit is operating as an Internet firewall for a private network. The port39 interface of the FortiProxy unit is connected to the Internet, and the port38 interface is connected to the internal network.

All HTTP traffic on port80 that is received at the port38 interface of the FortiProxy unit is accepted by a port39-to-port38 firewall policy with WCCP enabled. All other traffic received at the port2 interface is allowed to connect to the Internet by adding a general port38-to-port39 firewall policy below the HTTP-on-port-80 firewall policy.

A WCCP service group is added to the FortiProxy unit with a service ID of 0 for caching HTTP traffic on port80. The port1 interface of the FortiProxy unit is configured for WCCP communication.

A FortiProxy unit connects to the Internet through the FortiProxy unit. To allow for this, a port1-to-port39 firewall policy is added to the FortiProxy unit.

NOTE: The WCCP client can operate in L2 mode. The WCCP client firewall policy must specify which ingress interface is receiving the L2-forwarded traffic. This is different from GRE-mode, which uses the w.root interface.

Configure the WCCP client

You can configure the WCCP client in the GUI or CLI.

To configure the FortiProxy unit as a WCCP client using the GUI:

1. Go to *Network > Interfaces*.
2. Select an interface and then click *Edit*. If there are no interfaces in the list, select *Create New*.
3. Move the slider for *Enable WCCP Protocol* to enable WCCP on this interface and Click *OK* to save your changes.
4. Go to *Web Cache > WCCP Settings* and select *Create New*.
5. Configure the following settings:

Server ID	Enter the WCCP service group identifier. Enter *90* for the example network.
Cache ID	Enter the IP address that is known by all web cache routers. Enter *10.51.101.10* for the example network.

Router List	Enter the IP addresses of potential cache servers. Enter *10.51.101.100* for the example network.
Authentication	Enable or disable MD5 authentication. Select *Disable* for the example network.
Cache Engine Method	Select the method for forwarding traffic to the routers and for returning traffic to the cache engine, either *GRE* or *L2*. Select *GRE* or *L2* for the example network.
Assignment Method	Select the preferred assignment method for the hash key, either *HASH* or *MASK*. Select *HASH* or *MASK* for the example network.

6. Click *OK* to create the WCCP client.

To configure the FortiProxy unit as a WCCP client using the CLI:

Use the following steps to configure the FortiProxy unit as the WCCP client for the example network. The example steps only describe the WCCP-related configuration.

1. Enable the L2 mode:
```
config system wccp
   edit <Service-ID>
      set cache-engine-method L2
   next
end
```

2. Configure the FortiProxy unit to operate as a WCCP client:
```
config system settings
   set wccp-cache-engine enable
end
```



You cannot enter the `wccp-cache-engine enable` command if you have already added a WCCP service group. When you enter this command, an interface named w.root is added to the FortiProxy configuration. All traffic redirected from a WCCP router is considered to be received at this interface of the FortiProxy unit operating as a WCCP client. A default route to this interface with lowest priority is added.

3. Enable WCCP on the aggregate interface aggr1:
```
config system interface
   edit aggr1
      set ip 192.168.1.2 255.255.255.0
      set allowaccess ping https ssh snmp http telnet
      set type aggregate
      set explicit-web-proxy enable
      set member port1 port4
      set wccp enable
end
```

4. Add a WCCP service group with service ID 0:
```
config system wccp
```

```
      edit 0
         set router-list 192.168.1.2
         set cache-id 192.168.1.1
   end
```

5. Add a port-w.root-to-aggr1 firewall policy that accepts HTTP traffic on port80 and is configured for WCCP:

```
   config firewall policy
      edit 1
         set srcintf w.root
         set dstintf aggr1
         set srcaddr all
         set dstaddr all
         set action accept
         set schedule always
         set service HTTP
         set webcache enable
   end

config firewall central-snat-map
   edit 1
      set masquerade enable
      set srcintf w.root
      set dstintf aggr1
      set orig-addr "all"
      set dst-addr "all"
   next
end
```

NOTE: If the FortiProxy is operating in L2 mode, the firewall policy must specify the ingress interface where L2-forwarded traffic is being received:

```
config firewall policy
   edit 1
      set srcintf <port x>
      set dstintf <port y>
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service HTTP
      set webcache enable
end

config firewall central-snat-map
   edit 1
      set masquerade enable
      set srcintf <port x>
      set dstintf <port y>
      set orig-addr "all"
      set dst-addr "all"
   next
end
```

Verify the WCCP status

After setting up the FortiProxy unit as the WCCP client, you should verify to confirm that it is configured correctly.

```
diagnose test application wccp 2
   root: work mode:cache working NAT first_phy_id=8
      interface list:
         intf=aggr1, gid=8 phy_id=8
      service list:
         service: 0, cache_id=192.168.1.2, group=0.0.0.0, auth(no)
            forward=1, return=1, assign=1.
         router list:
            192.168.1.1
         port list:
            ecache_id=192.168.1.2

diagnose test application wccp 6
   service-0 in root
   erouter_list: 1 routers in total
      0. 192.168.1.1
      receive_id:23573 change_number:2
      cache servers seen by this router:
         0. 192.168.1.2 weight:0 (*Designated Web Cache)
```

WCCP packet flow

The following packet flow sequence assumes you have configured a FortiProxy unit to be a WCCP server and one or more FortiProxy units to be WCCP clients.

1. A user's web browser sends a request for web content.
2. The FortiProxy unit configured as a WCCP server includes a firewall policy that intercepts the request and forwards it to a FortiProxy WCCP client.
3. The firewall policy can apply UTM features to traffic accepted by the policy.
4. The FortiProxy WCCP client receives the WCCP session.
5. The client either returns requested content to the WCCP server if it is already cached or connects to the destination web server, receives and caches the content, and then returns it to the WCCP server.
6. The WCCP server returns the requested content to the user's web browser.
7. The WCCP router returns the request to the client web browser. The client web browser is not aware that all this is taking place and does not have to be configured to use a web proxy.

Configure forward and return methods and adding authentication

The WCCP forwarding method determines how intercepted traffic is transmitted from the WCCP router to the WCCP cache engine. FortiProxy units use GRE forwarding.

GRE forwarding encapsulates the intercepted packet in an IP GRE header with a source IP address of the WCCP router and a destination IP address of the target WCCP cache engine. The result is a tunnel that allows the WCCP router to be multiple hops away from the WCCP cache server.

By default, the WCCP communication between the router and cache servers is unencrypted. If you are concerned about attackers sniffing the information in the WCCP stream, you can use the following command to enable hash-based authentication of the WCCP traffic. You must enable authentication on the router and the cache engines, and all must have the same password.

```
config system wccp
   edit 1
      set authentication enable
      set password <password>
end
```

Purging specific cached content

You can purge specific cached content with the following CLI command:

```
execute webcache delete [pattern_type] [pattern_string]
```

For *[pattern_type]*, there are three choices:

- `simple`—a simple string following the pattern [domain_string]:[port_string]/[path_string]
- `wildcard`—a wild-card match following the pattern [domain_wildcard]:[port_wildcard]/[path_wildcard]
- `regexp`—a Perl regular expression

To delete all cached content from www.domain.com/path:

```
execute webcache delete simple www.domain.com:80/path
```

To delete all content from .com www sites

```
execute webcache delete wildcard www.*.com:*/*
```

To verify the status of a purge request

```
execute webcache delete status
```

WCCP messages

When the WCCP service is active on a web cache server, it periodically sends a WCCP HERE I AM broadcast or unicast message to the FortiProxy unit operating as a WCCP router. This message contains the following information:

- Web cache identity (the IP address of the web cache server)
- Service information (the service group to join)

If the information received in this message matches what is expected, the FortiProxy unit replies with a WCCP I SEE YOU message that contains the following details:

- Router identity (the FortiProxy unit's IP address)
- Sent to IP (the web cache IP addresses to which the packets are addressed)

When both ends receive these two messages, the connection is established, the service group is formed, and the designated web cache is elected.

Troubleshooting WCCP

Two types of debug commands are available for debugging or troubleshooting a WCCP connection between a FortiProxy unit operating as a WCCP router and its FortiProxy WCCP cache engines.

Real-time debugging

The following commands can capture live WCCP messages:

```
diagnose debug enable
diagnose debug application wccpd <debug level>
```

Application debugging

The following commands display information about WCCP operations:

```
get test wccpd <integer>
diagnose test application wccpd <integer>
```

Where `<integer>` is a value between 1 and 5:

1. Display WCCP statistics
2. Display WCCP configuration
3. Display WCCP cache servers
4. Display WCCP services
5. Display WCCP assignment

Enter the following command to view the debugging output:

```
diagnose test application wccpd 3
```

Sample output from a successful WCCP connection:

```
service-0 in root: num=1, usable=1
cache server ID:
len=44, addr=172.16.78.8, weight=4135, status=0
rcv_id=6547, usable=1, fm=1, nq=0, dev=3(k3),
to=192.168.11.55
ch_no=0, num_router=1:
192.168.11.55
```

Sample output from the same command from an unsuccessful WCCP connection (because of a service group password mismatch):

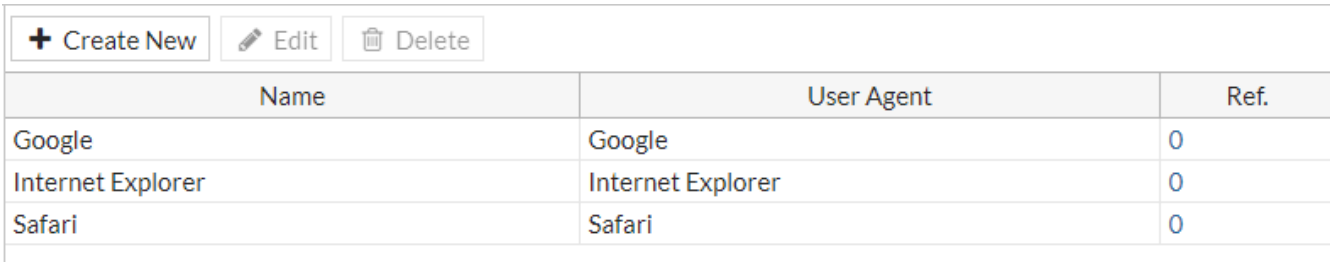
```
service-0 in root: num=0, usable=0
diag debug application wccpd -1
Sample output:
wccp_on_recv()-98: root recv: num=160, dev=3(3),
```

```
172.16.78.8->192.168.11.55
wccp2_receive_pkt()-1124: len=160, type=10, ver=0200,
length=152
wccp2_receive_pkt()-1150: found component:t=0, len=20
wccp2_receive_pkt()-1150: found component:t=1, len=24
wccp2_receive_pkt()-1150: found component:t=3, len=44
wccp2_receive_pkt()-1150: found component:t=5, len=20
wccp2_receive_pkt()-1150: found component:t=8, len=24
wccp2_check_security_info()-326: MD5 check failed
```

User Agent

You can specify which computer programs are used to preload URLs. Multiple browsers are supported, such as Chrome, Safari, Firefox, and Internet Explorer. After you define a user agent, you can select it when you create prefetch URLs or reverse cache prefetch URLs.

To see the list of user agents, go to *Web Cache* > *User Agent*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

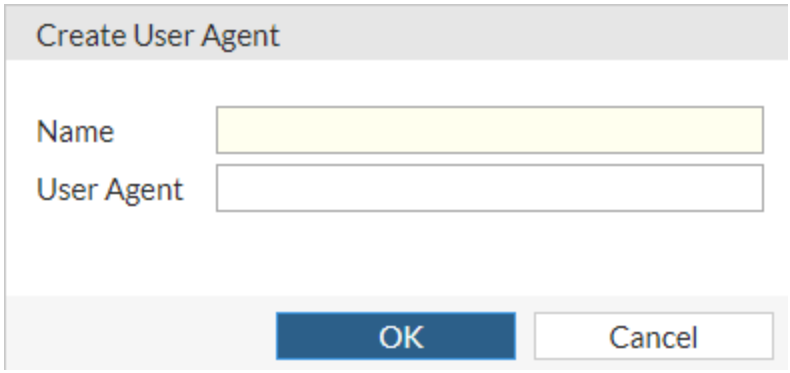
The following options are available:

Create New	Add a new user agent. See Create or edit a user agent on page 767.
Edit	Edit the selected user agent. See Create or edit a user agent on page 767.
Delete	Delete the selected user agent.
Name	The name of the user agent.
User Agent	The name of the computer program to use to preload the URLs.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a user agent

To create a user agent:

1. Go to *Web Cache* > *User Agent* and select *Create New* from the toolbar. The *Create User Agent* window opens.



2. Configure the following settings:

Name	Enter a name for the user agent.
User Agent	Enter the name of the browser.

3. Click *OK* to create the new user agent.

To edit a user agent:

1. Go to *Web Cache* > *User Agent*.
2. Select the user agent you want to edit and then click *Edit* from the toolbar or double-click on the server in the table. The *Edit User Agent* window opens.
3. Edit the information as required and then click *OK* to apply your changes.

VPN

FortiProxy supports site-to-site IPsec VPN, which allows offices in multiple, fixed locations to establish secure connections with each other over a public network such as the Internet. One use case is branch offices using the Internet to access the main office's intranet. To achieve this, you can install a FortiProxy unit on a private branch network and another on the headquarter network.

Instead of remotely logging on to a private network using an unencrypted and insecure Internet connection, the use of a VPN ensures that unauthorized parties cannot access the office network and cannot intercept any of the information that is exchanged between the branch offices and the headquarter office.

The following topics are included in this section:

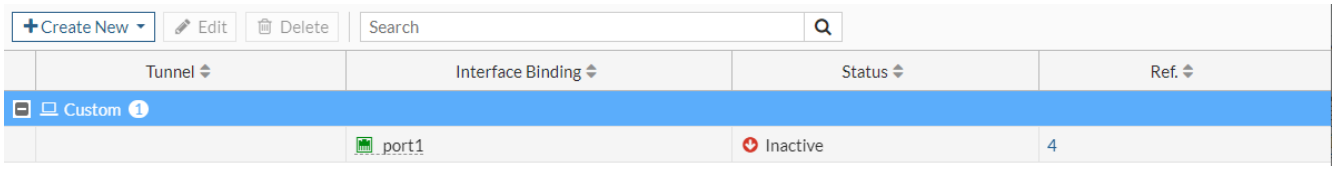
- IPsec Tunnels on page 768
- IPsec Wizard on page 773
- IPsec Tunnel Template on page 780

IPsec Tunnels

The data path between a user's computer and a private network through a VPN is referred to as a tunnel. Like a physical tunnel, the data path is accessible only at both ends. Encapsulation makes this possible. IPsec packets pass from one end of the tunnel to the other and contain data packets that are exchanged between the local user and the remote private network. Encryption of the data packets ensures that any third-party who intercepts the IPsec packets can not access the data.

In FortiProxy, you can create a VPN tunnel between a FortiProxy unit in the branch office and a FortiProxy unit on the office private network.

To view a list of IPsec tunnels, go to *VPN > IPsec Tunnels*. After you create an IPsec VPN tunnel, it appears in the VPN tunnel list.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

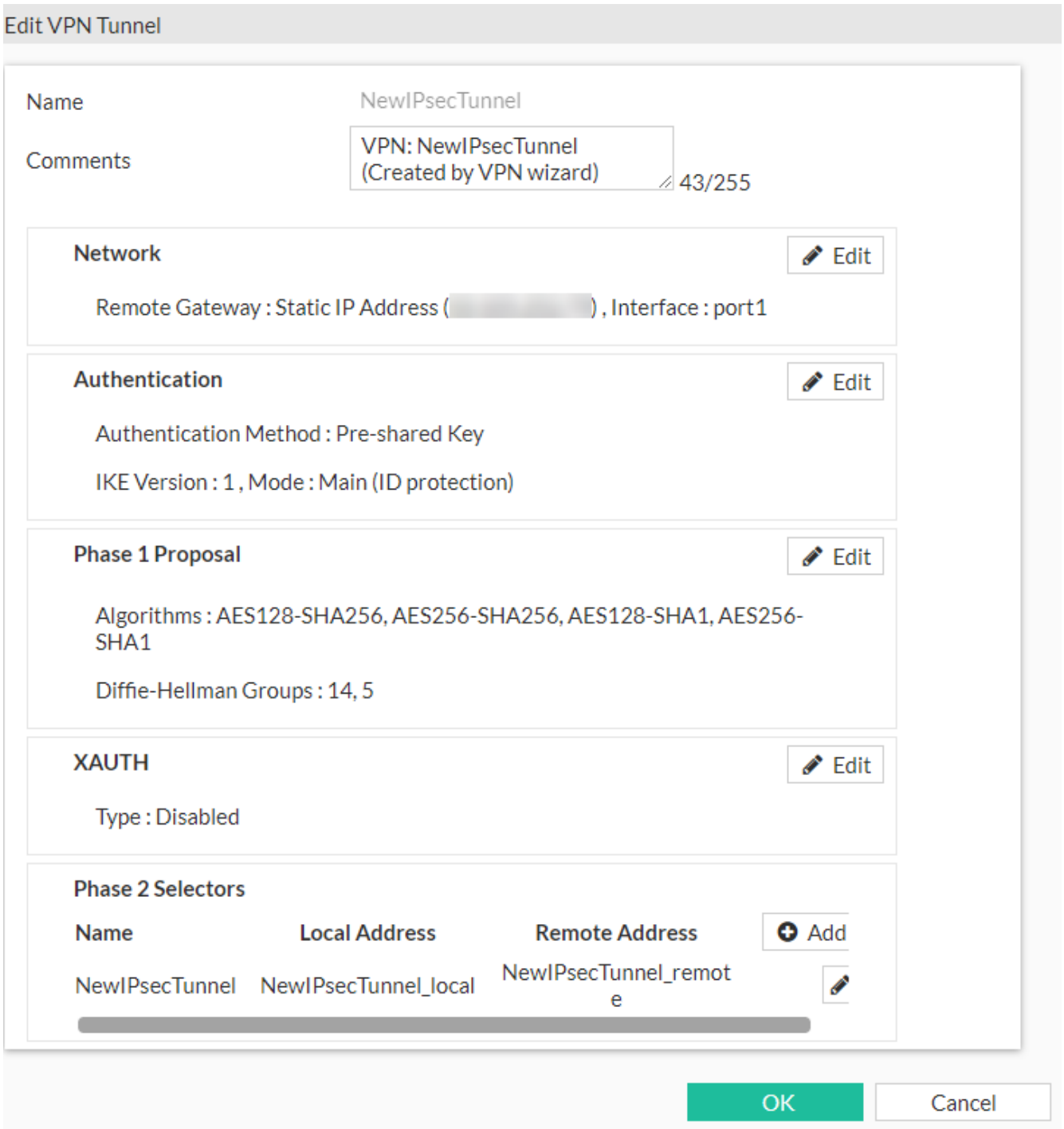
The following options are available:

Create New > IPsec Tunnel	Run the IPsec Wizard and create an IPsec tunnel. See IPsec Wizard on page 773.

Edit	Edit an IPsec tunnel. See Edit an IPsec tunnel on page 769.
Delete	Delete the selected IPsec tunnel.
Search	Enter a search term to find in the list.
Tunnel	The name of the IPsec tunnel.
Interface Binding	Select the name of the interface through which remote peers connect to the FortiProxy unit.
Status	The status is *Active* or *Inactive*.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.
Aggregate Weight	The aggregate weight.
Comments	An optional description of the IPsec tunnel.
IKE Version	The default IKE version is 1.
Mode	The mode is *Aggressive* or *Main (ID Protection)*: • *Main (ID Protection)*—The Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*—The Phase 1 parameters are exchanged in single message with authentication information that is not encrypted.
Phase 2 Selectors	The name of phase 2.

Edit an IPsec tunnel

Select an IPsec tunnel and then click *Edit* to open the *Edit VPN Tunnel* page.



Configure the following settings in the *Edit VPN Tunnel* page. After each editing a section, select the checkmark icon to save your changes. After you make all of your changes, click *OK*.

Name	The name of the IPsec tunnel cannot be changed.
Comments	An optional description of the IPsec tunnel.

Network	Select *Edit* to make changes.
IP Version	This option is set to *IPv4*.
Remote Gateway	This option is set to *Static IP Address* for a remote peer that has a static IP address.
IP Address	Enter the IP address of the remote peer.
Interface	Select the name of the interface through which remote peers connect to the FortiProxy unit.
Local Gateway	Enable this option to configure a local gateway and then select *Primary IP*, *Secondary IP*, or *Specify*. Enter or select the IP address.
NAT Traversal	Select *Enable* if a NAT device exists between the local FortiProxy unit. and the VPN peer or client. The local FortiProxy unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably. Additionally, you can force IPsec to use NAT traversal. If this option is set to *Forced*, the FortiProxy unit uses a port value of zero when constructing the NAT discovery hash for the peer. This causes the peer to think it is behind a NAT device, and it will use UDP encapsulation for IPsec, even if no NAT is present. This approach maintains interoperability with any IPsec implementation that supports the NAT-T RFC.
Keepalive Frequency	If you selected *Enable* or *Forced* for the NAT traversal, enter a keep-alive frequency.
Forward Error Correction	Select *Egress* or *Ingress*.
Add route	Select *Enabled* if you want to add a route.
Auto discovery sender	Select *Enabled* to automatically discover the sender.
Auto discover receiver	Select *Enabled* to automatically discover the receiver.
Authentication	Select *Edit* to make changes.
Method	Select *Pre-shared Key* or *Signature*: • *Pre-shared Key*—A preshared key contains at least six random alphanumeric characters. Users of the VPN must obtain the preshared key from the person who manages the VPN server and add the preshared key to their VPN client configuration. • *Signature*—Use one or more certificates for authentication.
Pre-shared Key	If you selected *Pre-shared Key* for the authentication method, enter the pre-shared key that the FortiProxy unit will use to authenticate itself to the remote peer or dial-up client during Phase 1 negotiations. You must define the same key at the remote peer or client.

	The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. The limit is 128 characters.
Certificate Name	If you selected *Signature* for the authentication method, select + and then select one or more certificates that the FortiProxy unit will use to authenticate itself.
Version	IKE version 1 is selected by default.
Mode	Select *Aggressive* or *Main (ID protection)*: • *Main (ID protection)*—The Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*—The Phase 1 parameters are exchanged in single message with authentication information that is not encrypted.
Phase 1 Proposal	Select *Edit* to make changes. Select *Add* to get another row of Encryption and Authentication options.
Encryption	Select *DES*, *3DES*, *AES128*, *AES192*, *AES256*to use as the encryption algorithm.
Authentication	Select *MD5*, *SHA1*, *SHA256*, *SHA384*, or *SHA512* to use for authentication.
Diffie-Hellman Groups	Select one or more Diffie-Hellman (DH) asymmetric key algorithms for public key cryptography.
Key Lifetime (seconds)	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key lifetime can be from 120 to 172,800 seconds.
Local ID	A Local ID is an alphanumeric value.
XAUTH	Select *Edit* to make changes.
Type	Select *Client* to require an additional user name and password for authentication.
Username	If you selected *Client*, enter a user name for authentication.
Password	If you selected *Client*, enter a password for authentication.
Phase 2 Selectors	Select *Add* to enter new phase-2 information.
Name	Enter the Phase-2 name.
Comments	An optional description of the VPN tunnel.
Local Address	Select *Subnet*, *IP Range*, *IP Address*, *Named Address,IPv6 Subnet*, *IPv6 Range*, *IPv6 Address*, or *Named IPv6 Address* and then enter the specified information.

Remote Address	Select *Subnet*, *IP Range*, *IP Address*, *Named Address*,*IPv6 Subnet*, *IPv6 Range*, *IPv6 Address*, or *Named IPv6 Address* and then enter the specified information.
Phase 2 Proposal	Select *Add* to get another row of Encryption and Authentication options.
Encryption	Select *DES*, *3DES*, *AES128*, *AES128GCM*, *AES192*, *AES256* or *CHACHA20POLY1305* to use as the encryption algorithm.
Authentication	Select *MD5*, *SHA1*, *SHA256*, *SHA384*, or *SHA512* to use for authentication.
Enable Replay Detection	Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
Enable Perfect Forward Secrecy (PFS)	Enable for PFS.
Local Port	Select *All* or enter the local port number.
Remote Port	Select *All* or enter the remote port number.
Protocol	Select *All* or enter the protocol number.
Auto-negotiate	Enable the option if you want the tunnel to be automatically renegotiated when the tunnel expires.
Autokey Keep Alive	Select the check box if you want the tunnel to remain active when no data is being processed.
Key Lifetime	Select the method for determining when the Phase 2 key expires: *Seconds*, *Kilobytes*, or *Both*. If you select *Both*, the key expires when either the time has passed or the number of kilobytes have been processed.
Seconds	If you selected *Seconds* or *Both* for the key lifetime, enter the number of seconds.
Kilobytes	If you selected *Kilobytes* or *Both* for the key lifetime, enter the number of kilobytes.

IPsec Wizard

To set up an IPsec VPN:

1. Go to *VPN > IPsec Wizard*.
2. Configure the VPN setup and then select *Next*:

Name	Enter a unique descriptive name (15 characters or less) for the VPN tunnel.

Template Type	Select *Site to Site* or *Custom*: • *Site to Site*—Static tunnel between this FortiProxy unit and a remote FortiProxy unit through the Internet. • *Custom*—No template. See Create a custom VPN tunnel on page 775.
NAT Configuration	If you selected *Site to Site*, select *No NAT between sites*, *This site is behind NAT*, or *The remote site is behind NAT*.
Remote Device type	If you selected *Site to Site*, select *FortiProxy* or *Cisco*.

3. Configure the authentication and then select *Next*:

Remote Device	If you selected *Site to Site* for the template type, select *IP Address* or *Dynamic DNS*.
Remote IP Address	If you selected *IP Address* for the remote address, enter the IP address of the remote peer.
FQDN	If you selected *Dynamic DNS* for the remote address, enter the domain name of the remote peer.
Outgoing Interface	If you selected *Site to Site* for the template type, select the outgoing interface from the drop-down list.
Incoming Interface	If you selected *Remote Access* for the template type, select the incoming interface from the drop-down list.
Authentication Method	Select *Pre-shared Key* or *Signature*: • *Pre-shared Key*—A preshared key contains at least six random alphanumeric characters. Users of the VPN must obtain the preshared key from the person who manages the VPN server and add the preshared key to their VPN client configuration. • *Signature*—Use one or more certificates for authentication.
Pre-shared Key	If you selected *Pre-shared Key* for the authentication method, enter the pre-shared key that the FortiProxy unit will use to authenticate itself to the remote peer or dial-up client during Phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. The limit is 128 characters.
Certificate Name	If you selected *Signature* for the authentication method, select + and then select one or more certificates that the FortiProxy unit will use to authenticate itself.
Peer Certificate CA	If you selected *Signature* for the authentication method, select a peer certificate authority.

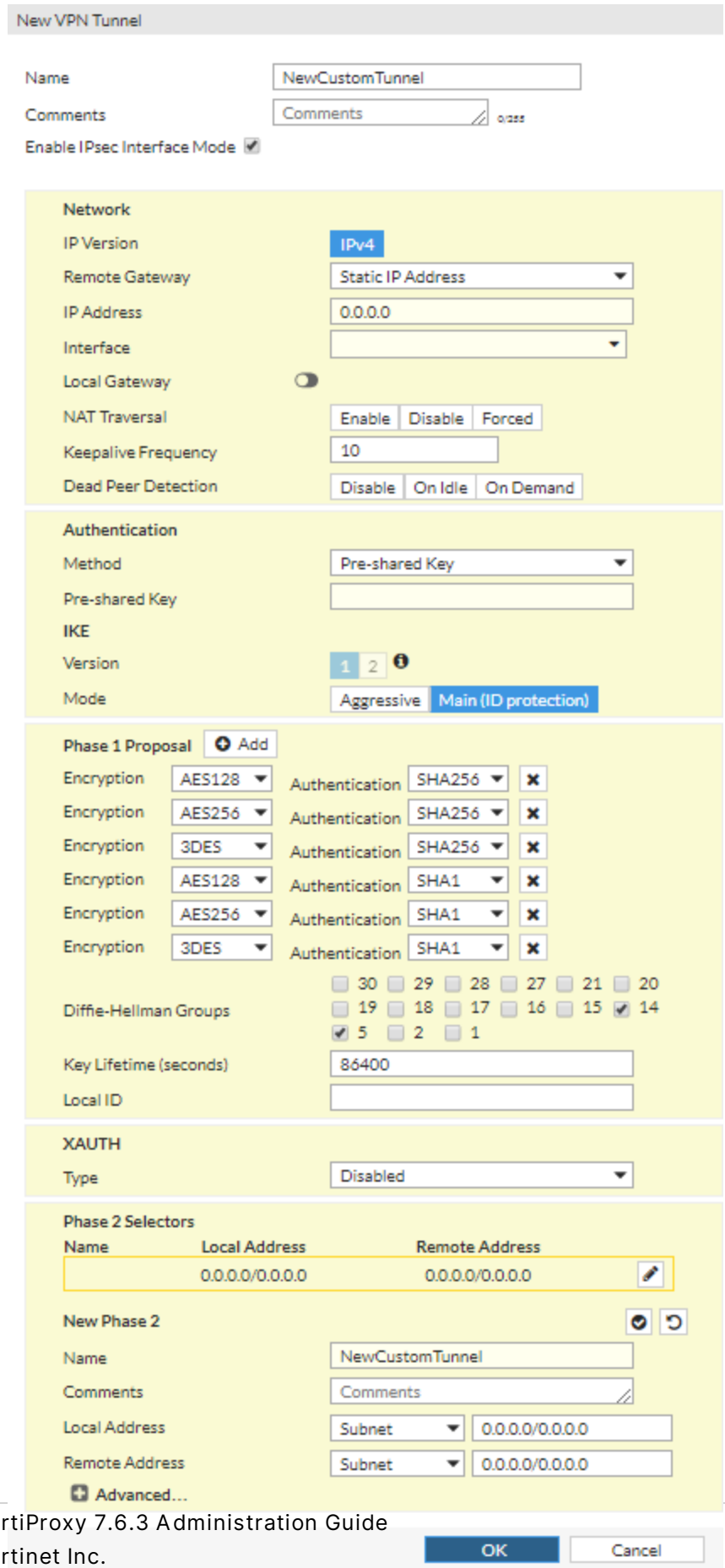
4. Configure the policy and routing settings:

Local Interface	Select the name of the interface through which remote peers or dial-up clients connect to the FortiProxy unit.
Local Subnets	If you selected *Site to Site* for the template type, enter a local subnet. Select + to enter another local subnet.
Remote Subnets	Enter a remote subnet. Select + to enter another remote subnet.
Internet Access	Select *None*, *Share Local*, or *Use Remote*. • *None*—Site-to-site devices communicate over the VPN, but Internet access does not require VPN. • *Share Local*—Allow the remote site to use this FortiProxy as an Internet gateway. • *Use Remote*—This FortiProxy unit will use a tunnel for Internet access from the remote location.
Shared WAN	If you selected *Share Local* for Internet access, select the WAN interface.
Local Gateway	If you selected *Use Remote* for Internet access, enter the local gateway address.

5. Select *Create*.
6. Select *Add Another* to start at the beginning of the IPsec Wizard or select *Show Tunnel List* to see the available IPsec tunnels.

Create a custom VPN tunnel

If you select *Custom* for the template type in the IPsec Wizard and then select *Next*, the *New VPN Tunnel* window opens.


New VPN Tunnel
Name
NewCustomTunnel
Comments
Comments
0/255
Enable IPsec Interface Mode
Network
IP Version
IPv4
Remote Gateway
Static IP Address
IP Address
0.0.0.0
Interface
Local Gateway
NAT Traversal
Enable
Disable
Forced
Keepalive Frequency
10
Dead Peer Detection
Disable
On Idle
On Demand
Authentication
Method
Pre-shared Key
Pre-shared Key
IKE
Version
1
2
Mode
Aggressive
Main (ID protection)
Phase 1 Proposal
Add
Encryption
AES128
Authentication
SHA256
Encryption
AES256
Authentication
SHA256
Encryption
3DES
Authentication
SHA256
Encryption
AES128
Authentication
SHA1
Encryption
AES256
Authentication
SHA1
Encryption
3DES
Authentication
SHA1
Diffie-Hellman Groups
30
29
28
27
21
20
19
18
17
16
15
14
5
2
1
Key Lifetime (seconds)
86400
Local ID
XAUTH
Type
Disabled
Phase 2 Selectors
Name
Local Address
Remote Address
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0
New Phase 2
Name
NewCustomTunnel
Comments
Comments
Local Address
Subnet
0.0.0.0/0.0.0.0
Remote Address
Subnet
0.0.0.0/0.0.0.0
Advanced...
OK
Cancel

Configure the following settings and then click *OK*:

Name	Type a name for the Phase 1 definition.
Comments	An optional description of the VPN tunnel.
Enable IPsec Interface Mode	Select this option if you want to create an IPsec VPN tunnel.
IP Version	This option is set to *IPv4*.
Remote Gateway	This option is set to *Static IP Address* for a remote peer that has a static IP address.
IP Address	Enter the IP address of the remote peer.
Interface	Select the name of the interface through which remote peers connect to the FortiProxy unit.
Local Gateway	Enable this option to configure a local gateway and then select *Primary IP*, *Secondary IP*, or *Specify*. Enter or select the IP address.
NAT Traversal	Select *Enable* if a NAT device exists between the local FortiProxy unit. and the VPN peer or client. The local FortiProxy unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably. Additionally, you can force IPsec to use NAT traversal. If this option is set to *Forced*, the FortiProxy unit uses a port value of zero when constructing the NAT discovery hash for the peer. This causes the peer to think it is behind a NAT device, and it will use UDP encapsulation for IPsec, even if no NAT is present. This approach maintains interoperability with any IPsec implementation that supports the NAT-T RFC.
Keepalive Frequency	If you selected *Enable* or *Force*d for the NAT traversal, enter a keep-alive frequency.
Dead Peer Detection	Select *On Idle* to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. With *On Idle* or *On Demand* selected, you can use the `config vpn ipsec phase1` (tunnel mode) or `config vpn ipsec phase1-interface` (interface mode) CLI command to optionally specify a retry count and a retry interval.
Method	Select *Pre-shared Key* or *Signature*: • *Pre-shared Key*—A preshared key contains at least six random alphanumeric characters. Users of the VPN must obtain the preshared key from the person who manages the VPN server and add the preshared key to their VPN client configuration. • *Signature*—Use one or more certificates for authentication.

Pre-shared Key	If you selected *Pre-shared Key* for the authentication method, enter the pre-shared key that the FortiProxy unit will use to authenticate itself to the remote peer or dial-up client during Phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. The limit is 128 characters.
Certificate Name	If you selected *Signature* for the authentication method, select + and then select one or more certificates that the FortiProxy unit will use to authenticate itself.
Version	IKE version 1 is selected by default.
Mode	Select *Aggressive* or *Main (ID protection)*: • *Main (ID protection)*—The Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*—The Phase 1 parameters are exchanged in single message with authentication information that is not encrypted.
Accept Types	If you selected *Pre-shared Key* for the authentication method and selected aggressive mode, select *Any peer ID* or *Specific peer ID*. If you select *Specific peer ID*, enter the peer ID. If you selected *Signature* for the authentication method, select *Any peer ID*, *Specific peer ID*, or *Peer certificate*.
Peer ID	If you selected *Any peer ID*, enter the peer ID.
Peer certificate	If you selected *Peer certificate* for the authentication method, select the certificate.
Phase 1 Proposal	Select *Add* to get another row of Encryption and Authentication options.
Encryption	Select *DES*, *3DES*, *AES128*, *AES192*, and *AES256* to use as the encryption algorithm. *AES256* is the most secure; *DES* is the least secure.
Authentication	Select *MD5*, *SHA1*, *SHA256*, *SHA384*, *SHA512*, or *SHA256* to use for authentication.
Diffie-Hellman Groups	Select one or more Diffie-Hellman (DH) asymmetric key algorithms for public key cryptography.
Key Lifetime (seconds)	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key lifetime can be from 120 to 172,800 seconds.
Local ID	A Local ID is an alphanumeric value.

Type	Select *Client* to require an additional user name and password for authentication.
User Name	If you selected *Client*, enter a user name for authentication.
Password	If you selected *Client*, enter a password for authentication.
Name	By default, the Phase-2 name is the same as the Phase-1 name.
Comments	An optional description of the VPN tunnel.
Local Address	Select *Subnet*, *IP Range*, *IP Address*, *Named Address*,*IPv6 Subnet*, *IPv6 Range*, *IPv6 Address*, or *Named IPv6 Address* and then enter the specified information.
Remote Address	Select *Subnet*, *IP Range*, *IP Address*, *Named Address*,*IPv6 Subnet*, *IPv6 Range*, *IPv6 Address*, or *Named IPv6 Address* and then enter the specified information.
Phase 2 Proposal	Select *Add* to get another row of Encryption and Authentication options.
Encryption	Select *NULL*, *DES*, *3DES*, *AES128*, *AES128GCM*, *AES192*, *AES256*, or *AES256GCM* to use as the encryption algorithm. *NULL* is the least secure; *AES256GCM* is the most secure.
Authentication	Select *NULL*, *MD5*, *SHA1*, *SHA256*, *SHA384*, or *SHA512* to use for authentication.
Enable Replay Detection	Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
Enable Perfect Forward Secrecy (PFS)	Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
Local Port	Select *All* or enter the local port number.
Remote Port	Select *All* or enter the remote port number.
Protocol	Select *All* or enter the protocol number.
Auto-negotiate	Enable the option if you want the tunnel to be automatically renegotiated when the tunnel expires.
Autokey Keep Alive	Select the check box if you want the tunnel to remain active when no data is being processed.
Key Lifetime	Select the method for determining when the Phase 2 key expires: *Seconds*, *Kilobytes*, or *Both*. If you select *Both*, the key expires when either the time has passed or the number of kilobytes have been processed.
Seconds	If you selected *Seconds* or *Both* for the key lifetime, enter the number of seconds.
Kilobytes	If you selected *Kilobytes* or *Both* for the key lifetime, enter the number of kilobytes.

IPsec Tunnel Template

Several tunnel templates are available in the IPsec VPN Wizard that cover a variety of different types of IPsec VPN. Go to *VPN > IPsec Tunnel Template* to see a list and descriptions of these templates:

- Site to Site - FortiProxy
- Site to Site - Cisco

Select a template and then select *View* to see the template details.

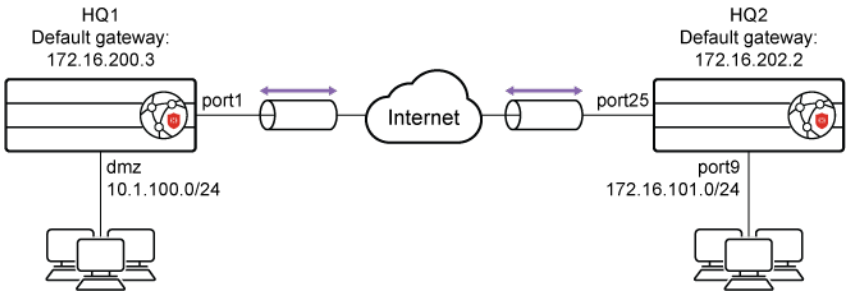
FortiProxy-to-FortiProxy

This section contains the following topics about FortiProxy-to-FortiProxy VPN configurations:

- Basic site-to-site VPN with pre-shared key on page 780
- Site-to-site VPN with digital certificate on page 785
- GRE over IPsec on page 791

Basic site-to-site VPN with pre-shared key

This is a sample configuration of IPsec VPN authenticating a remote FortiProxy peer with a pre-shared key.



To configure IPsec VPN authenticating a remote FortiProxy peer with a pre-shared key in the GUI:

1. Configure the HQ1 FortiProxy.
   a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
      i. Enter a VPN name.
      ii. For *Template Type*, select *Site to Site*.
      iii. For *Remote Device Type*, select *FortiProxy*.
      iv. For *NAT Configuration*, select *No NAT Between Sites*.
      v. Click *Next*.

   b. Configure the following settings for *Authentication*:
      i. For *Remote Device*, select *IP Address*.
      ii. For the IP address, enter *172.16.202.1*.
      iii. For *Outgoing interface*, enter *port1*.
      iv. For *Authentication Method*, select *Pre-shared Key*.
      v. In the *Pre-shared Key* field, enter *sample* as the key.
      vi. Click *Next*.
   c. Configure the following settings for *Policy & Routing*:
      i. From the *Local Interface* dropdown menu, select the local interface.
      ii. Configure the *Local Subnets* as *10.1.100.0*.
      iii. Configure the *Remote Subnets* as *172.16.101.0*.
      iv. Click *Create*.
2. Configure the HQ2 FortiProxy.
   a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
      i. Enter a VPN name.
      ii. For *Template Type*, select *Site to Site*.
      iii. For *Remote Device Type*, select *FortiProxy*.
      iv. For *NAT Configuration*, select *No NAT Between Sites*.
      v. Click *Next*.
   b. Configure the following settings for *Authentication*:
      i. For *Remote Device*, select *IP Address*.
      ii. For the IP address, enter *172.16.2001*.
      iii. For *Outgoing interface*, enter *port25*.
      iv. For *Authentication Method*, select *Pre-shared Key*.
      v. In the *Pre-shared Key* field, enter *sample* as the key.
      vi. Click *Next*.
   c. Configure the following settings for *Policy & Routing*:
      i. From the *Local Interface* dropdown menu, select the local interface.
      ii. Configure *Local Subnets* as *172.16.101.0*.
      iii. Configure the *Remote Subnets* as *10.1.100.0*.
      iv. Click *Create*.

To configure IPsec VPN authenticating a remote FortiProxy peer with a pre-shared key using the CLI:

1. Configure the WAN interface and default route. The WAN interface is the interface connected to the ISP. The IPsec tunnel is established over the WAN interface.
   a. Configure HQ1.

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 172.16.200.1 255.255.255.0
    next
end
config router static
```

```
    edit 1
        set gateway 172.16.200.3
        set device "port1"
    next
end
```

b. Configure HQ2.

```
config system interface
    edit "port25"
        set vdom "root"
        set ip 172.16.202.1 255.255.255.0
    next
end
config router static
    edit 1
        set gateway 172.16.202.2
        set device "port25"
    next
end
```

2. Configure the internal (protected subnet) interface. The internal interface connects to the corporate internal network. Traffic from this interface routes out the IPsec VPN tunnel.
   a. Configure HQ1.

```
config system interface
    edit "dmz"
        set vdom "root"
        set ip 10.1.100.1 255.255.255.0
    next
end
```

   b. Configure HQ2.

```
config system interface
    edit "port9"
        set vdom "root"
        set ip 172.16.101.1 255.255.255.0
    next
end
```

3. Configure the IPsec phase1-interface.
   a. Configure HQ1.

```
config vpn ipsec phase1-interface
    edit "to_HQ2"
        set interface "port1"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 172.16.202.1
        set psksecret sample
```

```
    next
end
```

b. Configure HQ2.

```
config vpn ipsec phase1-interface
    edit "to_HQ1"
        set interface "port25"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 172.16.200.1
        set psksecret  sample
    next
end
```

4. Configure the IPsec phase2-interface.

a. Configure HQ1.

```
config vpn ipsec phase2-interface
    edit "to_HQ2"
        set phase1name "to_HQ2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set auto-negotiate enable
    next
end
```

b. Configure HQ2.

```
config vpn ipsec phase2-interface
    edit "to_HQ2"
        set phase1name "to_HQ1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set auto-negotiate enable
    next
end
```

5. Configure the static routes. Two static routes are added to reach the remote protected subnet. The blackhole route is important to ensure that IPsec traffic does not match the default route when the IPsec tunnel is down.

a. Configure HQ1.

```
config router static
    edit 2
        set dst 172.16.101.0 255.255.255.0
        set device "to_HQ2"
    next
```

b. Configure HQ2.

```
config router static
    edit 2
        set dst 10.1.100.0 255.255.255.0
        set device "to_HQ1"
    next
```

6. Configure two firewall policies to allow bidirectional IPsec traffic flow over the IPsec VPN tunnel.
   a. Configure HQ1.

```
config firewall policy
    edit 1
        set name "inbound"
        set srcintf "to_HQ2"
        set dstintf "dmz"
        set srcaddr "172.16.101.0"
        set dstaddr "10.1.100.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "outbound"
        set srcintf "dmz"
        set dstintf "to_HQ2"
        set srcaddr "10.1.100.0"
        set dstaddr "172.16.101.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

   b. Configure HQ2.

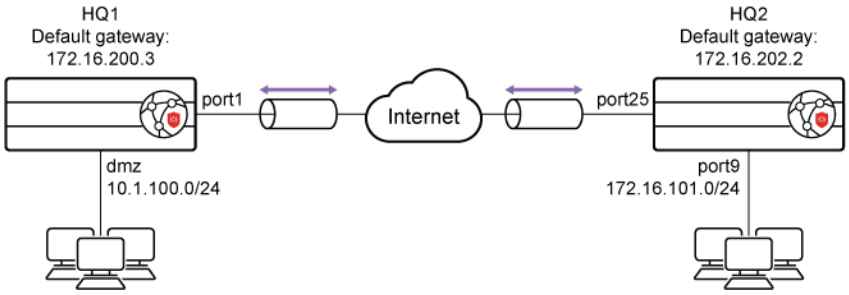
```
config firewall policy
    edit 1
        set name "inbound"
        set srcintf "to_HQ1"
        set dstintf "port9"
        set srcaddr "10.1.100.0"
        set dstaddr "172.16.101.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "outbound"
        set srcintf "port9"
        set dstintf "to_HQ1"
        set srcaddr "172.16.101.0"
        set dstaddr "10.1.100.0"
```

```
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

7. Run `diagnose` commands. The `diagnose ipsec list-sa`, `diagnose ipsec list-conn`, and `diagnose ipsec p1-status` commands are the key to troubleshoot why the IPsec tunnel failed to establish.

Site-to-site VPN with digital certificate

This is a sample configuration of IPsec VPN authenticating a remote FortiProxy peer with a certificate. The certificate on one peer is validated by the presence of the CA certificate installed on the other peer.



To configure IPsec VPN authenticating a remote FortiProxy peer with a digital certificate in the GUI:

1. Import the certificate.
2. Configure user peers.
3. Configure the HQ1 FortiProxy.
   a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
      i. Enter a VPN name.
      ii. For *Template Type*, select *Site to Site*.
      iii. For *Remote Device Type*, select *FortiProxy*.
      iv. For *NAT Configuration*, select *No NAT Between Sites*.
      v. Click *Next*.
   b. Configure the following settings for *Authentication*:
      i. For *Remote Device*, select *IP Address*.
      ii. For the IP address, enter *172.16.202.1*.
      iii. For *Outgoing interface*, enter *port1*.
      iv. For *Authentication Method*, select *Signature*.
      v. In the *Certificate name* field, select the imported certificate.
      vi. From the *Peer Certificate CA* dropdown list, select the desired peer CA certificate.
      vii. Click *Next*.

   c. Configure the following settings for *Policy & Routing*:
      i. From the *Local Interface* dropdown menu, select the local interface.
      ii. Configure the *Local Subnets* as *10.1.100.0*.
      iii. Configure the *Remote Subnets* as *172.16.101.0*.
      iv. Click *Create*.
4. Configure the HQ2 FortiProxy.
   a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
      i. Enter a VPN name.
      ii. For *Template Type*, select *Site to Site*.
      iii. For *Remote Device Type*, select *FortiProxy*.
      iv. For *NAT Configuration*, select *No NAT Between Sites*.
      v. Click *Next*.
   b. Configure the following settings for *Authentication*:
      i. For *Remote Device*, select *IP Address*.
      ii. For the IP address, enter *172.16.2001*.
      iii. For *Outgoing interface*, enter *port25*.
      iv. For *Authentication Method*, select *Signature*.
      v. In the *Certificate name* field, select the imported certificate.
      vi. From the *Peer Certificate CA* dropdown list, select the peer CA certificate.
      vii. Click *Next*.
   c. Configure the following settings for *Policy & Routing*:
      i. From the *Local Interface* dropdown menu, select the local interface.
      ii. Configure *Local Subnets* as *172.16.101.0*.
      iii. Configure the *Remote Subnets* as *10.1.100.0*.
      iv. Click *Create*.

To configure IPsec VPN authenticating a remote FortiProxy peer with a digital certificate using the CLI:

1. Configure the WAN interface and default route. The WAN interface is the interface connected to the ISP. The IPsec tunnel is established over the WAN interface.
   a. Configure HQ1.

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 172.16.200.1 255.255.255.0
    next
end
config router static
    edit 1
        set gateway 172.16.200.3
        set device "port1"
    next
end
```

b. Configure HQ2.

```
config system interface
    edit "port25"
        set vdom "root"
        set ip 172.16.202.1 255.255.255.0
    next
end
config router static
    edit 1
        set gateway 172.16.202.2
        set device "port25"
    next
end
```

2. Configure the internal (protected subnet) interface. The internal interface connects to the corporate internal network. Traffic from this interface routes out the IPsec VPN tunnel.
   a. Configure HQ1.

```
config system interface
    edit "dmz"
        set vdom "root"
        set ip 10.1.100.1 255.255.255.0
    next
end
```

   b. Configure HQ2.

```
config system interface
    edit "port9"
        set vdom "root"
        set ip 172.16.101.1 255.255.255.0
    next
end
```

3. Configure the import certificate and its CA certificate information. The certificate and its CA certificate must be imported on the remote peer FortiProxy and on the primary FortiProxy before configuring IPsec VPN tunnels. If the built-in Fortinet_Factory certificate and the Fortinet_CA CA certificate are used for authentication, you can skip this step.
   a. Configure HQ1.

```
config vpn certificate local
    edit "test1"
        ...
        set range global
    next
end
config vpn certificate ca
    edit "CA_Cert_1"
        ...
        set range global
```

```
   next
end
```

b. Configure HQ2.

```
config vpn certificate local
    edit "test2"
        ...
        set range global
    next
end
config vpn certificate ca
    edit "CA_Cert_1"
        ...
        set range global
    next
end
```

4. Configure the peer user. The peer user is used in the IPsec VPN tunnel peer setting to authenticate the remote peer FortiProxy.

a. If not using the built-in Fortinet_Factory certificate and Fortinet_CA CA certificate, do the following:

i. Configure HQ1.

```
config user peer
    edit "peer1"
        set ca "CA_Cert_1"
    next
end
```

ii. Configure HQ2.

```
config user peer
    edit "peer2"
        set ca "CA_Cert_1"
    next
end
```

b. If the built-in Fortinet_Factory certificate and Fortinet_CA CA certificate are used for authentication, the peer user must be configured based on Fortinet_CA.

i. Configure HQ1.

```
config user peer
    edit "peer1"
        set ca "Fortinet_CA"
    next
end
```

ii. Configure HQ2.

```
config user peer
    edit "peer2"
```

```
        set ca "Fortinet_CA"
    next
end
```

5. Configure the IPsec phase1-interface.
   a. Configure HQ1.

```
config vpn ipsec phase1-interface
    edit "to_HQ2"
        set interface "port1"
        set authmethod signature
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 172.16.202.1
        set certificate "test1"
        set peer "peer1"
    next
end
```

   b. Configure HQ2.

```
config vpn ipsec phase1-interface
    edit "to_HQ1"
        set interface "port25"
        set authmethod signature
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 172.16.200.1
        set certificate "test2"
        set peer "peer2"
    next
end
```

6. Configure the IPsec phase2-interface.
   a. Configure HQ1.

```
config vpn ipsec phase2-interface
    edit "to_HQ2"
        set phase1name "to_HQ2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set auto-negotiate enable
    next
end
```

   b. Configure HQ2.

```
config vpn ipsec phase2-interface
    edit "to_HQ2"
        set phase1name "to_HQ1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
```

```
        set auto-negotiate enable
    next
end
```

7. Configure the static routes. Two static routes are added to reach the remote protected subnet. The blackhole route is important to ensure that IPsec traffic does not match the default route when the IPsec tunnel is down.
   a. Configure HQ1.

```
config router static
    edit 2
        set dst 172.16.101.0 255.255.255.0
        set device "to_HQ2"
    next
end
```

   b. Configure HQ2.

```
config router static
    edit 2
        set dst 10.1.100.0 255.255.255.0
        set device "to_HQ1"
    next
```

8. Configure two firewall policies to allow bidirectional IPsec traffic flow over the IPsec VPN tunnel.
   a. Configure HQ1.

```
config firewall policy
    edit 1
        set name "inbound"
        set srcintf "to_HQ2"
        set dstintf "dmz"
        set srcaddr "172.16.101.0"
        set dstaddr "10.1.100.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "outbound"
        set srcintf "dmz"
        set dstintf "to_HQ2"
        set srcaddr "10.1.100.0"
        set dstaddr "172.16.101.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

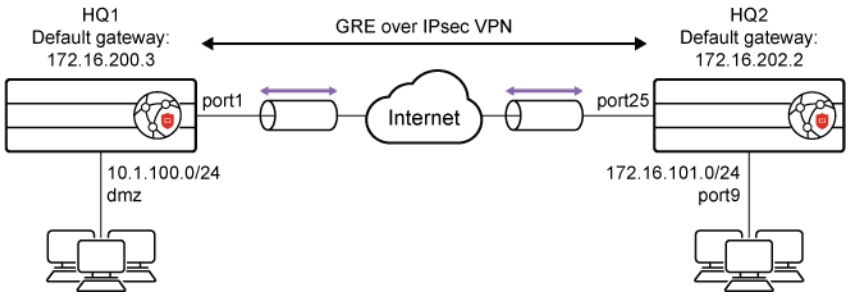
b. Configure HQ2.

```
config firewall policy
    edit 1
        set name "inbound"
        set srcintf "to_HQ1"
        set dstintf "port9"
        set srcaddr "10.1.100.0"
        set dstaddr "172.16.101.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "outbound"
        set srcintf "port9"
        set dstintf "to_HQ1"
        set srcaddr "172.16.101.0"
        set dstaddr "10.1.100.0"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

9. Run `diagnose` commands. The `diagnose ipsec list-sa`, `diagnose ipsec list-conn`, and `diagnose ipsec p1-status`commands are the key to troubleshoot why the IPsec tunnel failed to establish.

GRE over IPsec

This is an example of GRE over an IPsec tunnel using a static route over GRE tunnel and `tunnel-mode` in the `phase2-interface` settings.



To configure GRE over an IPsec tunnel:

1. Enable subnet overlapping at both HQ1 and HQ2.

```
config system settings
    set allow-subnet-overlap enable
end
```

2. Configure the WAN interface and static route.
   a. HQ1.

```
config system interface
    edit "port1"
        set ip 172.16.200.1 255.255.255.0
    next
    edit "dmz"
        set ip 10.1.100.1 255.255.255.0
    next
end
config router static
    edit 1
        set gateway 172.16.200.3
        set device "port1"
    next
end
```

   b. HQ2.

```
config system interface
    edit "port25"
        set ip 172.16.202.1 255.255.255.0
    next
    edit "port9"
        set ip 172.16.101.1 255.255.255.0
    next
end
config router static
    edit 1
        set gateway 172.16.202.2
        set device "port25"
    next
end
```

3. Configure IPsec phase1-interface and phase2-interface.
   a. HQ1.

```
config vpn ipsec phase1-interface
    edit "greipsec"
        set interface "port1"
        set peertype any
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 172.16.202.1
        set psksecret sample
        next
end
config vpn ipsec phase2-interface
    edit "greipsec"
        set phase1name "greipsec"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
```

```
        set protocol 47
    next
end
```

b. HQ2.

```
config vpn ipsec phase1-interface
    edit "greipsec"
        set interface "port25"
        set peertype any
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 172.16.200.1
        set psksecret sample
        next
end
config vpn ipsec phase2-interface
    edit "greipsec"
        set phase1name "greipsec"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
        set protocol 47
    next
end
```

4. Configure IPsec tunnel interface IP address.

a. HQ1.

```
config system interface
    edit "greipsec"
        set ip 10.10.10.1 255.255.255.255
        set remote-ip 10.10.10.2 255.255.255.255
    next
end
```

b. HQ2.

```
config system interface
    edit "greipsec"
        set ip 10.10.10.2 255.255.255.255
        set remote-ip 10.10.10.1 255.255.255.255
    next
end
```

5. Configure the GRE tunnel.

a. HQ1.

```
config system gre-tunnel
    edit "gre_to_HQ2"
        set interface "greipsec"
        set remote-gw 10.10.10.2
        set local-gw 10.10.10.1
```

```
   next
end
```

b. HQ2.

```
config system gre-tunnel
    edit "gre_to_HQ1"
        set interface "greipsec"
        set remote-gw 10.10.10.1
        set local-gw 10.10.10.2
    next
end
```

6. Configure the firewall policy.

a. HQ1.

```
config firewall policy
    edit 1
        set srcintf "dmz"
        set dstintf "gre_to_HQ2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set srcintf "gre_to_HQ2"
        set dstintf "dmz"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set srcintf "greipsec"
        set dstintf "greipsec"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

b. HQ2.

```
config firewall policy
    edit 1
        set srcintf "port9"
        set dstintf "gre_to_HQ1"
```

```
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set srcintf "gre_to_HQ1"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set srcintf "greipsec"
        set dstintf "greipsec"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

7. Configure the static route.
   a. HQ1.

```
config router static
    edit 2
        set dst 172.16.101.0 255.255.255.0
        set device "gre_to_HQ2"
    next
end
```

   b. HQ2.

```
config router static
    edit 2
        set dst 10.1.100.0 255.255.255.0
        set device "gre_to_HQ1"
    next
end
```

8. Configure central SNAT in HQ1 and HQ2:
   a. HQ1.

```
config firewall central-snat-map
    edit 7
        set srcintf "gre_to_HQ2"
        set dstintf "dmz"
```

```
        set src-addr "all"
        set dst-addr "all"
    next
end
```

b. HQ2.

```
config firewall central-snat-map
    edit 7
        set srcintf "gre_to_HQ1"
        set dstintf "port9"
        set src-addr "all"
        set dst-addr "all"
    next
end
```

User & Authentication

The *User & Authentication* menu allows you to configure user accounts, user groups, guests, authentication settings, and FortiTokens.

FortiProxy units support the use of external authentication servers. An authentication server can provide password checking for selected FortiProxy users, or it can be added as a member of a FortiProxy user group.

NOTE: If you are going to use authentication servers, you must configure the servers before you configure the FortiProxy users or user groups that require them.

This section describes the following topics:

- User Definition on page 797
- User Groups on page 807
- Guest Management on page 811
- LDAP Servers on page 818
- RADIUS Servers on page 821
- TACACS+ Servers on page 828
- Kerberos on page 830
- SAML on page 835
- FortiTokens on page 844

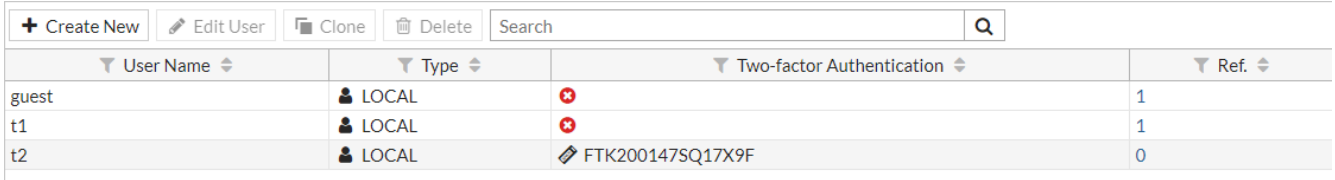
User Definition

A user is defined in a user account that consists of a user name, password and, in some cases, other information that can be configured on the unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group.

A local user is a user configured on a unit. The user can be authenticated with a password stored on the unit or with a password stored on an authentication server. The user name must match a user account stored on the unit, and the user name and password must match a user account stored on the authentication server associated with the user.

Go to *User & Authentication > User Definition* and select *Create New* to create new users with the *Users/Groups Creation Wizard*.

To configure users, go to *User & Authentication > User Definition*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Run the Users/Groups Creation Wizard and create a user. You can also use the wizard to create new groups. See Creating or editing a user on page 798.
Edit User	Edit a user.
Clone	Make a copy of a user.
Delete	Delete a user or users.
Search	Enter a search term to find in the user list.
User Name	The name of the user.
Type	The type of user, such as *Local* or *LDAP*.
Two-factor Authentication	Displays whether the user has token two-factor authentication enabled.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Creating or editing a user

Use the *Users/Groups Creation Wizard* to create user accounts. From the *User Definition* page, select *Create New* or select a user and click *Edit* to start the wizard.

To create a local user:

1. In the *User Type* page, select *Local User* and then select *Next*.
2. In the *Login Credentials* page, enter a user name and password for the new user and then select *Next*.
3. In the *Contact Info* page, enter an email address for the user and then select *Next*. Alternatively, you can supply the user's SMS contact information. To assign a FortiToken to the user, enable *Two-factor Authentication* and select a token from the drop-down menu provided. The *Contact Info* page is optional.

   FortiProxy supports the following 2FA options:

   - **FortiToken**—You can use hard tokens or mobile tokens.
     - Hard tokens must be registered and activated first before they appear in the dropdown list. See Registering and activating a hard token on page 846.
     - FortiProxy provides two trial mobile tokens ready for use from the dropdown list. You cannot add or import any other mobile tokens.

- **FortiToken Cloud on page 857**—A Fortinet Identity and Access Management as a Service (IDaaS) cloud service that enables FortiProxy and FortiAuthenticator customers to add 2FA for their users using Mobile or hard tokens.

  You can activate a free one-month FortiToken Cloud trial subscription for registered FortiCare accounts using the link in the GUI option or the `execute fortitoken-cloud trial` command in the CLI.

  To verify the activation status, run `exe fortitoken-cloud show`. To view the user list, run `diagnose fortitoken-cloud show users`.

  The FortiToken Cloud free trial can only be activated once. The option will not be available if another FortiToken Cloud trial subscription has been activated on the FortiProxy or with the registered FortiCare accounts.

- **Email**—Enter an email address to send a 2FA code to that address.
- **SMS**—Select the *Country Dial Code* and enter the *Phone Number* (`sms-phone` in the CLI) to send a 2FA code to. SMS messages can also be sent to the FortiGuard SMS server or a custom server.

4. In the *Extra Info* page, select *Enabled* to make the new user active. To place the user into a group, enable *User Group* and then select a group from the drop-down menu. For information on user groups, see Create or edit a user group on page 809.
5. Select *Submit* to create the new local user.

To create a remote RADIUS user:

1. In the *User Type* page, select *Remote RADIUS User* and then select *Next*.
2. In the *RADIUS Server* page, enter a user name, select a RADIUS server from the drop-down menu, and then select *Next*. For information on RADIUS servers, see Create or edit a RADIUS server on page 822.
3. In the *Contact Info* page, enter an email address for the user and then select *Next*. Alternatively, you can supply the user's SMS contact information. To assign a FortiToken to the user, enable *Two-factor Authentication* and select a token from the drop-down menu provided. The *Contact Info* page is optional.
   a. FortiProxy supports the following 2FA options:
      - **FortiToken**—You can use hard tokens or mobile tokens.
        - Hard tokens must be registered and activated first before they appear in the dropdown list. See Registering and activating a hard token on page 846.
        - FortiProxy provides two trial mobile tokens ready for use from the dropdown list. You cannot add or import any other mobile tokens.
      - **FortiToken Cloud on page 857**—A Fortinet Identity and Access Management as a Service (IDaaS) cloud service that enables FortiProxy and FortiAuthenticator customers to add 2FA for their users using Mobile or hard tokens.

        You can activate a free one-month FortiToken Cloud trial subscription for registered FortiCare accounts using the link in the GUI option or the `execute fortitoken-cloud trial` command in the CLI.

        To verify the activation status, run `exe fortitoken-cloud show`. To view the user list, run `diagnose fortitoken-cloud show users`.

The FortiToken Cloud free trial can only be activated once. The option will not be available if another FortiToken Cloud trial subscription has been activated on the FortiProxy or with the registered FortiCare accounts.

- **Email**—Enter an email address to send a 2FA code to that address.
- **SMS**—Select the *Country Dial Code* and enter the *Phone Number* (`sms-phone` in the CLI) to send a 2FA code to. SMS messages can also be sent to the FortiGuard SMS server or a custom server.

4. In the *Extra Info* page, select *Enabled* to enable the new user. To place the user into a group, enable *User Group* and then select a group from the drop-down menu. For information on user groups, see Create or edit a user group on page 809.
5. Select *Submit* to create the new RADIUS user.

To create a remote TACACS+ user:

By default, the *TACACS+ Servers* option under *User & Device* is not visible unless you add a server using the following CLI command:

```
config user tacacs+
    edit <name>
        set server <IP_address>
    next
end
```

1. In the *User Type* page, select *Remote TACACS+ User* and then select *Next*.
2. In the *TACACS+ Server* page, enter a user name, select a TACACS+ server from the drop-down menu, and then select *Next*. For information on TACACS+ servers, see Create or edit a TACACS server on page 829
3. In the *Contact Info* page, enter an email address for the user and then select *Next*. Alternatively, you can supply the user's SMS contact information. To assign a FortiToken to the user, enable *Two-factor Authentication* and select a token from the drop-down menu provided. The *Contact Info* page is optional.
   a. FortiProxy supports the following 2FA options:
      - **FortiToken**—You can use hard tokens or mobile tokens.
        - Hard tokens must be registered and activated first before they appear in the dropdown list. See Registering and activating a hard token on page 846.
        - FortiProxy provides two trial mobile tokens ready for use from the dropdown list. You cannot add or import any other mobile tokens.
      - **FortiToken Cloud on page 857**—A Fortinet Identity and Access Management as a Service (IDaaS) cloud service that enables FortiProxy and FortiAuthenticator customers to add 2FA for their users using Mobile or hard tokens.

        You can activate a free one-month FortiToken Cloud trial subscription for registered FortiCare accounts using the link in the GUI option or the `execute fortitoken-cloud trial` command in the CLI.

To verify the activation status, run `exe fortitoken-cloud show`. To view the user list, run `diagnose fortitoken-cloud show users`.



The FortiToken Cloud free trial can only be activated once. The option will not be available if another FortiToken Cloud trial subscription has been activated on the FortiProxy or with the registered FortiCare accounts.

- **Email**—Enter an email address to send a 2FA code to that address.
- **SMS**—Select the *Country Dial Code* and enter the *Phone Number* (`sms-phone` in the CLI) to send a 2FA code to. SMS messages can also be sent to the FortiGuard SMS server or a custom server.

4. In the *Extra Info* page, select *Enabled* to enable the new user. To place the user into a group, enable *User Group* and then select a group from the drop-down menu. For information on user groups, see Create or edit a user group on page 809.
5. Select *Submit* to create the new TACACS+ user.

To create a remote LDAP user:

1. In the *User Type* page, select *Remote LDAP User* and then select *Next*.
2. In the *LDAP Server* page, select an existing LDAP server from the drop-down menu or create an LDAP server and then select *Next*. To create an LDAP server, select the *Create New* icon in the drop-down menu, enter the required information, and then click *OK*. For information on LDAP servers, see Create or edit an LDAP server on page 819.
3. In the *Remote Users* page, enter and apply the LDAP filter, enter a search term to search the server, and select a user from the results.
4. Select *Submit* to create the remote LDAP user.

To use Fortinet Single Sign-On (FSSO):

1. In the *User Type* page, select *FSSO* and then select *Next*.
2. In the *Remote Groups* page, select the FSSO agent, select an AD group, and then select *Next*.
   To create an AD group, see To create an AD group:.
3. In the *Local Group* page, select *Choose Existing* or *Create New*.
   If you select *Choose Existing*, select the FSSO group name from the drop-down menu.
   If you select *Create New*, enter the name of the FSSO group in the field.
4. Select *Submit* to use FSSO.
5. Click *OK* in the confirmation dialog box.

To create an AD group:

```
config user adgrp
   edit <AD_group_name>
      set server-name <FSSO_agent_name>
   next
end
```

For example:

```
config user adgrp
   edit adgroup1
      set server-name NewFSSOserver
   next
end
```

To enable DNS service lookup:

```
config user domain-controller
    edit "win2016"
        set ad-mode ds
        set dns-srv-lookup enable
        set hostname "win2016"
        set username "replicate"
        set password **********
        set domain-name "SMB2016.LAB"
    next
end
```

To specify the source IP and port for the fetching domain controller:

```
config user domain-controller
    edit "win2016"
        set ad-mode ds
        set hostname "win2016"
        set username "replicate"
        set password **********
        set ip-address 172.18.52.188
        set source-ip-address 172.16.100.1
        set source-port 2000
        set domain-name "SMB2016.LAB"
    next
end
```

To use an LDAP server as a credential store:

1. Configure the LDAP server:

```
config user ldap
    edit "openldap"
        set server "172.18.60.214"
        set cnid "cn"
        set dn "dc=qafsso,dc=com"
        set type regular
        set username "cn=Manager,dc=qafsso,dc=com"
        set password **********
        set antiphish enable
        set password-attr "userPassword"
    next
end
```

2. Configure the web filter profile:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            config filters
                edit 1
                    set action block
                next
            end
        end
        config antiphish
            set status enable
            config inspection-entries
                edit "cat34"
                    set fortiguard-category 34
                    set action block
                next
            end
            set authentication ldap
            set ldap "openldap"
        end
        set log-all-url enable
    next
end
```

To configure Active Directory in LDS mode:

```
config user domain-controller
    edit "win2016adlds"
        set ad-mode lds
        set hostname "win2016adlds"
        set username "foo"
        set password **********
        set ip-address 192.168.10.9
        set domain-name "adlds.local"
        set adlds-dn "CN=adlds1part1,DC=ADLDS,DC=COM"
        set adlds-ip-address 192.168.10.9
        set adlds-port 3890
    next
end
```

Customizing complexity options for the local user password policy NEW

The local firewall user password policy can be customized with various settings, such as minimum length, character types, and password reuse. These settings are similar to the ones available for the system administrator password policy, which offer more security and flexibility than the previous local user password policy.

```
config user password-policy
    edit <name>
        set minimum-length <integer>
        set min-lower-case-letter <integer>
        set min-upper-case-letter <integer>
        set min-non-alphanumeric <integer>
        set min-number <integer>
        set min-change-characters <integer>
        set expire-status {enable | disable}
        set reuse-password {enable | disable}
    next
end
```

`minimum-length <integer>`	Set the minimum password length (8 - 128, default = 8).
`min-lower-case-letter <integer>`	Set the minimum number of lowercase characters in the password (0 - 128, default = 0).
`min-upper-case-letter <integer>`	Set the minimum number of uppercase characters in the password (0 - 128, default = 0).
`min-non-alphanumeric <integer>`	Set the minimum number of non-alphanumeric in the password (0 - 128, default = 0).
`min-number <integer>`	Set the minimum number of numeric characters in the password (0 - 128, default = 0).
`min-change-characters <integer>`	Set the minimum number of unique characters in new password, which do not exist in the old password (0 - 128, default = 0). This attribute overrides `reuse-password` if both are enabled.
`set expire-status {enable | disable}`	Enable/disable password expiration (default = disable).
`set reuse-password {enable | disable}`	Enable/disable password reuse (default = enable. If both `reuse-password` and `min-change-characters` are enabled, `min-change-characters` overrides it.

After upgrading, users must activate the user password policy using the CLI. The previous password policy settings will remain valid, but they will not be effective unless the password policy password expiration is enabled (`expire-status`). If the password policy password expiration is not enabled, the `expire-days <integer>` option will not force users to change their password after number of specified days.

Example

The following user password policy is configured before upgrading:

```
config user password-policy
    edit "1"
        set expire-days 1
        set warn-days 1
        set expired-password-renewal enable
```

```
    next
end
```

To configure the user password policy options:

1. Check the user password policy settings after the upgrade:

```
config user password-policy
    edit 1
        get
            name                : 1
            expire-days         : 1
            warn-days           : 1
            expired-password-renewal: enable
            minimum-length      : 8
            min-lower-case-letter: 0
            min-upper-case-letter: 0
            min-non-alphanumeric: 0
            min-number          : 0
            min-change-characters: 0
            expire-status       : disable
            reuse-password      : enable
    next
end
```

2. Edit the user password policy settings, including enabling password expiration:

```
config user password-policy
    edit "1"
        set expire-days 1
        set warn-days 1
        set expired-password-renewal enable
        set min-lower-case-letter 1
        set min-upper-case-letter 1
        set min-non-alphanumeric 3
        set min-number 3
        set min-change-characters 2
        set expire-status enable
        set reuse-password disable
    next
end
```

3. Change a password for a local user.
   a. In the CLI when the password meets the criteria:

```
config user local
    edit pwd-test1
        set passwd CCbcset123!!!
    next
end
```

b. In the CLI when the password does not meet the criteria (only two numbers, so an error message appears):

```
config user local
    edit pwd-test1
        set passwd CCbXsetp23!!!
New password must conform to the password policy enforced on this user:
Password must:
        Be a minimum length of 8
        Include at least 1 lower case letter(s) (a-z)
        Include at least 1 upper case letter(s) (A-Z)
        Include at least 3 non-alphanumeric character(s)
        Include at least 3 number(s) (0-9)
        Have at least 2 unique character(s) which don't exist in the old password
        Not be same as last two passwords

node_check_object fail! for passwd CCbXsetp23!!!

value parse error before 'CCbXsetp23!!!'
Command fail. Return code -49
```

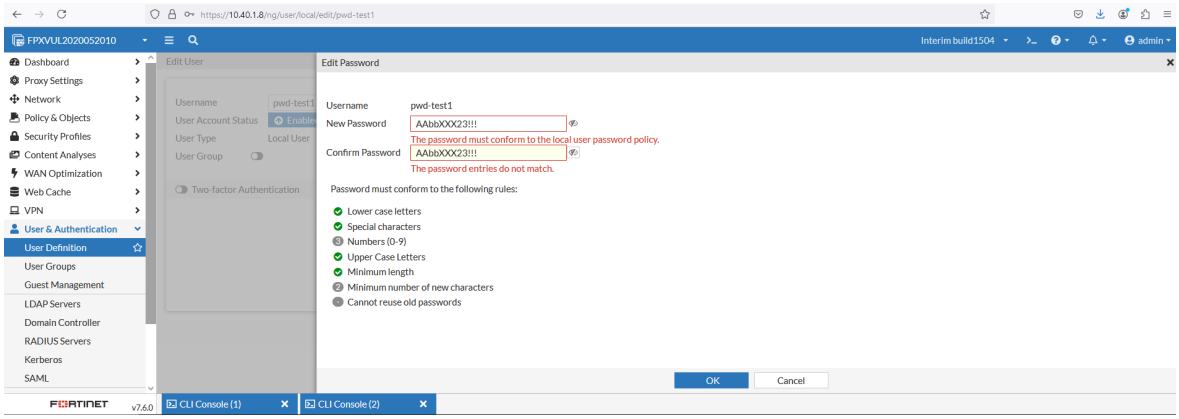
c. In the GUI:

i. Go to *User & Authentication* > *User Definition* and edit a local user.

ii. Click *Change Password*.

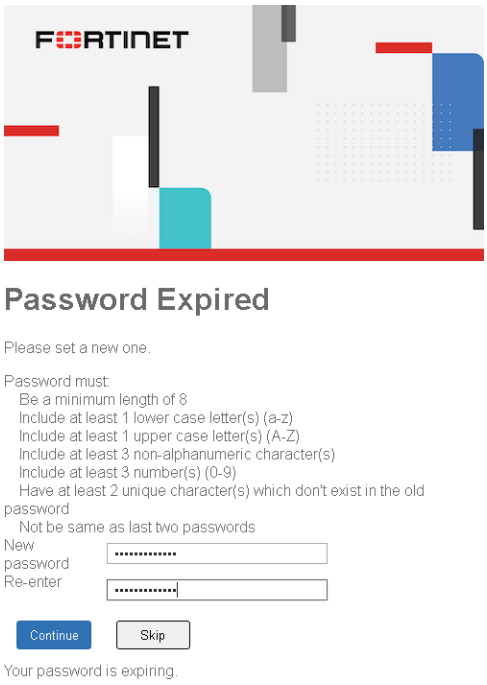
iii. Enter the *New Password*.

iv. Enter the password again (*Confirm Password*). A warning will appear when the password does not match the criteria and indicates which parameters must be fixed. In this example, there are less than three numbers used.



v. Click *OK*.

Sample prompt when a local user needs to update their password for firewall authentication:



User Groups

A user group is a list of user identities. An identity can be one of the following:

- a local user account (user name and password) stored on the Fortinet unit
- a local user account with a password stored on a RADIUS, LDAP, or TACACS+ server
- a RADIUS, LDAP, or TACACS+ server (all identities on the server can authenticate)
- a user or user group defined on a Directory Service server

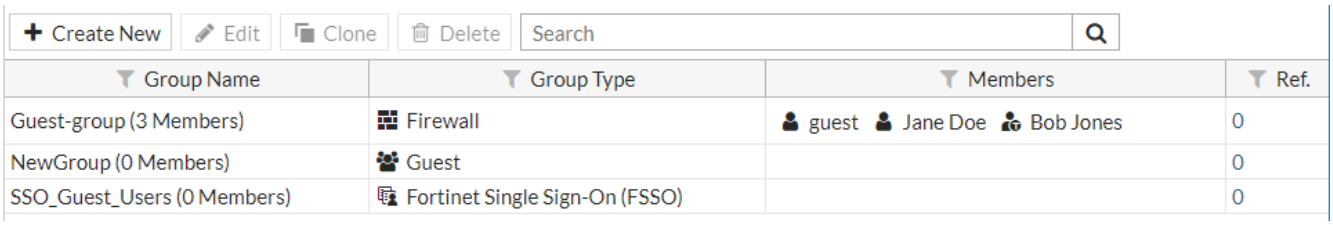
There are four types of user groups:

- Firewall
- Fortinet Single Sign-On (FSSO)
- RADIUS Single Sign-On (RSSO)
- Guest

For each resource that requires authentication, you specify which user groups are permitted access. You need to determine the number and membership of user groups appropriate to your authentication needs.

Users that are associated with multiple groups have access to all services within those user groups. This access is only available in the CLI with the `auth-multi-group` command, which is enabled by default. This feature checks all groups a user belongs to for firewall authentication.

To configure user groups, go to *User & Authentication > User Groups*.



The *SSO_Guest_Users* group is an FSSO group that FortiProxy automatically creates for FSSO users that do not belong to any FSSO groups monitored by the collector agent. This group is read-only, which means you cannot add or delete users in the group.

If a policy is configured to allow the *SSO_Guest_Users* group, users that fall in this group will be granted access without authentication by default. You can configure FortiProxy to block access from such users using the following command:

```
config web-proxy explicit
   set strict-guest enable
end
```

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

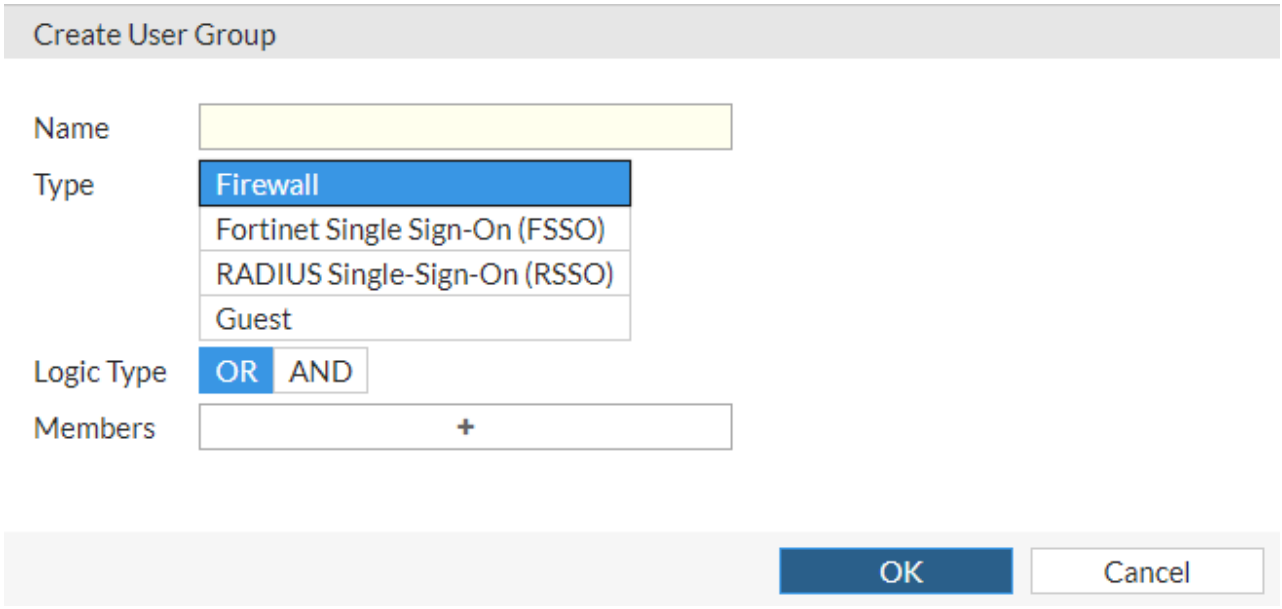
The following options are available:

Create New	Create a user group. See Create or edit a user group on page 809.
Edit	Edit a user group. See Create or edit a user group on page 809.
Clone	Make a copy of a user group.
Delete	Delete a group or groups.
Search	Enter a search term to search the user group list.
Group Name	The name of the user group.
Group Type	The type of group: *Firewall*, *Fortinet Single Sign-On (FSSO)*, *RADIUS Single-Sign-On (RSSO)*, or *Guest*.
Members	The names of the members in the group.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a user group

To create a user group:

1. In the user group list, select *Create New* from the toolbar. The *Create User Group* window opens.



2. Enter a name for the group in the *Name* field.
3. Select the group type in the *Type* field, one of: *Firewall*, *Fortinet Single Sign-On (FSSO)*, *RADIUS Single-Sign-On (RSSO)*, or *Guest*.
4. Enter the following information, depending on the group type selected:

Firewall	This type of group can be selected in any security policy that requires firewall authentication.
Logic Type	Select whether OR or AND logic is used for matching memberships of a user group.
Members	If you selected a Firewall user group, select users to add to the group from the drop-down list.
Fortinet Single Sign-On (FSSO)	This type of group can be selected in any security policy that requires FSSO authentication.
Logic Type	Select whether OR or AND logic is used for matching memberships of a user group.
Members	If you selected the FSSO user group, select users to add to the group from the drop-down list.
RADIUS Single Sign-On (RSSO)	This type of group can be selected in any security policy that requires RSSO authentication.

RADIUS Attribute Value	If you selected the RSSO user group, enter the RADIUS attribute value. This value matches the value from the RADIUS Accounting-Start attribute.
Guest	This type of group can be selected in any security policy that allows guest authentication.
Batch Guest Account Creation	If you selected the Guest user group, enable the creation of batches of guest accounts. When enabled, only the *Maximum Accounts*, *Start Countdown*, and *Time* options are available.
User ID	If you selected the Guest user group, select a user identifier option: • *Email*: The user identifier is emailed. • *Auto Generated*: The user identifier is generated automatically. • *Specify*: The user identifier must be specified.
Maximum Accounts	If you selected the Guest user group, enable *Maximum Accounts* to limit how many accounts exist and then enter the maximum number in the field.
Require Name	If you selected the Guest user group, enable *Require Name* to require names for guests.
Require Email	If you selected the Guest user group, enable *Require Email* to require email addresses for guests.
Require SMS	If you selected the Guest user group, enable *Require SMS* to require SMS contact information for guests.
Password	If you selected the Guest user group, enable *Password* to require passwords for guests and then select a password option: • *Auto Generated*: The password is generated automatically. • *Specify*: The password must be specified.
Sponsor	If you selected the Guest user group, enable *Sponsor* and select *Required* to make a sponsor a requirement for guests.
Company	If you selected the Guest user group, enable *Company* and select *Required* to make a company a requirement for guests.
Start Countdown	If you selected the Guest user group, select when the expiration countdown begins for the user group, either *On account Creation* or *After first login*.
Time	If you selected the Guest user group, select the expiration time for the user group in *Days*, *Hours*, *Minutes*, and *Seconds*.

5. Click *OK* to create the new user group.

To edit a user group:

1. Select the group you want to edit and then click *Edit* from the toolbar or double-click on the group in the table. The *Edit User Group* window opens.
2. Edit the information as required and then click *OK* to apply your changes.

Guest Management

Visitors to your premises might need user accounts on your network for the duration of their stay. If you are hosting a large event such as a conference, you might need to create many such temporary accounts. The FortiProxy Guest Management feature is designed for this purpose.

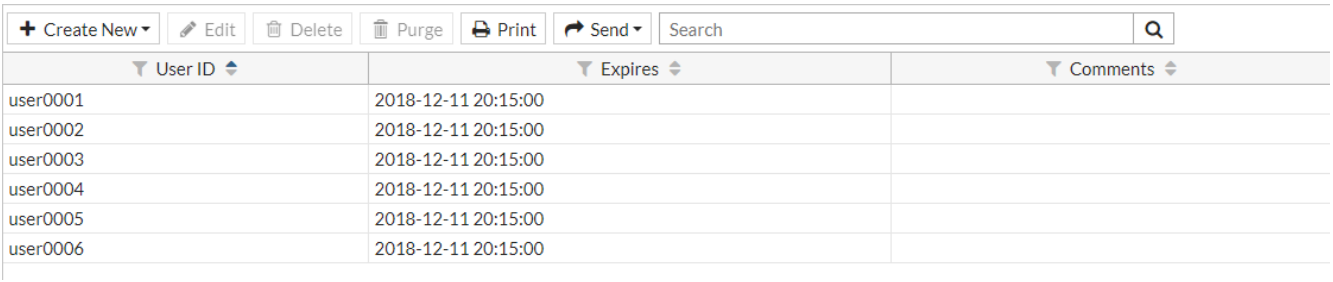
A guest user account User ID can be the user's email address, a randomly generated string, or an ID that the administrator assigns. Similarly, the password can be administrator-assigned or randomly generated.

You can create many guest accounts at the same time using randomly generated User IDs and passwords. This reduces administrator workload for large events.

To set up guest user access, you need to create at least one guest user group and add guest user accounts. Optionally, you can create a guest management administrator whose only function is the creation of guest accounts in specific guest user groups. Otherwise, any administrator can do guest management.

To manage guest access, go to *User & Authentication > Guest Management*.

NOTE: You must create a user group with the Guest group type before the toolbar is displayed on the Guest Management page.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

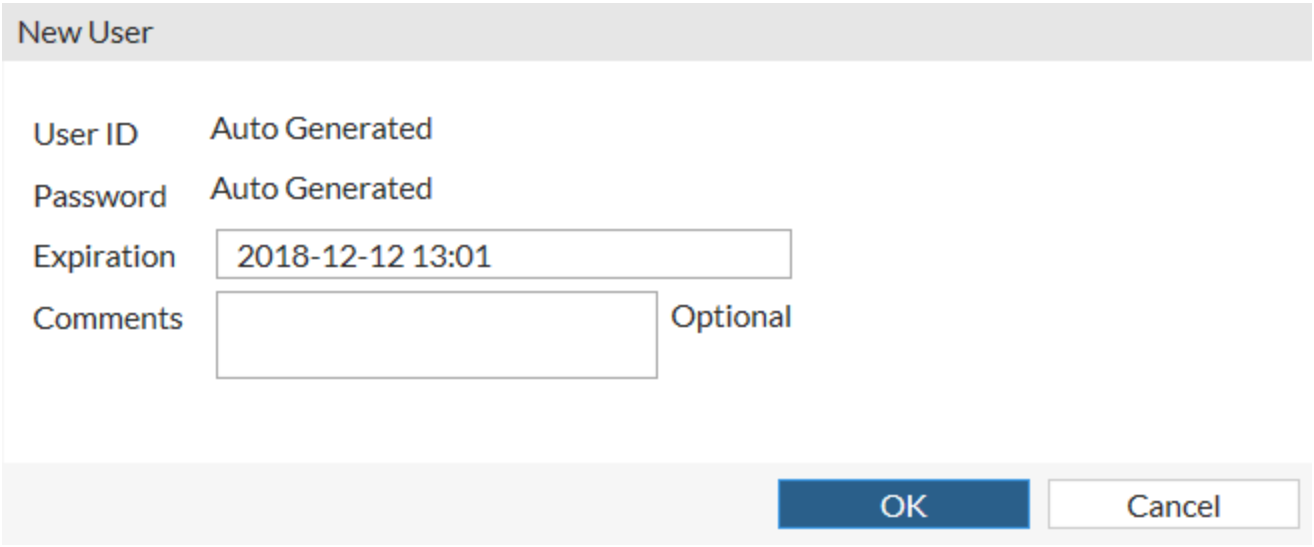
The following options are available:

Create New > User	Create a guest user account. See Create or edit a guest user account on page 812.
Create New > Multiple Users	Create more than one guest user account at the same time. See Create multiple guest user accounts on page 813.
Edit	Modify a guest user account. See Create or edit a guest user account

	on page 812.
Delete	Remove the selected guest user account.
Purge	Remove all expired accounts from the list.
Print	Print the network guest access credentials, including the user identifiers, passwords, and expiration date and time.
Search	Enter a search term to find in the guest user list
User ID	An automatically generated number to identify the guest user.
Expires	Date and time when the guest user account becomes inactive.
Comments	An optional description of the guest user account.

Create or edit a guest user account

Select *Create New* > *User* to open the *New User* page.



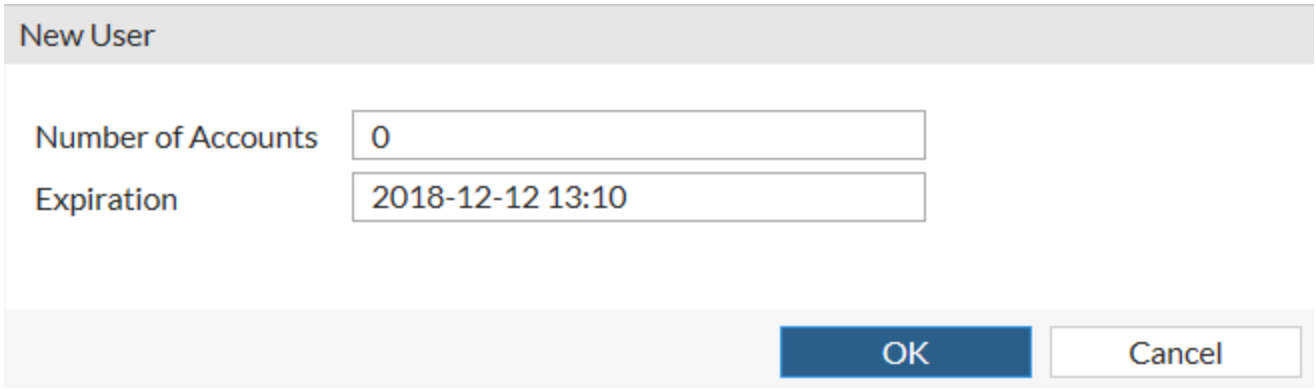
Select a guest user account and then click *Edit* to open the *Edit User* page.

Configure the following settings in the *New User* page or *Edit User* page and then click *OK*:

User ID	The user identifier is automatically generated when you create a guest user account, but you can edit it.
Password	The password is automatically generated when you create a guest user account, but you can edit it.
Expiration	Date and time when the guest user account becomes inactive.
Comments	An optional description of the guest user account.

Create multiple guest user accounts

Select *Create New* > *Multiple Users* to open the *New User* page.



Configure the following settings in the *New User* page and then click *OK*:

Number of Accounts	Enter the number of guest user accounts that you want to create.
Expiration	Date and time when the guest user accounts become inactive.

Basic authentication with cached client certificates

With basic authentication, client certificates can be cached and used as authentication cookies, eliminating the need for repeated user authentication.

In this example, a CA signs a client certificate. The client certificate is installed on two endpoints, and the root CA certificate is imported to FortiProxy.

During the authentication process, the client certificate from the endpoint is verified against the CA certificate. Once this verification is successful, the user is prompted to enter login credentials for user authentication. Once authenticated, the client certificate is stored as an authentication cookie so that subsequent access does not require any user authentication as long as the client certificate remains present on the endpoint.

To configure client certificates as authentication cookies:

1. Prepare the certificate:
   a. Use a CA to sign the client certificate.
   b. Import the root CA certificate that signed the client certificate to FortiProxy.
   c. Install the client certificate on all endpoints.
2. In FortiProxy, configure an authentication scheme to apply authentication against the local user database.

```
config authentication scheme
                                        edit "test-ztna-basic"
                                        set method basic
                                        set user-database "local-user-db"
                                        next
                                    end
```

3. Configure an authentication rule to enable the client certificate to be cached.

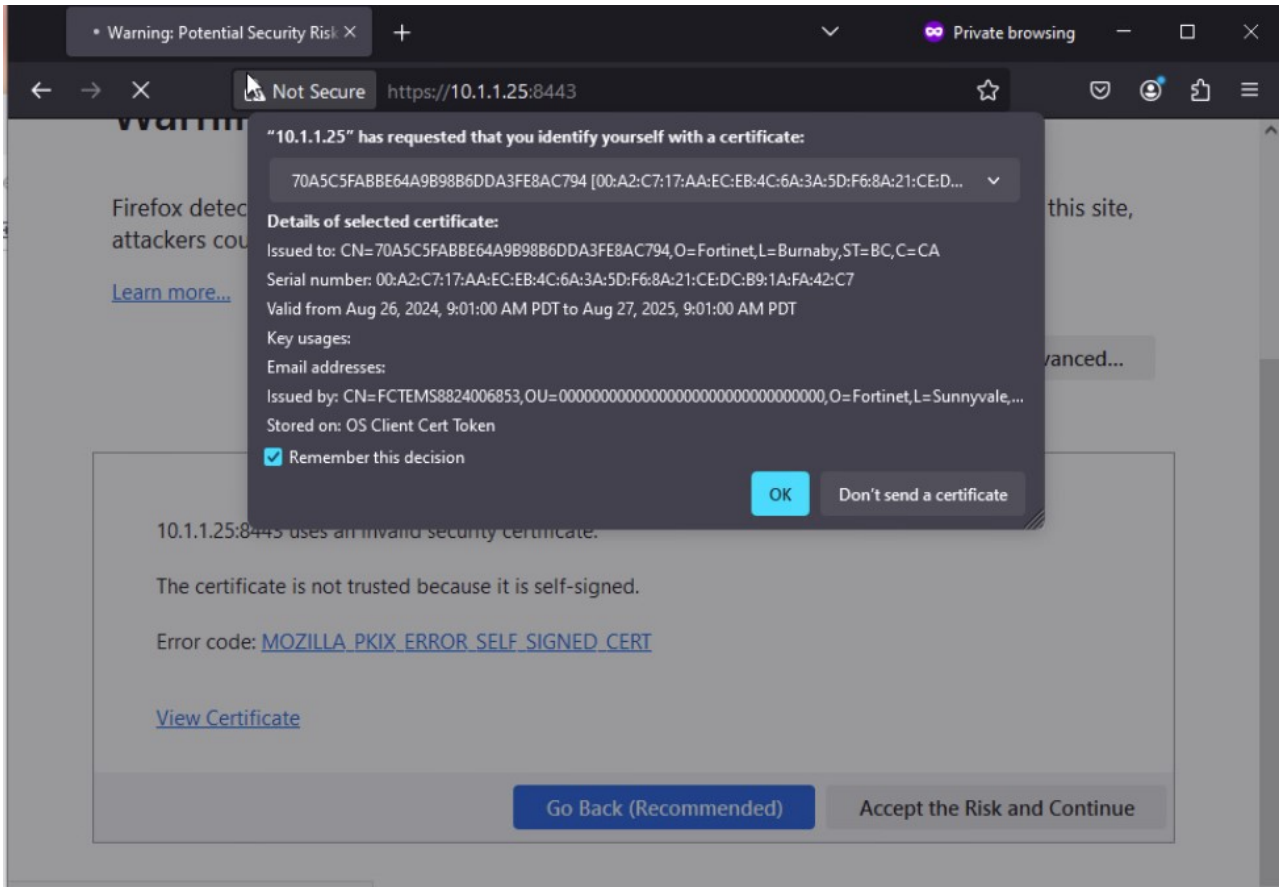
```
config authentication rule
                                        edit "test-ztna-rules"
                                        set srcaddr "all"
                                        set ip-based disable
                                        set active-auth-method "test-ztna-basic"
                                        set cert-auth-cookie enable
                                        next
                                    end
```

4. Configure verification of the client certificate with the root CA.

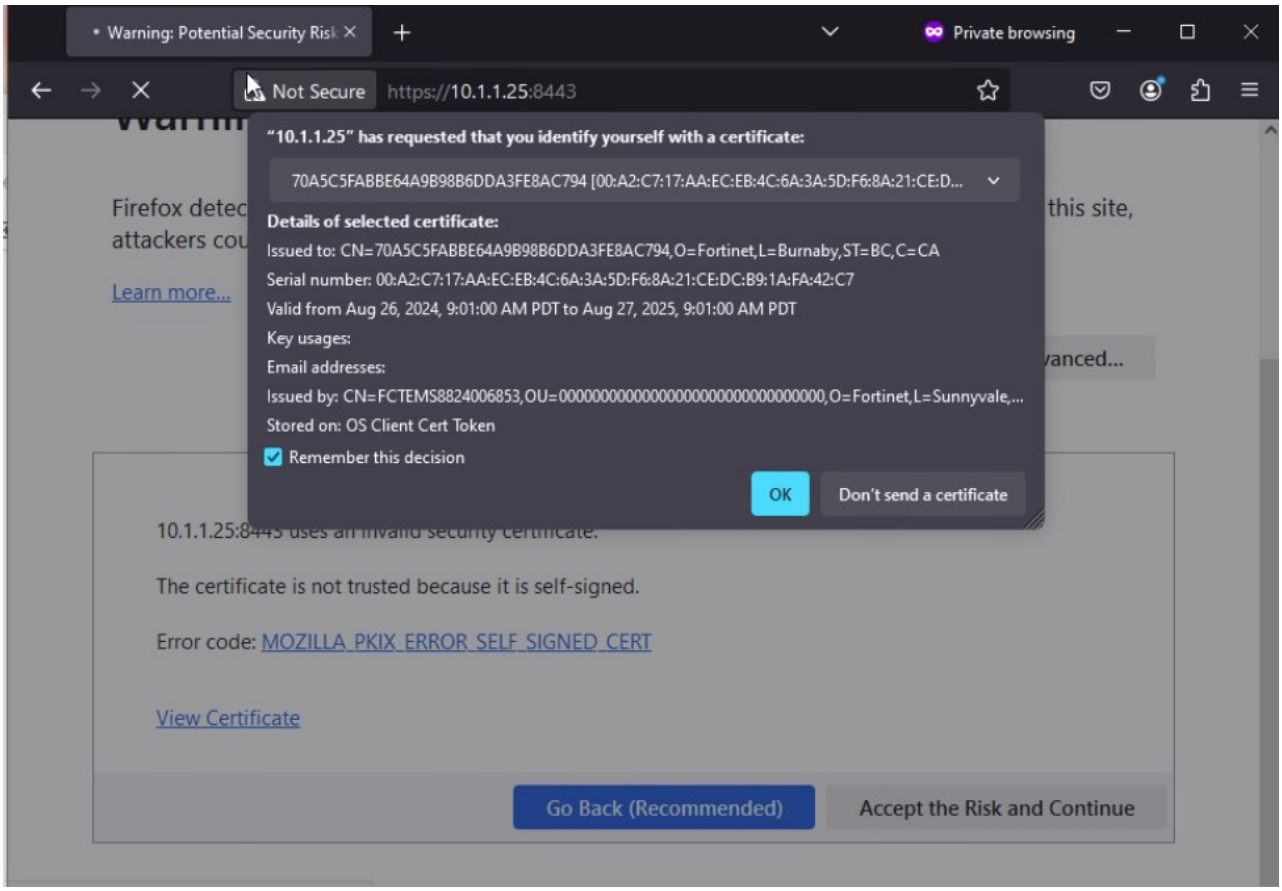
```
config authentication setting
                                        set user-cert-ca "Fortinet_CA_SSL"
                                    end
```

When the user accesses a resource, such as a web site, for the first time:

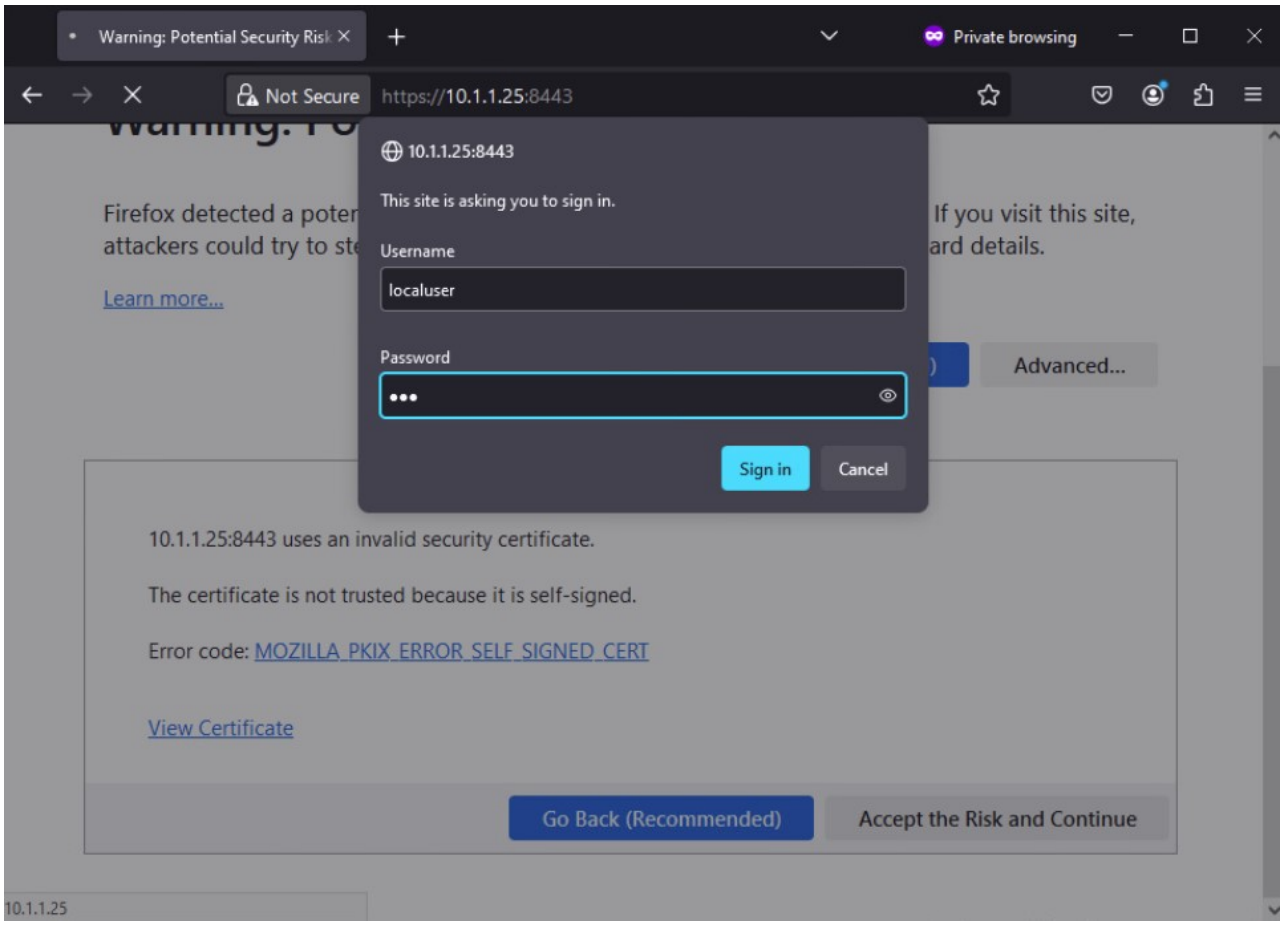
1. The browser prompts the user for a client certificate. The user selects the certificate and clicks *OK*. Then the endpoint device presents the client certificate to FortiProxy for verification.



2. Once the certificate verification passes, an authentication dialog box is displayed.



3. The user enters their username and password to authenticate with FortiProxy and successfully access the web site.



FortiProxy also logs the first access in the traffic log:

```
date=2024-09-24 time=10:51:14 eventtime=1727200273867863612 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.33 srcport=65460
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.1.1.25 dstport=8443 dstintf="port1" dstintfrole="undefined" sessionid=187004326
service="tcp/8443" proxyapptype="http" proto=6 action="accept" policyid=2 policytype="proxy-
policy" poluuid="a98f9846-6f96-51ef-ceb1-1a3cf607c973" policyname="httptest" trandisp="snat"
transip=10.120.1.209 transport=0 clientip=10.120.1.33 duration=0 vip="httpsvip"
accessproxy="httpsvip" clientdevicemanageable="unknown" clientcert="yes" wanin=0 rcvdbyte=0
wanout=0 lanin=653 sentbyte=653 lanout=1930 fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794"
unauthuser="usera" unauthusersource="forticlient" srcremote=207.102.138.19 appcat="unscanned"
```

When the user accesses the resource from the same endpoint device for the second and subsequent times, FortiProxy uses the cached authentication cookie to grant access, as long as the client certificate remains present on the endpoint.

When the user has multiple endpoint devices with the same certificate installed, the certificate will match the cached authentication cookie on the FortiProxy, and the user can access resources without additional authentication.

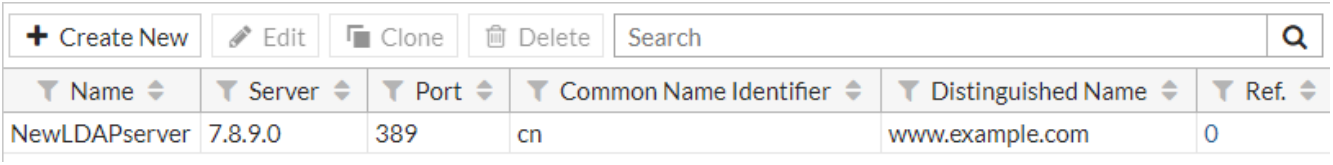
This log shows a user accessing a website from a different PC (IP address 10.1.100.78) without needing to provide user credentials.

```
date=2024-09-24 time=10:56:51 eventtime=1727200611445887844 tz="-0700" logid="0005000024"
type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.120.1.35 srcport=49153
srcintf="port1" srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved"
dstip=10.1.1.25 dstport=8443 dstintf="port1" dstintfrole="undefined" sessionid=187004406
service="tcp/8443" proxyapptype="http" proto=6 action="accept" policyid=2 policytype="proxy-
policy" poluuid="a98f9846-6f96-51ef-ceb1-1a3cf607c973" policyname="httptest" trandisp="snat"
transip=10.120.1.209 transport=0 clientip=10.120.1.35 duration=0 vip="httpsvip"
accessproxy="httpsvip clientdevicemanageable="unknown" clientcert="yes" wanin=0 rcvdbyte=0
wanout=0 lanin=653 sentbyte=653 lanout=1930 fctuid="70A5C5FABBE64A9B98B6DDA3FE8AC794"
unauthuser="usera" unauthusersource="forticlient" srcremote=207.102.138.19 appcat="unscanned"
```

LDAP Servers

LDAP is an Internet protocol used to maintain authentication data that can include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

To manage LDAP servers, go to *User & Authentication > LDAP Servers*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

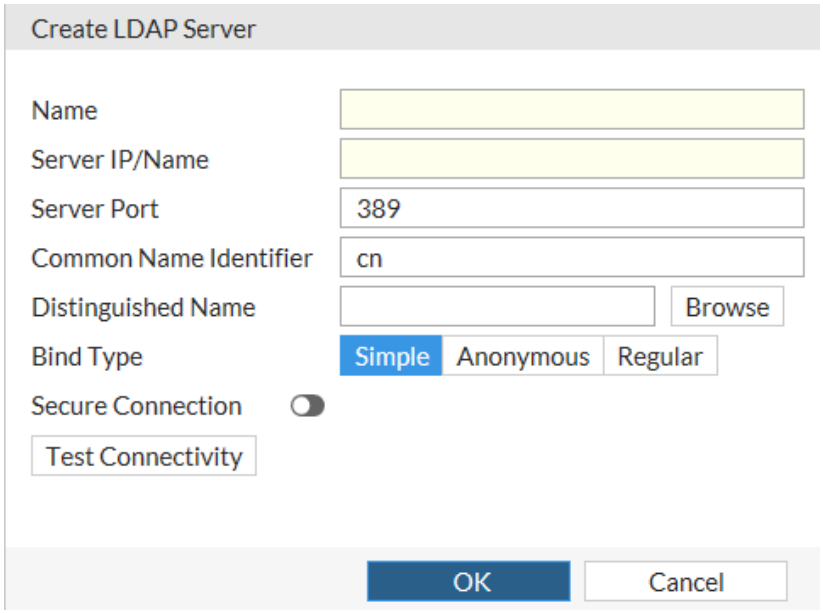
Create New	Create an LDAP server. See Create or edit an LDAP server on page 819.
Edit	Modify an LDAP server. See Create or edit an LDAP server on page 819.
Clone	Make a copy of an LDAP server.
Delete	Remove a server or servers.
Search	Enter a search term to find in the LDAP server list.
Name	The name that identifies the LDAP server on the Fortinet unit.
Server	The domain name or IP address of the LDAP server.
Port	The TCP port used to communicate with the LDAP server. By default, LDAP uses port 389.
Common Name Identifier	The common name identifier for the LDAP server.

Distinguished Name	The base distinguished name for the server using the correct X.500 or LDAP format. The unit passes this distinguished name unchanged to the server.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an LDAP server

To add a new LDAP server:

1. In the LDAP server list, select *Create New* from the toolbar. The *Create LDAP Server* window opens.



2. Configure the following:

Name	Enter the name that identifies the LDAP server on the FortiProxy unit.
Server IP/Name	Enter the domain name or IP address of the LDAP server.
Server Port	Enter the TCP port used to communicate with the LDAP server. By default, LDAP uses port 389. If you use a secure LDAP server, the default port changes if you select *Secure Connection*.
Common Name Identifier	Enter the common name identifier for the LDAP server. The maximum number of characters is 20.

Distinguished Name	Enter the base distinguished name for the server using the correct X.500 or LDAP format. The unit passes this distinguished name unchanged to the server. The maximum number of characters is 512. You can also select *Browse* to contact and retrieve the specified LDAP server.
Bind Type	Select the type of binding for LDAP authentication. • *Simple*: Connect directly to the LDAP server with user name/password authentication. • *Anonymous*: Connect as an anonymous user on the LDAP server and then retrieve the user name/password and compare them to given values. • *Regular*: Connect to the LDAP server directly with user name and password and then receive acceptance or rejection based on search of given values. Enter the user name and password of the user to be authenticated in the *Username* and *Password* fields.
Secure Connection	Enable to use a secure LDAP server connection for authentication.
Protocol	If you enabled *Secure Connection*, select a secure LDAP protocol to use for authentication, either *STARTTLS* or *LDAPS*. Depending on your selection, the server port changes to the default port for the selected protocol: • *STARTTLS*: port 389 • *LDAPS*: port 636
Certificate	If you enabled *Secure Connection*,select a certificate to use for authentication from the list.
Test Connectivity	Select *Test Connectivity* to test if the LDAP server can be contacted.

3. Click *OK* to create the new LDAP server.

To edit an LDAP server:

1. Select the LDAP server you want to edit and then click *Edit* from the toolbar or double-click on the address in the address table. The *Edit LDAP Server* window opens.
2. Edit the server information as required and click *OK* to apply your changes.

Creating an administrator that can be authenticated by an LDAP server

You can configure a least privileges user account (read access only) in Active Directory for FortiProxy admin users which can be authenticated by an LDAP server:

1. Configure an LDAP server. See Create or edit an LDAP server on page 819. Alternatively, use the `configure user ldap` command.

2. To allow only a particular group of members to login to the FortiProxy as administrators, configure an LDAP user group under *User & Authentication > User Group* to limit the access. Alternatively, use the `configure user group` command.
3. Configure an administrator to authenticate with the LDAP server under *System > Administrators*. See Administrators on page 864. Alternatively, use the `config system admin` command.
4. Verify the configuration is successful by accessing the FortiProxy GUI using the credentials of the configured LDAP user(s).

RADIUS Servers

RADIUS is a broadly supported client server protocol that provides centralized authentication, authorization, and accounting functions. RADIUS clients are built into gateways that allow access to networks such as Virtual Private Network (VPN) servers, Network Access Servers (NASs), as well as network switches and firewalls that use authentication. FortiProxy units fall into the last category.

RADIUS servers use UDP packets to communicate with the RADIUS clients on the network to do the following:

- Authenticate users before allowing them access to the network
- Authorize access to resources by appropriate users
- Account or bill for those resources that are used

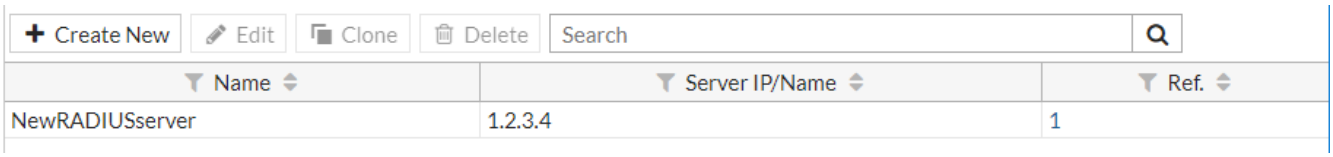
RADIUS servers are currently defined by RFC 2865 (RADIUS) and RFC 2866 (Accounting). They listen on either UDP ports 1812 (authentication) and 1813 (accounting) or ports 1645 (authentication) and 1646 (accounting) requests. RADIUS servers exist for all major operating systems.

You must configure the RADIUS server to accept the FortiProxy unit as a client. FortiProxy units use the authentication and accounting functions of the RADIUS server.

When a configured user attempts to access the network, the FortiProxy unit forwards the authentication request to the RADIUS server, which then matches the user name and password remotely. After authentication succeeds, the RADIUS server passes the Authorization Granted message to the FortiProxy unit, which then grants the user permission to access the network.

The RADIUS server uses a “shared secret” key, along with MD5 hashing, to encrypt information passed between RADIUS servers and clients, including the FortiProxy unit. Typically, only user credentials are encrypted.

To manage RADIUS servers, go to *User & Authentication > RADIUS Servers*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

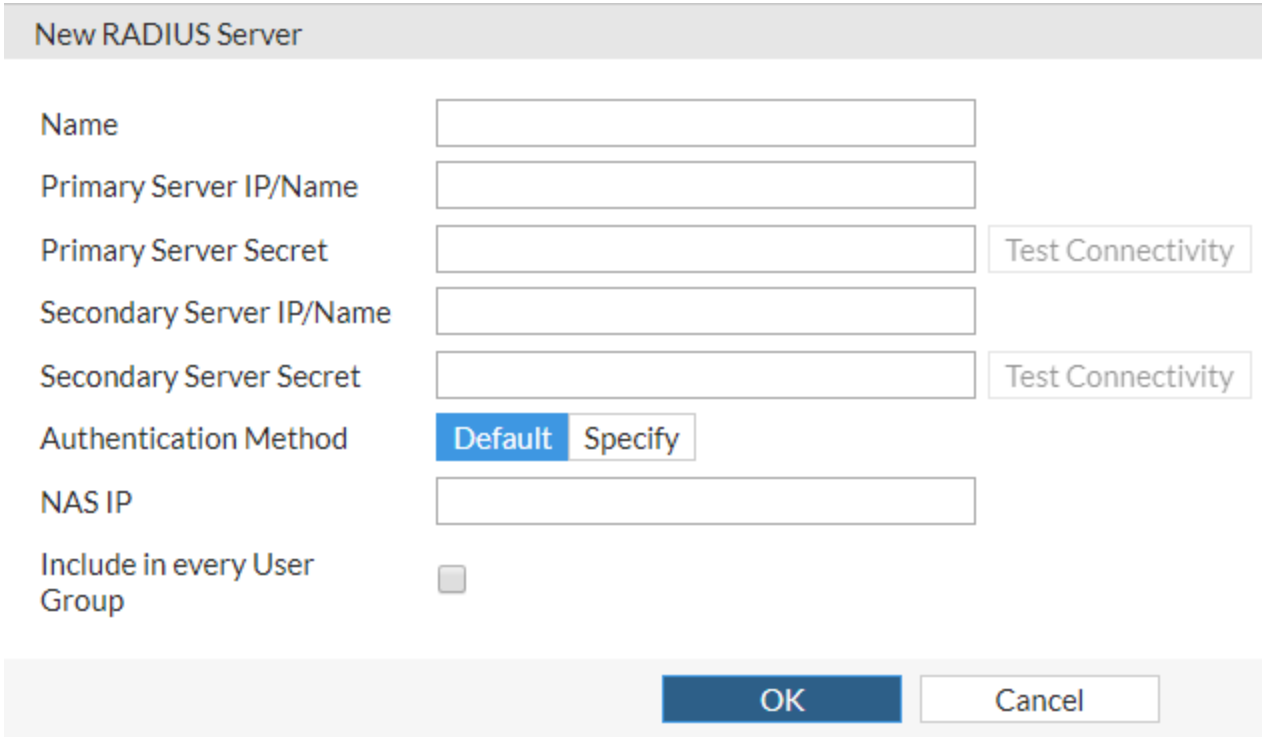
The following options are available:

Create New	Create a RADIUS server. See Create or edit a RADIUS server on page 822.
Edit	Modify a RADIUS server. See Create or edit a RADIUS server on page 822.
Clone	Make a copy of a RADIUS server.
Delete	Remove a server or servers.
Search	Enter a search term to find in the RADIUS server list.
Name	The name that identifies the RADIUS server on the unit.
Server IP/Name	The domain name or IP address of the primary and, if applicable, secondary, RADIUS server.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a RADIUS server

To add a RADIUS server:

1. In the RADIUS server list, select *Create New* from the toolbar. The *New RADIUS Server* window opens.



2. Configure the following:

Name	Enter the name that is used to identify the RADIUS server on the FortiProxy unit.
Primary Server IP/Name	Enter the domain name or IP address of the primary RADIUS server.
Primary Server Secret	Enter the RADIUS server secret key for the primary RADIUS server. The primary server secret key length can be up to a maximum of 16 characters. For security reason, it is recommended that the server secret key be the maximum length.
Test Connectivity	Select *Test Connectivity* to test if the primary and secondary RADIUS servers can be contacted using the domain name or IP address and secret provided.
Secondary Server IP/Name	Enter the domain name or IP address of the secondary RADIUS server, if applicable.
Secondary Server Secret	Enter the RADIUS server secret key for the secondary RADIUS server. The secondary server secret key can be up to a maximum length of 16 characters.
Authentication Method	Select *Default* to authenticate with the default method. Select *Specify* to override the default authentication method and then select the protocol from the list: *MSCHAP-v2*, *MS-CHAP*, *CHAP*, or *PAP*.
NAS IP	Optionally, enter the NAS IP address (RADIUS Attribute 31, outlined in RFC 2548). In this configuration, the FortiProxy unit is the NAS, which is how the RADIUS server registers all valid servers that use its records. If you do not enter an IP address, the IP address that the Fortinet interface uses to communicate with the RADIUS server is applied.
Include in every User Group	Enable to have the RADIUS server automatically included in all user groups.

3. Click *OK* to create the new RADIUS server.

To edit a RADIUS server:

1. Select the RADIUS server you want to edit and then click *Edit* from the toolbar or double-click on the address in the address table. The *Edit RADIUS Server* window opens.
2. Edit the server information as required and click *OK* to apply your changes.

Configuring a RADSEC client

FortiProxy supports RADSEC clients in order to secure the communication channel over TLS for all RADIUS traffic, including RADIUS authentication and RADIUS accounting over port 2083. A FortiProxy acting as a TLS client can initiate the TLS handshake with a remote RADIUS server. Administrators can specify a client certificate, perform a server identity check (enabled by default), and verify against a particular trust anchor (CA certificate). During a TLS handshake, the SNI check will use the RADIUS server FQDN if configured.

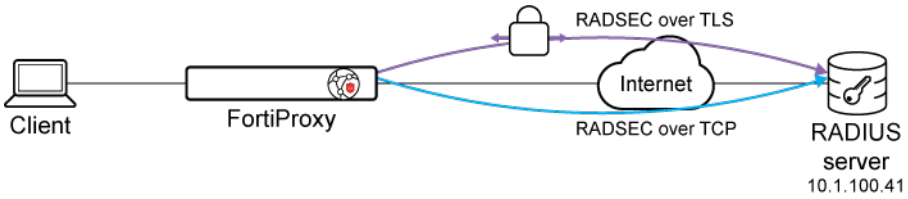
This enhancement also adds support for TCP connections, which use port 1812 for authentication and port 1813 for accounting.

```
config user radius
    edit <name>
        set transport-protocol {udp | tcp | tls}
        set ca-cert <string>
        set client-cert <string>
        set tls-min-proto-version {default | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2}
        set server-identity-check {enable | disable}
    next
end
```

`transport-protocol {udp | tcp | tls}`	Set the type of transport protocol to use: • `udp`: use UDP (default) • `tcp`: use TCP, but no TLS security • `tls`: use TLS over TCP
`ca-cert <string>`	Set the CA certificate of server to trust under TLS.
`client-cert <string>`	Set the client certificate to use under TLS.
`tls-min-proto-version {default | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2}`	Set the minimum supported protocol version for TLS connections: • `default`: follow the system global setting • `SSLv3`: use SSLv3 • `TLSv1`: use TLSv1 • `TLSv1-1`: use TLSv1.1 • `TLSv1-2`: use TLSv1.2
`server-identity-check {enable | disable}`	Enable/disable RADIUS server identity check, which verifies the server domain name/IP address against the server certificate (default = enable).

Examples

The following topology is used to demonstrate configurations using RADSEC over TLS and RADSEC over TCP.



Example 1: RADSEC over TLS

When using TLS, FortiProxy uses port 2083 for RADIUS authentication and RADIUS accounting. There is no need to configure the RADIUS accounting separately.

Before configuring RADSEC over TLS, make sure that the CA certificate (which issues the remote RADIUS server certificate) is imported into the FortiProxy trusted root store. If a customized local FortiProxy client certificate is used, both the certificate and private key are imported into local FortiProxy certificate store.

To configure RADSEC over TLS:

1. Configure the RADIUS server:

```
config user radius
    edit "radius-tls"
        set server "10.1.100.41"
        set secret ********
        set acct-interim-interval 600
        set radius-port 2083
        set auth-type pap
        set transport-protocol tls
        set ca-cert "CA_Cert_2"
        set client-cert "portal.fortinet-fsso"
        config accounting-server
            edit 1
                set status enable
                set server "10.1.100.41"
                set secret ********
            next
        end
    next
end
```

2. Enable fnbamd debug messages on the FortiProxy to verify the RADIUS authentication triggered by client traffic requesting access to external networks, which requires user authentication by the firewall policy. Note the highlighted initial RADSEC TLS authentication, successfully completed TLS handshake, and RADIUS accounting using TLS over port 2083:

```
# diagnose debug application fnbamd -1
Debug messages will be on for 30 minutes.

# diagnose debug enable
...
```

```
[629] __fnbamd_cfg_add_radius_by_user-
[1726] fnbamd_match_and_update_auth_user-Found a matching user in CMDB 'test1'
[462] fnbamd_rad_get-vfid=0, name='radius-tls'
[635] __fnbamd_cfg_add_radius_by_user-Loaded RADIUS server 'radius-tls' for user 'test1'
(16777236)
[905] fnbamd_cfg_get_radius_list-Total rad servers to try: 1
...
[806] __fnbamd_rad_get_next_addr-Next available address of rad 'radius-tls': 10.1.100.41:2083.
[981] __auth_ctx_start-Connection starts radius-tls:10.1.100.41, addr 10.1.100.41:2083 proto:
TCP over TLS
[449] __rad_tcps_open-vfid 0, addr 10.1.100.41, src_ip (null), ssl_opt 1284
...
[618] create_auth_session-Total 1 server(s) to try
[1772] handle_req-r=4
[418] __rad_tcps_connect-tcps_connect(10.1.100.41) is established.
[716] __rad_rxtx-fd 10, state 1(Auth)
...
[565] fnbamd_rad_make_access_request-
[329] __create_access_request-Compose RADIUS request
[549] __create_access_request-Created RADIUS Access-Request. Len: 139.
...
[963] __auth_ctx_svr_push-Added addr 10.1.100.41:2083 from rad 'radius-tls'
[806] __fnbamd_rad_get_next_addr-Next available address of rad 'radius-tls': 10.1.100.41:2083.
[981] __auth_ctx_start-Connection starts radius-tls:10.1.100.41, addr 10.1.100.41:2083 proto:
TCP over TLS
[449] __rad_tcps_open-vfid 0, addr 10.1.100.41, src_ip (null), ssl_opt 1284
[481] __rad_tcps_open-Server identity check is enabled.
[495] __rad_tcps_open-Still connecting 10.1.100.41.
...
[1393] create_acct_session-Acct type 6 session created, 0x9827960
[418] __rad_tcps_connect-tcps_connect(10.1.100.41) is established.
[716] __rad_rxtx-fd 10, state 4(Acct)
...
[956] fnbamd_rad_make_acct_request-
[905] __create_acct_request-Compose RADIUS request
[944] __create_acct_request-Created RADIUS Acct-Request. Len: 129.
[572] __rad_tcps_send-Sent 129/129.
[574] __rad_tcps_send-Sent all. Total 129.
[749] __rad_rxtx-Sent radius req to server 'radius-tls': fd=10, IP=10.1.100.41
(10.1.100.41:2083) code=4 id=33 len=123
[758] __rad_rxtx-Start rad conn timer.
...
```

Example 2: RADSEC over TCP

When using TCP, the default RADIUS ports remain same as with UDP: 1812 for authentication and 1813 for accounting.

To configure RADSEC over TCP:

1. Configure the RADIUS server:

```
config user radius
    edit "radius-tcp"
        set server "10.1.100.41"
        set secret ********
        set acct-interim-interval 600
        set transport-protocol tcp
        config accounting-server
            edit 1
                set status enable
                set server "10.1.100.41"
                set secret ********
            next
        end
    next
end
```

2. Enable fnbamd debug messages on the FortiProxy to verify the RADIUS authentication triggered by client traffic requesting access to external networks, which requires user authentication by the firewall policy. Note the highlighted initial RADIUS authentication over TCP: 1812 and initial RADIUS accounting over TCP: 1813:

```
# diagnose debug application fnbamd -1
Debug messages will be on for 30 minutes.

# diagnose debug enable
...

[806] __fnbamd_rad_get_next_addr-Next available address of rad 'radius-tcp': 10.1.100.41:1812.
[981] __auth_ctx_start-Connection starts radius-tcp:10.1.100.41, addr 10.1.100.41:1812 proto:
TCP
[449] __rad_tcps_open-vfid 0, addr 10.1.100.41, src_ip (null), ssl_opt 0
...
[1772] handle_req-r=4
[418] __rad_tcps_connect-tcps_connect(10.1.100.41) is established.
[716] __rad_rxtx-fd 10, state 1(Auth)
...
[565] fnbamd_rad_make_access_request-
[329] __create_access_request-Compose RADIUS request
[549] __create_access_request-Created RADIUS Access-Request. Len: 139.
[572] __rad_tcps_send-Sent 139/139.
[574] __rad_tcps_send-Sent all. Total 139.
[749] __rad_rxtx-Sent radius req to server 'radius-tcp': fd=10, IP=10.1.100.41
(10.1.100.41:1812) code=1 id=40 len=139
[758] __rad_rxtx-Start rad conn timer.
...
[806] __fnbamd_rad_get_next_addr-Next available address of rad 'radius-tcp': 10.1.100.41:1813.
[981] __auth_ctx_start-Connection starts radius-tcp:10.1.100.41, addr 10.1.100.41:1813 proto:
TCP
[449] __rad_tcps_open-vfid 0, addr 10.1.100.41, src_ip (null), ssl_opt 0
```

```
...
[1393] create_acct_session-Acct type 6 session created, 0x982b280
[418] __rad_tcps_connect-tcps_connect(10.1.100.41) is established.
[716] __rad_rxtx-fd 10, state 4(Acct)
...
[574] __rad_tcps_send-Sent all. Total 129.
[749] __rad_rxtx-Sent radius req to server 'radius-tcp': fd=10, IP=10.1.100.41
(10.1.100.41:1813) code=4 id=41 len=123
[758] __rad_rxtx-Start rad conn timer.
...
```

TACACS+ Servers

TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices through one or more centralized servers. TACACS+ allows a client to accept a user name and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies the user access to the network.

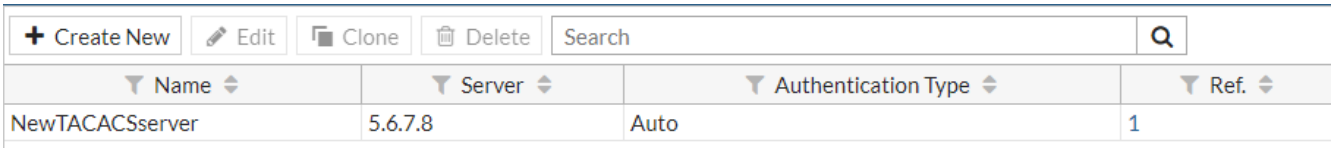
TACACS+ offers fully encrypted packet bodies and supports both IP and AppleTalk protocols. TACACS+ uses TCP port 49, which is seen as more reliable than RADIUS's UDP.



By default, the *TACACS+ Servers* option under *User & Device* is not visible unless you add a server using the following CLI command:

```
config user tacacs+
    edit <name>
        set server <IP_address>
    next
end
```

To manage TACACS+ servers, go to *User & Authentication* > *TACACS+ Servers*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

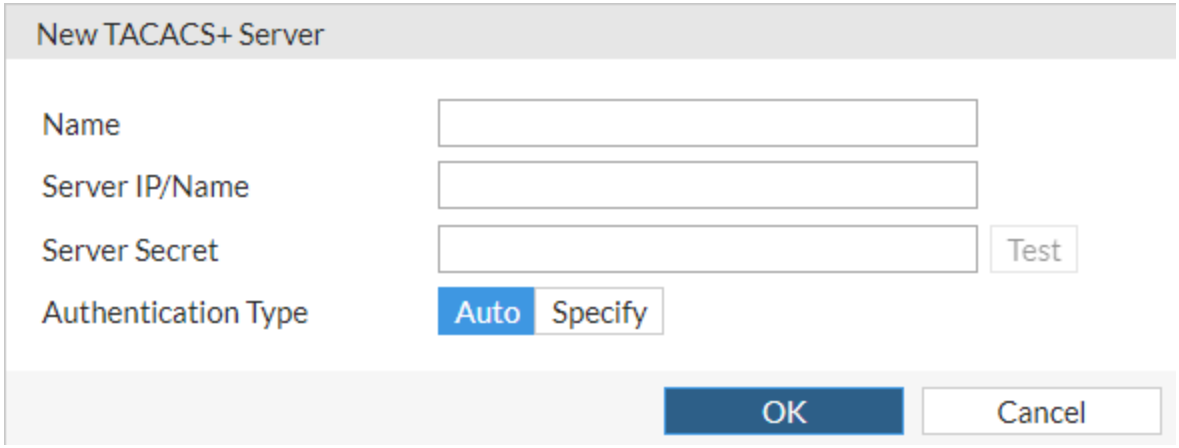
Create New	Create a TACACS+ server. See Create or edit a TACACS server on page 829.

Edit	Modify a TACACS+ server. See Create or edit a TACACS server on page 829.
Clone	Make a copy of a TACACS+ server.
Delete	Remove a server or servers.
Search	Enter a search term to find in the TACACS+ server list.
Name	The name that identifies the TACACS+ server on the unit.
Server	The domain name or IP address of the TACACS+ server.
Authentication Type	The authentication type used by the server.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a TACACS server

To add a TACACS+ server:

1. In the TACACS+ server list, select *Create New* from the toolbar. The *New TACACS+ Server* window opens.



2. Configure the following:

Name	Enter the name of the TACACS+ server.
Server IP/Name	Enter the server domain name or IP address of the TACACS+ server.
Server Secret	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.

Authentication Type	Select the authentication type to use for the TACACS+ server: Auto, MSCHAP, CHAP, PAP, or ASCII. Auto authenticates using PAP, MSCHAP, and CHAP, in that order. For more information, see Authentication protocols.

3. Click *OK* to create the new TACACS+ server.

To edit a TACACS+ server:

1. Select the TACACS+ server you want to edit and then click *Edit* from the toolbar or double-click on the address in the address table. The *Edit TACACS+ Server* window opens.
2. Edit the server information as required and click *OK* to apply your changes.

Authentication protocols

ASCII	Machine-independent technique that uses representations of English characters. Requires user to type a user name and password that are sent in clear text (unencrypted) and matched with an entry in the user database, which is stored in ASCII format.
PAP	Password Authentication Protocol (PAP). Used to authenticate PPP connections. Transmits passwords and other user information in clear text.
CHAP	Challenge-Handshake Authentication Protocol (CHAP). Provides the same functionality as PAP but is more secure because it does not send the password and other user information over the network to the security server.
MSCHAP	Microsoft Challenge-Handshake Authentication Protocol v1 (MSCHAP). Microsoft-specific version of CHAP.
Auto	The default protocol configuration, Auto, uses PAP, MSCHAP, and CHAP, in that order.

Kerberos

Kerberos authentication is a method for authenticating both explicit web proxy and transparent web proxy users. It has several advantages over NTLM challenge response:

- Does not require FSSO/AD agents to be deployed across domains.
- Requires fewer round-trips than NTLM SSO, making it less latency sensitive.
- Is (probably) more scalable than challenge response.
- Uses existing Windows domain components rather than added components.
- NTLM may still be used as a fallback for non-Kerberos clients.

To configure Kerberos authentication service, go to *User & Authentication > Kerberos*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

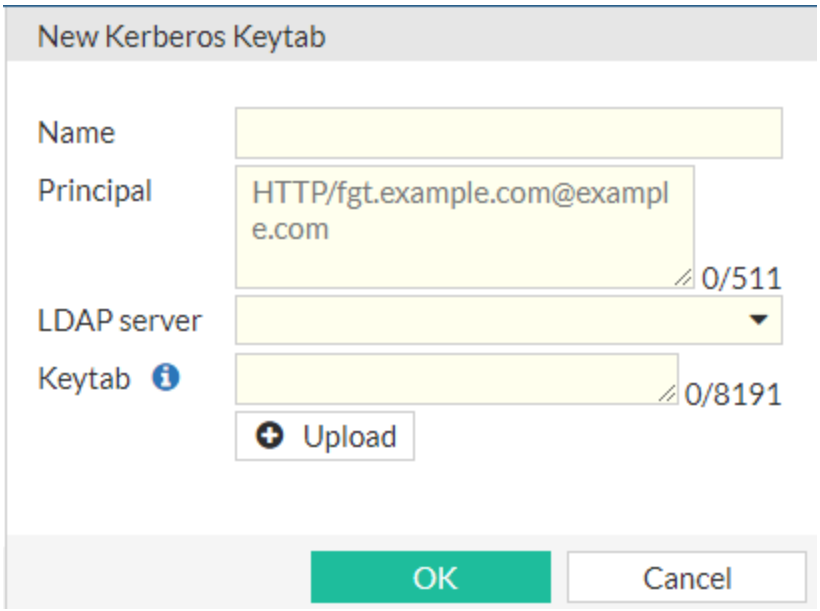
The following options are available:

Create New	Create a Kerberos authentication service. See Create or edit a Kerberos authentication service on page 831.
Edit	Modify a Kerberos authentication service. See Create or edit a Kerberos authentication service on page 831.
Delete	Remove a Kerberos authentication service or services.
Name	The name of the Kerberos authentication service.
Principal	The server domain name of the Kerberos authentication service.
LDAP Server	The name of the LDAP server used for authorization.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a Kerberos authentication service

To add a new Kerberos authentication service:

1. In the Kerberos service list, select *Create New* from the toolbar. The *New Kerberos Keytab* window opens.



2. Configure the following:

Name	Enter the name of the Kerberos authentication service.
Principal	Enter the server domain name of the Kerberos authentication service.
LDAP server	Enter the name of the LDAP server used for authorization.
Keytab	Select *Upload* and then navigate to the file that contains the shared secret. Use the `ktpass` command (found on Windows servers and many domain workstations) to generate the Kerberos keytab.

3. Click *OK* to create the new Kerberos authentication service.

To edit the Kerberos authentication service:

1. Select the Kerberos authentication service you want to edit and then click *Edit* from the toolbar or double-click on the service in the service table. The *Edit Kerberos Keytab* window opens.
2. Edit the service information as required and click *OK* to apply your changes.

Using Kerberos authentication with Windows AD cross-forest

FortiProxy supports Windows AD cross-forest for Kerberos authentication. Below is an example to demonstrate how FortiProxy uses Kerberos authentication rules to support complex cross-forest authentication scenarios while adhering to the AGDLP best practices for managing access permissions.

Scenario

For the following forests:

- **Forest A**: CONTOSO.LOCAL (trusting forest)
- **Forest B**: FABRIKAM.COM (trusted forest)

We want to allow users from FABRIKAM.COM to access resources in CONTOSO.LOCAL through FortiProxy.

To implement the AGDLP model:

1. Create user accounts in FABRIKAM.COM: john.doe@fabrikam.com, jane.smith@fabrikam.com.
2. Create global groups in FABRIKAM.COM: for example, FABRIKAM_Sales_Team.
3. Add john.doe@fabrikam.com and jane.smith@fabrikam.com to FABRIKAM_Sales_Team.
4. Create domain local groups in CONTOSO.LOCAL: for example, CONTOSO_Sales_Resources_Access, CONTOSO_IT_Admin.
5. Add FABRIKAM.COM's FABRIKAM_Sales_Team to CONTOSO_Sales_Resources_Access.
6. Grant appropriate access permissions to CONTOSO_Sales_Resources_Access on sales-related resources in CONTOSO.LOCAL.

To configure FortiProxy:

1. Enable LDAP user cache for explicit and transparent proxy users:

```
config web-proxy global
  set ldap-user-cache enable
end
```

2. Configure Kerberos realm:

```
config user krb-keytab
   edit "CONTOSO-KRB"
      set pac-data disable
      set principal "HTTP/fortiproxy.contoso.local@CONTOSO.LOCAL"
      set ldap-server "CONTOSO-AD"
      set keytab "ENC
            Zc53UXsUiHFfqUtvbjrkLUjhhXhbulBUp+qmtJFjNgl/jcskECWZ0MVJDiYjBcpvmc6eqLB817wiHZq64rV69
            JJgNlKGsgzI+3c3yWe3RRxuLuz8LlGCitGpPxnP+GwZnuftGh9ii7KBnFhKVDItTQLhRzV81g6pgU9saCz2eq
            Gu0aV026k9ClOnTeREbo476cR7BW5IsBwxFKtFxT2pV3QRFPd8ix045ndoJD4M4QGevLs0O9vUkyP4jR+inYk
            LBoPqLtE6z4X0Vyzr1J3DyBg1nCuiRA+EAOoUxcjCAD1s0mLdJT0E8x19I4cpm2MNcZdujELaaJtsKu3EIpPX
            09Eyg0z9vrUQ+62K8YpOgBtQEkmVmr/Em+UHBn7QvQMHRk3KA4TADk2aXfSQNHFURPJAIMWD7m3ldlvaYgA56
            xZ7dz7iF7dN+Ta9F6aBxz6JN191tOq+71NY592/ZXPMHQ2Z3ibGADURkQqihu0VrFZQJ24IyL7+F2PgTdZATM
            ifjxsyvSK8rpOeHuEnMw5ZQgymvgV0ycsn+L9NV+pJb77r+xI8DMm8fKUI9CMvLWiEzbaif8rKb+qFONsc1NT
            xt2d1ypJmJfpOZRKwaNqH0+yMVZFVfiDVimIywZFS0x4E8QBdCIGX1xM3zFGjoRcsd4MqrPdpHCuOVBdsh6KD
            Cae0xRdtD+dmjDDkStEInWhv9r0PIA=="
   next
end
```

3. Create an LDAP server:

```
config user ldap
   edit "CONTOSO-AD"
      set server "10.0.1.100"
      set cnid "sAMAccountName"
      set dn "dc=contoso,dc=local"
      set type regular
```

```
        set username "svc_fortiproxy"
        set password ENC
              YXRhbFg8uvof/JrL06vpvBbR/Yghbmyp6LTdKDjy5ZX+X/4AGK4/MOSZd3JDBcJ6GLHwOeQ0d4lPvjqiHRJ7y
              NonLWGhrr/RKhmyrfsvYrB9cwc9Rbpx0B5vRT6Psmlbqi84JZsdg64tFkHyJ8JQCxrvzsM7S0MMtPCpAJ0LqL
              xkukwH31wC3gk5Vli59J3kYRXRFQ== set port 3268 set account-key-processing strip set
              account-key-filter "(&(sAMAccountName=%s)(!
              (UserAccountControl:1.2.840.113556.1.4.803:=2)))"
    next
end
```

4. Configure Kerberos authentication scheme to enable searching all LDAP databases to find groups:

```
config authentication scheme
  edit "krb"
      set method negotiate
      set negotiate-ntlm disable
      set kerberos-keytab "krb213"
      set search-all-ldap-databases enable
  next
end
```

5. Set up Kerberos authentication rule:

```
config authentication rule
   edit "CROSS-FOREST-AUTH"
      set status enable
      set protocol http https ftp
      set srcaddr "all"
      set ip-based disable
      set active-auth-method "CONTOSO-KRB"
   next
end
```

To verify the cross-forest authentication:

1. Check user authentication status using the following command:

   ```
   diagnose test application wad 2500
   ```

2. View user info cache and group information using the following command:

   ```
   diagnose test application wad 159
   ```

Example output:

```
FPXVULTM24000048 # dia test app wad 159
```

```
uname=john.doe,pwd=no,vd=root ldap=FABRIKAM-AD,ref_cnt=1,upd=0,wait=0 sid-auth=0,status=2 last_
access=Wed Sep  4 15:31:58 2024
```

```
user id=1, refresh_time=Wed Sep  4 15:31:58 2024
```

```
user dn=CN=John Doe,CN=Users,DC=fabrikam,DC=com
```

```
sid:S-1-5-21-2445926238-1237732657-140748957-513 name=CN=Domain Users,CN=Users,DC=fabrikam,DC=com
```

```
uname=john.doe,pwd=no,vd=root ldap=CONTOSO-AD,ref_cnt=1,upd=0,wait=0 sid-auth=1,status=2 last_
access=Wed Sep  4 15:31:58 2024

user id=2, refresh_time=Wed Sep  4 15:31:58 2024

sid:S-1-5-21-2262484555-2078175199-1088017096-12365 name=CN=CONTOSO_Sales_Resources_
Access,CN=Users,DC=contoso,DC=local

uname=jane.smith,pwd=no,vd=root ldap=CONTOSO-AD,ref_cnt=1,upd=0,wait=0 sid-auth=1,status=2 last_
access=Wed Sep  4 15:32:08 2024

user id=3, refresh_time=Wed Sep  4 15:32:08 2024

sid:S-1-5-21-2262484555-2078175199-1088017096-12365 name=CN=CONTOSO_Sales_Resources_
Access,CN=Users,DC=contoso,DC=local

sid:S-1-5-21-2262484555-2078175199-1088017096-12380 name=CN=CONTOSO_IT_
Admin,CN=Users,DC=contoso,DC=local

uname=jane.smith,pwd=no,vd=root ldap=FABRIKAM-AD,ref_cnt=1,upd=0,wait=0 sid-auth=0,status=2 last_
access=Wed Sep  4 15:32:08 2024

user id=4, refresh_time=Wed Sep  4 15:32:08 2024

user dn=CN=Jane Smith,CN=Users,DC=fabrikam,DC=com

sid:S-1-5-21-2445926238-1237732657-140748957-513 name=CN=Domain Users,CN=Users,DC=fabrikam,DC=com
```

In this output, we can see successful authentication for users from both domains and group membership information for each user. `sid-auth=1` for cross-forest authentication (`CONTOSO-AD`) indicates successful cross-forest group resolution.

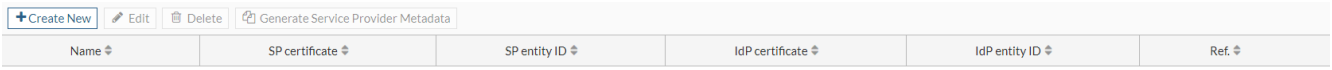
SAML

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between two security domains: an Identity Provider (IdP) and a Service Provider (SP). The FortiProxy unit supports the SAML protocol and will act as a Service Provider.

In SAML-SP authentication, the FortiProxy unit redirects unauthenticated users to the IdP (FortiAuthenticator, Okta Identity, Microsoft ADFS, or similar) for authentication. After the user is

authenticated with the IdP, the user is redirected to the FortiProxy unit with SAML assertion information using the POST method. The assertion information includes the authentication result, user name, and group in attribute assertions (or claim in terms of ADFS). Based on that information, the FortiProxy unit executes both authentication and authorization (matching the user to the group). If the IdP is Microsoft ADFS, the FortiProxy unit supports resolving the user group information through the LDAP query with Kerberos or NTLM authentication.

To manage SAML servers, go to *User & Authentication > SAML*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

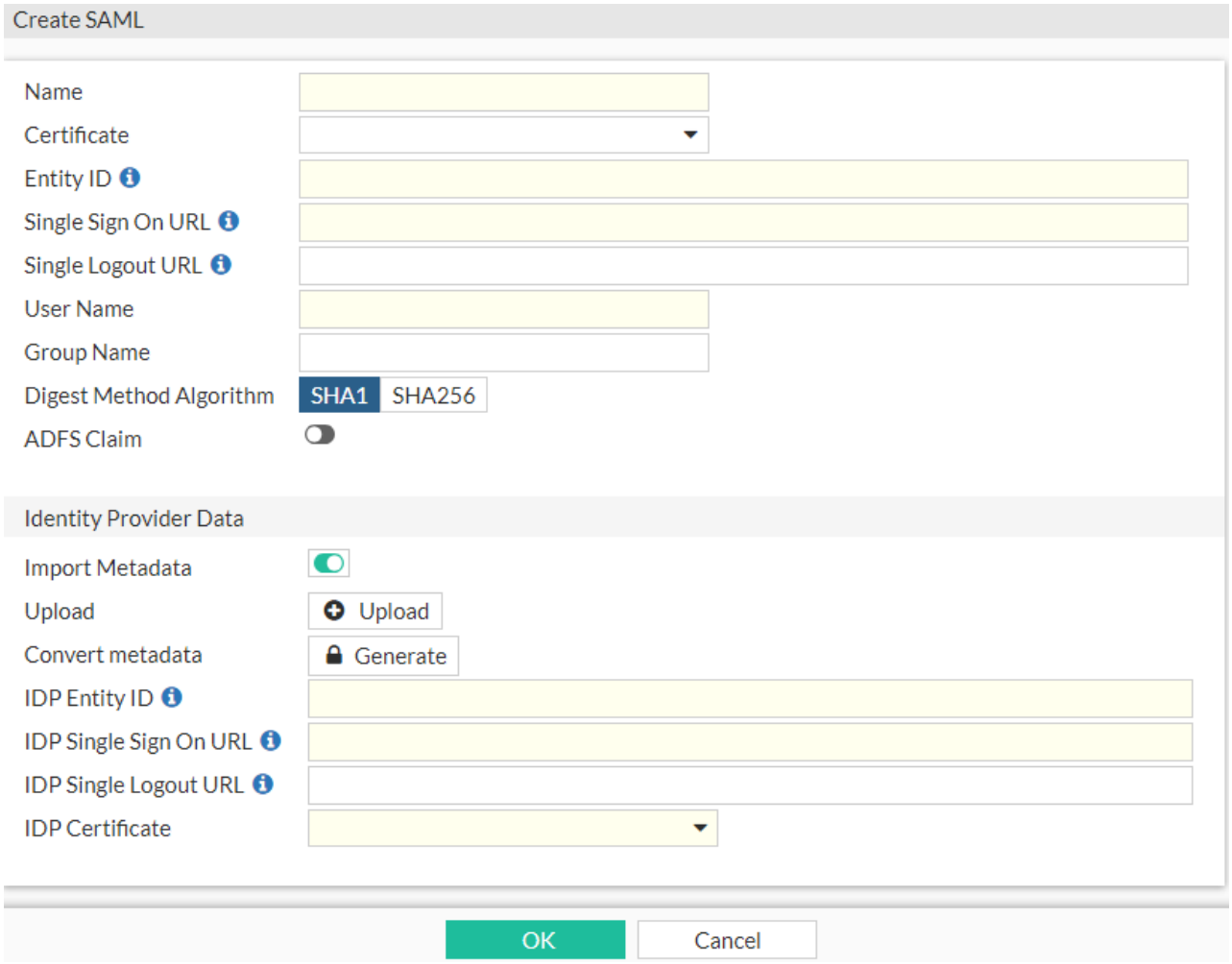
Create New	Create a SAML server. See Create or edit a SAML server on page 837.
Edit	Modify a SAML server. See Create or edit a SAML server on page 837.
Delete	Remove a server or servers.
Generate Service Provider Metadata	Exports the SAML IdP metadata of the selected SAML server in the list. This button is disabled if no SAML server is selected.
Name	The name that identifies the SAML server on the Fortinet unit.
SP certificate	Certificate from the service provider (SP).
SP entity ID	The SP entity identifier.
IdP certificate	Certificate from the identity provider (IdP).
IdP entity ID	The IDP entity identifier.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.
ADFS Claim	Enable or disable the ADFS claim for the user and group attributes in the assertion statement.
digest-method	Which algorithm is used for the digest method.
Group Claim Type	The group claim in the assertion statement.
Group Name	The group name in assertion statement.
IDP Single Logout URL	The IDP single logout URL.
IDP Single Sign On URL	The IDP single sign-on URL.
Single Logout URL	The SP single logout URL.

Single Sign On URL	The SP single sign-on URL.
User Claim Type	The user name claim in the assertion statement.
User Name	The user name in the assertion statement.

Create or edit a SAML server

To add a new SAML server in the GUI:

1. In the SAML server list, click *Create New* from the toolbar. The *Create SAML* window opens.



2. Configure the following:

Name	Enter the name that identifies the SAML server on the FortiProxy unit.
Certificate	Select the certificate to sign SAML messages.

Entity ID	Enter the service provider entity identifier. The URL must start with `http://` or `https://`.
Single Sign On URL	Enter the service provider single sign-on URL. The URL must start with `http://` or `https://`.
Single Logout URL	Enter the service provider single logout URL. The URL must start with `http://` or `https://`.
User Name	Enter the user name in the assertion statement.
Group Name	Enter the group name in the assertion statement.
Digest Method Algorithm	Select the algorithm used for the digest method.
ADFS Claim	Enable or disable the ADFS claim for the user and group attributes in the assertion statement.
Identity Provider Data	
Import Metadata	Enable or disable importing metadata. When enabled, use the *Upload* or *Convert metadata* fields to import an IdP metadata file or convert the metadata to a user SAML CLI configuration.
Upload	Click *Upload* to import an IdP metadata file.
Convert metadata	Click *Generate* to convert the metadata to a user SAML CLI configuration.
IDP Entity ID	Enter t he identity provider entity identifier. The URL must start with `http://` or `https://`.
IDP Single Sign On URL	Enter the identity provider single sign-on UR. The URL must start with `http://` or `https://`.
IDP Single Logout URL	Enter the identity provider single logout URL. The URL must start with `http://` or `https://`.
IDP Certificate	Enter the identity provider certificate name.

3. Click *OK* to create the new SAML server.

To edit a SAML server in the GUI:

1. Select the SAML server you want to edit and then click *Edit* from the toolbar. The *Edit SAML* window opens.
2. Edit the server information as required and click *OK* to apply your changes.

To add a new SAML server or edit an existing SAML server in the CLI:

Use the `config user saml` command.

OIDC

OpenID Connect (OIDC) is a widely adopted JSON-based identity layer built on top of the OAuth 2.0 protocol. If you have an Identity Provider (IdP) like FortiAuthenticator, Azure AD, Google Identity, or any other service that supports OIDC, you can use it to authenticate users seamlessly across your FortiProxy instance and other integrated systems.

Like SAML, OIDC facilitates secure transfer of user authentication and authorization data between an Identity Provider (IdP) and a Relying Party (RP)—in this case, the FortiProxy unit. In OIDC-based authentication, the FortiProxy unit redirects unauthenticated users to the IdP (such as Azure Active Directory, Okta, Google, or other OIDC-compliant providers) for authentication. After the user is verified by the IdP, the user is redirected back to the FortiProxy with an ID token and possibly additional tokens in a JSON-based format. These tokens carry essential information about the user's identity, group memberships, and authorization claims.

FortiProxy uses these claims to perform both authentication and authorization steps. Depending on your IdP's configuration, group information can be included as claims in the ID token or fetched from an external directory service. This streamlined approach reduces infrastructure overhead, accelerates user login, and leverages existing IdP services without requiring additional on-premises components.

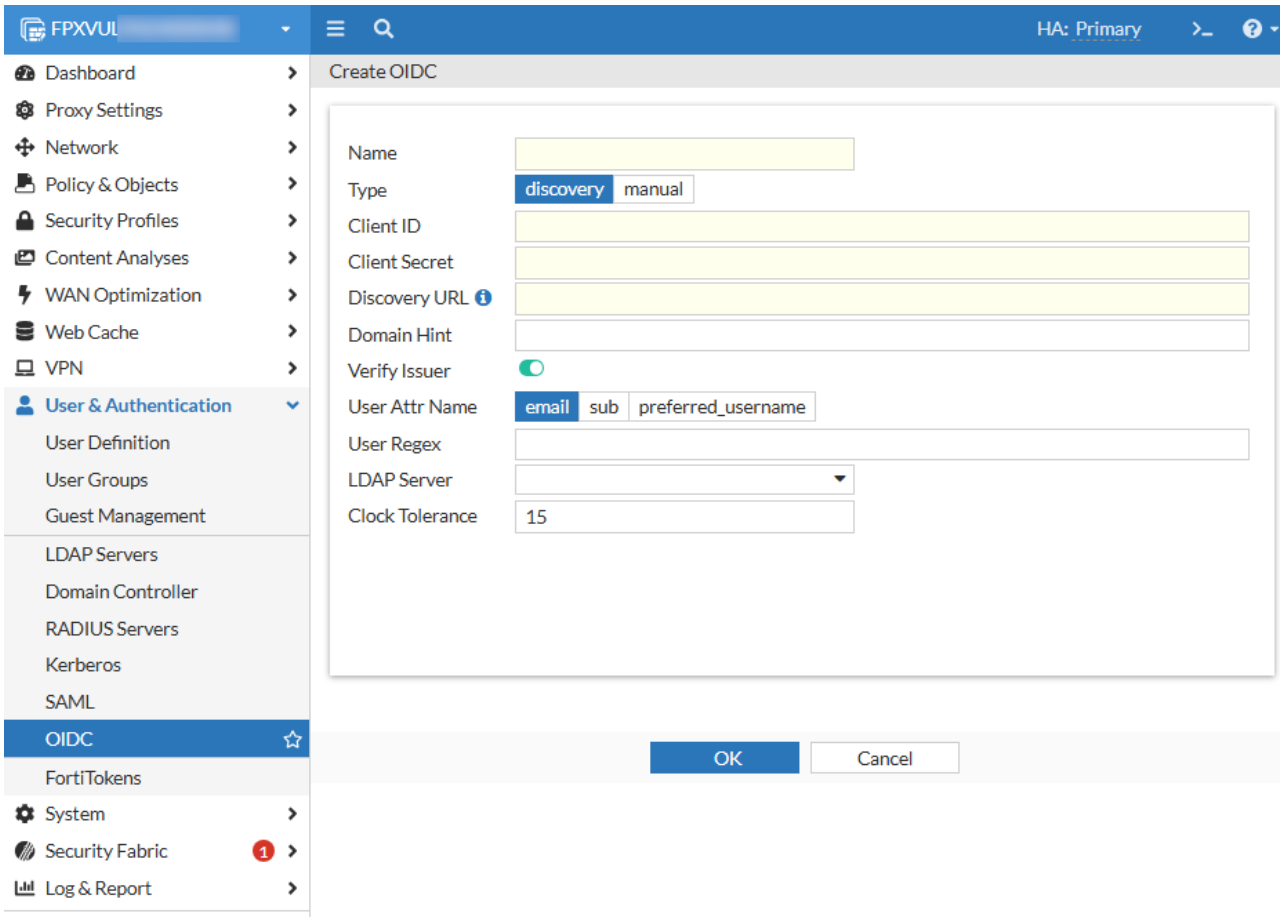
OIDC has the following advantages over other similar authentication schemes:

- OIDC builds on OAuth 2.0, which means it uses tokens for both authentication and authorization (access tokens and ID tokens), which is a more flexible and modern approach compared to traditional username/password methods, enhancing security using robust cryptographic methods and proven standards to reduce exposure of credentials.
- It improves user experience by allowing for single sign-on (SSO) across a wide range of applications and services, both on-premises and in the cloud, which simplifies deployment and scales efficiently across diverse IT ecosystems.
- OIDC is generally simpler to implement and use than SAML (Security Assertion Markup Language). While SAML is more widely used in enterprise contexts, it involves heavier XML-based messaging, which can be harder to integrate and troubleshoot.
- OIDC uses JSON Web Tokens (JWT), which are lightweight, easy to parse, and widely supported in modern web applications.

FortiProxy configuration

To configure an OIDC server in the FortiProxy GUI:

1. In the *User & Authentication* > *OIDC* tab, click *Create New* or select an existing OIDC server from the list and click *Edit*.
2. Configure the following options:



Name	Name that identifies the OIDC server on the FortiProxy unit.
Type	Select the type of OpenID Connect configuration that meets your automation and security needs.

Option	Description	Required parameters	Use case
discovery	Use an OIDC discovery URL to automatically retrieve endpoint configurations from the IdP.	discovery-url, client-id, client-secret, private-key (optional), verify-issuer (optional)	Recommended when the IdP supports the discovery mechanism, reducing manual configuration overhead.

	Option	Description	Required parameters	Use case
	manual	Use manual configuration, which requires manual input of all OIDC-related endpoints and configurations.	authorization-url, token-url, jwks-uri, client-id, client-secret	Useful when the IdP does not support discovery or when a more customized setup is required.

Client ID	OpenID Connect server client ID.
Client Secret	OpenID Connect server client secret.
Discovery URL	OpenID Connect server discovery URL. This option is available only if you selected *discovery* in *Type*.
Authorization URL	OpenID Connect server authorization URL. This option is available only if you selected *manual* in *Type*.
Token URL	OpenID Connect server token URL. This option is available only if you selected *manual* in *Type*.
JWKS URI	URL of the OP's JWK Set document. This option is available only if you selected *manual* in *Type*.
Domain Hint	Domain Hint.
Verify Issuer	Specifies whether to verify OpenID Connect server issuer. This option is available only if you selected *discovery* in *Type*.
Issuer	OpenID Connect server issuer. This option is available only if you selected *manual* in *Type*.
User Attr Name	Field in ID token to use as username.

Option	Description
email	Use email in ID token as username.
sub	Use sub in ID token as username.
preferred_username	Use preferred_username in ID token as username.

User Regex	Regular expressions that the username must match. This field is case insensitive.
LDAP Server	Select the LDAP server(s).
Clock Tolerance	Clock skew tolerance in seconds. The default is 15.

3. Click *OK*.

To configure an OIDC server in the FortiProxy CLI:

Use the `config user oidc` command. See an example below:

```
config user oidc
   edit "oidc-discovery"
      set client-id "********-****-****-****-************"
      set client-secret "**************************"
      set discovery-url "https://login.microsoftonline.com/common/v2.0/.well-known/openid-
            configuration"
      set verify-issuer disable
   next
   edit "oidc-1"
      set type manual
      set client-id "********-****-****-****-************"
      set client-secret "**************************"
      set authorization-url "https://login.microsoftonline.com/common/oauth2/v2.0/authorize"
      set token-url "https://login.microsoftonline.com/common/oauth2/v2.0/token"
      set ldap-server "AD1"
   next
   edit "oidc-google"
      set type manual
      set client-id "***************-**********************.apps.googleusercontent.com"
      set client-secret "GOCSPX-************************"
      set authorization-url "https://accounts.google.com/o/oauth2/v2/auth"
      set token-url "https://oauth2.googleapis.com/token"
      set jwks-uri "https://www.googleapis.com/oauth2/v3/certs"
   next
end
```



To avoid redirection errors during OIDC authentication, ensure that certain IdP resources are accessed directly by the application or user agent without going through any intermediary proxy.

For example, when using Google as your IdP, you must configure Google resources served from the following domains to bypass the proxy:

- `accounts.google.com`
- `.*gstatic.com`

Callback URL configuration in IdP

To fully integrate FortiProxy with an OIDC provider, you must configure the following callback URL (redirect URI) in your IdP (Azure AD, Google, Okta) and communicate the callback URL configuration to your IdP administrator:

`https://<FortiProxy_FQDN_or_IP>:7831/XX/YY/ZZ/oidc/callback`

where `<FortiProxy_FQDN_or_IP>` is the value of `authentication.settings.captive-portal` for transparent or explicit proxy deployments, or `ztna.web-portal.auth-virtual-host` for ZTNA web portal deployments.

Configuring multiple Identity Providers (IDP) NEW

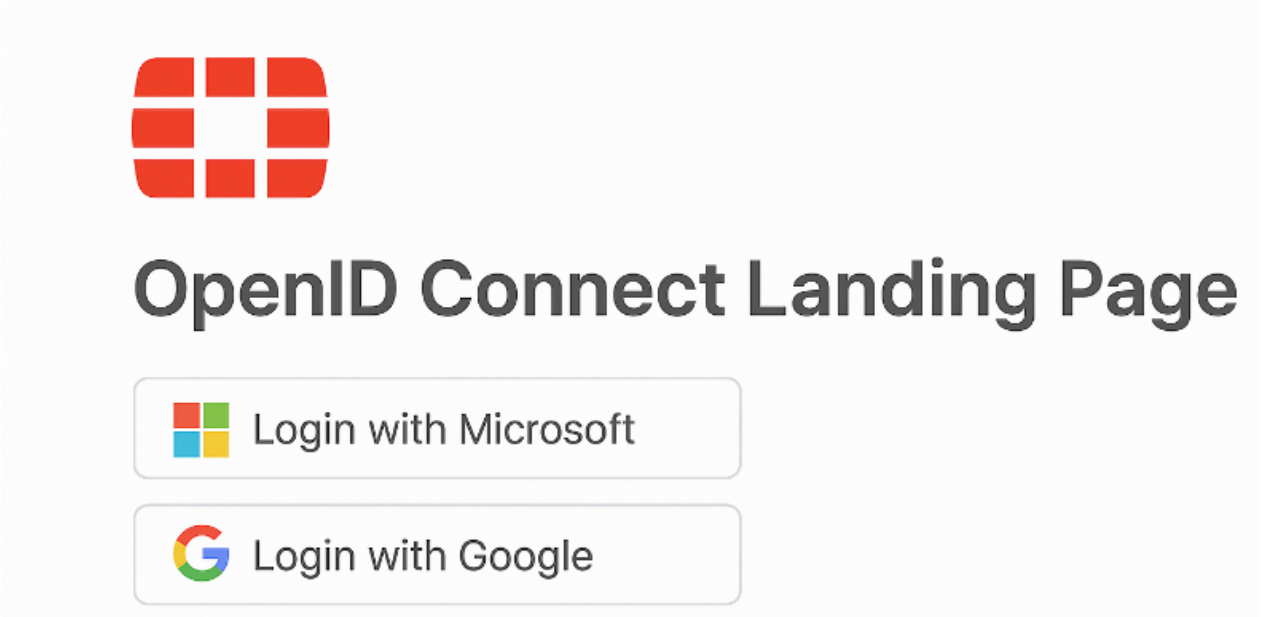
FortiProxy supports multiple OIDC identity providers (IdPs) in one authentication scheme. When multiple IdPs are configured, users can select which IdP to use in the OIDC landing page, allowing for flexible authentication across different user groups. This is useful in the following scenarios:

- The organization manages multiple IdPs for different user sets (e.g., Azure AD for employees, Google Identity for contractors).
- A transition between identity providers is required (e.g., migrating from Okta to Azure AD).
- Users need to choose their preferred IdP for authentication.

To configure multiple IdPs with a custom IdP selection page:

```
config user oidc
   edit "oidc-azure"
      set display-name "Login with Microsoft"
      set icon-url "xxxxxxxxxxxx"
      set client-id "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
      set auth_type private-key
      set private-key "oidc-key"
      set discovery-url "https://login.microsoftonline.com/tenant_id/v2.0/.well-known/openid-
            configuration"
      next
   edit "oidc-google"
      set display-name "Login with Google"
      set icon-url "xxxxxxxxxxxx"
      set type manual
      set client-id "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy"
      set client-secret "GOCSPX-************************"
      set authorization-url "https://accounts.google.com/o/oauth2/v2/auth"
      set token-url "https://oauth2.googleapis.com/token"
      set jwks-uri "https://www.googleapis.com/oauth2/v3/certs"
   next
end
config user group
   edit "group-all"
      set member "oidc-azure" "oidc-google"
   next
end
config authentication scheme
   edit "oidc-auth-scheme"
      set method oidc
      set oidc-server "oidc-azure" "oidc-google"
   next
end
```

With this configuration, users are presented with a custom IdP selection page and can choose which provider they want to authenticate with.



They are then redirected to the selected IdP's authentication portal and then redirected back to FortiProxy with an OIDC token to complete the authentication process after successful authentication.

FortiTokens

FortiTokens are security tokens used as part of a multi-factor authentication (MFA) system on FortiProxy and FortiAuthenticator to apply MFA to FortiProxy user, administrator, and captive portal authentication. A security token is a 6-digit or 8-digit (configurable) one-time password (OTP) for authenticating one's identity electronically as a prerequisite for accessing network resources. FortiToken is available as a mobile or a physical (hard) token. The encryption seeds of the tokens are stored on the cloud and are always encrypted whether in motion or at rest.

Mobile tokens can be purchased as a license, or consumed with points as part of the FortiToken Cloud service. FortiToken Mobile is an OATH compliant, event- and time-based one-time password (OTP) generator application that provides an easy and flexible way to deploy and provision FortiTokens to your end users through mobile devices without the need for a physical token. FortiToken Mobile supports the following platforms:

Platform	Device and firmware support
iOS	iPhone, iPad, and iPod Touch with iOS 6.0 and later.
Android	Phones and tablets with Android Jellybean 4.1 and later.
Windows	Windows 10 (desktop and mobile), Windows Phone 8.1, and Windows Phone 8.

Platform	Device and firmware support
	FortiToken is a Windows Universal Platform (UWP) application. To download FortiToken for Windows 10 desktop and mobile platforms, see FortiToken for Windows on the Microsoft Store.

A FortiToken can only be registered to a single FortiProxy or FortiAuthenticator for security purposes. This prevents malicious third parties from making fraudulent requests to hijack your FortiTokens by registering them on another FortiProxy or FortiAuthenticator. If re-registering a FortiToken mobile or hard Token on another FortiProxy is required, you must contact Fortinet Customer Support.

The MFA process commonly involves:

- **Something you know**: User password
- **Something you have**: The FortiToken OTP

A third factor of authentication is added to the authentication process:

- **Something you are**: Your fingerprint or face

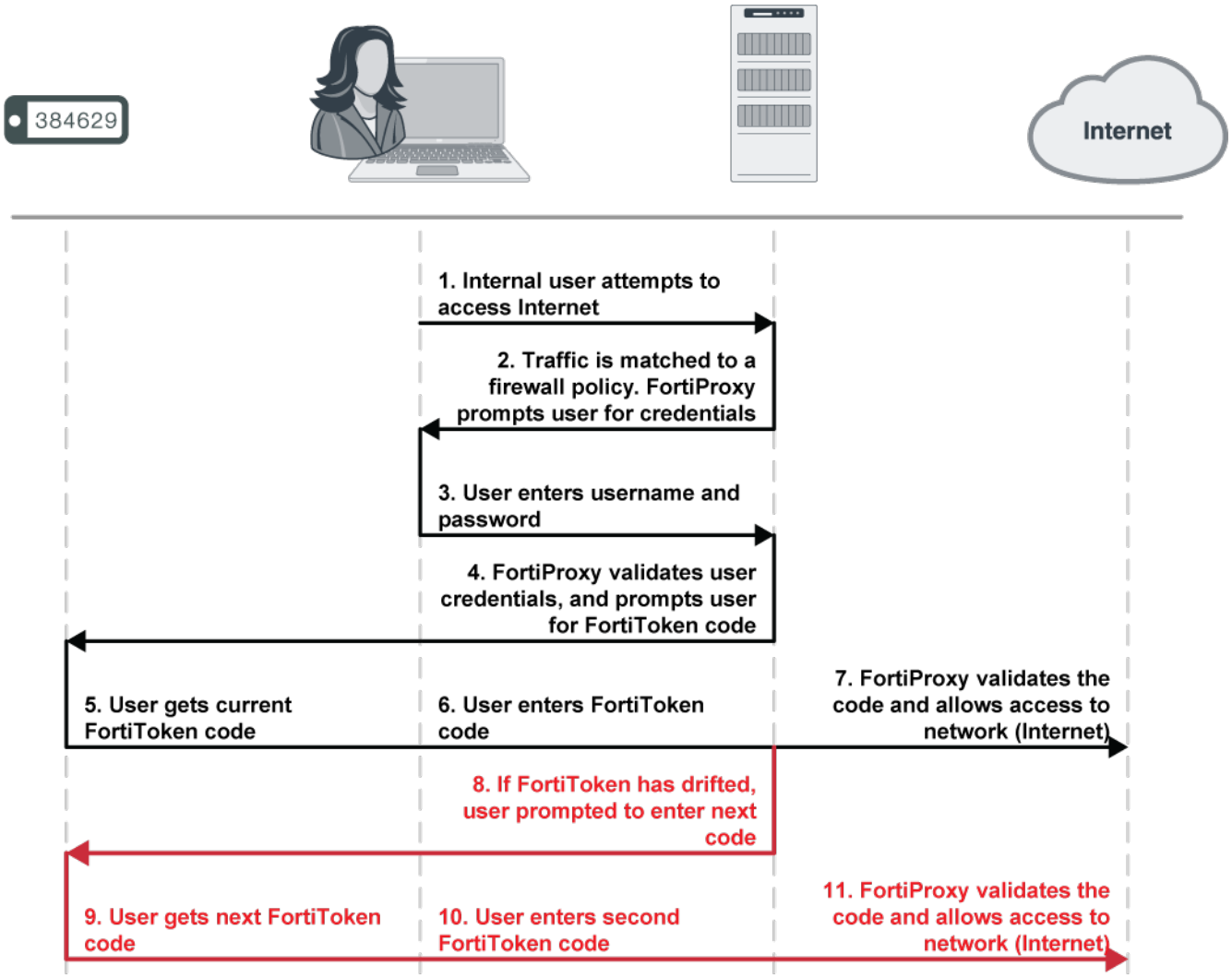
To enable the third factor, refer to the Activating a mobile token on page 851 section.

The following illustrates the FortiToken MFA process:

1. The user attempts to access a network resource.
2. FortiProxy matches the traffic to an authentication security policy and prompts the user for the username and password.
3. The user enters the username and password.
4. FortiProxy verifies their credentials. If valid, it prompts the user for the FortiToken code.
5. The user views the current code on their FortiToken and enters the code at the prompt.
6. FortiProxy verifies the FortiToken code. If valid, it allows the user access to network resources.

If the FortiToken has drifted, the following must take place for the FortiToken to resynchronize with FortiProxy:

1. FortiProxy prompts the user to enter a second code to confirm.
2. The user gets the next code from the FortiToken and enters the code at the prompt.
3. FortiProxy uses both codes to update its clock to match the FortiToken.



This section includes the following topics to quickly get started with FortiTokens:

- Registering and activating a hard token on page 846
- Assigning a FortiToken to a user account on page 848
- Activating a mobile token on page 851
- Managing FortiTokens on page 855
- FortiToken Cloud on page 857
- Synchronizing LDAP Active Directory users to FortiToken Cloud using the two-factor filter on page 857
- Troubleshooting and diagnosis on page 861

Registering and activating a hard token

Hard tokens must be registered and activated before they can be assigned to a user (see Assigning a FortiToken to a user account on page 848).

The activation requires connection to FortiGuard servers so that FortiProxy can successfully query FortiGuard servers about the validity of the token. Each token can only be used on a single FortiProxy or FortiAuthenticator. Tokens already registered are deemed invalid for re-activation on another device. FortiProxy encrypts the serial number and information before sending it for added security.

To register and activate hard tokens in the GUI:

1. Go to *User & Authentication* > *FortiTokens*.
2. Click *Create New*.
3. In the *Serial Number* field, enter one or more FortiToken serial numbers. Alternatively, click *Import* and upload a serial number file or seed file.



Seed files are only used with FortiToken-200CD. These are special hardware tokens that come with FortiToken seeds on a CD. See the FortiToken Comprehensive Guide for details.

4. Click *OK*.
5. In the token list, right-click the token(s) you just registered (with an *Available* status) and click *Activate*.
6. Click *Refresh*. The selected hard tokens are activated.

To register individual hard tokens by serial number in the CLI:

activate hard tokens in the FortiProxy CLI:

```
config user fortitoken
   edit <serial_number>
   next
   edit <serial_number2>
   next
end
```

To import hard tokens to the FortiProxy unit via a serial number file or seed file in the CLI:

```
execute fortitoken import ftp <file name> <ip>[:ftp port] <Enter> <user> <password>
execute fortitoken import tftp <file name> <ip>
execute fortitoken import usb <file name>
```



The serial number file must be a text file with one FortiToken serial number per line. FortiToken seed files can be imported from FTP and TFTP servers, or a USB drive.

To activate hard tokens in the CLI:

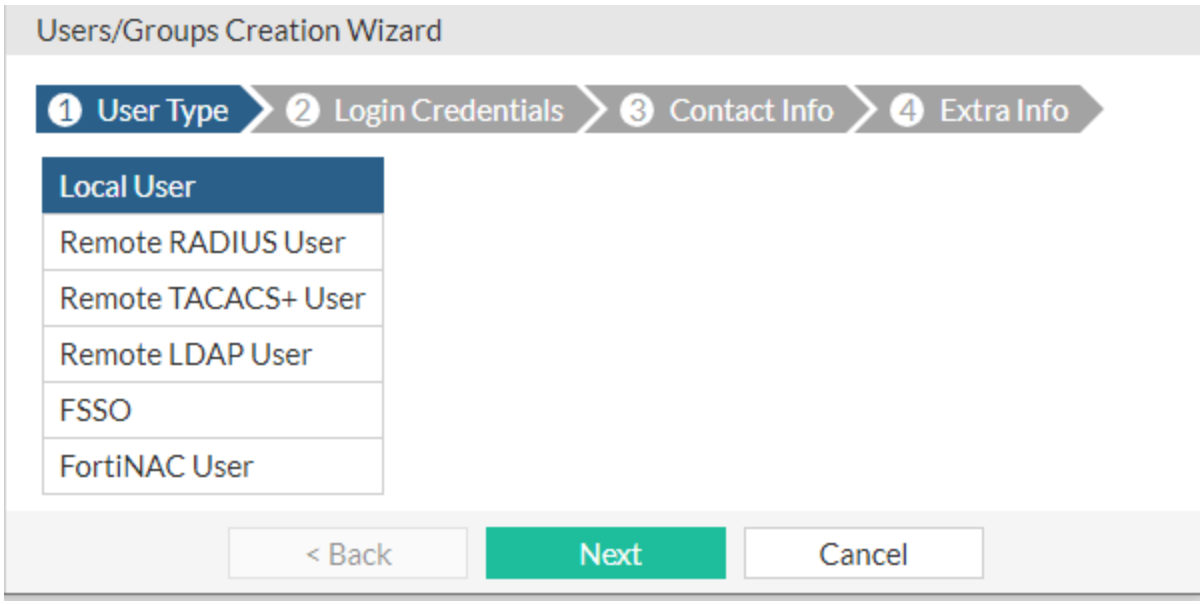
```
config user fortitoken
   edit <token_serial_num>
      set status activate
   next
end
```

Assigning a FortiToken to a user account

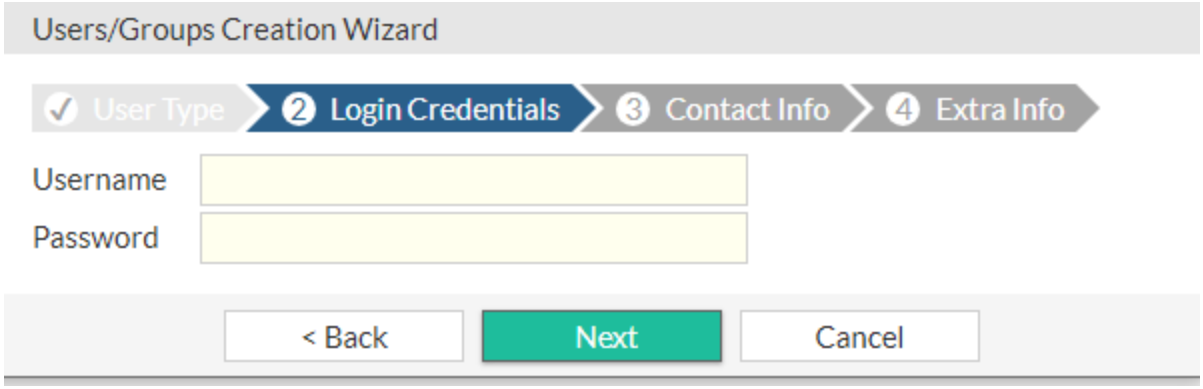
FortiTokens need to be assigned to users before they can be used for two-factor authentication. In this example, you will assign a FortiToken to a local user. Similar steps can be taken for other types of users (see Creating or editing a user on page 798). You can also assign a token to administratorsand captive portal users.

To assign a FortiToken to a local user in the FortiProxy GUI:

1. For hard tokens, ensure that you have registered and activated them. See Registering and activating a hard token on page 846.
2. Go to *User & Authentication* > *User Definition*, and click *Create New*. The *Users/Groups Creation Wizard* appears.
3. In the *User Type* tab, select *Local User*, and click *Next*.



4. In the *Login Credentials* tab, enter a *Username* and *Password* for the user, and click *Next*.



5. In the *Contact Info* tab:
   a. Enable the *Two-factor Authentication* toggle.
   b. Select *FortiToken* for *Authentication Type*.

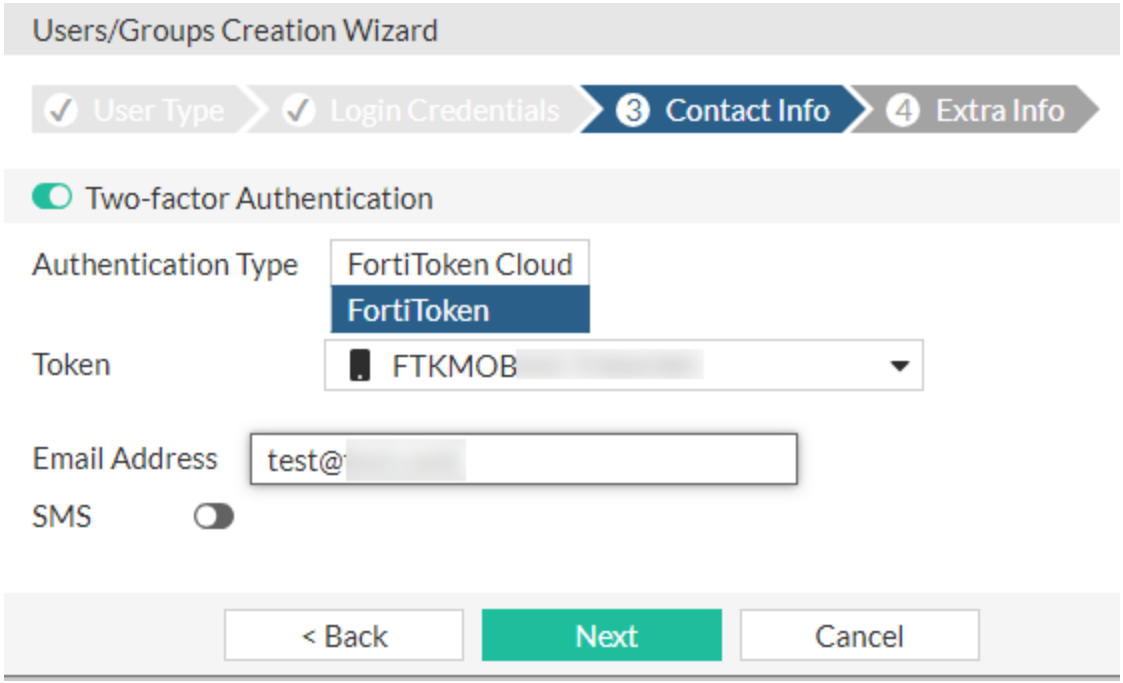
c. Select a *Token* to assign to the user from the dropdown list.

- Hard tokens must be registered and activated first before they appear in the dropdown list. See Registering and activating a hard token on page 846.
- Mobile tokens are limited to the two free trial tokens on FortiProxy. You cannot add or import any other mobile tokens.

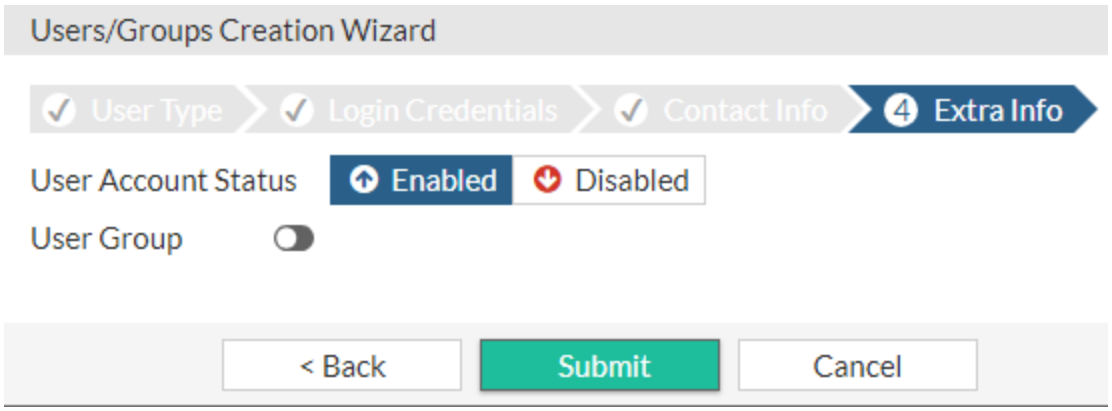
d. Enter the user's email address in the *Email Address* field.
For mobile tokens, FortiProxy will send the QR code for activation to this email.

FortiProxy has the *Email Service* setting configured using the server *notifications.fortinet.net* by default. To see configuration, go to *System > Settings > Email Service*.

e. Click *Next*.



6. In the *Extra Info* tab, make sure the *User Account Status* field is set to *Enabled*. You can also optionally assign the user to a user group by enabling the *User Group* toggle.



7. Click *Submit*.
   For mobile tokens, an activation code will be sent to the created user by email or SMS, depending upon the configured delivery method. By default, the activation code expires if not activated within 3 days. You can configure the expiry time period (in hours) by running the following command:

```
config system global
   set two-factor-ftm-expiry <1-168>
end
```

To resend the email or SMS with the activation code, refer to the Managing FortiTokens on page 855 section.

To assign a FortiToken to a local user account in the FortiProxy CLI:

```
config user local
   edit <username>
      set type password
      set passwd "myPassword"
      set two-factor fortitoken
      set fortitoken <serial_number>
      set email-to "username@example.com"
      set status enable
   next
end
```

Before you can use a new FortiToken, you may need to synchronize it due to clock drift.

Users assigned a mobile token must follow the steps in Activating a mobile token on page 851 to activate the mobile token before using it.

Activating a mobile token

After your system administrator assigns you a mobile token, you will receive a notification with an activation code and expiry date via SMS or email. You must activate the mobile token by the expiry date. If the activation code expires, contact your system administrator to reassign a mobile token for activation.

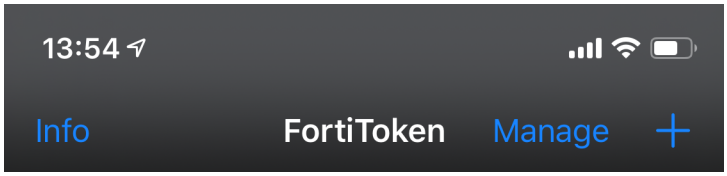
The following procedure provides an example of activating a mobile token using FortiToken Mobile for iOS on an iPhone. Procedures may vary depending on your device and firmware.

To activate your mobile token on iOS on an iPhone:

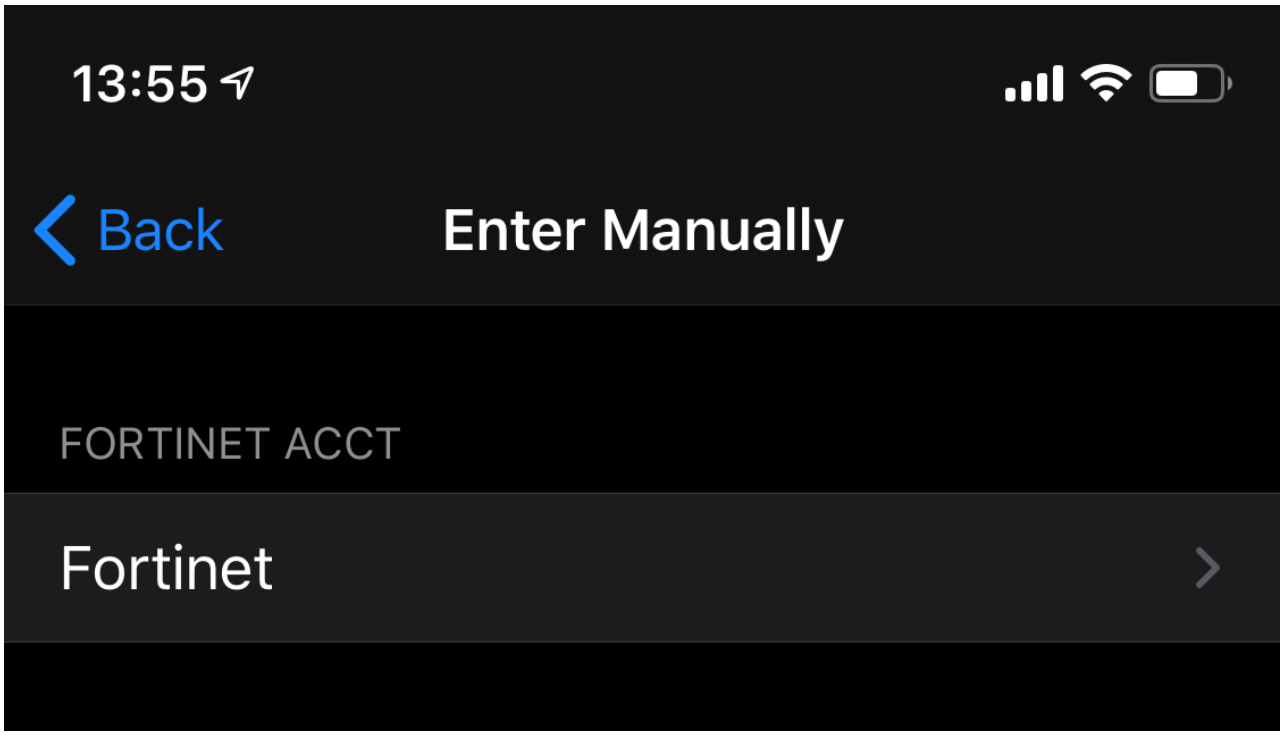
1. Make sure your mobile device and the FortiProxy unit are connected to the Internet.
2. Tap on the FortiToken application icon to open the application. If this is your first time opening the application, it may prompt you to create a PIN for secure access to the application and tokens.



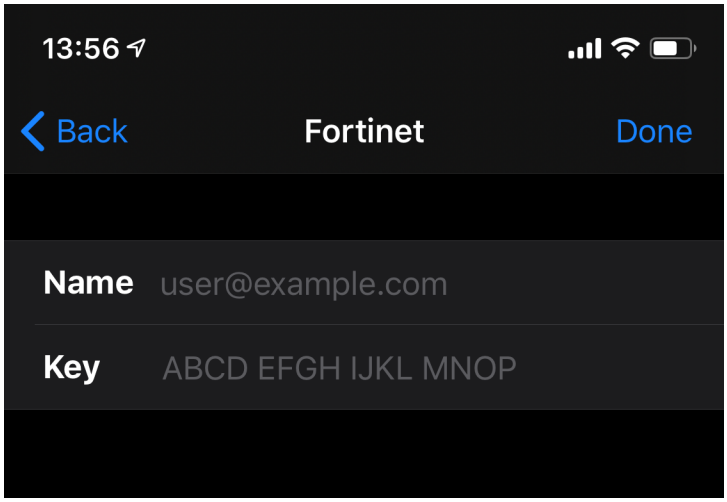
3. Tap on the + icon. The *Scan Barcode* screen appears.



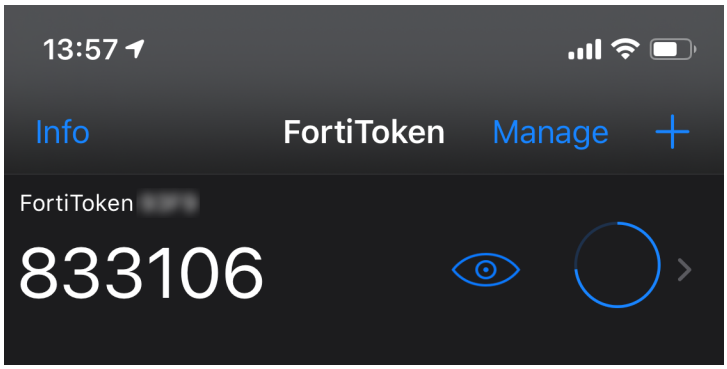
4. If you received the QR code via email, locate and scan the QR code in your email.
   OR
   If you received the activation key via SMS, tap on *Enter Manually* at the bottom of the screen, and tap on *Fortinet*.



Enter your email address in the *Name* field, the activation key in the *Key* field, and tap *Done*.



5. FortiToken Mobile activates your token, and starts generating OTP digits immediately. To view or hide the OTP digits, tap the eye icon.

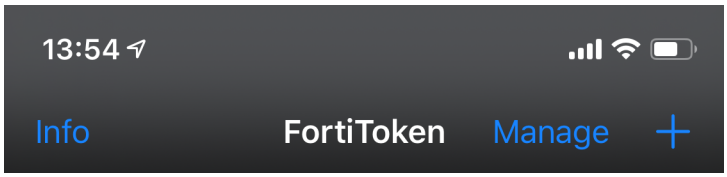


After you open the application, FortiToken Mobile generates a new 6-digit OTP every 30 seconds. All configured tokens display on the application home screen.

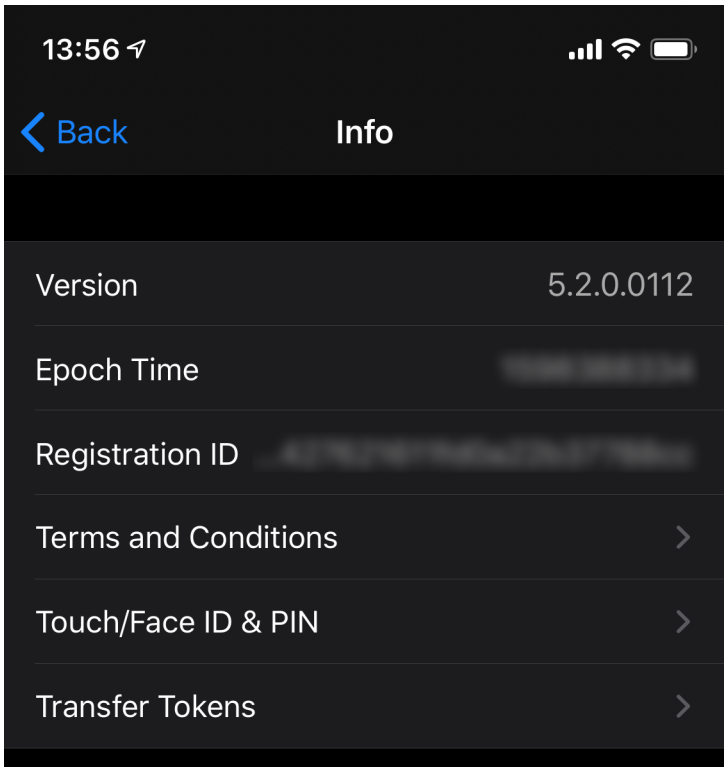
The FortiToken Mobile activation process described above caters to the MFA process that involves two factors (password and OTP) of the authentication process. A third factor (fingerprint or face) can be enabled as well.

To enable *Touch/Face ID* on iOS for FortiToken Mobile:

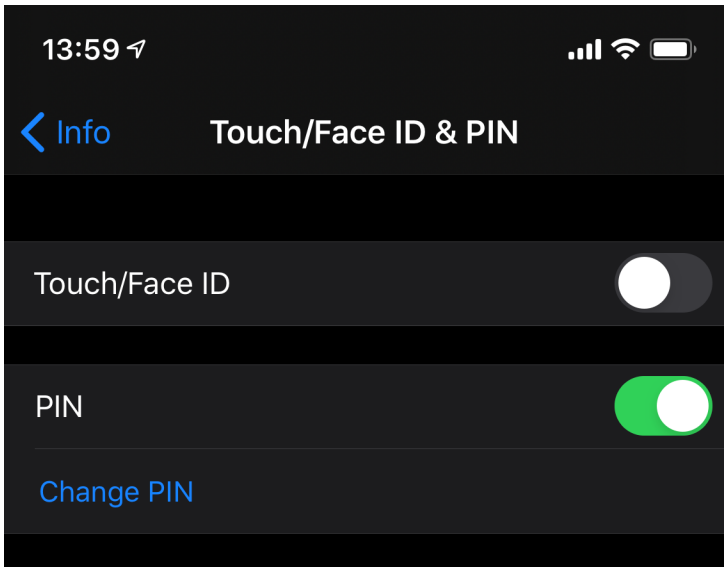
1. Open the FortiToken application and tap on *Info*.



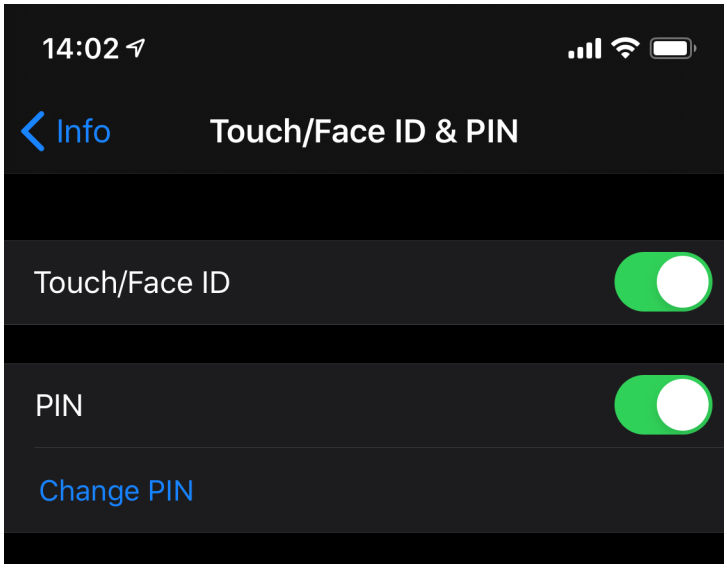
2. Tap on *Touch/Face ID & PIN*.



3. Enable and set up a 4-digit *PIN* for the application. The *PIN* is required to be enabled before you can enable *Touch/Face ID*.

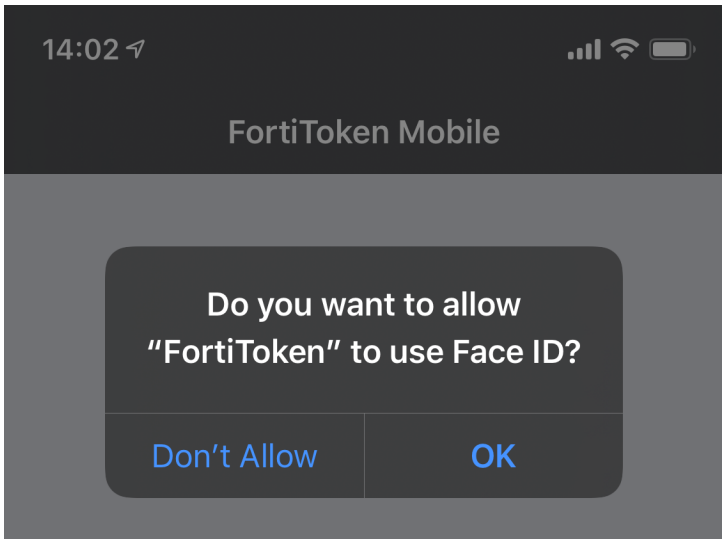


4. Enable *Touch/Face ID*.



You cannot enable *Touch/Face ID* for FortiToken if *Touch/Face ID* is not set up and enabled for device unlock (*iPhone Unlock* in this case) on iOS. You must first set up and enable *Touch/Face ID* from *Settings* on your iOS device.

5. When prompted by iOS, allow the FortiToken application to use *Touch/Face ID* by tapping on *OK* in the prompt.



After the mobile token is activated, you can generate OTPs in the FortiToken Mobile application on you mobile device without network access.

Managing FortiTokens

This section focuses on the following:

- Resending an activation email on page 855
- Locking/unlocking FortiTokens on page 855
- Managing FortiTokens drift on page 856
- Deactivating FortiTokens on page 856
- Moving FortiTokens to another device on page 857

Resending an activation email

To resend an activation email/SMS for a mobile token on a FortiProxy:

1. Go to *User & Authentication* > *User Definition* and edit the user.
2. Click *Send Activation Code Email* from the *Two-factor Authentication* section.

Locking/unlocking FortiTokens

A FortiToken can be associated with only one account on one FortiProxy unit. If a user loses the FortiToken, lock the FortiToken using the FortiProxy unit so it will not be used to falsely access the network. Later if found, you can unlock FortiToken on the FortiProxy unit to allow access once again.

To change FortiToken status to active or to lock:

```
config user fortitoken
   edit <token_serial_num>
      set status <active | lock>
   next
```

```
end
```

A user attempting to log in using a locked FortiToken cannot successfully authenticate.

Managing FortiTokens drift

If the FortiToken has drifted, the following must take place for the FortiToken to resynchronize with FortiProxy:

1. FortiProxy prompts the user to enter a second code to confirm.
2. The user gets the next code from the FortiToken and enters the code at the prompt.
3. FortiProxy uses both codes to update its clock to match the FortiToken.

If you still experience clock drift, it may be the result of incorrect time settings on your mobile device. If so, make sure that the mobile device clock is accurate by confirming the network time and the correct timezone.

If the device clock is set correctly, the issue could be the result of the FortiProxy and FortiTokens being initialized prior to setting an NTP server. This will result in a time difference that is too large to correct with the synchronize function. To avoid this, manually drift adjust the selected tokens.

To show current drift and status for each FortiToken:

```
diagnose fortitoken info
FORTITOKEN DRIFT STATUS
FTK200XXXXXXXXXC 0 token already activated, and seed won't be returned
FTK200XXXXXXXXXE 0 token already activated, and seed won't be returned
FTKMOBXXXXXXXXXA 0 provisioned
FTKMOBXXXXXXXXX4 0 new
Total activated token: 0
Total global activated token: 0
Token server status: reachable
```

This command lists the serial number and drift for each configured FortiToken. You can check if it is necessary to synchronize the FortiProxy and any particular FortiTokens.

To adjust Mobile FortiToken for drift:

```
# execute fortitoken sync <FortiToken_ID> <token_code1> <next_token_code2>
```

Deactivating FortiTokens

To deactivate FortiToken on a FortiProxy:

1. Go to *User & Authentication > User Definition*.
2. Select and edit the user for which you want to deactivate the token.
3. Disable the *Two-factor Authentication* toggle.
4. Click *OK*. The token will be removed from the user's *Two-factor Authentication* column. The user will also be removed from the token's *User* column under *User & Authentication > FortiTokens*.

Moving FortiTokens to another device

FortiTokens can only be activated on a single FortiProxy or FortiAuthenticator. To move FortiTokens to another device, you would first have to reset the registered FortiTokens on a device and then reactivate them on another device.

To reset hard tokens registered to a FortiProxy appliance (non-VM model), you can reset all hardware FTK200 tokens from the Support Portal, or during RMA transfer. See the Migrating users and FortiTokens to another FortiProxy KB article, for more information.



The above process will reset all hard tokens and you cannot select individual tokens to reset.

To reset FortiToken Mobile, a single hard token, a hard token registered to a VM, and so on, an administrator must contact Customer Support and/or open a ticket on the Support Portal.

Once reset, the FortiTokens can be activated on another FortiProxy or FortiAuthenticator.

Migrate FortiToken Mobile users from FortiProxy to FortiToken Cloud

You can migrate FortiToken Mobile users from the FortiProxy unit to FortiToken Cloud with a time-based subscription license using the `execute fortitoken-cloud migrate-ftm <license> <vdom>` command.

A request must be made to Fortinet Customer Service to initiate and pre-authorize the transfer. All current active FortiToken Mobile users will be migrated to the FortiToken Cloud license with no changes to the FortiToken Mobile serial number. The FortiProxy user or administrator's two-factor setting is automatically converted from `fortitoken` to `fortitoken-cloud`. After migration, end users will be able to authenticate as before without any changes to their FortiToken mobile app. See Migrate FTM tokens to FortiToken Cloud for more information.

FortiToken Cloud

FortiToken Cloud is an Identity and Access Management as a Service (IDaaS) cloud service offering by Fortinet. It enables FortiProxy and FortiAuthenticator customers to add MFA for their respective users, through the use of mobile tokens or hard tokens. It protects local and remote administrators as well as firewall users.

For information, see the FortiToken Cloud Administration Guide.

Synchronizing LDAP Active Directory users to FortiToken Cloud using the two-factor filter

To synchronize Active Directory users and apply two-factor authentication using FortiToken Cloud, two-factor authentication can be enabled in the `user ldap` object definition in FortiProxy. By default, FortiProxy retrieves all Active Directory users in the LDAP server with a valid email or mobile number

(`mail` and `mobile` attributes), and synchronizes the users to FortiToken Cloud. Users are then created on FortiToken Cloud and activation is sent out using email or SMS.

Two-factor filters can be used to reduce the number of the Active Directory users returned, and only synchronize the users who meet the filter criteria.

```
config user ldap
    edit <name>
        set dn <string>
        set two-factor {disable | fortitoken-cloud}
        set two-factor-filter <string>
    next
end
```

`dn <string>`	Set the distinguished name used to look up entries on the LDAP server. The search for users and groups starts here based on what is defined.
`two-factor {disable | fortitoken-cloud}`	Enable/disable two-factor authentication: • `disable`: disable two-factor authentication • `fortitoken-cloud`: use the FortiToken Cloud service
`two-factor-filter <string>`	Set the filter used to synchronize users to FortiToken Cloud.



When configuring an LDAP connection to an Active Directory server, an administrator must provide Active Directory user credentials.

- To secure this connection, use LDAPS on both the Active Directory server and FortiProxy. See Create or edit an LDAP server on page 819 and Setting up an authentication captive portal using client certificate.
- Apply the principle of least privilege. For the LDAP regular bind operation, do not use credentials that provide full administrative access to the Windows server when using credentials. See Creating an administrator that can be authenticated by an LDAP server on page 820.

Two-factor filter examples

In the following examples, a `user ldap` object is defined to connect to an Active Directory on a Windows server. The search will begin in the root of the fortinet-fsso.com directory.

To configure a default LDAP server configuration without a two-factor filter:

```
config user ldap
    edit "ad-ldap-auth"
        set server <ip_address>
        set cnid "cn"
        set dn "dc=fortinet-fsso,dc=com"
        set type regular
        set two-factor fortitoken-cloud
        set username "cn=Administrator,cn=users,dc=fortinet-fsso,dc=com"
```

```
        set password **********
    next
end
```

When a two-factor filter is not used, all users in the Active Directory with a valid email or mobile number will be retrieved.

Example 1: specific users and email address with wildcard

With this `two-factor-filter`, users under fortinet-fsso.com that have oliver* in their username and *fortinet* in their email will be matched.

```
config user ldap
    edit "ad-ldap-auth"
        set two-factor-filter "(&(SAMAccountName=oliver*)(mail=*fortinet*))"
    next
end
```

Example 2: all users with matching email

With this `two-factor-filter`, all users under fortinet-fsso.com with *fortinet* in their email will be matched.

```
config user ldap
    edit "ad-ldap-auth"
        set two-factor-filter "(&(SAMAccountName=*)(mail=*fortinet*))"
    next
end
```

Example 3: all users in a group

With this `two-factor-filter`, all users within the group fortinet-fsso.com > Testing > ftc-users will be matched.

```
config user ldap
    edit "ad-ldap-auth"
        set two-factor-filter "(&(objectCategory=Person)(sAMAccountName=*)( memberOf=cn=ftc-
users,ou=Testing,dc=fortinet-fsso,DC=com))"
    next
end
```

Example configuration

In this example, Active Directory users are configured to be synchronized to FortiToken Cloud. The same two-factor filter is used from example 1 and searches the Active Directory for users named oliver* with email *fortinet*.

Before configuring the FortiProxy:

1. Gather the information to connect to the Active Directory server through LDAP. Include all necessary fields, such as the server IP, port, CN name identifier, DN for the start of the search, bind type, and username associated with a regular bind.
2. Consider the users or groups that require two-factor authentication and should be synchronized. If necessary, group the users under the same group in the Active Directory.
3. If using a two-factor filter, formulate the `two-factor-filter` string to limit the match. For this example, `(&(SAMAccountName=oliver*)(mail=*fortinet*))`.
4. Test the filter by using the FortiProxy CLI to perform a quick LDAP search:

```
# diagnose test authserver ldap-search <server_ip> 389 "ou=Testing,dc=fortinet-fsso,DC=com" cn
Administrator@fortinet-fsso.com PASSWORD 0 '(&(SAMAccountName=oliver*)(mail=*fortinet*))' 2

searching 'ou=Testing,dc=fortinet-fsso,DC=com, cn=cn' on 10.1.100.131:389 for
(Administrator@fortinet-fsso.com, PASSWORD), secure(0), filter((&(SAMAccountName=oliver*)
(mail=*fortinet*))), flag(0x2), page_no(0)...
CN=oliver2022,OU=Testing,DC=Fortinet-FSSO,DC=COM (oliver2022, 0 entries)
```

   The user, `oliver2022`, was found.
5. Estimate how many users will be retrieved, and ensure that the FortiToken Cloud account has enough user licenses to support the number of users.

To configure Active Directory users to be synchronized to FortiToken Cloud:

1. Configure the user LDAP settings:

```
config user ldap
    edit "ad-ldap-auth"
        set server "10.1.100.131"
        set cnid "cn"
        set dn "dc=fortinet-fsso,dc=com"
        set type regular
        set two-factor fortitoken-cloud
        set username "cn=Administrator,cn=users,dc=fortinet-fsso,dc=com"
        set password **********
        set two-factor-filter "(&(SAMAccountName=oliver*)(mail=*fortinet*))"
    next
end
```

2. In the background, the FortiProxy FAS daemon scans the LDAP server for users to be synchronized based on the two-factor filter pattern, but will not send them to the FortiToken Cloud server yet. Optionally, verify the users that are retrieved from the Active Directory based on the filter:

```
# diagnose fortitoken-cloud debug enable
# diagnose debug enable
# diagnose fortitoken-cloud sync
...
fas_sync_ftc[2788]: Sending packet to FTC server: "IP-of-FTC-server" Port: 8686(length:444)
fas_sync_ftc[2792]: FTC User Sync Packet(length:444):
POST /api/v1/user_sync HTTP/1.1
Host: ftc.fortinet.com
```

```
Connection: keep-alive
User-Agent: FortiProxy-400G v7.4.4,build****
Content-Type: application/json
Content-Length: 246
{"users":[{"username":"oliver2022","vdom":"vdom1","email":"o****@fortinet.com","mobile_
number":"XXXXXXXXXXX","user_data":1,"action":"create"}],"sn":"FG4H1E5819900000","cluster_
members":[ "FG4H1E5819900000" ],"group_name":"FGT400D","group_id":"0"}
Reminder: User sync packet not actually sent out because of diagnose purpose!
```

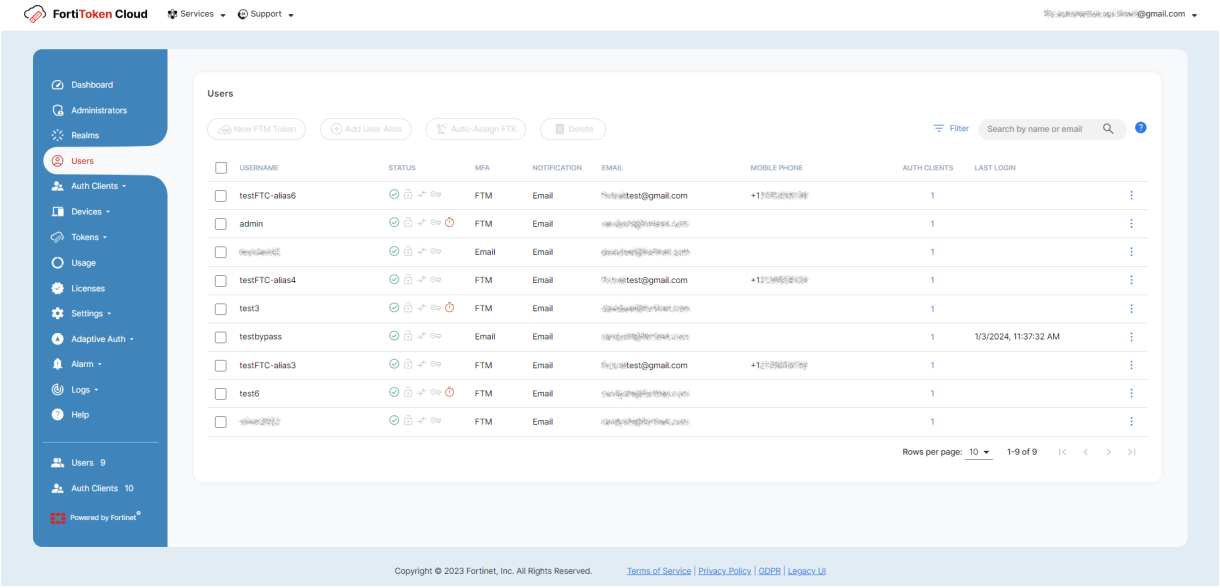
As expected, only the user that matches the current filter is returned.

3. Manually trigger the synchronization process with FortiToken Cloud:

```
# execute fortitoken-cloud sync
```

The user is added to FortiToken Cloud, and an activation email or SMS message is sent to the user.

4. In FortiToken Cloud, go to *Users* to verify that the user was added.



If the activation email was sent, but user has not downloaded and activated the mobile token yet, a pending symbol appears in the *Status* column (such as for the *admin*, *test6*, and *test3* users).

5. In FortiProxy, add the `ad-ldap-auth` object in a user group. The user group can be used for VPN, firewall authentication, and so on.



The `ldap user` object should not be used in remote LDAP user groups that require group matching because it is not supported.

Troubleshooting and diagnosis

This section contains some common scenarios for FortiTokens troubleshooting and diagnosis:

- FortiToken Statuses on page 862
- Recovering lost Administrator FortiTokens on page 863

FortiToken Statuses

When troubleshooting FortiToken issues, it is important to understand different FortiToken statuses. FortiToken status may be retrieved either from the CLI or the GUI, with a slightly different naming convention.

Before you begin, verify that the FortiProxy has Internet connectivity and is also connected to both the FortiGuard and registration servers:

```
# execute ping fds1.fortinet.com
# execute ping directregistration.fortinet.com
# execute ping globalftm.fortinet.net
```

If there are connectivity issues, retrieving FortiToken statuses or performing FortiToken activation could fail. Therefore, troubleshoot connectivity issues before continuing.

To retrieve FortiToken statuses:

- In the CLI:
  `# diagnose fortitoken info`
- In the GUI:
  Go to *User & Authentication* > *FortiTokens*.

The FortiToken can be in the following statuses:

CLI	GUI	Description
`new`	*Available*	Newly added, not pending, not activated, not yet assigned.
`active`	*Assigned*	Assigned to a user, hardware token.
`provisioning`	*Pending*	Assigned to a user and waiting for activation on the FortiToken Mobile app.
`provisioned`	*Assigned*	Assigned to user and activated on the FortiToken Mobile app.
`provision timeout`		Token provided to user but not activated on the FortiToken Mobile app. To fix, the token needs to be re-provisioned and activated in time.
`token already activated, and seed won't be returned`	*Error*	Token is locked by FortiGuard FDS. The hardware token was already activated on another device and locked by FDS.
`locked`		Either manually locked by an Administrator (`set status lock`), or locked automatically, for example, when the token is unassigned and the FortiCare FTM provisioning server was unreachable to process that change.



Recovering lost Administrator FortiTokens

If an Administrator loses their FortiToken or the FortiToken is not working, they will not be able to log into the admin console through the GUI or the CLI. If there is another Administrator that can log into the device, they may be able to reset the two-factor settings configured for the first Administrator, or create a new Admin user for them. Note that a *super_admin* user will be able to edit other admin user settings, but a *prof_admin* user will not be able to edit *super_admin* settings.

In the case where there are no other administrators configured, the only option is to flash format the device and reload a backup config file. You must have console access to the device in order to format and flash the device. It is recommended to be physically on site to perform this operation.

Before formatting the device, verify that you have a backup config file. You may or may not have the latest config file backed up, though you should consider using a backed up config file, and reconfigure the rest of the recent changes manually. Otherwise, you may need to configure your device starting from the default factory settings.

To recover lost Administrator FortiTokens:

1. If you have a backed up config file:
   a. Open the config file and search for the specific admin user. For representational purposes we will use `Test` in our example.
   ```
   # edit "Test"
      set accprofile "super_admin"
      set vdom "root"
      set two-factor fortitoken
      set fortitoken "FTKXXXXXXXXXX"
      set email-to "admin@email.com"
      set password *********
      next
   end
   ```
   b. Once you find the settings for the `Test` user, delete the `fortitoken`-related settings:
   ```
   # edit "Test"
      set accprofile "super_admin"
      set vdom "root"
      set password *********
      next
   end
   ```
2. Format the boot device during a maintenance window and reload the firmware image using instructions in Formatting and loading FortiProxy firmware image using TFTP on page 1199.
3. Once the reload is complete, log into the admin console from the GUI using the default admin user credentials, and go to *Configuration > Restore* from the top right corner to reload your config file created in Step 1 above.
4. Once the FortiProxy reboots and your configuration is restored, you can log in with your admin user credentials.

System

The *System* menu provides submenus for three areas: system administration, system configuration, and certificates.

System administration covers the following topics:

- Administrators on page 864
- Admin Profiles on page 872
- Fabric Management on page 875
- Settings on page 879

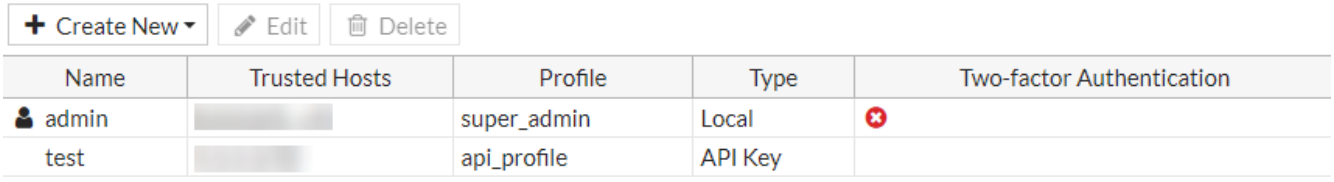
System configuration covers the following topics:

- HA on page 904
- SNMP on page 923
- Replacement Messages on page 944
- Replacement Message Groups on page 960
- FortiGuard on page 962
- Feature Visibility on page 970

Certificates on page 973 covers generating, editing, deleting, importing, viewing, and downloading certificates.

Administrators

Administrators are configured in *System* > *Administrators*. There is already a default administrator account on the unit named `admin` that uses the super_admin administrator profile.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

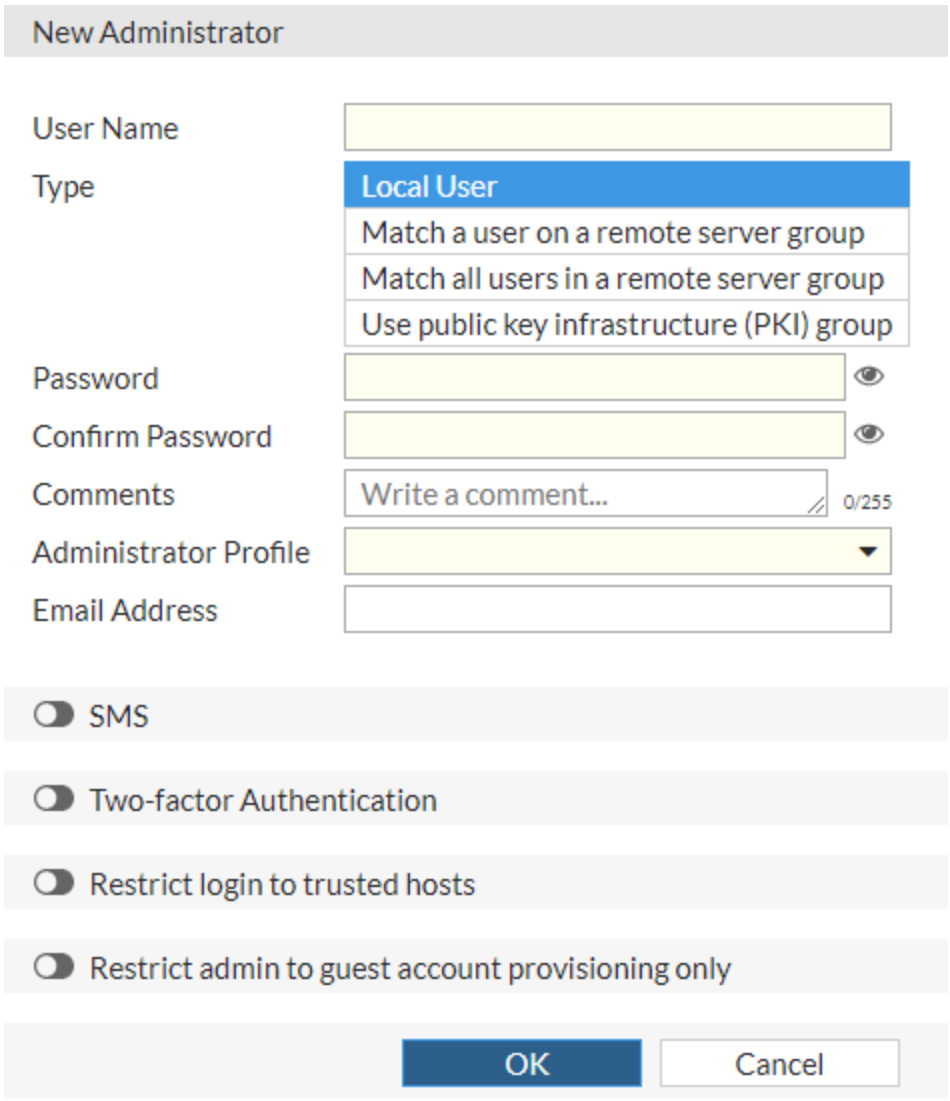
You need to use the default `admin` account, an account with the super_admin admin profile, or an administrator with read-write access control to add new administrator accounts and control their permission levels. If you log in with an administrator account that does not have the super_admin admin profile, the administrators list shows only the administrators for the current virtual domain.

The *Administrators* page lists the default super_admin administrator account, and all administrator accounts that you have created. The following options are available:

Create New	Creates a new administrator account. See Create or edit an administrator on page 866 or Create or edit a REST API administrator on page 870.
Edit	Modifies settings within an administrator's account. When you select *Edit*, the *Edit Administrator* page opens. See Create or edit an administrator on page 866 or Create or edit a REST API administrator on page 870.
Delete	Remove an administrator account. You cannot delete the original *admin* account until you create another user with the super_admin profile, log out of the *admin* account, and log in with the alternate user that has the super_admin profile. To remove multiple administrator accounts, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Name	The login name for an administrator account.
Trusted Hosts	The IP address and netmask of trusted hosts from which the administrator can log in.
Profile	The admin profile for the administrator.
Type	The type of authentication for this administrator, one of the following: • *Local*: Authentication of an account with a local password stored on the FortiProxy unit. • *Remote*: Authentication of a specific account on a RADIUS, Lightweight Directory Access Protocol (LDAP), or Terminal Access Controller Access-Control System (TACACS+) server. • *Remote+Wildcard*: Authentication of any account on an LDAP, RADIUS, or TACACS+ server. • *PKI*: PKI-based certificate authentication of an account.
Two-factor Authentication	Two-factor authentication (2FA) status. When enabled, the administrator must supply another factor in addition to the password during authentication. FortiProxy supports the following 2FA options: • FortiToken—See FortiTokens on page 844 for more information. • FortiToken Cloud—See FortiToken Cloud on page 857 for more information. • Email • SMS
Comments	A description of the administrator account.

Create or edit an administrator

Select *Create New* > *Administrator* to open the *New Administrator* page. It provides settings for configuring an administrator account. When you are configuring an administrator account, you can enable authentication for an admin from an LDAP, RADIUS, or local server.



Select an administrator and then click *Edit* to open the Edit Administrator page.

Configure the following settings in the New Administrator page or Edit Administrator page and then click *OK*:

User Name	Enter the login name for the administrator account. The name of the administrator should not contain the characters <, >, (,), #, ", or '. Using these characters in the administrator account name can result in a cross-site scripting (XSS) vulnerability.
Type	Select the type of administrator account.

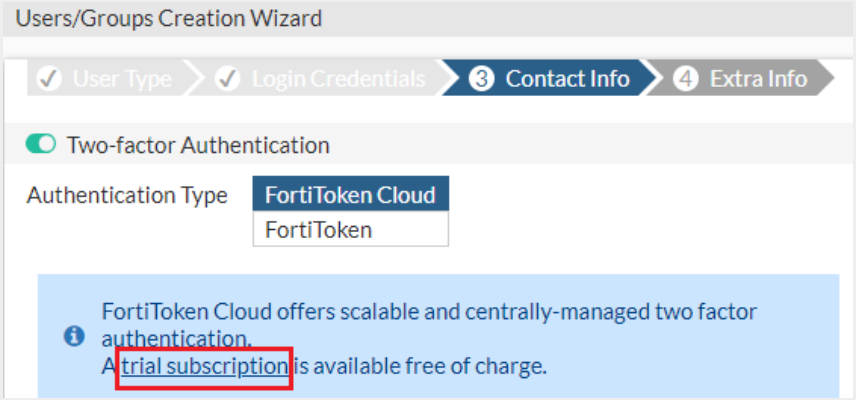
	• *Local User*—Select to create a local administrator account. • *Match a user on a remote server group*—Select to authenticate the administrator using a RADIUS, LDAP, or TACACS+ server. Server authentication for administrators must be configured first. See Creating an administrator that can be authenticated by an LDAP server on page 820. • *Match all users on a remote server group*—Select to authenticate all users using a specific RADIUS, LDAP, or TACACS+ server. Server authentication for administrators must be configured first. See .Creating an administrator that can be authenticated by an LDAP server on page 820 • *Use public key infrastructure (PKI) group*—Select to enable certificate-based authentication for the administrator. Only one administrator can be logged in with PKI authentication enabled.
Password	Enter a password for the administrator account. For improved security, the password should be at least 6 characters long. Select the eye icon to view the password. This option is only available if *Type* is *Local User*.
Confirm Password	Type the password for the administrator account a second time to confirm that you have typed it correctly. Select the eye icon to view the password. This option is not available if *Type* is *Use public key infrastructure (PKI) group*.
Backup Password	Enter a backup password for the administrator account. For improved security, the password should be at least 6 characters long. Select the eye icon to view the password. This option is only available if *Type* is *Match a user on a remote server group* or *Match all users in a remote server group*.
Comments	Optionally, enter comments about the administrator account.
Administrator Profile	Select an administrator profile to use for the new administrator. To create an administrator profile, see Create or edit an administrator profile on page 874.
Force Password Change	Specifies whether to force the administrator to change the password during the next login.
Email Address	If email is used for two-factor authentication, provide the email address at which the user will receive token password codes.
Two-factor Authentication	Specifies whether to enable two-factor authentication (2FA) for the administrator, which requires the administrator to supply another factor in addition to the password during authentication.

Before enabling 2FA, it is recommended that you create second administrator account that is configured to guarantee administrator access to the FortiProxy if you are unable to authenticate on the main account for any reason.

FortiProxy supports the following 2FA options:

- **FortiToken**—You can use hard tokens or mobile tokens.
  - Hard tokens must be registered and activated first before they appear in the dropdown list. See Registering and activating a hard token on page 846.
  - FortiProxy provides two trial mobile tokens ready for use from the dropdown list. You cannot add or import any other mobile tokens.
- **FortiToken Cloud on page 857**—A Fortinet Identity and Access Management as a Service (IDaaS) cloud service that enables FortiProxy and FortiAuthenticator customers to add 2FA for their users using Mobile or hard tokens.

  You can activate a free one-month FortiToken Cloud trial subscription for registered FortiCare accounts using the following GUI option or the `execute fortitoken-cloud trial` command in the CLI.



  To verify the activation status, run `exe fortitoken-cloud show`. To view the user list, run `diagnose fortitoken-cloud show users`.

  The FortiToken Cloud free trial can only be activated once. The option will not be available if another FortiToken Cloud trial subscription has been activated on the FortiProxy or with the registered FortiCare accounts.

- **Email**—Enter an email address to send a 2FA code to that address.
- **SMS**—Select the *Country Dial Code* and enter the *Phone Number* (`sms-phone` in the CLI) to send a 2FA code to. SMS messages can

	also be sent to the FortiGuard SMS server or a custom server.
Remote User Group	Select the administrator user group that includes the remote server/PKI (peer) users as members of the *Remote User Group*. The administrator user group cannot be deleted after the group is selected for authentication. This option is only available if *Type* is *Match a user on a remote server group* or *Match all users in a remote server group*.
PKI Group	Select to allow all accounts on the RADIUS, LDAP, or TACACS+ server to be administrators. This option is only available if *Type* is *Use public key infrastructure (PKI) group*.
Restrict login to trusted hosts	Enable to restrict this administrator login to specific trusted hosts and then enter the IPv4 or IPv6 addresses and netmasks of the trusted hosts. You can specify up to 10 trusted hosts and 10 IPv6 trusted hosts.
Restrict admin to guest account provisioning only	Enable to create a guest management administrator exclusively for guest user management without requiring full administrative access to FortiProxy. You can then select the guest group for the administrator (see User Groups on page 807).

Regular (password) authentication for administrators

You can use a password stored on the local unit to authenticate an administrator. When you select *Local User* for *Type*, you will see *Local* as the entry in the *Type* column when you view the list of administrators.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator can connect only through the subnet or subnets that you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

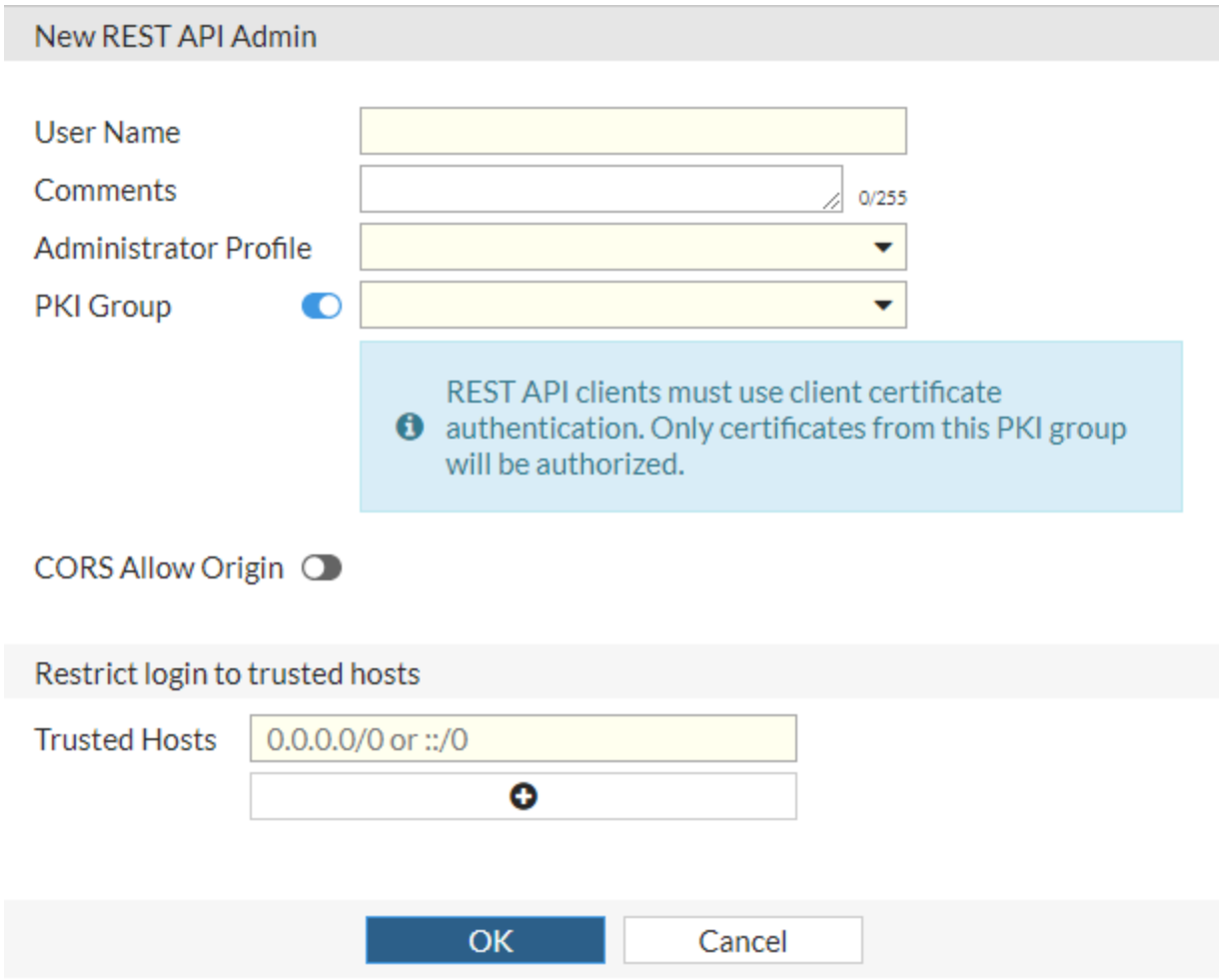
When you set trusted hosts for all administrators, the unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply to the GUI, Ping, SNMP, and the CLI when accessed through Telnet or SSH. CLI access through the console port is not affected.

The trusted host addresses all default to 0.0.0.0/0.0.0.0. If you set one of the zero addresses to a nonzero address, the other zero addresses will be ignored. The only way to use a wildcard entry is to leave the trusted hosts at 0.0.0.0/0.0.0.0. However, this configuration is less secure.

Create or edit a REST API administrator

Select *Create New* > *REST API Admin* to open the *New REST API Admin* page. It provides settings for configuring a REST API administrator account.



Select a REST API administrator and then click *Edit* to open the Edit REST API Admin page.

Configure the following settings in the New REST API Admin page or Edit REST API Admin page and then click *OK*:

User Name	Enter the login name for the administrator account. The name of the administrator should not contain the characters <, >, (,), #, ", or '. Using these characters in the administrator account name can result in a cross-site scripting (XSS) vulnerability.
Comments	Optionally, enter comments about the administrator account.
Administrator Profile	Select an administrator profile to use for the new administrator. To create an administrator profile, see Create or edit an administrator profile on page 874.

PKI Group	Enable this option for REST API clients and then select which PKI group to accept.
CORS Allow Origin	Enable this option for cross-origin resource sharing (CORS) and then specify the URL that can access the REST API.
Trusted Hosts	Enter the trusted hosts allowed to log in to the REST API.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator can connect only through the subnet or subnets that you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply to the GUI, Ping, SNMP, and the CLI when accessed through Telnet or SSH. CLI access through the console port is not affected.

The trusted host addresses all default to 0.0.0.0/0.0.0.0. If you set one of the zero addresses to a nonzero address, the other zero addresses will be ignored. The only way to use a wildcard entry is to leave the trusted hosts at 0.0.0.0/0.0.0.0. However, this configuration is less secure.

Separating the SSHD host key from the administration server certificate

Separating the SSHD host key from the administration server certificate addresses the issue where the administration server key tends to overwrite one of the key files, which can lead to complications. This resolves the problem where the SSH module regenerates the host key files after a factory reset. This action previously prompted a warning message when an older SSH client attempted to log in to the FortiProxy using SSH.

```
config system ssh-config
    set ssh-hostkey-override {enable | disable}
    set ssh-hostkey-password <password>
    set ssh-hostkey <encrypted_private_key>
end
```

The `ssh-hostkey-algo` option under `config system global` supports ECDSA 384 and ECDSA 256, allowing the SSHD to accommodate the most commonly used host key algorithms.

To configure SSH host key override in SSHD:

1. Using the ssh-keygen tool, generate the host key (ecdsa-sha2-nistp384 is used in this example).
2. Configure the SSH host key override settings:

```
config system ssh-config
    set ssh-hostkey-override enable
    set ssh-hostkey-algo ecdsa-sha2-nistp384
    set ssh-hostkey-password **********
    set ssh-hostkey <encrypted_private_key>
end
```

3. On a PC, attempt to log in to the FortiProxy with the defined ecdsa-sha2-nistp384 algorithm:

```
root@PC05:~# ssh admin@172.16.200.1
The authenticity of host '172.16.200.1 (172.16.200.1)' can't be established.
ECDSA key fingerprint is SHA256:mcrMXSjtN/YjY3zQgZpxk77ezxPVGGGOL/GUOG8Oijs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.200.1' (ECDSA) to the list of known hosts.
```

4. Verify the server host key algorithms:

```
root@PC05:~# nmap -sV --script ssh2-enum-algos 172.16.200.1
Starting Nmap 7.01 ( https://nmap.org ) at 2023-11-07 15:47 PST
Nmap scan report for FPX_A (172.16.200.1)
Host is up (0.00013s latency).
Not shown: 995 filtered ports
PORT    STATE  SERVICE      VERSION
22/tcp  open   ssh          (protocol 2.0)
| ssh2-enum-algos:
|   kex_algorithms: (8)
|       diffie-hellman-group14-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group-exchange-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|   server_host_key_algorithms: (1)
|       ecdsa-sha2-nistp384
|   encryption_algorithms: (3)
```

Admin Profiles

Each administrator account belongs to an admin profile. The admin profile separates FortiProxy features into access control categories for which an administrator with read-write access can enable none (deny), read-only, or read-write access.

Read-only access for a GUI page enables the administrator to view that page. However, the administrator needs write access to change the settings on the page.

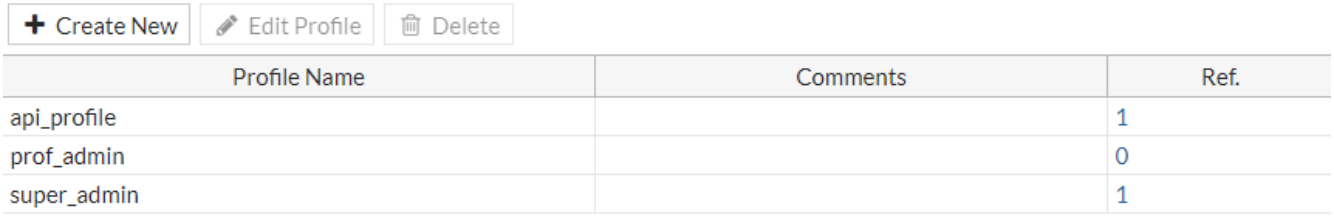
The admin profile has a similar effect on administrator access to CLI commands. You can access `get` and `show` commands with *Read Only* access, but access to `config` commands requires *Read-Write* access.

When an administrator has read-only access to a feature, the administrator can access the GUI page for that feature but cannot make changes to the configuration. There are no *Create* or *Apply* buttons, and lists display only the *View* icon instead of icons for *Edit*, *Delete*, or other modification commands.

You need to use the admin account or an account with read-write access to create or edit admin profiles.

The *Admin Profile* page lists all administration profiles that you created as well as the default admin profiles. On this page, you can edit, delete, or create an admin profile.

To view administrator profiles, go to *System* > *Admin Profiles*.



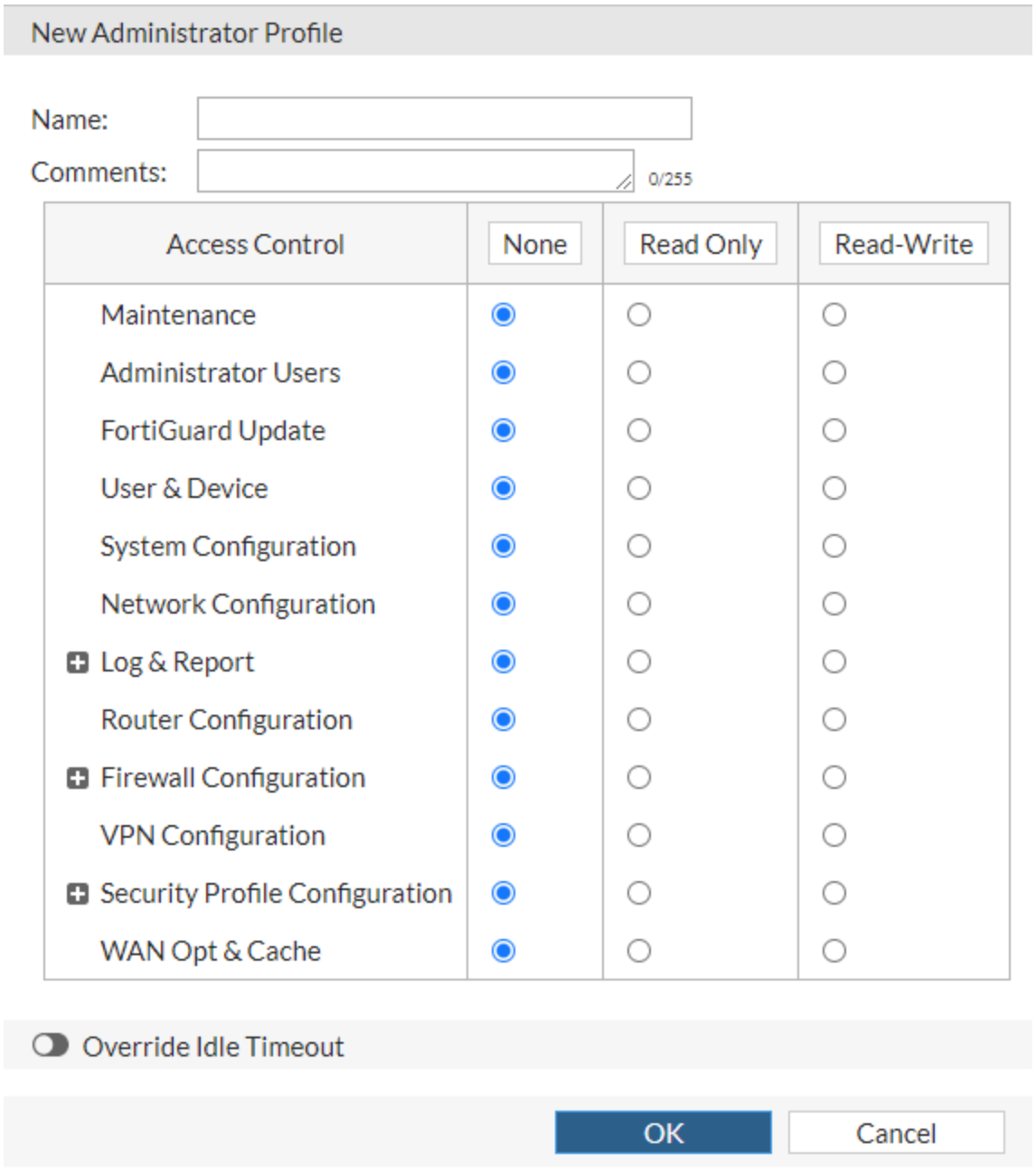
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Creates an administrator profile. See Create or edit an administrator profile on page 874.
Edit Profile	Modifies the selected administrator profile. When you click *Edit Profile*, the Edit Administrator Profile page opens. See Create or edit an administrator profile on page 874. **NOTE:** You cannot edit the super_admin profile.
Delete	Removes the admin profile from the list on the page. You cannot delete an admin profile that has administrators assigned to it. To remove multiple admin profiles, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Profile Name	The name of the admin profile.
Comments	Comments about the admin profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an administrator profile

Select *Create New* to open the *New Administrator Profile* page. It provides settings for configuring an administrator profile.



Select an administrator profile and then click *Edit Profile* to open the *Edit Administrator Profile* page.

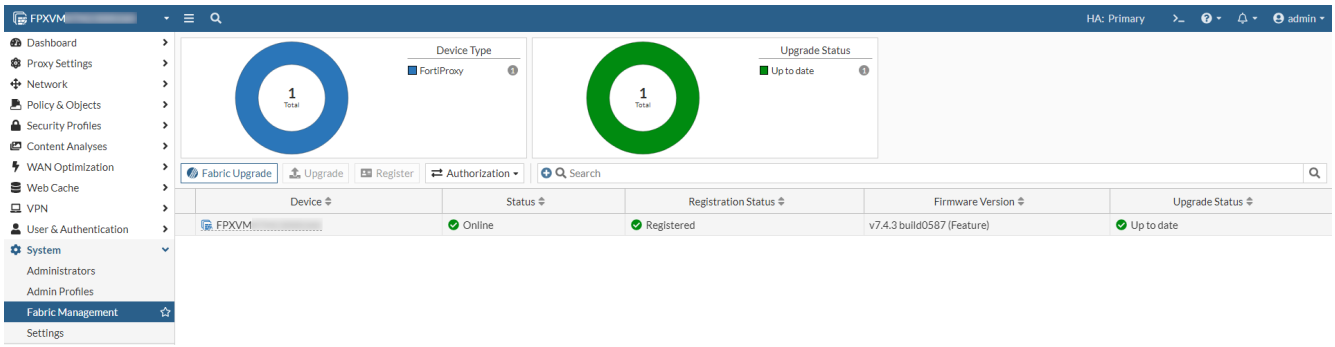
Configure the following settings in the New Administrator Profile page or Edit Administrator Profile page and then click *OK*.

NOTE: You cannot edit the super_admin profile.

Name	Enter a name for the new administrator profile. After an administrator profile is created, you cannot change the name.
Comments	Optionally, add comments about the administrator profile.
Access Control	List of the items that can customize access control settings if configured.
None	Deny access for the *Access Control* category.
Read Only	Enable read-only access for the *Access Control* category.
Read-Write	Allow read-write access for the *Access Control* category.
Access Control (categories)	Make specific access control selections as required. • Maintenance • Administrator Users • FortiGuard Update • User & Device • System Configuration • Network Configuration • Log & Report • Router Configuration • Firewall Configuration • VPN Configuration • Security Profile Configuration • WAN Opt & Cache
Override Idle Timeout	Enable to change how many minutes the FortiProxy unit is idle before the session closes.
Timeout	Select *Idle Countdown* to specify the number of minutes that the system is idle before the session closes. Select *Never Timeout* to prevent the FortiProxy unit from closing idle sessions.
Idle	Enter the number of minutes that the FortiProxy unit is idle before the session closes. The default is 10 minutes.

Fabric Management

The *Fabric Management* page allows administrators to manage the firmware running on each FortiProxy in the Security Fabric, and to authorize and register these Fabric devices.



The *Fabric Management* page displays a summary of devices in the Security Fabric that includes:

- Total number of devices in the Fortinet Security Fabric and the types of devices
- Upgrade status
- Device name
- Device status
- Registration status
- Firmware version and maturity level
- Upgrade status

Please note a valid *Firmware & General Updates* (FMWR) license is a prerequisite for upgrading to a major or minor firmware release in FortiProxy.

From the *Fabric Management* page, administrators can perform the following actions:

Fabric Upgrade	Use to upgrade firmware for the root FortiProxy as well as all Fabric devices. You can also use this option to upgrade firmware for a non-Security Fabric FortiProxy. The *Fabric Upgrade* option uses released firmware images from FortiGuard.
Upgrade	Use to upgrade firmware for the selected device. The *Upgrade* option uses released firmware images from FortiGuard. Alternately you can download a firmware file from the Fortinet Customer Service & Support website, and upload it for the upgrade process. See Upgrading individual device firmware on page 877.
Register	Use the *Register* option to register a selected device to FortiCare.
Authorization	Use the *Authorization* option to authorize, deauthorize, or reject the selected device. See Authorizing devices on page 878.

Before you upgrade FortiProxy firmware, it is recommended to learn about firmware updates, firmware maturity levels, Special Technical Support (STS) firmware, and selected availability (SA) versions.

Upgrading individual device firmware

You can upgrade you FortiProxy version by uploading a new firmware image from your computer:

1. Download the target firmware from the Fortinet support site. See Downloading a firmware image on page 878
2. Go to *System > Fabric Management*.
3. Select a device and click *Upgrade*.
4. In the *File Upload* tab, click *Browse*.
5. Select the file on your PC and click *Open*.
6. Click *Confirm and Backup Config*.
   If you are upgrading from a mature to a feature firmware version, the *Confirm* pane opens with a warning message.
7. Review the warning, and click *Confirm* to continue. A warning message is displayed.
8. Click *Continue* to initiate the upgrade.
   The FortiProxy unit backs up the current configuration to the management computer, uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

To upgrade individual device firmware in the CLI:

1. Make sure that the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log in to the CLI.
4. Ping the TFTP server to ensure that the FortiProxy can connect to it:
   ```
   execute ping <tftp_ipv4>
   ```
5. Enter the following command to copy the firmware image from the TFTP server to the FortiProxy unit:
   ```
   execute restore image tftp <filename> <tftp_ipv4>
   ```
   The FortiProxy unit responds with the message:
   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```
6. Type y. The FortiProxy unit uploads the firmware image file, verifies the signature of the firmware image, and determines the firmware maturity level.
   When you are upgrading to a feature firmware image, you are asked to confirm whether to continue with the upgrade.
   When you proceed with the upgrade, the upgrade image is installed and FortiProxy restarts. This process takes a few minutes.

```
Please wait...
Connect to tftp server 172.16.200.55 ...
#################################################################################
Get image from tftp server OK.
Verifying the signature of the firmware image.

Warning: Upgrading to an image with Feature maturity notation.
```

```
Image file uploaded is marked as a Feature image, are you sure you want to upgrade?
Do you want to continue? (y/n)y
Please confirm again. Are you sure you want to upgrade using uploaded file?
Do you want to continue? (y/n)y
Checking new firmware integrity ... pass
Please wait for system to restart.
Firmware upgrade in progress ...
Done.
The system is going down NOW !!
```

7. Reconnect to the CLI.
8. Update the antivirus and attack definitions:
   ```
   execute update-now
   ```

To upgrade all FortiProxies in an HA cluster, see Upgrading FortiProxies in an HA cluster on page 922.

Authorizing devices

If there are any notifications in the top banner dropdown for unauthorized devices or devices that require authorization, clicking the notification redirects the user to the *System > Fabric Management* page.

On the *Fabric Management* page, the unauthorized devices are grayed out, and their status is *Unauthorized*.

To authorize a Security Fabric device from the Firmware & Registration page:

1. Go to *System > Fabric Management*, and select an unauthorized device.
2. Click *Authorization > Authorize* (below the donut charts), or right-click and select *Authorization > Authorize*.

   A notification appears when the device is authorized.
3. Refresh the page. The device's status should now be *Online*.

To deauthorize a Security Fabric device from the Firmware & Registration page:

1. Go to the *System > Fabric Management* page, and select a device.
2. Click *Authorization > Deauthorize*.
3. Refresh the page to see that the device has been deauthorized.

Downloading a firmware image

Firmware images for all FortiProxy units are available on the Fortinet Customer Service & Support website.

To download firmware:

1. Log into the support site with your user name and password.
2. Go to *Support* > *Firmware Download*.
   A list of Release Notes is shown. If you have not already done so, download and review the Release Notes for the firmware version that you are upgrading your FortiProxy unit to.
3. In the *Select Product* dropdown menu, select *FortiProxy*.
4. On the *Download* tab, navigate to the FortiProxy firmware file for your FortiProxy model or VM platform in the *Image Folders/Files* section. `.out` files are for upgrade or downgrade. `.zip` and `.gz` files are for new deployments.
5. Click *HTTPS* to download the firmware that meets your needs.



Firmware can also be downloaded using FTP, but as FTP is not an encrypted file transferring protocol, HTTPS downloading is recommended.

After you download the firmware, continue with Upgrading individual device firmware on page 877.

Settings

Use the system settings to configure general settings for administration access, password policies, system time settings, and display settings.

Go to *System* > *Settings* to configure system settings.

Configure the following settings and then select *Apply*:

System Settings	
Host name	The host name of the FortiProxy unit. The only administrators that can change a host name are administrators whose admin profiles permit system configuration write access. If the FortiProxy unit is part of an HA cluster, you should use a unique host name to distinguish the FortiProxy unit from others in the cluster.
System Time	
Time Zone	Select the time zone of your FortiProxy unit.
Set Time	Select either *NTP*, *PTP*, or *Manual settings*. • *NTP*: To use an NTP server other than FortiGuard, the CLI must be used. In the *Sync interval* field, enter how often, in minutes, that the device synchronizes its time with the NTP server. • *PTP*: • Set the *Mode* to *Multicast* or *Hybrid*.

	• Select the *Delay mechanism*: *E2E* or *P2P*. • Set the *Request interval*, in seconds. • Select the *Interface*. • *Manual settings*: Manually enter the *Date*, and *Time*.
Setup device as local NTP server	Enable to configure the FortiProxy as a local NTP server. This option is not available if *Set Time* is *PTP*. In the *Listen on Interfaces* field, set the interface or interfaces that the FortiProxy will listen for NTP requests on.
Administration Settings	
HTTP port	Enter the TCP port to be used for administrative HTTP access. The default is 80.
Redirect to HTTPS	Enable *Redirect to HTTPS* to force redirection from HTTP to HTTPS.
HTTPS port	Enter the TCP port to be used for administrative HTTPS access. The default is 443.
HTTPS server certificate	Select *Fortinet_Factory* or search for a certificate.
SSH port	Enter the TCP port to be used for administrative SSH access. The default is 22.
Telnet port	Enter the TCP port to be used for administrative Telnet access. The default is 23.
Idle timeout	Change the time after which the GUI logs out idle system administration settings, from 1 to 480 minutes.
ACME interface	Select the interface that the ACME client will listen to for challenges to provision and renew certificates.
Allow concurrent sessions	Concurrent administrator sessions occur when multiple people concurrently access the FortiProxy unit using the same administrator account. This behavior is allowed by default.
Password Policy	
Password Scope	Select *Admin*, *IPsec*, or *Both* to change the policy for the administrator password. Select *Off* to apply no policy for the administrator password
Minimum Length	If you select *Admin*, *IPsec*, or *Both*, set the minimum acceptable length for passwords, from 8 to 128 characters.
Character requirements	If you select *Admin*, *IPsec*, or *Both*, select to enable special character types, upper or lower case letters, or numbers. Enter information for one or all of the following. Each selected type must occur at least once in the password. • *Upper case*—A, B, C, ... Z • *Lower case*—a, b, c, ... z

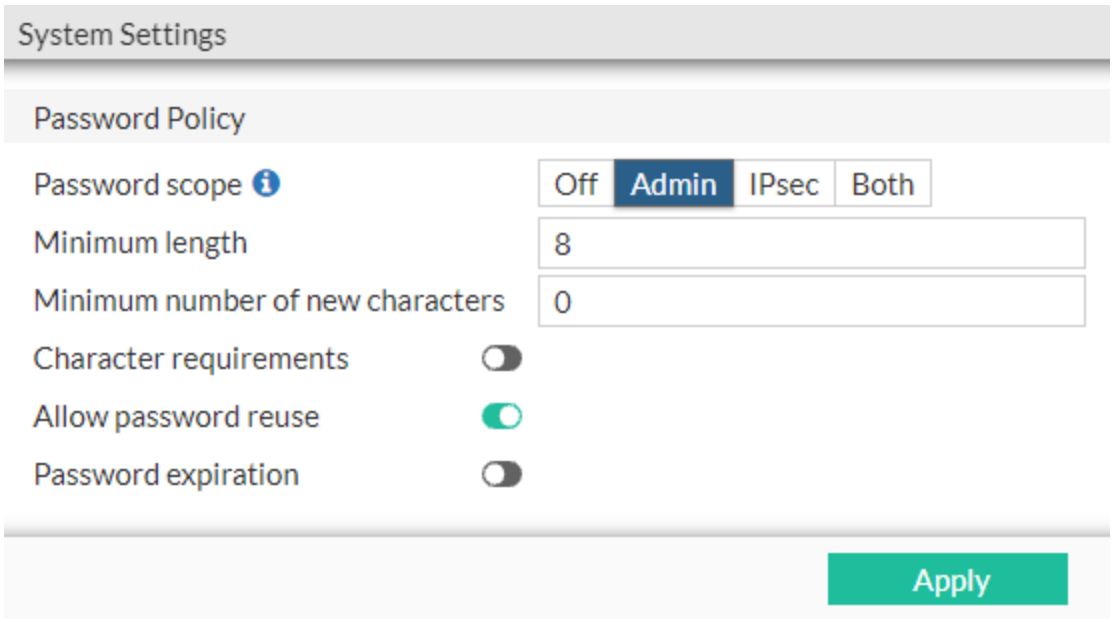
	• *Numbers (0-9)*—0, 1, 2, ... 9 • *Special*—@, ?, #, ... %
Allow password reuse	If you select *Admin*, you can select this option to allow passwords to be reused.
Password expiration	If you select *Admin*, *IPsec*, or *Both*, you can require administrators to change the password after a specified number of days. Enter the number of days in the field. The default is 90 days.
View Settings	
Language	The language the GUI uses: *English*, *French*, *Spanish*, *Portuguese*, *Japanese*, *Traditional Chinese*, *Simplified Chinese*, or *Korean*. You should select the language that the operating system of the management computer uses.
Date/Time display	Display the time in either the *FortiProxy timezone* or the *Browser timezone*.
System Operation Settings	
Virtual Domains	Enable or disable VDOMs.

Defining the password policy with a minimum character change

Administrators can set a minimum number of unique characters in the new password that do not exist in the old password. This setting overrides the password reuse option if both are enabled.

To configure the password policy in the GUI:

1. Go to *System* > *Settings* and navigate to the *Password Policy* section.
2. For *Password scope*, select *Admin*.
3. Enter a value for *Minimum number of new characters*.



4. Click *Apply*.

To configure the password policy in the CLI:

```
config system password-policy
    set status enable
    set min-change-characters <0-128>
end
```

Using the default certificate for HTTPS administrative access

By default, the FortiProxy uses the certificate named Fortinet_GUI_Server for HTTPS administrative access. This certificate is generated and signed by the built-in Fortinet_CA_SSL certificate, which dynamically updates the SAN field of the Fortinet_GUI_Server certificate with the IP addresses of all interfaces enabled for HTTPS. After installing the Fortinet_CA_SSL CA certificate on a PC, administrators can access the FortiProxy GUI through a browser without any warnings.

How the certificate works

The Fortinet_GUI_Server certificate is generated by the built-in certificate authority (CA) with the Fortinet_CA_SSL certificate, which is unique to each FortiProxy. This CA certificate is also used in SSL deep inspection. When the Fortinet_GUI_Server certificate is generated, the SAN (Subject Alternative Name) extension field is populated with the IP addresses of all physical and logical (VLAN, loopback, and so on) interfaces enabled for HTTPS. It is also populated with the management IP address whenever this field is an IP address and not an FQDN. If there are any changes to the IP addresses on the interface or management IP, the Fortinet_GUI_Server certificate is updated and regenerated with

the new IP. If the Fortinet_CA_SSL certificate itself is updated, the Fortinet_GUI_Server certificate is regenerated.

Because the root CA is not a public CA, the Fortinet_CA_SSL CA certificate must be installed in the trusted certificate store on the client PC in order for the trusted certificate chain to be recognized by a browser. This certificate can be downloaded from the FortiProxy in several ways.



The Fortinet_GUI_Server certificate can only be used for HTTPS administrative access. It cannot be used anywhere else.

Example

The HTTPS server certificate can be configured in the GUI or CLI.

To configure the HTTPS server certificate in the GUI:

1. On an administrative PC, log in to the FortiProxy GUI and go to *System > Settings*.
2. In the *Administration Settings* section, set the *HTTPS server certificate* to *Fortinet_GUI_Server*.
3. Download the Fortinet_CA_SSL certificate using one of the following methods:
   - On the *System > Settings* page, click *Download HTTPS CA certificate* (below the *HTTPS server certificate* option).
   - Go to *System > Certificates*. In the *Local CA Certificate* section, select *Fortinet_CA_SSL*, and click *Download*.
   - Go to *Dashboard > Status*. In the *Administrator* widget, click *Download HTTPS CA certificate*.
4. Install the certificate in the PC's trusted certificate store. Refer to your OS documentation if needed.
5. Reload the FortiProxy GUI. The browser now trusts the certificate and does not display a certificate warning.
6. If you are connecting to the FortiProxy over DNAT or port forwarding, the certificate needs to add the NATed management IP into the SAN field so that the browser does not display a warning about an invalid CN. Configure the management IP in the global settings:

```
config system global
    set management-ip <IP_address>
end
```

To configure the HTTPS server certificate in the CLI:

1. Configure the HTTPS server certificate:

```
config system global
    set admin-server-cert Fortinet_GUI_Server
end
```

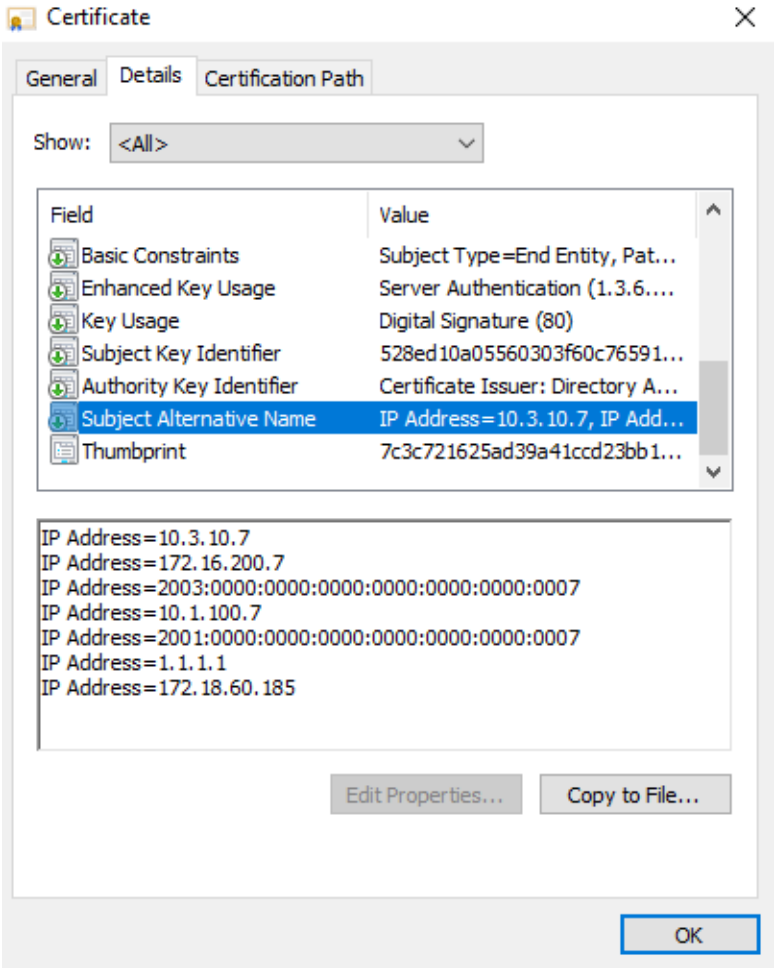
2. Download the Fortinet_CA_SSL certificate on the administrative PC through TFTP:

```
# execute vpn certificate local export tftp Fortinet_CA_SSL cer <file_name> <server_IP>

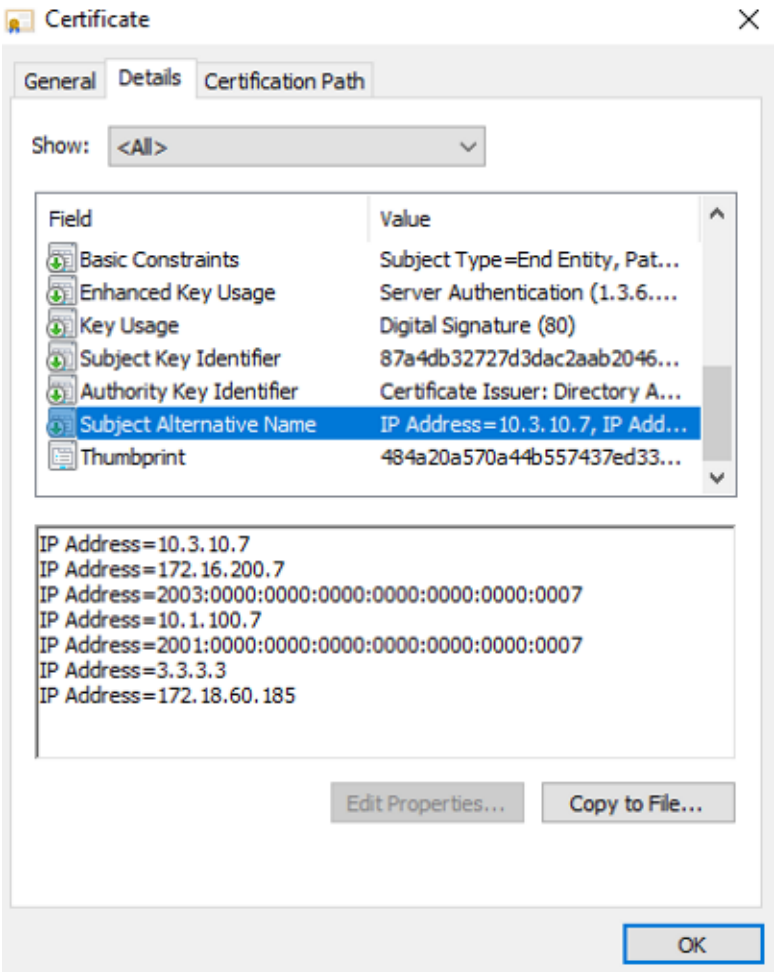
Done.
```

To verify the connection:

1. Access the FortiProxy from a browser and verify the certificate information. For example, in Chrome:
   a. In the left side of the address bar, click the icon to view the site information.
   b. Click *Certificate*.
   c. Click the *Details* tab.
   d. Locate the *Subject Alternative Name* (SAN) field, and note the IP addresses that are listed (*1.1.1.1*).



   e. Click *OK*.
2. In FortiProxy, change one of the interface addresses. In this example, the port11 address is changed from 1.1.1.1 to 3.3.3.3.
3. Reload the browser and review the certificate information again. The IP 1.1.1.1 in the SAN field is updated to *3.3.3.3*.



4. In FortiProxy, go to *System > Certificates* and double-click *Fortinet_GUI_Server* to view the *Certificate Details*.
5. At the bottom of the pane, the *X509v3 Subject Alternative Name* field displays the IP addresses from the certificate.
6. Verify the logs when the certificate is regenerated:

```
# execute log filter category 1
# execute log display
12 logs found.
10 logs returned.
```

```
1: date=2022-06-23 time=09:11:44 eventtime=1656000704674434910 tz="-0700" logid="0100022205"
type="event" subtype="system" level="information" vd="root" logdesc="Certificate succeed to
auto-generate" user="system" action="certificate-generate" status="successful" name="Fortinet_
GUI_Server" msg="Successfully generated GUI management cert"
```

```
2: date=2022-06-23 time=09:11:44 eventtime=1656000704674432668 tz="-0700" logid="0101041986"
type="event" subtype="vpn" level="information" vd="root" logdesc="Certificate regenerated"
action="info" user="N/A" ui="forticron" name="Fortinet_GUI_Server" msg="A certificate is
regenerated" cert-type="Local" status="success"
```

```
3: date=2022-06-23 time=09:11:31 eventtime=1656000691825397831 tz="-0700" logid="0100044547"
type="event" subtype="system" level="information" vd="root" logdesc="Object attribute
configured" user="admin" ui="ssh(172.16.200.254)" action="Edit" cfgtid=35782662
cfgpath="system.interface" cfgobj="port11" cfgattr="ip[1.1.1.1 255.255.255.0->3.3.3.3
255.255.255.0]" msg="Edit system.interface port11"
```

TLS configuration

The minimum TLS version that is used for local out connections from the FortiProxy can be configured in the CLI:

```
config system global
    set ssl-min-proto-version {SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2 | TLSv1-3}
end
```

By default, the minimum version is TLSv1.2. The FortiProxy will try to negotiate a connection using the configured version or higher. If the server that FortiProxy is connecting to does not support the version, then the connection will not be made. Some FortiCloud and FortiGuard services do not support TLSv1.3.

Minimum SSL/TLS versions can also be configured individually for the following settings, not all of which support TLSv1.3:

Setting	CLI	TLSv1.3 Support
Email server	`config system email-server`	No
Certificate	`config vpn certificate setting`	No
FortiSandbox	`config system fortisandbox`	No
FortiGuard	`config log fortiguard setting`	No
FortiAnalyzer	`config log fortianalyzer setting`	Yes
Syslog	`config log syslogd setting`	No
User Authentication	`config user setting`	Yes
LDAP server	`config user ldap`	Yes
POP3 server	`config user pop3`	No
Exchange server	`config user exchange`	No

Trusted platform module support

On supported FortiProxy hardware devices, the Trusted Platform Module (TPM) can be used to protect your password and key against malicious software and phishing attacks. The dedicated module hardens the FortiProxy by generating, storing, and authenticating cryptographic keys. To help prevent

tampering, the chip is soldered on the motherboard to reduce the risk of data transaction interceptions from attackers.

By default, the TPM is disabled. To enable it, you must set the 32 hexadecimal digit master-encryption-password which encrypts sensitive data on the FortiProxy using AES128-CBC. With the password, TPM generates a 2048-bit primary key to secure the master-encryption-password through RSA-2048 encryption. The master-encryption-password protects the data. The primary key protects the master-encryption-password.



The TPM module does not encrypt the disk drive of eligible FortiProxy units.

The primary key binds the encrypted configuration file to a specific FortiProxy unit and never leaves the TPM. When backing up the configuration, the TPM uses the primary key to encrypt the master-encryption-password in the configuration file. When restoring a configuration that includes a TPM protected master-encryption-password:

- If TPM is disabled, then the configuration cannot be restored.
- If TPM is enabled but has a different master-encryption-password than the configuration file, then the configuration cannot be restored.
- If TPM is enabled and the master-encryption-password is the same in the configuration file, then the configuration can be restored.

For information on backing up and restoring the configuration, see Automatic backup to an FTP or TFTP server on page 1170.

Passwords and keys that can be encrypted by the master-encryption-key include:

- Admin password
- Alert email user's password
- BGP and other routing related configurations
- External resource
- FortiGuard proxy password
- FortiToken/FortiToken Mobile’s seed
- HA password
- IPsec pre-shared key
- Link Monitor, server side password
- Local certificate's private key
- Local, LDAP. RADIUS, FSSO, and other user category related passwords
- Modem/PPPoE
- NST password
- NTP Password
- SDN connector, server side password
- SNMP
- Wireless Security related password



In HA configurations, each cluster member must use the same master-encryption-key so that the HA cluster can form and its members can synchronize their configurations.

To check if your FortiProxy device has a TPM:

Verify all the following commands exist. Otherwise, the platform does not support it.

```
# diagnose hardware test info
List of test cases:
    bios: sysid
    bios: checksum
    bios: license
    bios: detect

# diagnose hardware deviceinfo tpm
TPM capability information of fixed properties:
============================================================
TPM_PT_FAMILY_INDICATOR: 2.0
TPM_PT_LEVEL: 0
TPM_PT_REVISION: 138
TPM_PT_DAY_OF_YEAR: 8
TPM_PT_YEAR: 2018
TPM_PT_MANUFACTURER: NTC
# diagnose hardware test tpm
========== Fortinet Hardware Test Report ==================
TPM
TPM Device Detection..................................... PASS
================ Fortinet Hardware Test PASSED ==============
# diagnose tpm
get-property Get TPM properties. [Take 0-1 arg(s)]
get-var-property Get TPM var properties.
read-clock Read TPM internal clock.
shutdown-prepare Prepare for TPM power cycle.
selftest Perform self tests.
generate-random-number Generate a 4-byte random number
SHA-1 HASH a sequence of num with SHA-1 algo
SHA-256 HASH a sequence of num with SHA-256 algo
```

To enable TPM and input the master-encryption-password:

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
********************************
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
********************************
Your private data encryption key is accepted.
```

VDOM

Virtual Domains (VDOMs) are used to divide a single FortiProxy into two or more virtual units that function independently. VDOMs can provide separate firewall policies and security profiles. In NAT mode, they provide separate routing configurations. When multi VDOM mode is enabled, the default VDOM is the *root* VDOM, and it cannot be deleted.

Multiple VDOMs allow users to combine NAT and transparent mode on a single FortiProxy; VDOMs can be independently configured to operate in NAT or transparent mode. In transparent mode, it is recommended to configure a dedicated management interface when out-of-band management is required. See Transparent mode management on page 898.

By default, most FortiProxy units support 5 VDOMs.

Global settings are configured outside of a VDOM. They effect the entire FortiProxy, and include settings such as interfaces, firmware, HA, and so on. Global settings should only be changed by top level administrators. Both VDOM specific and global security profiles can be created. Global security profiles are configured in the global VDOM, and can be used by any VDOM and have *g-* appended to their names to differentiate them from VDOM specific profiles.

Administrative users can be configured to have global access, or access to specific VDOMs. See Administrators on page 864 for more information about administrators.

Global administrators have complete visibility and access because the scope of their role is to manage the entire physical FortiProxy device. To create a global administrator that has access to all VDOMs and access to global settings, it must be created at the global level and must use the *super_admin* administrator profile. See Create Global VDOM administrators on page 891 for configuration details.

Per-VDOM administrators are unable to view global settings or VDOMs that are not assigned to them because the scope of their role is restricted to managing specific VDOMs only. They can only access the FortiProxy through interfaces that are assigned to the VDOM that they are assigned to. The interface must also be configured to allow management access. They can also connect to the FortiProxy using the console port. See Create per-VDOM administrators on page 892 for configuration details.

Configuration

VDOMs can be configured in the GUI and the CLI.

The following topics provide information on general VDOM configurations:

- Enable multi VDOM mode on page 890
- Disable multi VDOM mode on page 890
- Create VDOMs on page 891
- Delete VDOMs on page 891
- Create Global VDOM administrators on page 891
- Create per-VDOM administrators on page 892
- Assign interfaces to a VDOM on page 893

- Global and per-VDOM resources on page 894
- Inter-VDOM routing on page 896
- Configure global security profiles on page 897

To ensure that no VDOMs are accidentally configured in the CLI, prompts can be enabled. These prompts will display to ask for confirmation that the VDOM is meant to be configured in the CLI.

To configure confirmation prompts:

```
config system global
    set edit-vdom-prompt enable
end
```

Enable multi VDOM mode

To enable VDOMs in the GUI:

1. Go to *System* > *Settings*.
2. In the *System Operation Settings* sections, enable *Virtual Domains*.
3. Click *OK*.
   You will be logged out of the device when VDOM mode is enabled.

To enable VDOMs in the CLI:

```
config system global
    set vdom-mode multi-vdom
end
```

You will be logged out of the device when VDOM mode is enabled.

Disable multi VDOM mode

All non-root VDOMs must be deleted before multi VDOM mode can be disabled.

To disable VDOMs in the GUI:

1. In the Global VDOM, go to *System* > *Settings*.
2. Disable *Virtual Domains*.
3. Click *Apply*.

To disable VDOMs in the CLI:

```
config global
    config system global
        set vdom-mode no-vdom
```

```
    end
end
```

Create VDOMs

To create VDOMs in the GUI:

1. In the Global VDOM, go to *System* > *VDOM*.
2. Click *Create New*.
3. In the *Virtual Domain* field, enter a name for the VDOM.
4. Optionally, enter a comment describing the VDOM.
5. Click *OK*.

To create VDOMs in the CLI:

```
config global
    config vdom
        edit <vdom_a>
        next
        edit <vdom_b>
        next
    end
end
```

Delete VDOMs

The root VDOM and VDOMs that are referenced in the current configuration cannot be deleted.

To delete a VDOM in the GUI:

1. In the Global VDOM, go to *System* > *VDOM*.
2. Select the VDOM that you need delete.
3. Click *Delete*.
4. Click *OK*.

To delete a VDOM in the CLI:

```
config vdom
    delete <vdom>
end
```

Create Global VDOM administrators

Global administrators have complete visibility and access because the scope of their role is to manage the entire physical FortiProxy device. When global administrators log into the GUI, from the

VDOM: Global view they will see all pages for global settings shared between VDOMs, and VDOM-specific settings.

To create a global administrator that has access to all VDOMs and access to global settings, it must be created at the global level and must use the *super_admin* administrator profile.

To create a Global VDOM administrator in the GUI:

1. In the Global VDOM, go to *System* > *Administrators* and click *Create New* > *Administrator*.
2. Fill in the required information, setting the *Type* as *Local User*.
3. Set Administrator profile to *super_admin* or *super_admin_readonly*.
4. Click *OK*.

To create a Global VDOM administrator using the CLI:

```
config global
    config system admin
        edit <name>
            set accprofile "super_admin"
        next
    end
end
```

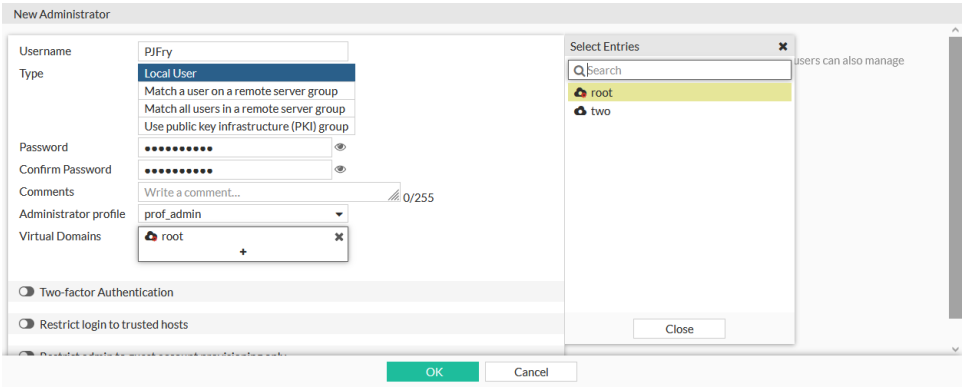
Create per-VDOM administrators

Per-VDOM administrators can be created that can access only the administrative or traffic VDOM. These administrators must use the *prof_admin*, *admin_no_access*, or a custom administrator profile.

To assign an administrator to multiple VDOMs, they must be created at the global level. When creating an administrator at the VDOM level, the *super_admin* administrator profile cannot be used.

To create a per-VDOM administrator in the GUI:

1. In the Global VDOM, go to *System* > *Administrators* and click *Create New* > *Administrator*.
2. Fill in the required information, setting the *Type* as *Local User*.
3. In the *Virtual Domains* field, add the VDOMs that the administrator will be assigned to.



4. Click *OK*.

To create a per-VDOM administrator using the CLI:

```
config global
    config system admin
        edit <name>
            set accprofile <profile>
            set vdom <vdom(s)>
            ...
        next
    end
end
```

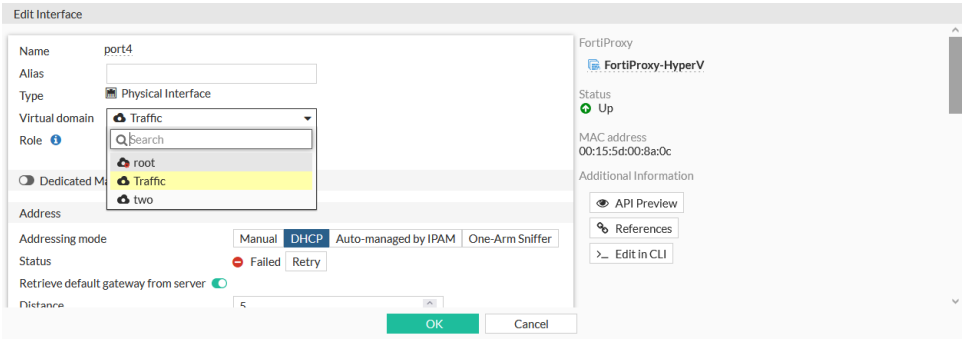
Assign interfaces to a VDOM

An interface can only be assigned to one of the VDOMs. An interface cannot be moved if it is referenced in an existing configuration. By default, all interfaces belong to the root VDOM.

In the GUI, the interface list *Ref.* column shows if the interface is referenced in an existing configuration, and allows you to quickly access and edit those references.

To assign an interface to a VDOM in the GUI:

1. In the Global VDOM, go to *Network* > *Interfaces*.
2. Select the interface that will be assigned to a VDOM and click *Edit*.
3. Select the VDOM that the interface will be assigned to from the *Virtual Domain* list.



4. Click *OK*.

To assign an interface to a VDOM using the CLI:

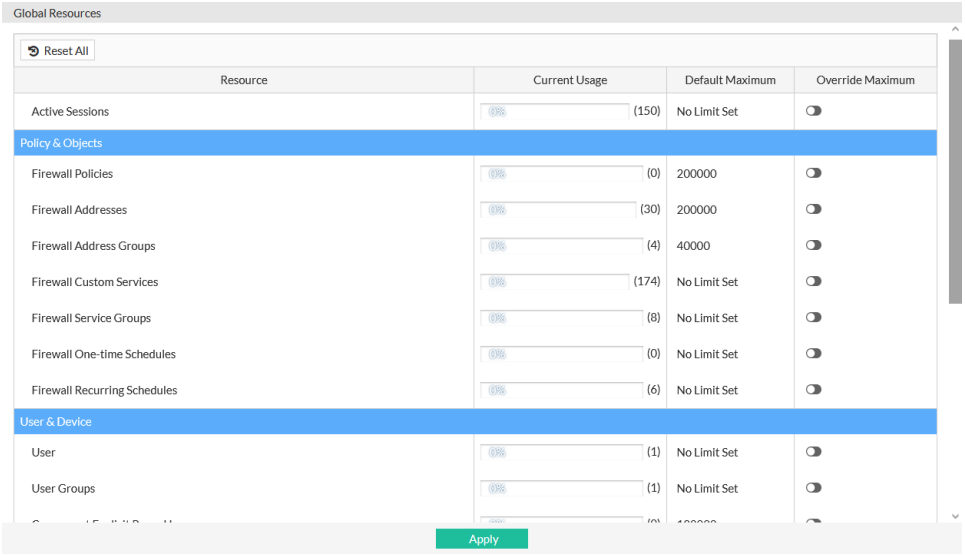
```
config global
    config system interface
        edit <interface>
            set vdom <vdom>
        next
    end
end
```

Global and per-VDOM resources

Global resources apply to resources that are shared by the whole FortiProxy, while per-VDOM resources are specific to each VDOM.

To configure global resources in the GUI:

1. In the Global VDOM, go to *System > Global Resources*.
2. Enable the resource's override in the *Override Maximum* column, then enter the override value.



3. Click *Apply*.
   To reset all of the override values, click *Reset All*.

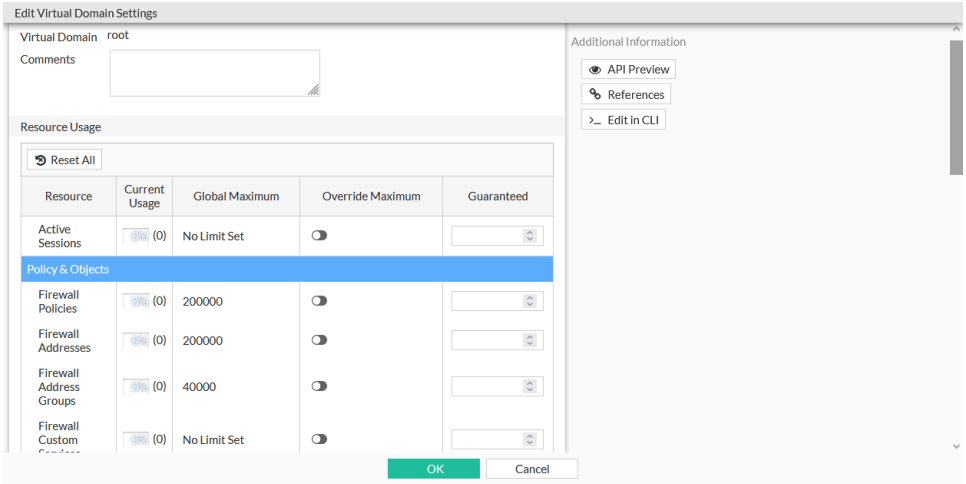
To configure global resources in the CLI:

```
config global
    config system resource-limits
        set log-disk-quota <integer>
        set session <integer>
        set ipsec-phase1-interface <integer>
        set ipsec-phase2-interface <integer>
        set firewall-policy <integer>
        set firewall-address <integer>
        set firewall-addrgrp <integer>
        set custom-service <integer>
        set service-group <integer>
        set onetime-schedule <integer>
        set recurring-schedule <integer>
        set user <integer>
        set user-group <integer>
        set sslvpn <integer>
        set proxy <integer>
        set log-disk-quota <integer>
```

```
    end
end
```

To configure per-VDOM resources in the GUI:

1. In the *Global* VDOM, go to *System > VDOM*.
2. Select the VDOM whose resources need to be configured and click *Edit*.
3. Enable the resource's override in the *Override Maximum* column, then enter the override value.
4. Optionally, enter a value in the *Guaranteed* column.



5. Click *OK*.
   To reset all of the override values, click *Reset All*.

To configure per-VDOM resources in the CLI:

```
config vdom
    edit <vdom>
        config system vdom-property
            edit <vdom>
                set session <max-number> [guaranteed-number]
                set ipsec-phase1-interface <max-number> [guaranteed-number]
                set ipsec-phase2-interface <max-number> [guaranteed-number]
                set firewall-policy <max-number> [guaranteed-number]
                set firewall-address <max-number> [guaranteed-number]
                set firewall-addrgrp <max-number> [guaranteed-number]
                set custom-service <max-number> [guaranteed-number]
                set service-group <max-number> [guaranteed-number]
                set onetime-schedule <max-number> [guaranteed-number]
                set recurring-schedule <max-number> [guaranteed-number]
                set user <max-number> [guaranteed-number]
                set user-group <max-number> [guaranteed-number]
                set sslvpn <max-number> [guaranteed-number]
                set proxy <max-number> [guaranteed-number]
                set log-disk-quota <integer>
            next
```

```
        end
    next
end
```

Inter-VDOM routing

VDOM links allow VDOMs to communicate internally without using additional physical interfaces. VDOM link does not support traffic offload.



A VDOM link cannot share the same name as a VDOM.

To configure a VDOM link in the GUI:

1. In the *Global* VDOM, go to *Network* > *Interfaces*.
2. Click *Create New* > *VDOM Link*.
3. Configure the fields, including the *Name*, *Virtual Domain*, IP information, *Administrative Access*, and so on, then click *OK*.

To configure a VDOM link in the CLI:

```
config global
    config system vdom-link
        edit "<vdom-link-name>"
            set type {ppp | ethernet}
        next
    end
    config system interface
        edit "<vdom-link-name0>"
            set vdom "<VDOM Name>"
            set type vdom-link
        next
        edit "<vdom-link-name1>"
            set vdom "<VDOM Name>"
            set type vdom-link
        next
    end
end
```

To delete a VDOM link in the GUI:

1. In the *Global* VDOM, go to *Network* > *Interfaces*.
2. Select a *VDOM Link* and click *Delete*.

To delete a VDOM link in the CLI:

```
config global
    config system vdom-link
        delete <VDOM-LINK-Name>
    end
end
```

Configure global security profiles

Global profiles can be configured globally across multiple VDOMs. Some or all profiles may be commonly-shared across VDOMs. Global profiles are available as read-only for VDOM-level administrators and can only be edited or deleted from within the global settings. The name for any global security profile must begin with *g-* for identification. Each security feature has at least one default global profile, available for all VDOMs to use.

Some security profile features, such as URL filters under web-filter, are not available for use in a global profile.

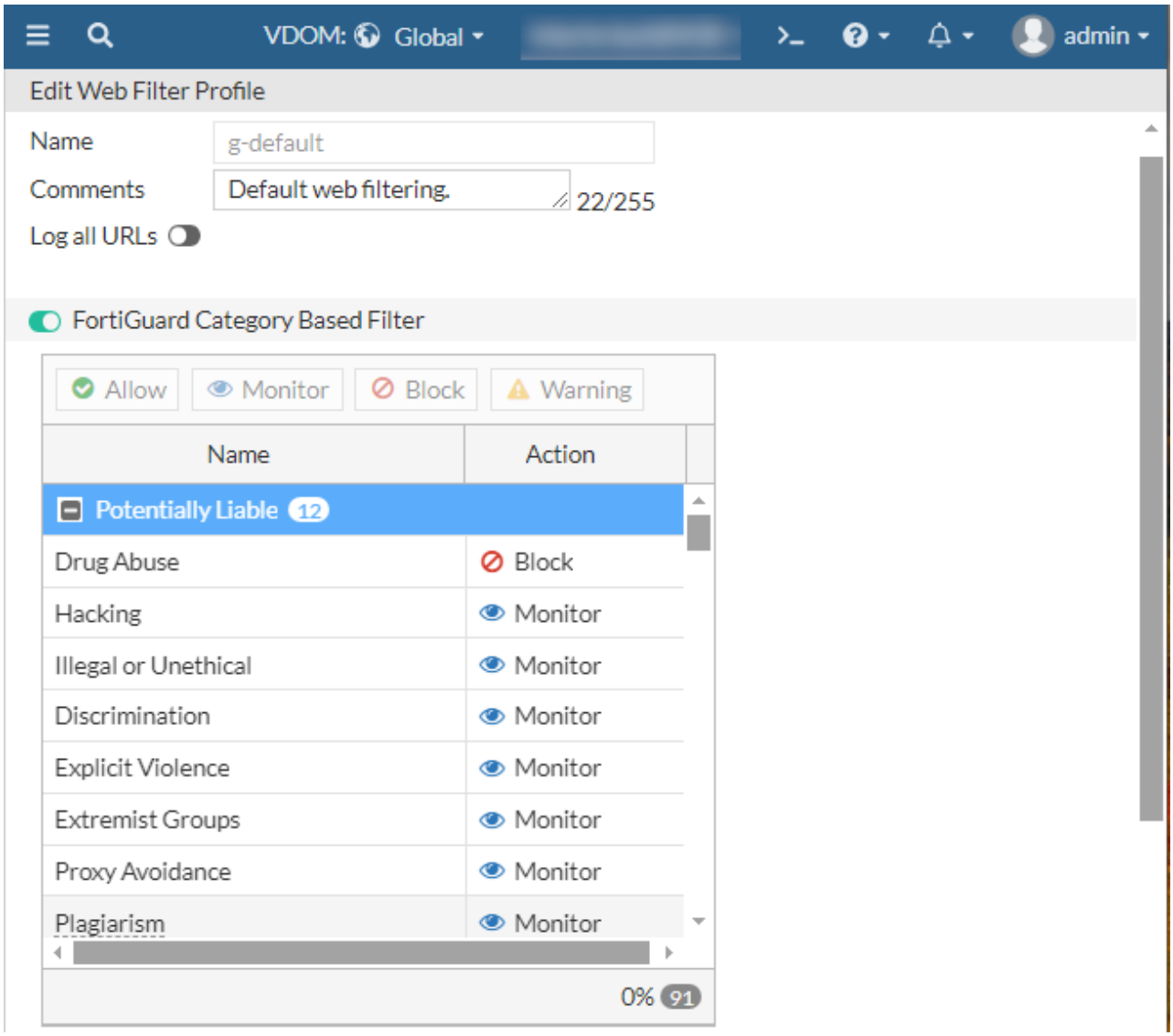
The following examples demonstrate configuring and editing Web Filter global security profiles. Similarly, you can view, edit, and configure other global security profiles for Antivirus, Application Control, Intrusion Prevention, and File Filter.

To configure a global security profile:

1. In the Global VDOM, go to *Security Profile* > *Web Filter*.
2. Click *Create new*.
3. Enter any suitable name that begins with *g-* and configure the web-filter settings required.
4. Click *OK*. This global web-filter is now available to be used in different VDOMs as required.

To view and edit a global security profile:

1. In the Global VDOM, go to *Security Profiles* > *Web Filter*. The names of the global web-filter security profile begins with *g-* for identification.
2. Select the default global web-filter profile named *g-default* and click *Edit*.
3. Under *FortiGuard Category Based Filter* select *Drug Abuse* and set the *Action* to *Block*.



4. Click *OK*.

Transparent mode management

In transparent mode, you can assign a single IP address to the FortiProxy for remote management access and configure multiple static routes for in-band management. When out-of-band management is required, it is recommended to configure a dedicated management interface.

The management interface supports only the following protocols for outgoing traffic: SNMP, NTP, LOG, Radius, FTP, TFTP, Telnet. To allow the management interface to handle outgoing traffic with an unsupported protocol, you must configure multiple VDOM on page 889s and dedicate the root VDOM to management traffic, which means assigning the management interface to the root VDOM while keeping all other interfaces for in-band traffic to user VDOMs.

In-band management

The management IP address is bound to all ports or VLANs that belong to the same bridge group. Remote access services are subject to the same rules as in NAT mode, and must be enabled on each interface.

To configure the management IP address:

```
config system settings
    set opmode transparent
    set manageip 10.1.1.100/255.255.255.0
end
config router static
    edit 1
        set gateway 10.1.1.254
    next
end
config system interface
    edit port1
        set allowaccess ping ssh https snmp
    next
end
```

To add a second IP address for management and additional default routes:

```
config system settings
    set manageip 192.168.182.136/255.255.254.0 10.1.1.1/255.255.255.0
end
config router static
    edit 1
        set gateway 192.168.183.254
    next
    edit 2
        set gateway 10.1.1.254
    next
end
```

Out-of-band management

When an interface is dedicated to management purposes only, it is removed from default switch group and becomes an isolated routing port. When the FortiProxy is running in transparent mode, it is recommended that one physical interface be kept as an out-of-band management interface to avoid layer 2 loops and allow for more routing flexibility.



The management interface must be assigned to the root VDOM and have IP connectivity to the management and monitoring network subnets.

To dedicate an interface to management:

1. Dedicate the interface to management:

```
config system interface
    edit port2
        set dedicated-to management
        set ip 192.168.1.10 255.255.255.0
        set allowaccess ping ssh https snmp
    next
end
```

2. Configure static routed to the management and monitoring subnets:

```
config router static
    edit 1
        set gateway 192.168.183.254
    next
    edit 2
        set dst 172.18.1.0 255.255.255.0
        set gateway 192.168.1.10 next
        set device "port2"
        set comment "To_MGMT_Monitoring_subnets"
    next
end
```

Backing up and restoring configurations in multi VDOM mode

When a FortiProxy is in multi VDOM mode, the configuration can be backed up or restored using the GUI or the CLI. Back up and restoration permissions depend on the VDOM administrator when in multi VDOM mode:

- A global *super_admin* can back up and restore the global configuration or the configuration of a specific VDOM.
- A VDOM administrator of one VDOM can only back up and restore the configuration of the current VDOM.
- A VDOM administrator of multiple VDOMs can back up and restore the configuration of multiple VDOMs.

To back up the configuration using the GUI:

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration > Backup*.
2. Select *VDOM* for the *Scope*. The *VDOM* dropdown menu is displayed.
3. Select the VDOM you want to back up.
4. Direct the backup to your *Local PC* or to a *USB Disk*.

5. Enable *Encryption*.



This is recommended to secure your backup configurations and prevent unauthorized parties from reloading your configuration.

6. Enter a password, and enter it again to confirm it. This password will be required to restore the configuration.
7. Click *OK*.
8. When prompted, select a location on the PC or USB disk to save the configuration file. The configuration file will have a .conf extension.

To restore the FortiProxy configuration using the GUI:

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration* > *Restore*.
2. Select *VDOM* for the *Scope*. The *VDOM* dropdown menu is displayed.
3. Select the VDOM that you want to restore the configuration for.
4. Identify the source of the configuration file to be restored: your *Local PC* or a *USB Disk*. The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.
5. Click *Upload*, locate the configuration file, and click *Open*.



Confirm that the configuration file you are uploading is for the same VDOM selected from the dropdown menu.

6. Enter the password if required.
7. Click *OK*.

Backing up configurations in the CLI

Configuration backups can be performed in the CLI using the `execute backup` commands. If you are backing up a VDOM configuration instead of the global configuration, first enter the commands:

```
config vdom
    edit <vdom_name>
```

Configurations can be backed up in FortiProxy and YAML format.

Configuration files can be backed up to various locations depending on the command:

- `flash`: Backup the configuration file to the flash drive.
- `ftp`: Backup the configuration file to an FTP server.
- `sftp`: Backup the configuration file to a SFTP server.
- `tftp`: Backup the configuration file to a TFTP server.
- `usb`: Backup the configuration file to an external USB drive.

Command	Description
`# execute backup config`	Back up the configuration in FortiProxy format. Backup your configuration file to: • flash • ftp • sftp • tftp • usb
`# execute backup full-config`	Backup the configuration, including backups of default configuration settings. Backup your configuration file to: • ftp • sftp • tftp • usb
`# execute backup yaml-config`	Backup the configuration in YAML format. Backup your configuration file to: • ftp • tftp

To back up the configuration in FortiProxy format using the CLI:

For FTP, note that port number and username are optional depending on the FTP site:

```
config vdom
    edit <vdom_name>
        execute backup config ftp <backup_filename> <ftp_server>[<:ftp_port>] [<user_name>]
[<password>] [<backup_password>]
```

or for TFTP:

```
config vdom
    edit <vdom_name>
        execute backup config tftp <backup_filename> <tftp_servers> [<backup_password>]
```

or for SFTP:

```
config vdom
    edit <vdom_name>
        execute backup config sftp <backup_filename> <sftp_server>[<:sftp_port>] <user> <password>
[<backup_password>]
```

or for an external USB:

```
config vdom
    edit <vdom_name>
        execute backup config usb <backup_filename> [<backup_password>]
```

To back up the configuration in YAML format using the CLI:

For FTP:

```
config vdom
    edit <vdom_name>
        execute backup yaml-config ftp <file_path> <ftp_server>[<:port>] [<user_name>] [<FTP
password>]
```

or for TFTP:

```
config vdom
    edit <vdom_name>
        execute backup yaml-config tftp <file_path> <tftp_server>
```

Restoring configurations in the CLI

Restoring configurations can be performed in the CLI using the `execute restore` command. If you are restoring a VDOM configuration instead of the global configuration, first enter the commands:

```
config vdom
    edit <vdom_name>
```

When restoring a VDOM configuration, ensure that the configuration file is for the correct VDOM specified.

Command	Description
`# execute restore config`	Restore a configuration that is in FortiProxy or YAML format. Configurations can be loaded from: • `dhcp`: Load the configuration though DHCP. • `flash`: Load the configuration file from flash to firewall. • `ftp`: Load the configuration file from an FTP server. • `tftp`: Load the configuration from a TFTP server. • `usb`: Load the configuration file from an external USB disk to firewall.

To restore the FortiProxy configuration in FortiProxy or YAML format using the CLI:

For FTP, note that port number and username are optional depending on the FTP site:

```
config vdom
    edit <vdom_name>
        execute restore config ftp <file_path> <ftp_server>[<:port>] [<user_name>] [<FTP
password>] [<password>]
```

or for TFTP:

```
config vdom
    edit <vdom_name>
        execute restore config tftp <file_name> <tftp_server> [<password>]
```

or for DHCP:

```
config vdom
    edit <vdom_name>
        execute restore config dhcp <port> [<VLAN_ID>]
```

or for flash:

```
config vdom
    edit <vdom_name>
        execute restore config flash <revision_ID>
```

or for an external USB:

```
config vdom
    edit <vdom_name>
        execute restore config usb <file_name> [<password>]
```

HA

NOTE: The HA clustering members must be the same hardware model running the same software version. The seat license does not have to be identical.

FortiProxy high availability (HA) provides a system management solution that synchronizes configuration changes among the clustering members. You can fine-tune the performance of the HA cluster to change how a cluster forms and shares information among clustering members.

The HA heartbeat keeps cluster units communicating with each other. The heartbeat consists of hello packets that are sent at regular intervals by the heartbeat interface of all cluster units. These hello packets describe the state of the cluster unit and are used by other cluster units to keep all the units synchronized.

HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8893. The default time interval between HA heartbeats is 200 ms.

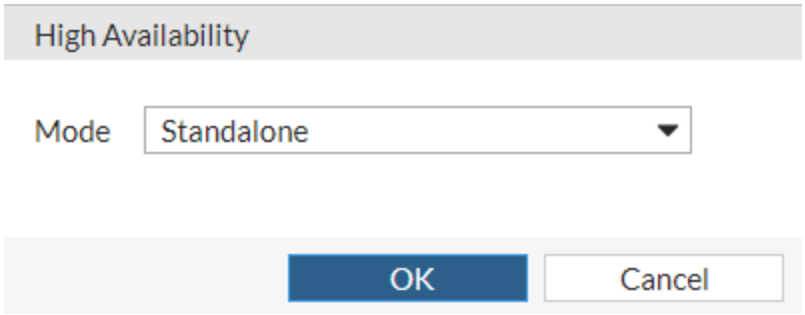
Your FortiProxy device can be configured as a standalone unit or you can configure two FortiProxy devices in the Active-Passive mode for failover protection. In active-passive mode, the FortiProxy shares available seats among the HA cluster (hardware and VM) by default. The primary FortiProxy unit automatically claims all license seats from all members in the HA cluster (hardware or VM). When a member joins the cluster, its associated license seats are added to the primary unit. When a member leaves the cluster, its associated license seats are removed from the primary unit after 14 days. When the primary unit goes down, the secondary unit that becomes the primary assumes all the license seats from the original primary unit.

NOTE: If you are using vSwitches:

- In Config-Sync mode, you need to select the promiscuous mode and accept MAC address changes on the VLANs or port groups of the heartbeat vSwitch. For the data interface's vSwitch, you can use the default vSwitch setting.
- In Active-Passive mode, you need to select the promiscuous mode and accept MAC address changes on the VLANs or port groups of the heartbeat vSwitch. For the data interface's vSwitch, the security setting must be the same as the heartbeat vSwitch.

To configure an HA cluster or to view the cluster member list in the GUI:

1. Select *System* > *HA*.



2. Configure the following settings and then click *OK*:

Mode	Select the mode from the drop-down menu. • *Standalone*—This option disables HA mode. No further configuration options are available. • *Config-Sync* • *Active-Passive*—Select this option to enable license sharing.
Device priority	You can set a different device priority for each cluster member to control the order in which cluster units become the primary unit (HA primary) when the primary unit fails. The device with the highest device priority becomes the primary unit. The default value is 128.
Cluster Settings	
Group name	Enter a name to identify the cluster. Must be the same for all members for authentication and membership identification.
Password	Select *Change* to enter a password to identify the HA cluster. The maximum password length is 15 characters. The password must be the same for all cluster FortiProxy units before the FortiProxy units can form the HA cluster. When the cluster is operating, you can add a password, if required. Two clusters on the same network must have different passwords.
Monitor interfaces	Select the specific ports to monitor.

	If a monitored interface fails or is disconnected from its network, the interface leaves the cluster and a link failover occurs. The link failover causes the cluster to reroute the traffic being processed by that interface to the same interface of another cluster that still has a connection to the network. This other cluster becomes the new primary unit.
Heartbeat Interfaces	Select to enable or disable the HA heartbeat communication for each interface in the cluster and then set the heartbeat interface priority. The heartbeat interface with the highest priority processes all heartbeat traffic. You must select at least one heartbeat interface. If the interface functioning as the heartbeat fails, the heartbeat is transferred to another interface configured as a heartbeat interface. If heartbeat communication is interrupted, the cluster stops processing traffic. Priority ranges from 0 to 512. Select + enter another management interface.
Management Interface Reservation	Enable or disable the management interface reservation. You can provide direct management access to individual cluster units by reserving a management interface as part of the HA configuration. After this management interface is reserved, you can configure a different IP address, administrative access, and other interface settings for this interface for each cluster unit. You can also specify static routing settings for this interface. Then by connecting this interface of each cluster unit to your network, you can manage each cluster unit separately from a different IP address. Refer to HA cluster out-of-band management on page 916 for detailed instructions about configuring a management interface for an HA cluster.
Unicast Heartbeat	Enable the unicast HA heartbeat in virtual machine (VM) environments that do not support broadcast communication. By default, the device notifies peers by multicasting which allows all devices sharing the same group credentials (name and password) in the LAN to join the HA group automatically.

Interface	Select the management interface.
Gateway	Enter the IPv4 address for the remote gateway.
IPv6 gateway	Enter the IPv6 address for the remote gateway.
Destination subnet	Enter the destination subnet.

Unicast Heartbeat Peer IP	Enter the IP address of the HA heartbeat interface of the other FortiProxy VM in the HA cluster.

To configure an HA cluster in the CLI:

```
config system ha
   set group-name {string}
    set password {password}
   set mode [standalone|config-sync-only|...]
   set hbdev <INTERFACE_NAME> <PRIORITY>
   set override enable
   set priority <PRIORITY>
   set unicast-hb enable
   set unicast-hb-peerip <PEER_IP>
end
```

Parameter	Description	Type	Size	Default
group-name	Cluster group name. Must be the same for all members for authentication and membership identification.	string	Maximum length: 32	
password	Cluster password. Must be the same for all members for authentication and membership identification.	password	Not Specified	
mode	HA mode. Must be the same for all members. FGSP requires standalone.	option	-	standalone
	Option / **Description** *standalone* — Disable HA feature. *config-sync-only* — Enable Config sync only *active-passive* — Enable Active-passive mode. This mode enables license sharing.			
hbdev	Heartbeat interfaces. HA devices notify and identify each other through heart beat. The heartbeat interface must be the same for all members. You can also specify multiple interfaces: `set hbdev <INTF_NAME_1> <PRIORITY_1> <INTF_NAME_2> <PRIORITY_2> ...` • `<INTERFACE_NAME>` means the interface name as configured in config system interface. • `<PRIORITY>` means the search priority when there are multiple interfaces.	user	Not Specified	

Parameter	Description	Type	Size	Default
(Optional) override	Enable and increase the priority of the unit that should always be primary. When disabled (default), the active (primary) unit is automatically determined based on its uptime etc.	option	-	disable
(Optional) priority	Increase the priority of the unit to make it the primary unit .	integer	Minimum value: 0 Maximum value: 255	128
(Optional) unicast-hb	Enable the unicast HA heartbeat in virtual machine (VM) environments that do not support broadcast communication. By default, the device notifies peers by multicasting which allows all devices sharing the same group credentials (name and password) in the LAN to join the HA group automatically.			
(Optional) unicast-hb-peerip	Unicast heartbeat peer IP, which is the IP address of the HA heartbeat interface of the other FortiProxy VM in the HA cluster.	ipv4-address	Not Specified	0.0.0.0

Refer to the config system ha topic in the CLI guide for more details about other available configurations for HA setup.

To view HA cluster information in the CLI:

- Run the `get system ha status` command to see the synchronization status of the HA cluster. For synchronized HA peers, the status should be `in-sync` in `Configuration Status`.
- Run the `diag system ha status` command to see the license serial number of connected peer devices.

HA multiple unicast peers

You can configure up to eight unicast Config-Sync HA clusters. Unicast configuration synchronization is supported on layer 3, allowing peers to be synchronized in cloud environments that do not support layer-2 networking. Configuring a unicast gateway allows peers to be in different subnets.

For example:

```
config system ha
   set mode config-sync-only
   set hbdev "port1" 50
   set override enable
   set unicast-status enable
   set unicast-gateway 10.0.0.1
   config unicast-peers
      edit 1
         set peer-ip 192.168.76.13
      next
```

```
      .........
   end
end
```

Note:

- Use the `set unicast-hb enable` command for a one-to-one unicast Active-Passive HA cluster or Config-Sync HA cluster.
- Use the *set unicast-status*, `set unicast-gateway`, and `config unicast-peers` commands for multiple peers in a Config-Sync HA cluster.

Cache Collaboration

When deployed in a cluster, depending on the deployed architecture, requests for the same URL might have hit each cache device and been cached separately on each. Methods are available to mitigate this through load balancing with FortiADC or WCCP.

FortiProxy has the Cache Collaboration feature, where the storage of all devices within the FortiProxy HA Cluster is accessible as a shared entity. This feature allows content cached by one device to be shared by other FortiProxy devices within the cluster, significantly increasing the cache rate.

CLI syntax

```
config wanopt cache-service
   set prefer-senario {balance | prefer-speed | prefer-cache} // Default is balance.
   set collaboration {enable | disable} // Default is disable.
   set device-id <name>
   set acceptable-connections {any | peers} // Default is any.
end
```

HA virtual cluster setup

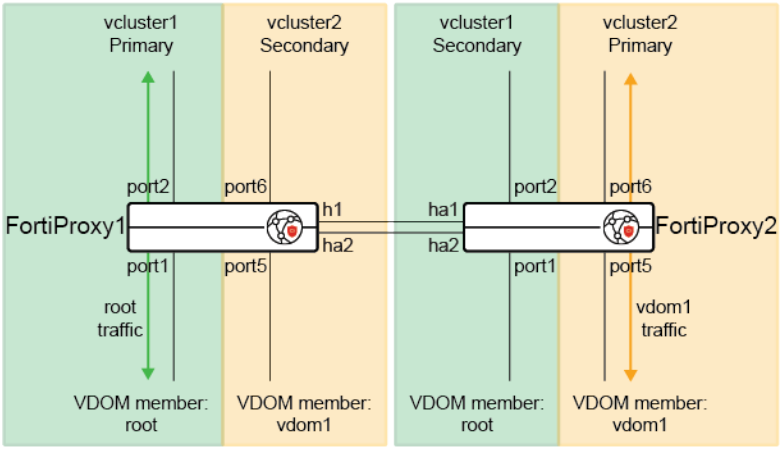
Virtual clustering is an extension of HA to allow multiple clusters to be formed between your HA members. In effect, each cluster consists of the same HA members, with the option to prioritize different members as the primary unit. Each cluster operates as its on active-passive HA cluster, with different virtual domains residing in the virtual cluster. The following custom settings can be configured per cluster:

```
config system ha
    set vcluster-status enable
    config vcluster
        edit <id>
            set override {enable | disable}
            set priority <integer>
            set vdom <vdom_1>, ... [vdom_n]
            set monitor <interface_1>, ... [interface_n]
            set pingserver-monitor-interface <interface_1>, ... [interface_n]
        next
    end
end
```

`override {enable | disable}`	Enable/disable override and increase the priority of the unit that should always be the primary.
`priority <integer>`	Increase the priority to select the primary unit (0 - 255, default = 128).
`vdom <vdom_1>, ... [vdom_n]`	Set the virtual domains in the virtual cluster.
`monitor <interface_1>, ... [interface_n]`	Set the interfaces to check for port monitoring (or link failure).
`pingserver-monitor-interface <interface_1>, ... [interface_n]`	Set the interfaces to check for remote IP monitoring.

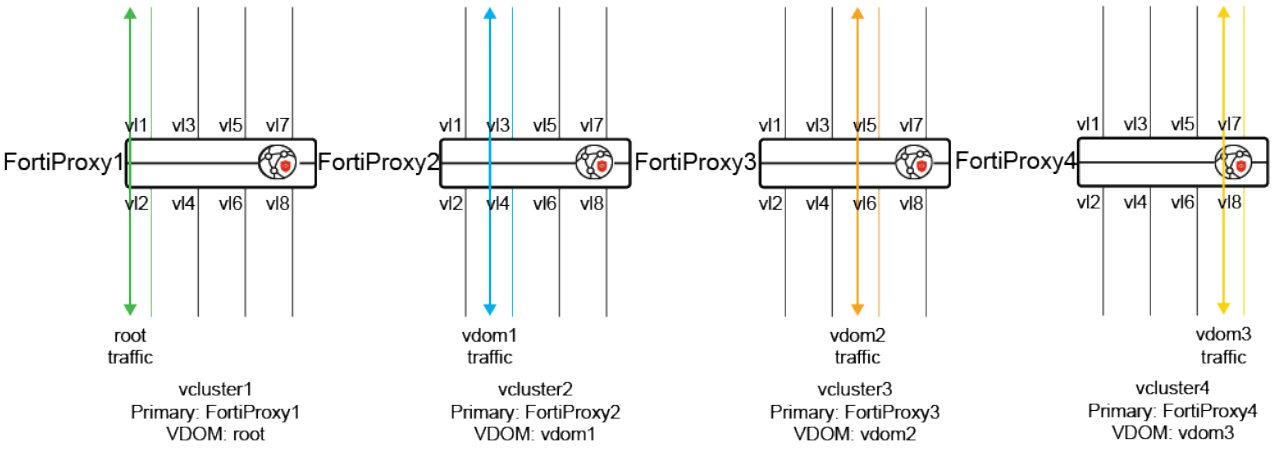
Active-passive virtual clustering uses VDOM partitioning to send traffic for some VDOMs to the primary FortiProxy and traffic for other VDOMs to the secondary FortiProxies. Traffic distribution between FortiProxies can potentially improve throughput. If a failure occurs and only one FortiProxy continues to operate, all traffic fails over to that FortiProxy, similar to normal HA. If the failed FortiProxies rejoin the cluster, the configured traffic distribution is restored.

In an active-passive virtual cluster of two FortiProxies, the first and second FortiProxies share traffic processing according to the VDOM partitioning configuration. The following is an example of two virtual clusters, with each member acting as primary for different vclusters.



If you add a third or fourth FortiProxy, the first and second FortiProxies process all traffic and the other one or two FortiProxies operate in standby mode. If the first or second FortiProxy fails, one of the other FortiProxies becomes the new primary or secondary FortiProxy and begins processing traffic.

For better load balancing, it is recommended to have as many vclusters as there are HA members. This way, each HA member can be a primary unit for each cluster, thereby processing traffic while standing by for the other vcluster as secondary. The following is an example of four FortiProxies in a cluster, with four vclusters and four VDOMs. Each FortiProxy is the primary unit for a vcluster and actively processes traffic as the primary member.



Virtual clustering and heartbeat interfaces

The HA heartbeat provides the same HA services in a virtual clustering configuration as in a standard HA configuration. One set of HA heartbeat interfaces provides HA heartbeat services for all of the VDOMs in the cluster. You do not have to add a heartbeat interface for each VDOM.

Support up to 8 virtual clusters

FortiProxy supports up to 8 virtual clusters, which allows more VDOMs to be spread across different virtual clusters without overlapping. Each virtual cluster supports its own failover conditions. Prior to 7.4.0, only two virtual clusters were supported.

When configuring virtual clusters, the `group-id` is limited to a value from 0 to 7. If the HA `group-id` is greater than 7, use the command line first to change the `group-id` before enabling virtual clusters.

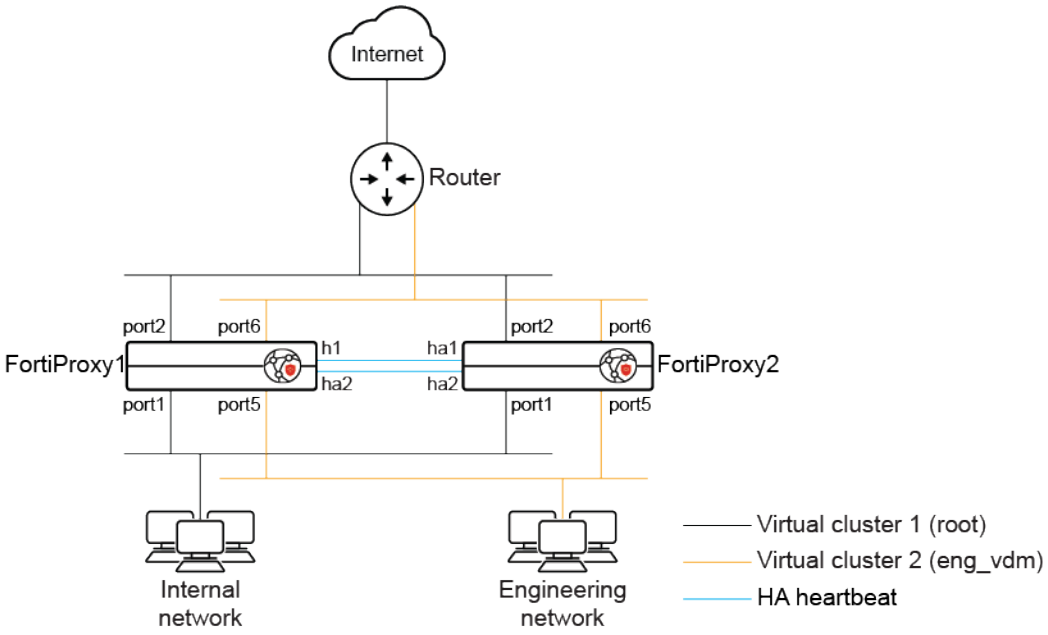
```
config system ha
    set group-id <integer>
end
```



When upgrading from 7.2, old virtual clusters will be lost if the `group-id` is larger than 7.

Basic configuration

This example shows a virtual cluster configuration consisting of two FortiProxies. The virtual cluster has two VDOMs, root and eng_vdm.



The root VDOM can only be associated with virtual cluster 1.

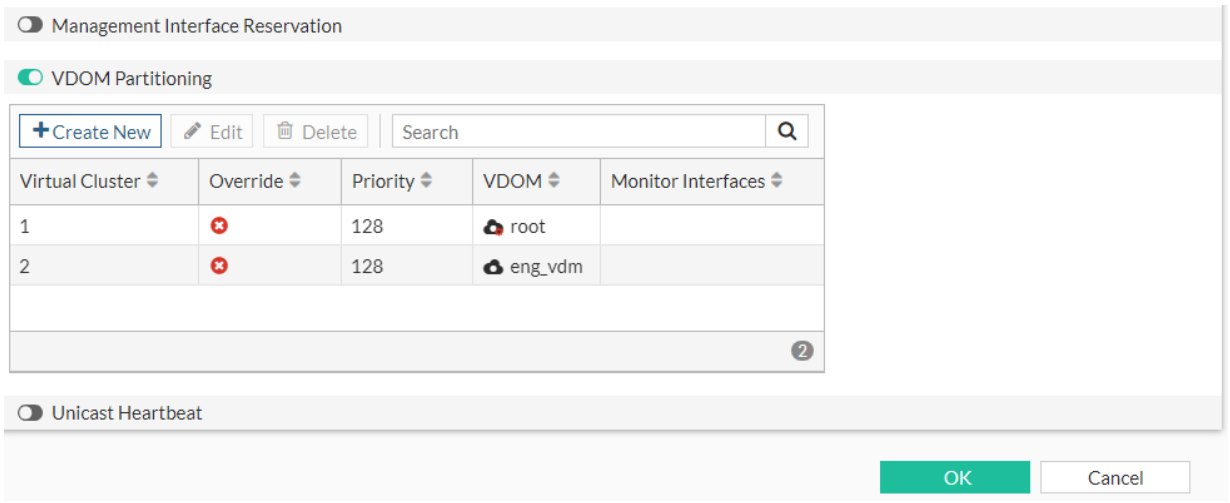
To set up an HA virtual cluster using the GUI:

1. Make all the necessary connections as shown in the topology diagram.
2. Configure a regular A-P cluster:
   a. Log in to one of the FortiProxies.
   b. Go to *System* > *HA* and set the following options:

Mode	Active-Passive
Device priority	128 or higher
Group name	Example_cluster
Heartbeat interfaces	ha1 and ha2

   Except for the device priority, these settings must be the same on all FortiProxies in the cluster.
   c. Leave the remaining settings as their default values. They can be changed after the cluster is in operation.
   d. Click *OK*.
   The FortiProxy negotiates to establish an HA cluster. Connectivity with the FortiProxy may be temporarily lost as the HA cluster negotiates and changes the MAC addresses of the FortiGate's interfaces.
   e. Factory reset the other FortiProxy that will be in the cluster, configure GUI access, then repeat step 2 (omitting setting the device priority) to join the cluster.
3. On the primary FortiProxy, go to *System* > *Settings* and enable *Virtual Domains*.

4. Click *Apply*. You will be logged out of the FortiProxy.
5. Log back in to the FortiProxy, and ensure that you are in the global VDOM.
6. Create the eng_vdm VDOM:
   a. Go to *System* > *VDOM* and click *Create New*. The *New Virtual Domain* pane opens.
   b. Enter the name in the *Virtual Domain* field, then click *OK*.
7. Implement a virtual cluster by moving the new VDOM to virtual cluster 2:
   a. Go to *System* > *HA* and enable *VDOM Partitioning*.
   b. In the table, click *Create New*. The *New Virtual Cluster* pane opens.
   c. Click the *+* and add the *eng_vdm* VDOM.
   d. Click *OK* to save the virtual cluster.



   e. Click *OK* to save the HA configuration.

To set up an HA virtual cluster using the CLI:

1. Make all the necessary connections as shown in the topology diagram.
2. Configure a regular A-P cluster. See HA on page 904.
3. Enable VDOMs:

```
config system global
    set vdom-mode multi-vdom
end
```

   You will be logged out of the FortiProxy.
4. Create the eng_vdm VDOM:

```
config vdom
    edit eng_vdm
    next
end
```

5. Reconfigure the HA settings to be a virtual cluster:

```
config system ha
    set vcluster-status enable
    config vcluster
        edit 1
            set vdom root
            set override disable
        next
        edit 2
            set vdom eng_vdm
            set override disable
        next
    end
end
```

Configuration with 8 virtual clusters

In this example, there are 8 customers managed by an MSSP on an HA cluster, and each customer VDOM needs to failover independently of other customer VDOMs. Each customer is assigned to a different virtual cluster with its own virtual cluster configuration. This may include different monitored interfaces, ping servers, and priority for the primary and secondary cluster members. Each virtual cluster will fail over according to its own virtual cluster configuration.

This example assumes an A-P cluster and VDOMs have already been configured. See HA on page 904 and VDOM on page 889 for more information.

For each virtual cluster, this example assumes that unit 1 has an HA priority of 200, while unit 2 has an HA priority of 100. By default, unit 1 will be the primary cluster member of all the virtual clusters.

To configure multiple virtual clusters in the GUI:

1. Go to *System* > *HA* and enable *VDOM Partitioning*.
2. Create a virtual cluster:
   a. In the table, click *Create New*. The *New Virtual Cluster* pane opens.
   b. Set the *Device priority* to *200*.
   c. Click the *+* and add the *Virtual domains*.
   d. Optionally, click the *+* and add the *Monitor interfaces*.
   e. Click *OK*.
3. Repeat step 2 to create the remaining virtual clusters.
4. Click *OK* to save the HA configuration. The *HA* page summary displays the multiple virtual clusters, each with a *Primary* and *Secondary* HA member.
5. Edit the priority settings for the secondary members to be 100:
   a. Select the *Secondary* member in the table, and click *Edit*.
   b. Set the *Priority* to *100*.
   c. Click *OK*.
6. Repeat step 5 for the remaining secondary members.

To configure multiple virtual clusters in the CLI:

1. Configure the primary FortiProxy:

```
config system ha
    set vcluster-status enable
    config vcluster
        edit 1
            set override disable
            set priority 200
            set vdom "vdom1"
        next
        edit 2
            set override disable
            set priority 200
            set vdom "vdom2"
        next
        ...
        edit 8
            set override disable
            set priority 200
            set vdom "vdom8"
        next
    end
end
```

2. Configure the secondary FortiProxy:

```
config system ha
    set vcluster-status enable
    config vcluster
        edit 1
            set override disable
            set priority 100
            set vdom "vdom1"
        next
        edit 2
            set override disable
            set priority 100
            set vdom "vdom2"
        next
        ...
        edit 8
            set override disable
            set priority 100
            set vdom "vdom8"
        next
    end
end
```

HA cluster out-of-band management

To provide direct management access to all cluster units, a management interface can be reserved as port of the HA configuration. After the management interface is reserved, the various interface settings, such as the IP address and administrative access, can be configured for each individual cluster unit. These settings are not synchronized to other cluster units. Connect the management interface of each cluster unit to your network to individually manage each unit with its unique IP address.

- Reserved management interfaces provide direct management access to each cluster unit, and give each cluster unit a different identity on your network. This simplifies using external services, such as SNMP, to monitor and manage each cluster units.
- Reserved management interfaces are not assigned HA virtual MAC addresses. They retain the permanent hardware address of the physical interface, unless you manually change it using the `config system interface` command.
- Reserved management interfaces and their IP addresses should not be used for managing a cluster using FortiManager. To manage a FortiProxy HA cluster with FortiManager, use the IP address of one of the cluster unit interfaces.
- Configuration changes to a reserved management interface are not synchronized to other cluster units. Other configuration changes are automatically synchronized to all cluster units.



For outgoing traffic, the management interface supports only the following protocols: SNMP, NTP, LOG, Radius, FTP, TFTP, telnet. For the management interface to handle outgoing traffic with an unsupported protocol, you must configure multiple VDOM on page 889s and dedicate the root VDOM to management traffic, which means assigning the management interface and the ha-sync interface to the root VDOM while keeping all other interfaces for in-band traffic to user VDOMs.

Management interface

Enable HTTPS or HTTP administrative access on the reserved management interfaces to connect to the GUI of each cluster unit. On secondary units, the GUI has the same features as the primary unit, except for unit specific information, for example:

- The *System Information* widget on the Dashboard shows the secondary unit's serial number, and also the same cluster information as on the primary unit.
- In the cluster list at *System* > *HA*, you can change the HA configuration for the unit that you are logged into, but you can only change the host name and device priority for the primary unit and other secondary units.
- The system events logs show logs for the device that you are logged into. To view logs for other cluster units, including the primary unit, use the cluster member list at *System* > *HA*.

Enable SNMP administrative access on a reserved management interface to use SNMP to monitor each cluster unit using the interface's IP address. Direct management of cluster members must also be enabled, see Configuration example on page 918.

Enable SSH or TELNET administrative access on the reserved management interfaces to connect to the CLI of each cluster unit. The CLI prompt includes the host of the cluster unit that you are connected to. Use the `execute ha manage` command to connect to other cluster unit CLIs.

SNMP, remote authentication server and other management services

By default, management services such as SNMP, remote authentication (LDAP, RADIUS, TACACS+, and others), remote logging, and others use a cluster interface. This means that communication from each cluster unit comes from a cluster interface, and not from an individual cluster unit's interface or the HA reserved management interface.

You can configure HA reserved management interfaces to be used for communication with management services by enabling the `ha-direct` option. This separates management traffic for each cluster unit, and allows each unit to be individually managed. This is especially useful when cluster units are in different physical locations.

The following management services will then use the HA reserved management interface:

- SNMP queries and traps
- Remote authentication and certificate verification
- Communication with FortiSandbox
- Remote logging

To use the HA reserved management interface for management:

```
config system ha
    set ha-direct enable
end
```



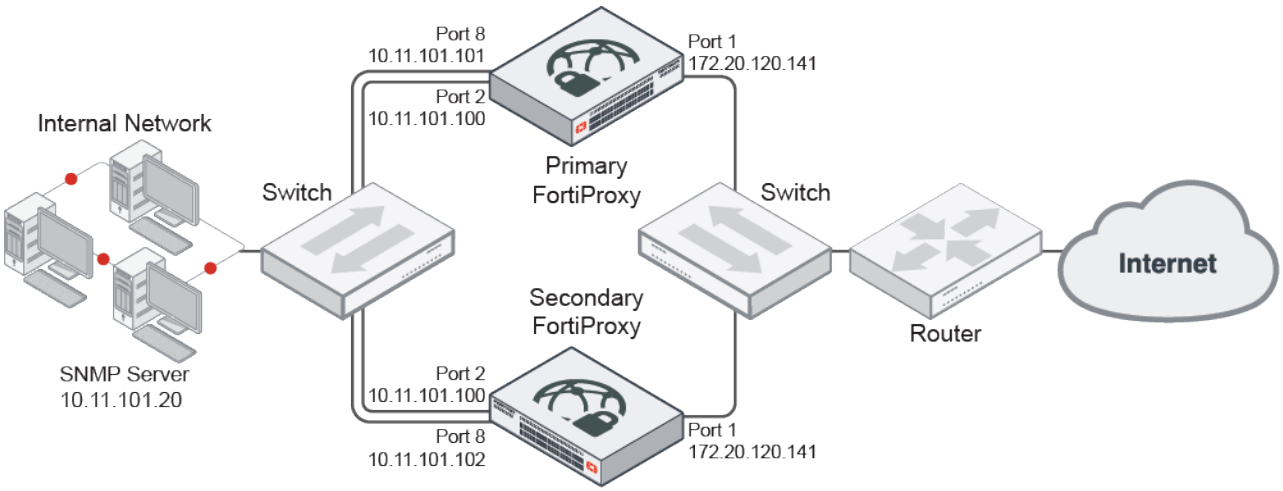
SNMP requires `ha-direct` to be configured under SNMP settings only. See below for more configuration options.

You can override the HA reserved management interface for a specific service using the `interface-select-method` option of the service configuration command. For example, to use a different interface than the HA reserved management interface for FortiAnalyzer logging, specify the interface using the following command:

```
config log fortianalyzer setting
  set status enable
  set interface-select-method specify
  set interface <interface name>
end
```

Configuration example

This example describes how to configure SNMP remote management of individual cluster units using an HA reserved management interface. The configuration consists of two FortiProxy units already operating as a cluster.



Two FortiProxy units are already operating in a cluster. On each unit, port8 is connected to the internal network through a switch and configured as an out-of-band reserved management interface.

Administrative access and default route for HA management interface

To configure the primary unit's reserved management interface, configure an IP address and management access on port8. Then, configure the necessary HA settings to enable the HA reserved management interface and its route.

To configure the secondary unit's reserved management interface, access the unit's CLI through the primary unit, and configure an IP address, management access on port8, and the necessary HA settings. Configuration changes to the reserved management interface are not synchronized to other cluster units.

To configure the primary unit reserved management interface in CLI:

1. From a computer on the internal network, connect to the CLI at 10.11.101.100 on port2.
2. Change the port8 IP address and management access:

```
config system interface
    edit port8
        set ip 10.11.101.101/24
        set allowaccess https ping ssh snmp
    next
end
```

3. Configure the HA settings for the HA reserved management interface by defining a default route to route to the gateway 10.11.101.2:

```
config system ha
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface port8
            set gateway 10.11.101.2
            set gateway6 2001:db8:0:2::20
        next
    end
end
```

You can now log into the primary unit's GUI by browsing to https://10.11.101.101. You can also log into the primary unit's CLI by using an SSH client to connect to 10.11.101.101.

To configure secondary unit reserved management interfaces to allow HTTPS, SSH, and ICMP access:

1. From a computer on the internal network, connect to the primary unit's CLI.
2. Connect to the secondary unit with the following command:

```
execute ha manage <unit id> <username> <password>
```

3. Change the port8 IP address and management access:

```
config system interface
    edit port8
        set ip 10.11.101.102/24
        set allowaccess https ping ssh snmp
    next
end
```

4. Configure the HA settings for the HA reserved management interface by defining a default route to route to the gateway 10.11.101.2:

```
config system ha
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface port8
            set gateway 10.11.101.2
            set gateway6 2001:db8:0:2::20
        next
    end
end
```

You can now log into the secondary unit's GUI by browsing to https://10.11.101.102. You can also log into the secondary unit's CLI by using an SSH client to connect to 10.11.101.102.

SNMP monitoring

The SNMP server can get status information from the cluster members. To use the reserved management interfaces, you must add at least one HA direct management host to an SNMP

community. If the SNMP configuration includes SNMP users with user names and passwords, HA direct management must be enabled for the users. The SNMP configuration is synchronized to all cluster units.

To configure the cluster for SNMP management using the reserved management interfaces:

1. Add an SNMP community with a host for the reserved management interface of each cluster member. The host includes the IP address of the SNMP server.

```
config system snmp community
    edit 1
        set name "Community"
        config hosts
            edit 1
                set ip 10.11.101.20 255.255.255.255
                set ha-direct enable
            next
        end
    next
end
```



Enabling `ha-direct` in a non-HA environment will make SNMP unusable.

2. Add an SNMP user for the reserved management interface:

```
config system snmp user
    edit "1"
        set notify-hosts 10.11.101.20
        set ha-direct enable
    next
end
```

3. Configure remaining settings as required.

To get CPU, memory, and network usage information from the SNMP manager for each cluster unit using the reserved management IP addresses:

1. Connect to the SNMP manager CLI.
2. Get resource usage information for the primary unit using the MIB fields:

```
snmpget -v2c -c Community 10.11.101.101 fgHaStatsCpuUsage
snmpget -v2c -c Community 10.11.101.101 fgHaStatsMemUsage
snmpget -v2c -c Community 10.11.101.101 fgHaStatsNetUsage
```

3. Get resource usage information for the primary unit using the OIDs:

```
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.3.1
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.4.1
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.5.1
```

4. Get resource usage information for the secondary unit using the MIB fields:

```
snmpget -v2c -c Community 10.11.101.102 fgHaStatsCpuUsage
snmpget -v2c -c Community 10.11.101.102 fgHaStatsMemUsage
snmpget -v2c -c Community 10.11.101.102 fgHaStatsNetUsage
```

5. Get resource usage information for the primary unit using the OIDs:

```
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.3.1
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.4.1
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.5.1
```

Remote authentication over dedicated HA management interface

If a dedicated management interface is configured on each cluster unit, and authentication on a remote server is used (administrator log in, firewall authentication, and so on), then the FortiProxy units can contact the remote authentication server using the HA management interface if `ha-direct` is enabled.

This shows an example configuration for a remote system administrator:

```
config system ha
    set group-id 110
    set group-name "leo_fpx_ha_11"
    set mode active-passive
    set hbdev "port5" 50
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.150.0.3
        next
    end
    set override enable
    set priority 111
    set unicast-hb enable
    set unicast-hb-peerip 10.150.51.12
end
```

```
config system admin
    edit "leo_rad"
        set remote-auth enable
        set accprofile "prof_admin"
        set remote-group "radius_grp_mgmt"
    next
end
```

```
config user radius
    edit "radius_mgmt"
        set server "10.150.0.111"
        set secret ************
```

```
    next
end
```

```
config user group
    edit "radius_grp_mgmt"
        set member "radius_mgmt"
    next
end
```

Upgrading FortiProxies in an HA cluster

You can upgrade the firmware on an HA cluster in the same way as on a standalone FortiProxy. During a firmware upgrade, the cluster upgrades the primary unit and all of the subordinate units to the new firmware image.



Before upgrading a cluster, back up your configuration (Configuration backups and reset on page 1006), schedule a maintenance window, and make sure that you are using a supported upgrade path (see Deployment information in the release notes).

Uninterrupted upgrade

An uninterrupted upgrade occurs without interrupting communication in the physical or virtual cluster.

To upgrade the cluster firmware without interrupting communication, use the following steps. These steps are transparent to the user and the network, and might result in the cluster selecting a new primary unit.

1. The administrator uploads a new firmware image using the GUI or CLI. See Upgrading individual device firmware on page 877 for details.
2. The firmware is upgraded on all of the subordinate units.
3. A new primary unit is selected from the upgraded subordinates.
4. The firmware is upgraded on the former primary unit.
5. Primary unit selection occurs, according to the standard primary unit selection process.

If all of the subordinate units crash or otherwise stop responding during the upgrade process, the primary unit will continue to operate normally, and will not be upgraded until at least one subordinate rejoins the cluster.

Interrupted upgrade

An interrupted upgrade upgrades all cluster members at the same time. This takes less time than an uninterrupted upgrade, but it interrupts communication in the cluster. Interrupted upgrade is disabled by default.

To enable interrupted upgrade:

```
config system ha
    set uninterruptible-upgrade disable
end
```

SNMP

The Simple Network Management Protocol (SNMP) allows you to monitor hardware on your network. You can configure the hardware, such as the FortiProxy SNMP agent, to report system information and traps.

SNMP traps alert you to events that happen, such as a log disk becoming full, or a virus being detected. These traps are sent to the SNMP managers. An SNMP manager (or host) is typically a computer running an application that can read the incoming traps and event messages from the agent and can send out SNMP queries to the SNMP agents. A FortiManager unit can act as an SNMP manager to one or more FortiProxy units.

By using an SNMP manager, you can access SNMP traps and data from any FortiProxy interface configured for SNMP management access. Part of configuring an SNMP manager is to list it as a host in a community on the FortiProxy unit it will be monitoring. Otherwise, the SNMP monitor will not receive any traps from, and be unable to query, that FortiProxy unit.

When using SNMP, you must also ensure you have added the correct Management Information Base (MIB) files to the unit, regardless of whether or not your SNMP manager already includes standard and private MIBs in a ready-to-use, compiled database. A MIB is a text file that describes a list of SNMP data objects used by the SNMP manager. See Fortinet MIBs on page 929 for more information.

The FortiProxy SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiProxy system information through queries and can receive trap messages from the unit.

The FortiProxy SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Authentication and encryption are configured in the CLI.



FortiProxy supports Low crypto (LENC) mode for LENC models.

Before a remote SNMP manager can connect to the FortiProxy agent, you must configure one or more FortiProxy interfaces to accept SNMP connections. Interfaces are configured in *Network* > *Interfaces*. See Interfaces on page 181.

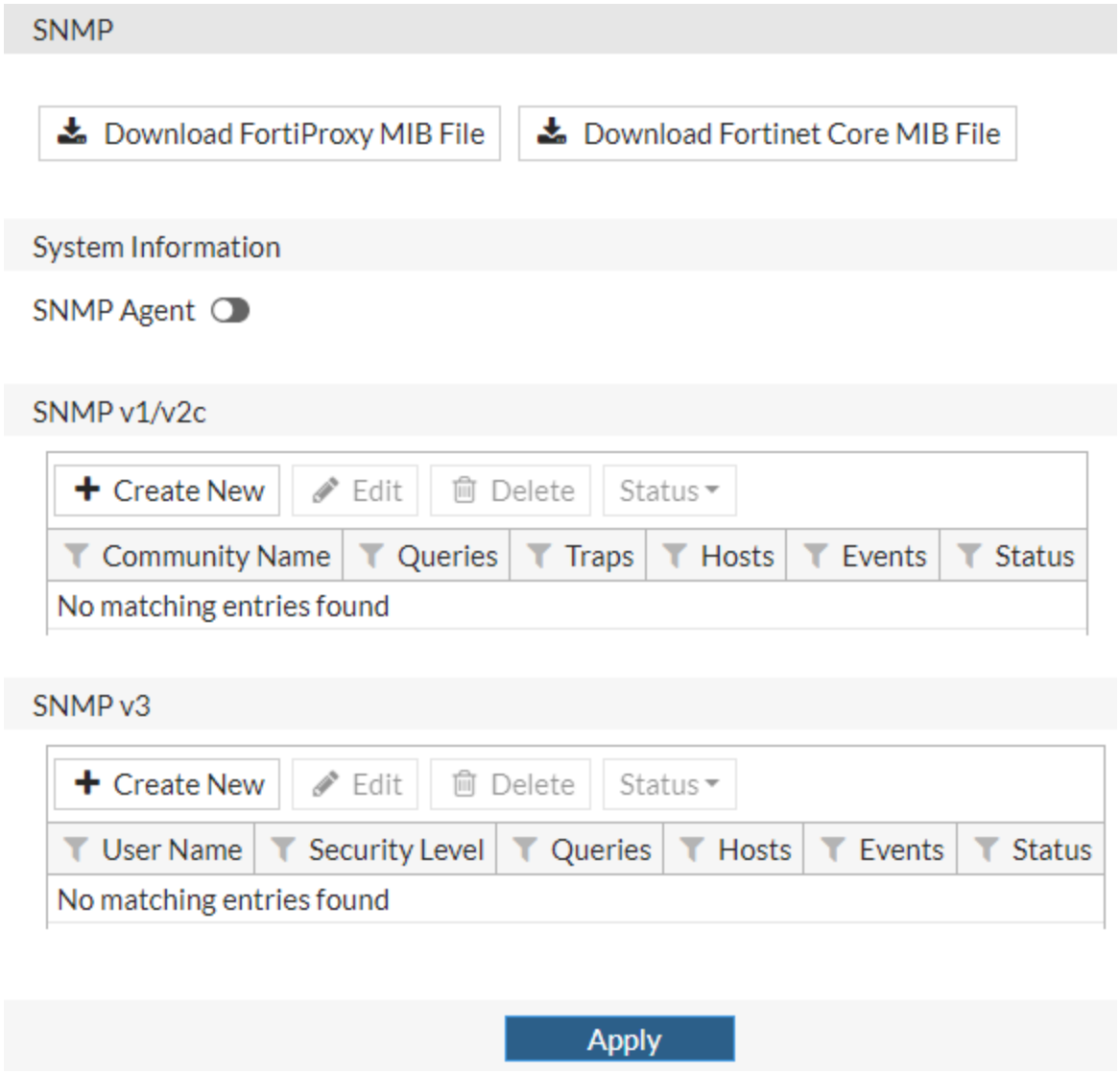


For security reasons, Fortinet recommends that neither “public” nor “private” be used for SNMP community names.

When the unit is in virtual domain mode, SNMP traps can only be sent on interfaces in the management virtual domain.

If you want to allow SNMP access on an interface, you must go to *Network* > *Interfaces* and select *SNMP* in the *Access* field in the settings for the interface that you want the SNMP manager to connect to.

For SNMP configuration, go to *System* > *SNMP*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

Configure the following settings and select *Apply*:

Download FortiProxy MIB File	Download the FortiProxy MIB file. See Fortinet MIBs on page 929.
Download Fortinet Core MIB File	Download the Fortinet MIB file. See Fortinet MIBs on page 929.
SNMP Agent	Enable the FortiProxy SNMP agent. See SNMP agent on page 931.
SNMP v1/v2c	Lists the communities for SNMP v1/v2c. From within this section, you can create, edit or remove SNMP communities.
Create New	Creates a new SNMP community. When you select *Create New*, the *New SNMP Community* page opens. See Create or edit an SNMP community on page 931.
Edit	Modifies settings within an SNMP community. When you click *Edit*, the *Edit SNMP Community* page opens.
Delete	Removes an SNMP community from the list. To remove multiple SNMP communities, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Status	Enable or disable the SNMP community.
Community Name	The name of the community.
Queries	Indicates whether queries protocols (v1 and v2c) are enabled or disabled. A check mark indicates that queries are enabled; a gray x indicates that queries are disabled. If one query is disabled and another one enabled, there will still be a check mark.
Traps	Indicates whether trap protocols (v1 and v2c) are enabled or disabled. A check mark indicates that traps are enabled; a gray x indicates that traps are disabled. If one query is disabled and another one enabled, there will still be a check mark.
Hosts	Number of hosts that are part of the SNMP community.
Events	Number of events that have occurred.
Status	Indicates whether the SNMP community is enabled or disabled.
SNMP v3	Lists the SNMP v3 users. From within this section, you can edit, create or remove an SNMP v3 user.
Create New	Creates a new SNMP v3 user. When you select *Create New*, the *Create New SNMP User* page opens. See Create or edit an SNMP user on page 934.
Edit	Modifies settings within the SNMP v3 user. When you click *Edit*, the *Edit SNMP User* page opens.
Delete	Removes an SNMP v3 user from the page. To remove multiple SNMP v3 users, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Status	Enable or disable the SNMP v3 user.

User Name	The name of the SNMP v3 user.
Security Level	The security level of the user.
Queries	Indicates whether queries are enabled or disabled. A green check mark indicates that queries are enabled; a gray x indicates that queries are disabled.
Hosts	Number of hosts.
Events	Number of SNMP events associated with the SNMPv3 user.
Status	Indicates whether the SNMPv3 user is enabled or disabled.

Basic configuration

SNMP configuration has four steps that should be configured in order:

1. Configure interface access

   Before a remote SNMP manager can connect to the FortiProxy SNMP agent, you must configure one or more FortiProxy interfaces to accept SNMP connections.
2. Configure the SNMP agent

   The SNMP agent sends SNMP traps originating on the FortiProxy to an external monitoring SNMP manager defined in an SNMP community. The SNMP manager can monitor the FortiProxy system to determine if it is operating properly or if any critical events are occurring.

   The description, location, and contact information for this FortiProxy system will be part of the information that the SNMP manager receives. This information is useful if the SNMP manager is monitoring many devices, and enables faster responses when the FortiProxy system requires attention.
3. Configure SNMP v1/v2c communities

   An SNMP community is a grouping of equipment for network administration purposes. A single device can belong to multiple communities. It is not mandatory if SNMP v3 is configured.

   You must add an SNMP community to the FortiProxy so that the SNMP manager can receive traps and system information. Up to three communities can be added.
4. Configure SNMP v3 users

   Authentication is used to ensure the identity of users. Privacy allows for the encryption of SNMP v3 messages to ensure the confidentiality of data. These protocols provide a higher level of security than is available in SNMP v1/v2c, which use community strings for security. Both authentication and privacy are optional.

To configure SNMP in the GUI:

1. Configure interface access:
   a. Go to *Network* > *Interfaces* and edit an interface.
   b. In the *Administrative Access* options, enable *SNMP*.
   c. Click *OK*.
2. Configure the SNMP agent:

a. Go to *System > SNMP*.
b. Enable *SNMP Agent* and configure the following:

Description	A description of the agent.
Location	The location of the FortiProxy.
Contact Info	A contact or administrator for the SNMP agent or FortiProxy.

c. Click *Apply*.

3. Configure an SNMP v1/v2c community:
a. Go to *System > SNMP*.
b. In the *SNMP v1/v2c* table, click *Create New*.
c. Configure the following:

Community Name	The name of the community.
Hosts	Enter the *IP Address* and select the *Host Type* for each SNMP manager.
Queries	Enable or disable v1 and v2c queries, then enter the port numbers that the SNMP managers in this community use for them.
Traps	Enable or disable v1 and v2c traps, then enter the local and remote port numbers that the SNMP managers in this community use for them.
SNMP Events	Enable or disable the events that activate traps in this community.

d. Click *OK*.

4. Configure an SNMP v3 user:
a. Go to *System > SNMP*.
b. In the *SNMP v3* table, click *Create New*.
c. Configure the following:

User Name	The name of the user.
Security Level	Configure the security level: • *No Authentication*: No authentication or encryption. • *Authentication*: Select the authentication algorithm and password. • *Authentication and Private*: Select both the authentication and encryption algorithms and password.
Hosts	The *IP Address* for each SNMP manager.
Queries	Enable or disable queries, then enter the port number that the SNMP managers use for them.
Traps	Enable or disable traps, then enter the local and remote port numbers that the SNMP managers use for them

SNMP Events	Enable or disable the events that activate traps.

d. Click *OK*.

To configure SNMP in the CLI:

1. Configure the Interface access:

```
config system interface
    edit <interface>
        append allowaccess snmp
        config ipv6
            append ip6-allowaccess snmp
        end
    next
end
```

2. Configure the SNMP agent:

```
config system snmp sysinfo
    set status enable
    set description <string>
    set contact-info <string>
    set location <string>
end
```

3. Configure an SNMP v1/v2c community:

```
config system snmp community
    edit <id>
        set name <string>
        set status {enable | disable}
        config hosts
            edit <host_id>
                set interface-select-method {auto | sdwan | specify}
                set ip <ip/mask>
                set source-ip <class_ip>
                set ha-direct {enable | disable}
                set host-type {any | query | trap}
            next
        end
        set query-v1-port <port_number>
        set query-v1-status {enable | disable}
        set query-v2c-port <port_number>
        set query-v2c-status {enable | disable}
        set trap-v1-lport <port_number>
        set trap-v1-rport <port_number>
        set trap-v1-status {enable | disable}
        set trap-v2c-lport <port_number>
        set trap-v2c-rport <port_number>
        set trap-v2c-status {enable | disable}
        set events <events>
```

```
    next
end
```

4. Configure an SNMP v3 user:

```
config system snmp user
    edit <user>
        set status {enable | disable}
        set trap-status {enable | disable}
        set trap-lport <port_number>
        set trap-rport <port_number>
        set queries {enable | disable}
        set query-port <port_number>
        set notify-hosts <class_ip> ... <class_ip>
        set source-ip <class_ip>
        set ha-direct {enable | disable}
        set interface-select-method {auto | sdwan | specify}
        set events <events>
        set security-level {no-auth-no-priv | auth-no-priv | auth-priv}
        set auth-proto {md5 | sha | sha224 | sha256 | sha384 | sha512}
        set auth-pwd <password>
        set priv-proto {aes | des | aes256 | aes256cisco}
        set priv-pwd <password>
    next
end
```

See SNMP examples on page 939 for sample configurations.

Fortinet MIBs

The FortiProxy SNMP agent supports Fortinet proprietary MIBs, as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiProxy unit configuration.

There are two MIB files for FortiProxy units; both files are required for proper SNMP data collection:

- The Fortinet MIB: contains traps, fields, and information that is common to all Fortinet products.
- The FortiProxy MIB: contains traps, fields, and information that is specific to FortiProxy units.

The Fortinet and FortiProxy MIB files are available for download on the Fortinet Customer Support site. Each Fortinet product has its own MIB—if you use other Fortinet products, you need to download their MIB files as well.

The Fortinet MIB and FortiProxy MIB, along with the two RFC MIBs, are listed in the table in this section.

To download the MIB files, go to *System* > *SNMP* and select a MIB link in the SNMP section. See SNMP on page 923.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database to have access to the Fortinet-specific information.



MIB files are updated for each version of FortiProxy. When upgrading the firmware, ensure that you update the Fortinet FortiProxy MIB file compiled in your SNMP manager as well.

MIB file name	Description
FORTINET-CORE-MIB.mib	The Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiProxy unit configuration settings and receive traps from the FortiProxy SNMP agent.
FORTINET-FORTIPROXY-MIB.mib	The FortiProxy MIB includes all system configuration information and trap information that is specific to FortiProxy units. Your SNMP manager requires this information to monitor FortiProxy configuration settings and receive traps from the FortiProxy SNMP agent. FortiManager systems require this MIB to monitor FortiProxy units.

SNMP get command syntax

Normally, to get configuration and status information for a FortiProxy unit, an SNMP manager would use an SNMP get command to get the information in a MIB field. The SNMP get command syntax would be similar to:

```
snmpget -v2c -c <community_name> <address_ipv4> {<OID> | <MIB_field>}
```

where:

- `<community_name>` refers to the SNMP community name added to the FortiProxy configuration. You can add more than one community name to a FortiProxy SNMP configuration. The most commonly used community name is `public`. For security reasons, Fortinet recommends that neither `public` nor `private` be used for SNMP community names.
- `<address_ipv4>` is the IP address of the FortiProxy interface that the SNMP manager connects to
- `{<OID> | <MIB_field>}` is the object identifier for the MIB field or the MIB field name itself.

For example, to query the firmware version running on the FortiProxy unit, the following command could be issued:

```
snmpget -v2c -c public 10.10.10.1 1.3.6.1.4.1.12356.109.4.1.1.0
```

In this example, the community name is `public`, the IP address of the interface configured for SNMP management access is `10.10.10.1`. The firmware version is queried using the MIB field `fchSysVersion`, the OID for which is `1.3.6.1.4.1.12356.109.4.1.1.0`.

The value returned is a string with a value of `v2.0,build0225,130213`.

SNMP agent

The FortiProxy SNMP agent must be enabled before configuring other SNMP options. Enter information about the FortiProxy unit to identify it so that when your SNMP manager receives traps from the FortiProxy unit, you will know which unit sent the information.

To configure the SNMP agent in the GUI:

1. Go to *System* > *SNMP*.
2. Enable the SNMP agent by moving the slider in the SNMP Agent field.
3. Enter a descriptive name for the agent. The description can be up to 35 characters long.
4. Enter the physical location of the unit. The system location description can be up to 35 characters long.
5. Enter the contact information for the person responsible for this FortiProxy unit. The contact information can be up to 35 characters.
6. Click *Apply* to save your changes.

To configure the SNMP agent with the CLI:

Enter the following CLI commands:

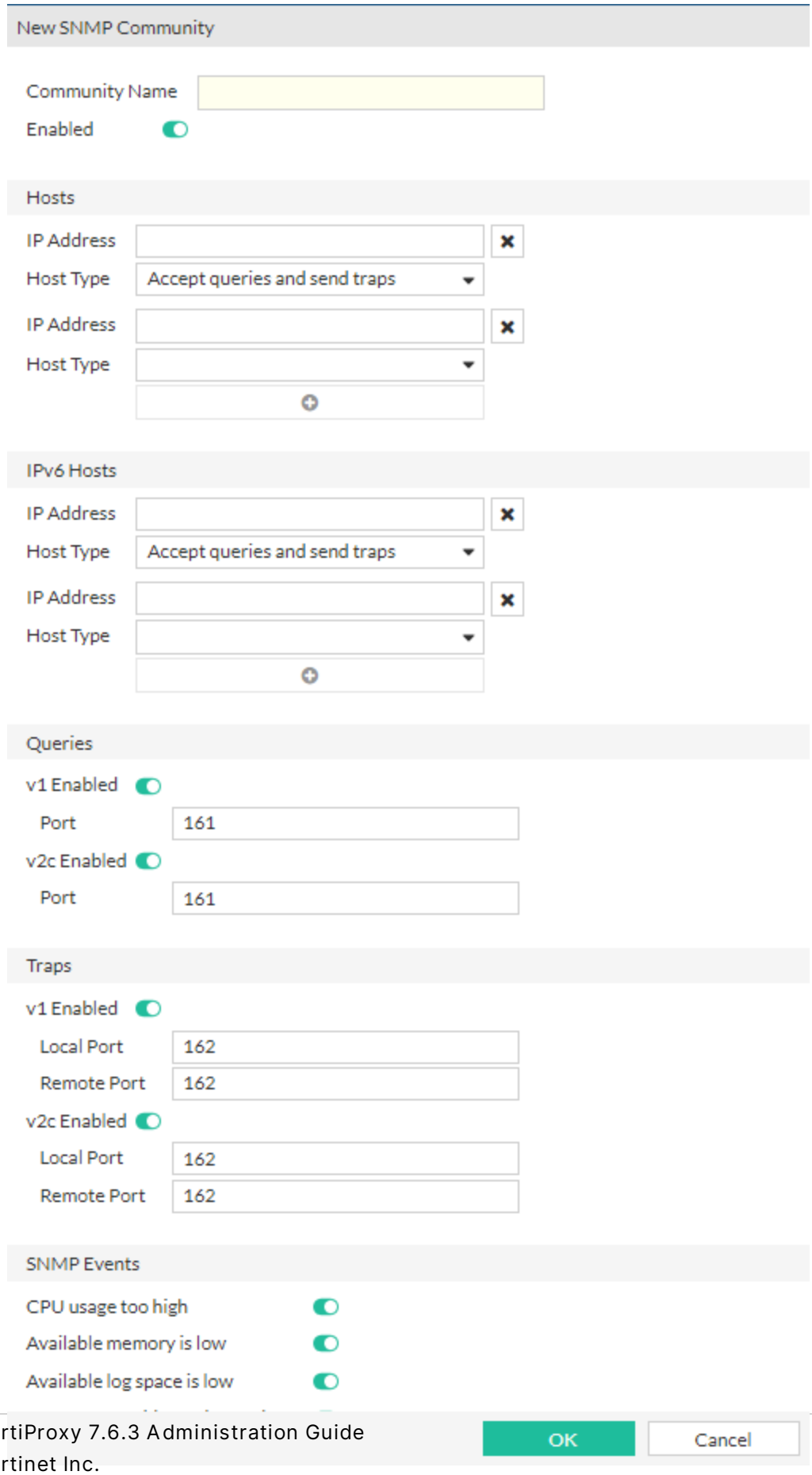
```
config system snmp sysinfo
   set status enable
   set contact-info <contact_information>
   set description <description_of_FortiProxy>
   set location <FortiProxy_location>
end
```

Create or edit an SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP and a printer SNMP community.

Add SNMP communities to your FortiProxy unit so that SNMP managers can view system information and receive SNMP traps. You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps and can be configured to monitor the FortiProxy unit for a different set of events. You can also add the IP addresses of up to eight SNMP managers to each community.

Selecting *Create New* on the *SNMP v1/v2c* table opens the *New SNMP Community* page, which provides settings for configuring a new SNMP community. Selecting a community from the list and selecting *Edit* opens the *Edit SNMP Community* page.


New SNMP Community
Community Name
Enabled
Hosts
IP Address
Host Type
Accept queries and send traps
IP Address
Host Type
IPv6 Hosts
IP Address
Host Type
Accept queries and send traps
IP Address
Host Type
Queries
v1 Enabled
Port
161
v2c Enabled
Port
161
Traps
v1 Enabled
Local Port
162
Remote Port
162
v2c Enabled
Local Port
162
Remote Port
162
SNMP Events
CPU usage too high
Available memory is low
Available log space is low
OK
Cancel

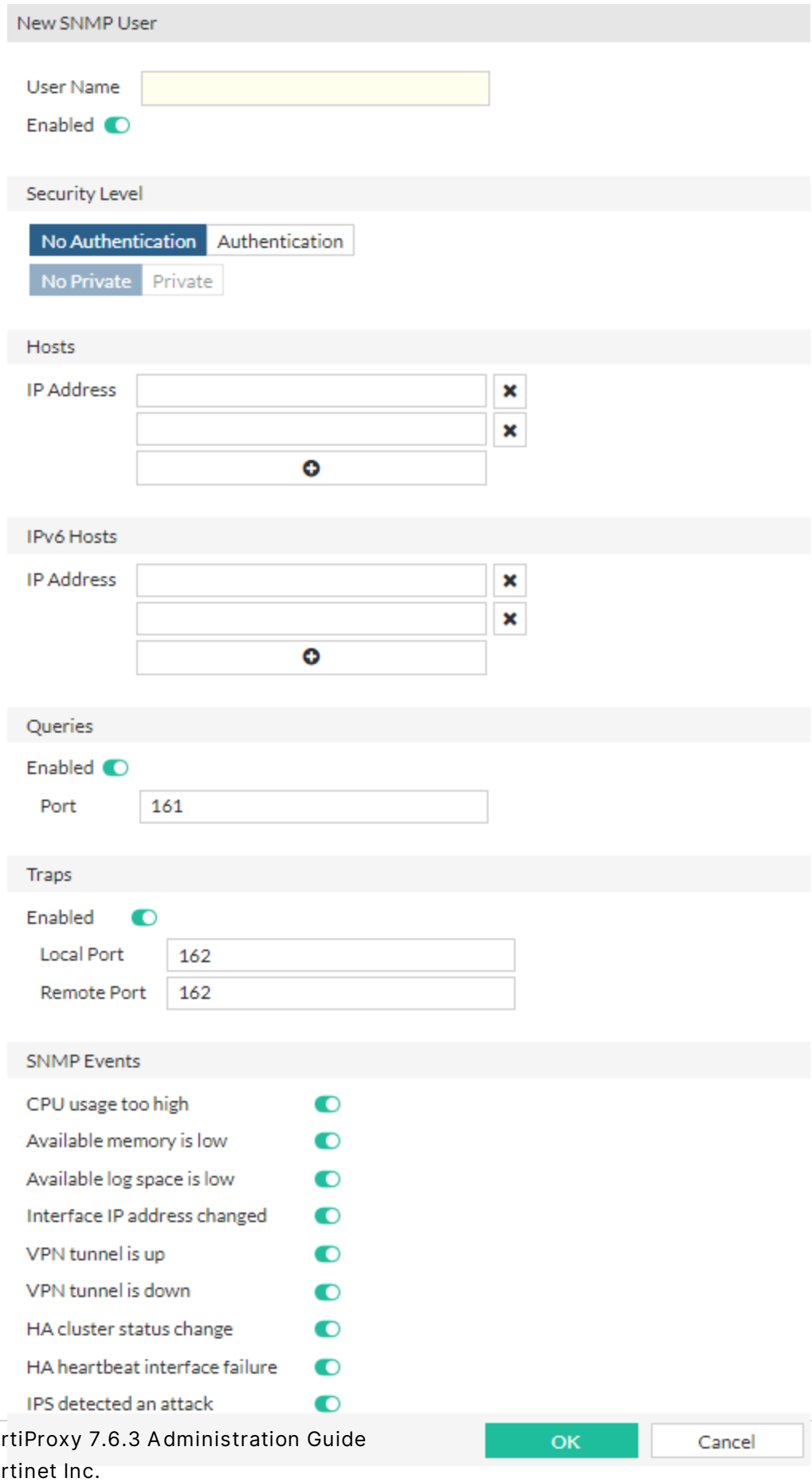
Configure the following settings in the New SNMP Community page or Edit SNMP Community page and click *OK*:

Community Name	Enter a name to identify the SNMP community. After you create the SNMP community, you cannot edit the name.
Enabled	Enable or disable the SNMP community.
Hosts	Settings for configuring the hosts of an SNMP community.
IP Address	Enter the IP address/netmask of the SNMP managers that can use the settings in this SNMP community to monitor the unit. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
Host Type	Select one of the following: *Accept queries and send traps*, *Accept queries only*, or *Send traps only*
X	Removes an SNMP manager from the list within the *Hosts* section.
+	Select to add a blank line to the Hosts list. You can add up to 16 SNMP managers to a single community.
Queries	Settings for configuring queries for both SNMP v1 and v2c.
v1 Enabled	Enable or disable SNMP v1 queries.
Port	Enter the port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the unit. The SNMP client software and the unit must use the same port for queries.
v2c Enabled	Enable or disable SNMP v2c queries.
Traps	Settings for configuring local and remote ports for both v1 and v2c.
v1 Enabled	Enable or disable SNMP v1 traps.
Local Port	Enter the remote port numbers (162 by default) that the unit uses to send SNMP v1 or SNMP v2c traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
Remote Port	Enter the remote port number (162 by default) that the unit uses to send SNMP traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
v2c Enabled	Enable or disable SNMP v2c traps.
SNMP Events	Enable each SNMP event for which the unit should send traps to the SNMP managers in this community.

Note: The *CPU usage too high* trap's sensitivity is slightly reduced by spreading values out over 8 polling cycles. This reduction prevents sharp spikes due to CPU intensive short-term events such as changing a policy.

Create or edit an SNMP user

Selecting *Create New* on the *SNMP v3* table opens the *New SNMP User* page, which provides settings for configuring a new SNMP v3 user. Selecting a user name from the route list and selecting *Edit* opens the *Edit SNMP User* page.


New SNMP User
User Name
Enabled
Security Level
No Authentication
Authentication
No Private
Private
Hosts
IP Address
IPv6 Hosts
IP Address
Queries
Enabled
Port
161
Traps
Enabled
Local Port
162
Remote Port
162
SNMP Events
CPU usage too high
Available memory is low
Available log space is low
Interface IP address changed
VPN tunnel is up
VPN tunnel is down
HA cluster status change
HA heartbeat interface failure
IPS detected an attack
OK
Cancel

Configure the following settings in the New SNMP User page or Edit SNMP User page and click *OK*:

User Name	Enter the name of the user. After you create an SNMP user, you cannot change the user name.
Enabled	Toggle the slider to enable or disable this SNMP user.
Security Level	Select the type of security level the user will have: • *No Authentication* • *Authentication* and *No Private*—Enter the authentication algorithm and password to use. • *Authentication* and *Private*—Enter the authentication algorithm and password to use.
Authentication Algorithm	If the security level is set to *Authentication* and *No Private*, you can select *MD5* or *SHA1* for the authentication algorithm. If the security level is set to *Authentication* and *Private*, you can select *AES*, *DES*, *AES256*, or *AES256 Cisco* for the authentication algorithm.
Password	If the security level is set to *Authentication*, select *Change* and enter a password in the *Password* field.
Hosts	Settings for configuring the hosts of an SNMP community.
IP Address	Enter the IP address of the notification host. If you want to add more than one host, select + to add another host. Up to 16 hosts can be added. Select *X* to delete any hosts.
Queries	Settings for configuring queries for both SNMP v1 and v2c.
Enabled	Enable or disable the query. By default, the query is enabled.
Port	Enter the port number in the *Port* field (161 by default).
SNMP Events	Select the SNMP events that will be associated with the user.

Important SNMP traps

Link Down and Link Up traps

This trap is sent when a FortiProxy port either goes down or is brought up.

For example, the following traps are generated when the state of port34 is set to down using `set status down`, and then brought up using `set status up`:

```
Oct 31 16:45:39 localhost snmptrapd[81079]: 2024-10-31 16:45:39 10.4.62.222 [10.4.62.222] (via
UDP: [10.4.62.222]:162->[10.4.62.181]:162) TRAP, SNMP v1, community test123#012#011SNMPv2-
MIB::snmpTraps Link Down Trap (0) Uptime: 1 day, 4:00:27.73#012#011IF-MIB::ifIndex.9 = INTEGER:
9#011IF-MIB::ifAdminStatus.9 = INTEGER: down(2)#011IF-MIB::ifOperStatus.9 = INTEGER: down
(2)#011SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FPXVULTM24000121"#011SNMPv2-
MIB::sysName.0 = STRING: FPX222#011IF-MIB::ifName.9 = STRING: port9#011IF-MIB::ifDescr.9 = STRING:
```

```
Oct 31 16:45:39 localhost snmptrapd[81079]: 2024-10-31 16:45:39 _gateway [UDP: [10.4.62.222]:162->
[10.4.62.181]:162]:#012DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (10082773) 1 day,
4:00:27.73#011SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown#011IF-MIB::ifIndex.9 = INTEGER:
9#011IF-MIB::ifAdminStatus.9 = INTEGER: down(2)#011IF-MIB::ifOperStatus.9 = INTEGER: down
(2)#011SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FPXVULTM24000121"#011SNMPv2-
MIB::sysName.0 = STRING: FPX222#011IF-MIB::ifName.9 = STRING: port9#011IF-MIB::ifDescr.9 = STRING:

Oct 31 16:45:41 localhost snmptrapd[81079]: 2024-10-31 16:45:41 10.4.62.222 [10.4.62.222] (via
UDP: [10.4.62.222]:162->[10.4.62.181]:162) TRAP, SNMP v1, community test123#012#011SNMPv2-
MIB::snmpTraps Link Up Trap (0) Uptime: 1 day, 4:00:30.03#012#011IF-MIB::ifIndex.9 = INTEGER:
9#011IF-MIB::ifAdminStatus.9 = INTEGER: up(1)#011IF-MIB::ifOperStatus.9 = INTEGER: up
(1)#011SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FPXVULTM24000121"#011SNMPv2-
MIB::sysName.0 = STRING: FPX222#011IF-MIB::ifName.9 = STRING: port9#011IF-MIB::ifDescr.9 = STRING:

Oct 31 16:45:41 localhost snmptrapd[81079]: 2024-10-31 16:45:41 _gateway [UDP: [10.4.62.222]:162->
[10.4.62.181]:162]:#012DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (10083004) 1 day,
4:00:30.04#011SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp#011IF-MIB::ifIndex.9 = INTEGER:
9#011IF-MIB::ifAdminStatus.9 = INTEGER: up(1)#011IF-MIB::ifOperStatus.9 = INTEGER: up
(1)#011SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FPXVULTM24000121"#011SNMPv2-
MIB::sysName.0 = STRING: FPX222#011IF-MIB::ifName.9 = STRING: port9#011IF-MIB::ifDescr.9 = STRING:
```

fgFmTrapIfChange trap

This trap is sent when any changes are detected on the interface. The change can be very simple, such as giving an IPV4 address.

For example, the user has given the IP address of 10.4.70.222/24 to port 10 and the EMS Manager has detected the following trap:

```
Oct 31 16:54:39 localhost snmptrapd[81079]: 2024-10-31 16:54:39 10.4.62.222 [10.4.62.222] (via
UDP: [10.4.62.222]:162->[10.4.62.181]:162) TRAP, SNMP v1, community test123#012#011SNMPv2-
SMI::enterprises.12356.101.1.10030 Enterprise Specific Trap (1004) Uptime: 1 day,
4:09:27.40#012#011SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FPXVULTM24000121"#011IF-
MIB::ifName.10 = STRING: port10#011SNMPv2-SMI::enterprises.12356.101.6.2.1.0 = IpAddress:
10.4.70.222#011SNMPv2-SMI::enterprises.12356.101.6.2.2.0 = IpAddress: 255.255.255.0#011SNMPv2-
SMI::enterprises.12356.101.6.2.3.0 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Memory usage traps

Both free memory usage and freeable memory of FortiProxy devices can be monitored through the Simple Network Management Protocol (SNMP). SNMP object identifier (OID) entries are available in Fortinet MIB files to show the percentage of free memory usage and freeable memory in an SNMP manager:

- `1.3.6.1.4.1.12356.101.4.1.36 .fgSysFreeMemUsage`
- `1.3.6.1.4.1.12356.101.4.1.37 .fgSysFreeableMemUsage`

The following commands are available to configure memory thresholds to trigger SNMP traps:

```
config system snmp sysinfo
    set trap-free-memory-threshold <integer>
    set trap-freeable-memory-threshold <integer>
end
```

`set trap-free-memory-threshold <integer>`	Use an integer from 1 to 100 (default 5) to identify what percentage of free memory usage will trigger an SNMP trap. SNMP traps are sent when the free memory is *lower* than the specified threshold. For example, the free memory threshold is set to 5, and SNMP traps are sent when free memory is lower than 5%.
`set trap-freeable-memory-threshold <integer>`	Use an integer from 1 to 100 (default 60) to identify what percentage of freeable memory will trigger an SNMP trap. SNMP traps are sent when the freeable memory is *higher* than the specified threshold. For example, the freeable memory threshold is set to 60, and SNMP traps are sent when freeable memory is higher than 60%.

Example

In this example, the SNMP agent is configured to monitor FortiProxy memory and send traps. The `trap-free-memory-threshold` is set to `50`, and the `trap-freeable-memory-threshold` is set to `10`. SNMP traps are triggered for both thresholds because:

- The free memory on the FortiProxy is 9%, which is lower than the threshold of 10.
- The freeable memory on the FortiProxy is 56%, which is higher than the threshold of 50.

To configure SNMP for monitoring memory usage on FortiProxies:

1. Configure the SNMP agent to monitor FortiProxy memory usage and freeable memory.
   In this example, the `trap-free-memory-threshold` is set to 10, and the `trap-freeable-memory-threshold` is set to 50.

   ```
   config system snmp sysinfo
       set status enable
       set description "FPX"
       set contact-info "FPXQA"
       set location "Burnaby"
       set trap-free-memory-threshold 10
       set trap-freeable-memory-threshold 50
   end
   ```

2. Verify that the SNMP manager can successfully query and receive a response on the current memory status of the FortiProxy.
   In the following example, the free memory on the FortiProxy is reported as 9%, and the freeable memory on the FortiProxy is reported as 56%.

   ```
   $ snmpwalk -v2c -c test123 10.4.62.222 1.3.6.1.4.1.12356.101.4.1.36
   FORTINET-CORE-MIB::fortinet.101.4.1.36.0 = Gauge32: 9
   ```

```
$ snmpwalk -v2c -c test123 10.4.62.222 1.3.6.1.4.1.12356.101.4.1.37
FORTINET-CORE-MIB::fortinet.101.4.1.37.0 = Gauge32: 56
```

3. Use the SNMP manager to monitor memory usage on the FortiProxy.
   Following is an example of the SNMP trap messages sent when thresholds are surpassed for freeable memory and free memory usage on FortiProxies:

```
Nov  6 14:58:51 localhost snmptrapd[81079]: 2024-11-06 14:58:51 _gateway [UDP:
[10.4.62.222]:162->[10.4.62.181]:162]:#012DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks:
(7854230) 21:49:02.30#011SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.12356.100.1.3.0.102#011SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING:
"FPXVULTM24000121"#011SNMPv2-MIB::sysName.0 = STRING: FPX222#011SNMPv2-
SMI::enterprises.12356.100.1.3.1.1 = STRING: "freeable memory percentage is too high"

Nov 6 13:59:13 localhost snmptrapd[81079]: 2024-11-06 13:59:13 _gateway [UDP:
[10.4.62.222]:162->[10.4.62.181]:162]:#012DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks:
(7496379) 20:49:23.79#011SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.12356.100.1.3.0.102#011SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING:
"FPXVULTM24000121"#011SNMPv2-MIB::sysName.0 = STRING: FPX222#011SNMPv2-
SMI::enterprises.12356.100.1.3.1.1 = STRING: "free memory percentage is too low"
```

SNMP examples

This topic includes examples that incorporate several SNMP settings:

- Example 1: SNMP traps for monitoring interface status using SNMP v3 user on page 939
- Example 2: SNMP traps and query for monitoring DHCP pool using SNMP v3 user on page 942

Example 1: SNMP traps for monitoring interface status using SNMP v3 user

This configuration enables the SNMP manager (10.4.62.181) to receive notifications when a FortiProxy port either goes down or is brought up. The SNMP manager can also query the current status of the FortiProxy port.

To configure SNMP for monitoring interface status in the GUI:

1. Configure interface access:
   a. Go to *Network* > *Interfaces* and edit *port4*.
   b. In the *Administrative Access* options, enable *SNMP*.
   c. Click *OK*.
2. Configure the SNMP agent:
   a. Go to *System* > *SNMP*.
   b. Enable *SNMP Agent* and enter the following:

Description	FPX
Location	Burnaby
Contact Info	FPXQA

c. Click *Apply*.

3. Configure an SNMP v3 user:
   a. Go to *System > SNMP*.
   b. In the *SNMP v3* table, click *Create New*.
   c. Configure the following:

User Name	test
Security Level	Authentication
Authentication Algorithm	SHA1
Password	*******
Hosts IP Address	10.4.62.181

   d. Click *OK*.

To configure SNMP for monitoring interface status in the CLI:

1. Configure interface access:

```
config system interface
    edit port4
        append allowaccess snmp
    next
end
```

2. Configure the SNMP agent:

```
config system snmp sysinfo
    set status enable
    set description FPX
    set contact-info FPXQA
    set location Burnaby
end
```

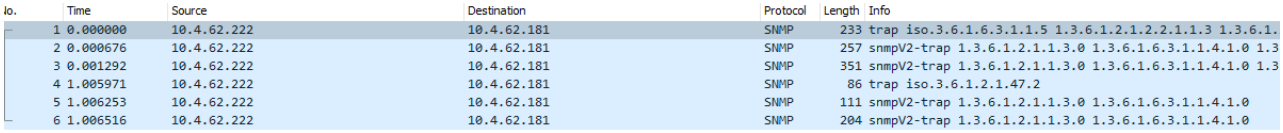
3. Configure an SNMP v3 user:

```
config system snmp user
    edit "test"
        set notify-hosts 10.4.62.181
        set events cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-hb-
failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented fm-if-change
fm-conf-change ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-oversize-
passed av-oversize-blocked ips-pkg-update ips-fail-open faz-disconnect faz load-balance-real-
server-down device-new per-cpu-high dhcp pool-usage cert-expiry
        set security-level auth-no-priv
```

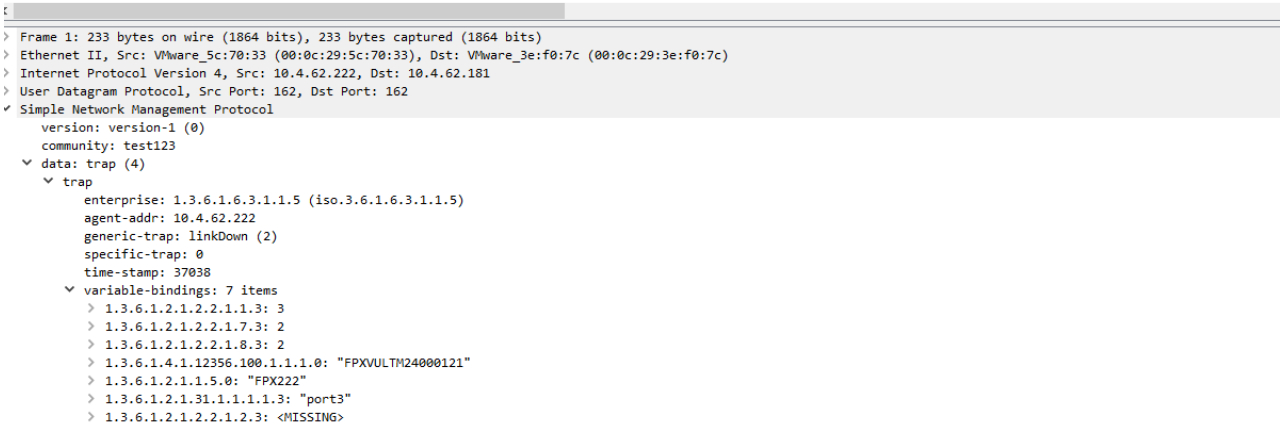
```
        set auth-pwd ENC  ********************
    next
end
    next
end
```

Verification

1. Start the packet capture on interface port4 with the filter set to port 162. See Diagnostics on page 218 for more information.
2. Turn off one of the FortiProxy interface statuses to down, in this case, port2.
3. Save the packet capture.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.4.62.222	10.4.62.181	SNMP	233	trap iso.3.6.1.6.3.1.1.5 1.3.6.1.2.1.2.2.1.1.3 1.3.6.1.
2	0.000676	10.4.62.222	10.4.62.181	SNMP	257	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3
3	0.001292	10.4.62.222	10.4.62.181	SNMP	351	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3
4	1.005971	10.4.62.222	10.4.62.181	SNMP	86	trap iso.3.6.1.2.1.47.2
5	1.006253	10.4.62.222	10.4.62.181	SNMP	111	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0
6	1.006516	10.4.62.222	10.4.62.181	SNMP	204	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0



```
> Frame 1: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits)
> Ethernet II, Src: VMware_5c:70:33 (00:0c:29:5c:70:33), Dst: VMware_3e:f0:7c (00:0c:29:3e:f0:7c)
> Internet Protocol Version 4, Src: 10.4.62.222, Dst: 10.4.62.181
> User Datagram Protocol, Src Port: 162, Dst Port: 162
v Simple Network Management Protocol
    version: version-1 (0)
    community: test123
  v data: trap (4)
    v trap
        enterprise: 1.3.6.1.6.3.1.1.5 (iso.3.6.1.6.3.1.1.5)
        agent-addr: 10.4.62.222
        generic-trap: linkDown (2)
        specific-trap: 0
        time-stamp: 37038
      v variable-bindings: 7 items
        > 1.3.6.1.2.1.2.2.1.1.3: 3
        > 1.3.6.1.2.1.2.2.1.7.3: 2
        > 1.3.6.1.2.1.2.2.1.8.3: 2
        > 1.3.6.1.4.1.12356.100.1.1.1.0: "FPXVULTM24000121"
        > 1.3.6.1.2.1.1.5.0: "FPX222"
        > 1.3.6.1.2.1.31.1.1.1.1.3: "port3"
        > 1.3.6.1.2.1.2.2.1.2.3: <MISSING>
```

   The SNMP v3 trap is transmitted from port4 to the SNMP manager. Note that `msgAuthenticationParameters` is configured, indicating that authentication is active. The absence of `msgPrivacyParameters` suggests that encryption is not configured. This is further confirmed by `plaintext` in `msgData`.
4. Verify that the SNMP manager has received the trap. See Important SNMP traps on page 936 for an example of a trap.
5. Verify that the SNMP manager can successfully query and receive receive a response on the current status of the FortiProxy ports:

```
$ snmpwalk -v3 -u test -l authNoPriv -a SHA -A xxxxxx 10.4.62.222 1.3.6.1.2.1.2.2.1.8
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: up(1)
IF-MIB::ifOperStatus.3 = INTEGER: down(2)
IF-MIB::ifOperStatus.4 = INTEGER: up(1)
IF-MIB::ifOperStatus.5 = INTEGER: up(1)
IF-MIB::ifOperStatus.6 = INTEGER: up(1)
```

Example 2: SNMP traps and query for monitoring DHCP pool using SNMP v3 user

This configuration enables the SNMP manager (10.4.62.181) to receive DHCP-related notifications from FortiProxy.

The SNMP DHCP event contains three traps and one query.

Traps are sent when:

- DHCP server IP pool usage reaches 90%
- DHCP server detect an IP address that is already in use
- DHCP client receives DHCP NAK

SNMP queries are accepted for DHCP lease usage information (OID = 1.3.6.1.4.1.12356.101.23). The query result is based on the leased out percentage.

To configure SNMP for monitoring DHCP pool in the GUI:

1. Configure interface access:
   a. Go to *Network* > *Interfaces* and edit *port4*.
   b. In the *Administrative Access* options, enable *SNMP*.
   c. Click *OK*.
2. Configure the SNMP agent:
   a. Go to *System* > *SNMP*.
   b. Enable *SNMP Agent* and enter the following:

Description	FPX
Location	Burnaby
Contact Info	FPXQA

   c. Click *Apply*.
3. Configure an SNMP v3 user:
   a. Go to *System* > *SNMP*.
   b. In the *SNMP v3* table, click *Create New*.
   c. Configure the following:

User Name	DHCP_Status
Security Level	Authentication
Authentication Algorithm	SHA384
Password	*******
Private	Enabled
Encryption Algorithm	AES256
Password	*******

Hosts IP Address	10.4.62.181

d. Click *OK*.

To configure SNMP for monitoring the DHCP pool in the CLI:

1. Configure interface access:

```
config system interface
    edit port4
        append allowaccess snmp
    next
end
```

2. Configure the SNMP agent:

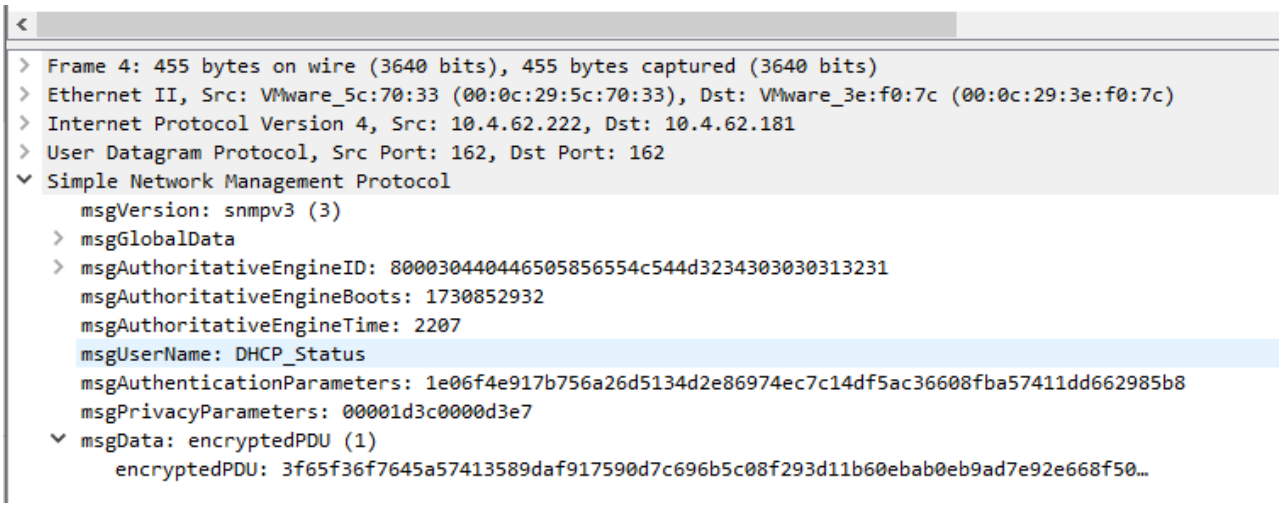
```
config system snmp sysinfo
    set status enable
    set description FPX
    set contact-info FPXQA
    set location Burnaby
end
```

3. Configure an SNMP v3 user:

```
config system snmp user
    edit "DHCP_Status"
        set notify-hosts 10.4.62.181
        set security-level auth-priv
        set auth-proto sha384
        set auth-pwd ********************
        set priv-proto aes256
        set priv-pwd **********************
    next
end
```

Verification

1. Start the packet capture on interface port4 with the filter set to port 162. See Diagnostics on page 218 for more information.
2. Overload the DHCP server IP pool.
3. Save the packet capture.



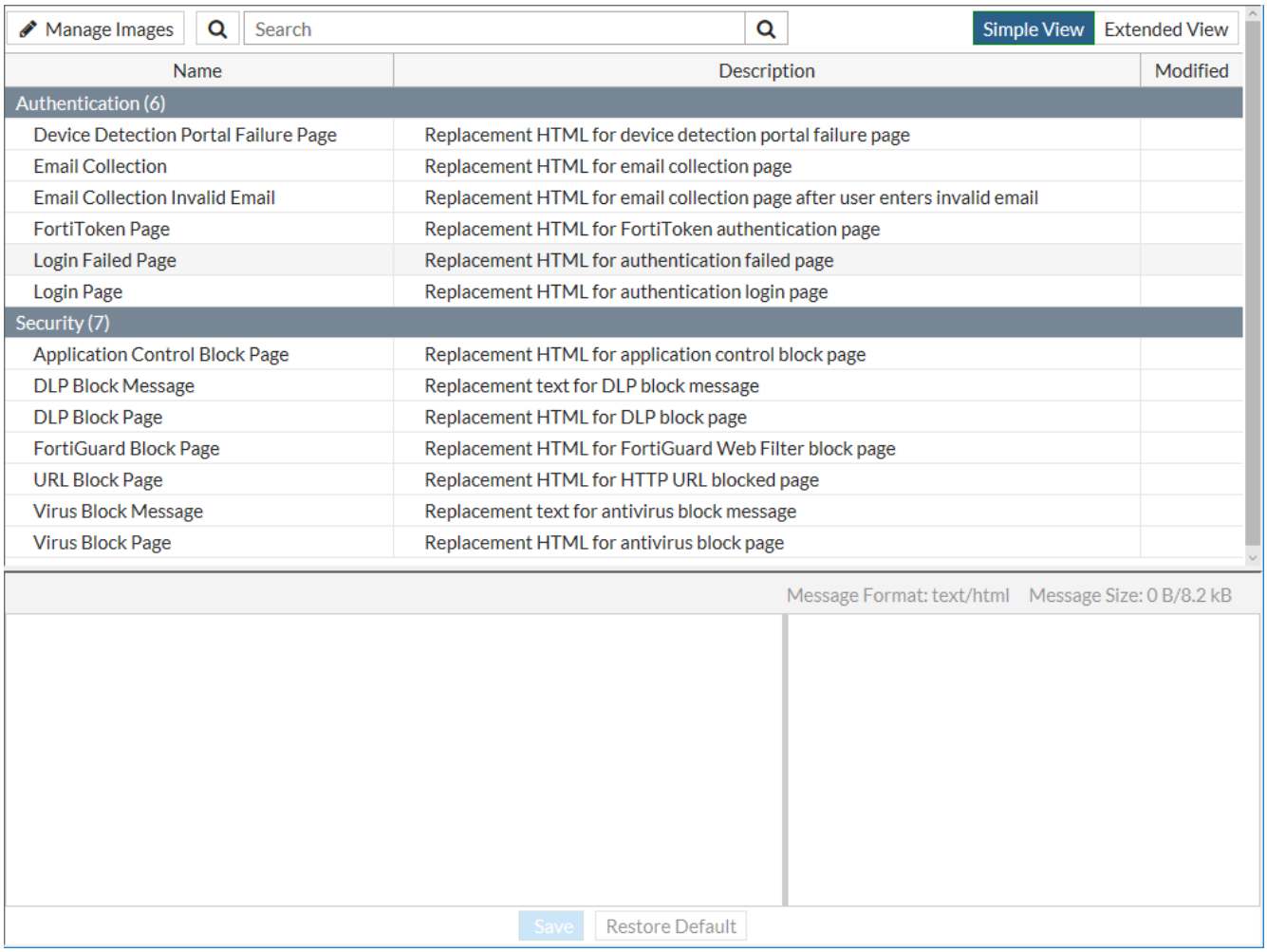
The SNMP v3 trap is transmitted from port4 to the SNMP manager. Note that both `msgAuthenticationParameters` and `msgPrivacyParameters` are set up, indicating that authentication and encryption are active. This is further confirmed by `encryptedPDU` in `msgData`.

4. Verify that the SNMP manager has received the trap. See Important SNMP traps on page 936 for an example of a trap.
5. Verify that the SNMP manager can successfully query and receive DHCP lease usage information for FortiProxy:

```
$ snmpwalk -v3 -u DHCP_Status  -l authPriv -a SHA384 -A xxxxxx -x AES256 -X xxxxxx 10.4.62.222
1.3.6.1.4.1.12356.101.23
SNMPv2-SMI::enterprises.12356.101.23.1.1.0 = INTEGER: 1
SNMPv2-SMI::enterprises.12356.101.23.2.1.1.2.1.1 = INTEGER: 100
```

Replacement Messages

Go to *System* > *Replacement Messages* to customize replacement pages as needed.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Manage Images	Select to view the available images and their respective tags and add new images. By default, images are embedded in replacement messages instead of using a URL.
	To use a URL:
	`config webfilter fortiguard`
	`  set embed-image disable`
	`end`

Search	Enter a search term to search the replacement message list.
Simple View or Extended View	Select the view: • *Simple View* displays a selection of *Security* and *Authentication* messages.

	• *Extended View* displays all messages. See the table at the end of this section for a list of all the messages.
Name	The message name.
Description	The message description.
Modified	A check mark is shown when the message has been modified.
Save	Save any customizations that you made to the message.
Restore Default	Restore the message back to its default state.
Preview	A preview of how the message looks.
Message HTML	The HTML code for the message that you can edit.

The following table outlines all of the messages that can be customized, as shown in *Extended View*:

Category	Messages	Description
Administrator	Post-login Disclaimer Message	Replacement message for post-login disclaimer.
	Pre-login Disclaimer Message	Replacement message for pre-login disclaimer.
Alert Email	alertmail-block	Alert email text for block incidents.
	alertmail-crit-event	Alert email text for critical event notification.
	alertmail-disk-full	Alert email text for disk-full events.
	alertmail-nids-event	Alert email text for IPS events.
	alertmail-virus	Alert email text for virus incidents.

Category	Messages	Description
Authentication	Authentication Rejection Page	Replacement HTML for authentication rejection page.

Category	Messages	Description
	Authentication Success Page	Replacement HTML for authentication success page.

Category	Messages	Description
	Block Notification Page	Replacement HTML for block notification page.

Category	Messages	Description
	Certificate Password Page	Replacement HTML for certificate password page.

Category	Messages	Description
	Declined Disclaimer Page	Replacement HTML for user declined disclaimer page.

Category	Messages	Description
	Declined Quarantine Page	Replacement HTML for user declined quarantine page.

Category	Messages	Description
	Disclaimer Page	Replacement HTML for authentication disclaimer page.

Category	Messages	Description
	Email Collection	Replacement HTML for email collection page.
	Email Collection Invalid Email	Replacement HTML for email collection page after user enters invalid email.
	Email Token Page	Replacement HTML for email-token authentication page.
	FortiToken Page	Replacement HTML for FortiToken authentication page.
	Guest User Email Template	Replacement text for guest-user credentials email message.
	Guest User Print Template	Replacement HTML for guest-user credentials print out.
	Keepalive Page	Replacement HTML for authentication keep-alive page.
	Login Challenge Page	Replacement HTML for authentication login-challenge page.
	Login Failed Page	Replacement HTML for authentication failed page.
	Login Page	Replacement HTML for authentication login page.
	Next FortiToken Page	Replacement HTML for next FortiToken authentication page.
	Password Expiration Page	Replacement HTML for password expiration page.
	Portal Page	Replacement HTML for post-authentication portal page.
	Quarantine Notification Page	Replacement HTML for quarantine notification page.
	SAML Login Page	Replacement HTML for SAML authentication login page.
	SMS Token Page	Replacement HTML for SMS-token authentication page.
	Success Message	Replacement text for authentication success message.
	Two-Factor Login Failed	Replacement HTML for two-factor authentication failed page.
	Two-Factor Login Page	Replacement HTML for two-factor authentication login page.
Automation	Automation Alert Email	Replacement HTML for automation alert email.

Category	Messages	Description
Device Detection Portal	Device Detection Portal Failure Page	Replacement HTML for device detection portal failure page.
Email	AV Engine Load Error Email Block Message	Replacement text for email blocked because the antivirus engine failed. to load.
	Email Decompressed Attachment Oversize Block Message	Replacement text indicating the removal of an oversized decompressed attachment from email.
	Email DLP Ban	Replacement text for emails blocked due to data leak detection.
	Email DLP Subject	Replacement text for subject of emails blocked due to data leak detection.
	Email File Block Message	Replacement text for message indicating removal of blocked attachment from email.
	Email File Size Block Message	Replacement text for message indicating removal of oversized attachment from email.
	Partial Email Block Message	Replacement text for emails rejected because they are fragmented.
	SMTP Decompressed Attachment Oversize Block Message	SMTP rejection text indicating rejection due to an oversized decompressed attachment.
	SMTP File Block Message	Replacement text for emails rejected due to blocked attachments.
	SMTP File Size Message	Replacement text for emails rejected due to file size limit.
FortiGuard Web Filtering	FortiGuard Block Page	Replacement HTML for FortiGuard web filter block page.
	FortiGuard HTTP Error Page	Replacement HTML for FortiGuard web filter HTTP error page.
	FortiGuard Override Page	Replacement HTML for FortiGuard web filter override page.
	FortiGuard Quota Page	Replacement HTML for FortiGuard web filter quota exceeded block page.
	FortiGuard Warning Page	Replacement HTML for FortiGuard web filter warning page.

Category	Messages	Description
FTP	Archive Block Message	Replacement text for FTP archive file block message.
	AV Engine Load Error Block Message	Replacement text for FTP blocked because the antivirus engine failed to load.
	Block Message	Replacement text for FTP permission-denied block message.
	DLP Ban Message	Replacement text for FTP data-leak detected ban message.
	Explicit Banner Message	Replacement text for explicit FTP proxy banner message.
	File Size Block Message	Replacement text for FTP oversized file block message.

Category	Messages	Description
HTTP	AntiPhish Block Message	Replacement HTML for AntiPhish credential block message.
	Archive Block Message	Replacement HTML for HTTP archive block message.
	Block Message	Replacement HTML for HTTP file block message.
	Blocked Certificate Message	Replacement HTML for blocked certificate message.
	Content Block Message	Replacement HTML for HTTP content-type block message.
	Content Block Page	Replacement HTML for HTTP file content block page.
	Content Upload Block Page	Replacement HTML for HTTP file upload content block page.
	DLP Ban Message	Replacement HTML for HTTP data-leak detected ban message.
	Invalid Certificate Message	Replacement HTML for HTTP invalid certificate message.
	Oversized File Message	Replacement HTML for HTTP oversized file block message.
	Oversized Upload Message	Replacement HTML for HTTP oversized file upload block message.
	POST Block Message	Replacement HTML for HTTP POST block message.
	Previously Infected Block Page	Replacement HTML for HTTP URL previously infected block page.
	Switching Protocols Blocked	Replacement HTML for HTTP Switching Protocols Blocked page.
	Untrusted Certificate Message	Replacement HTML for untrusted certificate message.
	Upload Archive Block Message	Replacement HTML for HTTP archive upload block message.
	Upload Block Message	Replacement HTML for HTTP file upload block message.
	URL Block Page	Replacement HTML for HTTP URL blocked page.
	URL Filter Error Message	Replacement HTML for HTTP web filter service error message.

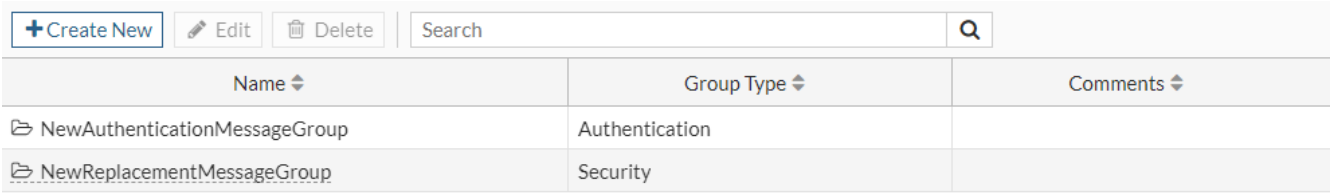
Category	Messages	Description
ICAP	icap-req-resp	Replacement HTML for HTTP POST action block message.
	ICAP REQMOD Response	Replacement message for ICAP REQMOD Response.
	icap-server-service	Replacement HTML for HTTP service action block message.
Network Quarantine	Network Quarantine Administrative Block Page	Replacement HTML for network quarantine administrative block page.
	Network Quarantine Application Block Page	Replacement HTML for network quarantine application block page.
	Network Quarantine AV Block Page	Replacement HTML for network quarantine antivirus block page.
	Network Quarantine DLP Block Page	Replacement HTML for network quarantine DLP block page.
	Network Quarantine DOS Block Page	Replacement HTML for network quarantine DOS block page.
	Network Quarantine IPS Block Page	Replacement HTML for network quarantine IPS block page.
NNTP	NNTP AV Engine Load Error Block Message	Replacement text for NNTP article blocked because the antivirus engine failed to load.
	NNTP Decompressed File Oversize Block Message	Replacement text indicating the removal of an oversized decompressed file.
	NNTP DLP Ban Message	Replacement text for NNTP user banned by data loss prevention.
	NNTP DLP Block Message	Replacement text for body of NNTP message blocked by data loss prevention.
	NNTP DLP Block Subject	Replacement text for subject of NNTP message blocked by data loss prevention.
	NNTP File Size Block Message	Replacement text for NNTP article too large block message.

Category	Messages	Description
Security	Application Control Block Page	Replacement HTML for Application Control block page.
	DLP Block Message	Replacement text for DLP block message.
	DLP Block Page	Replacement HTML for DLP block page.
	IPS Scan Failure Block Page	Replacement HTML for IPS scan failure block page.
	IPS Sensor Block Page	Replacement HTML for IPS sensor block page.
	Virus Block Message	Replacement text for antivirus block message.
	Virus Block Page	Replacement HTML for antivirus block page.
	Virus Upload Block Page	Replacement HTML for virus infected file upload block page.
	Web Application Firewall Block Page	Replacement HTML for web application firewall block page.
	Windows Executable Block Page	Replacement text for blocked Windows executables.
Spam	ASE Block Message	Replacement text for emails blocked due to detection by Advanced Antispam Engine (ASE).
	Banned Word Block Message	Replacement text for emails blocked due to prohibited content (banned words) in message.
	DNSBL Block Message	Replacement text for emails blocked due to detection by antispam DNSBL.
	False-Positive Submit Message	Replacement text for email submit message as false-positive message.
	FortiGuard Block Message	Replacement text for emails blocked due to IP blacklist by FortiGuard.
	HELO Block Message	Replacement text for emails blocked due to HELO check.
	IP Blacklist Message	Replacement text for emails blocked due to blacklisted sending IP addresses.
	MIME Header Block Message	Replacement text for emails blocked due to invalid MIME header.
	Reverse DNS Block Message	Replacement text for emails blocked due to invalid return domain.
	Sender Address Block Message	Replacement text for emails blocked due to blacklisted sender address.

Category	Messages	Description
Traffic Quota	Traffic Quota Limit Exceeded Page	Replacement HTML for traffic quota limit exceeded block page.
Web-proxy	Web-proxy Authentication Failed Page	Replacement HTML for web-proxy authentication failed page.
	Web-proxy Authorization Failed Page	Replacement HTML for web-proxy authorization failed page.
	Web-proxy Block Page	Replacement HTML for web-proxy block page.
	Web-proxy Challenge Page	Replacement HTML for web-proxy authentication required block page.
	Web-proxy HTTP Error Page	Replacement HTML for web-proxy HTTP error page.
	Web-proxy IP Blackout Page	Replacement HTML for web-proxy IP Blackout page.
	Web-proxy User Limit Page	Replacement HTML for web-proxy user limit block page.
	Web-proxy ZTNA block page	Replacement HTML for web-proxy ZTNA block page.

Replacement Message Groups

Go to *System* > *Replacement Message Groups* to configure custom replacement message groups.



To create a custom replacement message group in the GUI:

1. Click *Create New*.
2. In the *Name* field, enter a name for the custom replacement message group.
3. In the *Comments* field, enter an optional description of the custom replacement message group.
4. Select *Security* or *Authentication*.
5. Click *OK*.

To create a custom replacement message group in the CLI:

```
config system replacemsg-group
    edit <name>
        set comment <string>
        set group-type {utm | auth}
        config {webproxy | auth}
            edit <msg-type>
                set buffer <string>
                set header {none | http | 8bit}
                set format {none | text | html}
            next
        end
    next
end
```

Custom ZTNA virtual host replacement message

Custom messages can be configured for each ZTNA virtual host, to be shown when verification fails. The ZTNA detail tag (%%ZTNA_DETAIL_TAG%%) can be included to show the reason for the verification failure.

To use a custom replacement message:

1. Configure a replacement message group that includes the ZTNA detail tag in the message:

```
config system replacemsg-group
    edit "test-vhost"
        set comment ''
        set group-type utm
        config webproxy
            edit "ztna-block"
                set buffer "This is a test message: %%ZTNA_DETAIL_TAG%%"
                set header http
                set format html
            next
        end
    next
end
```

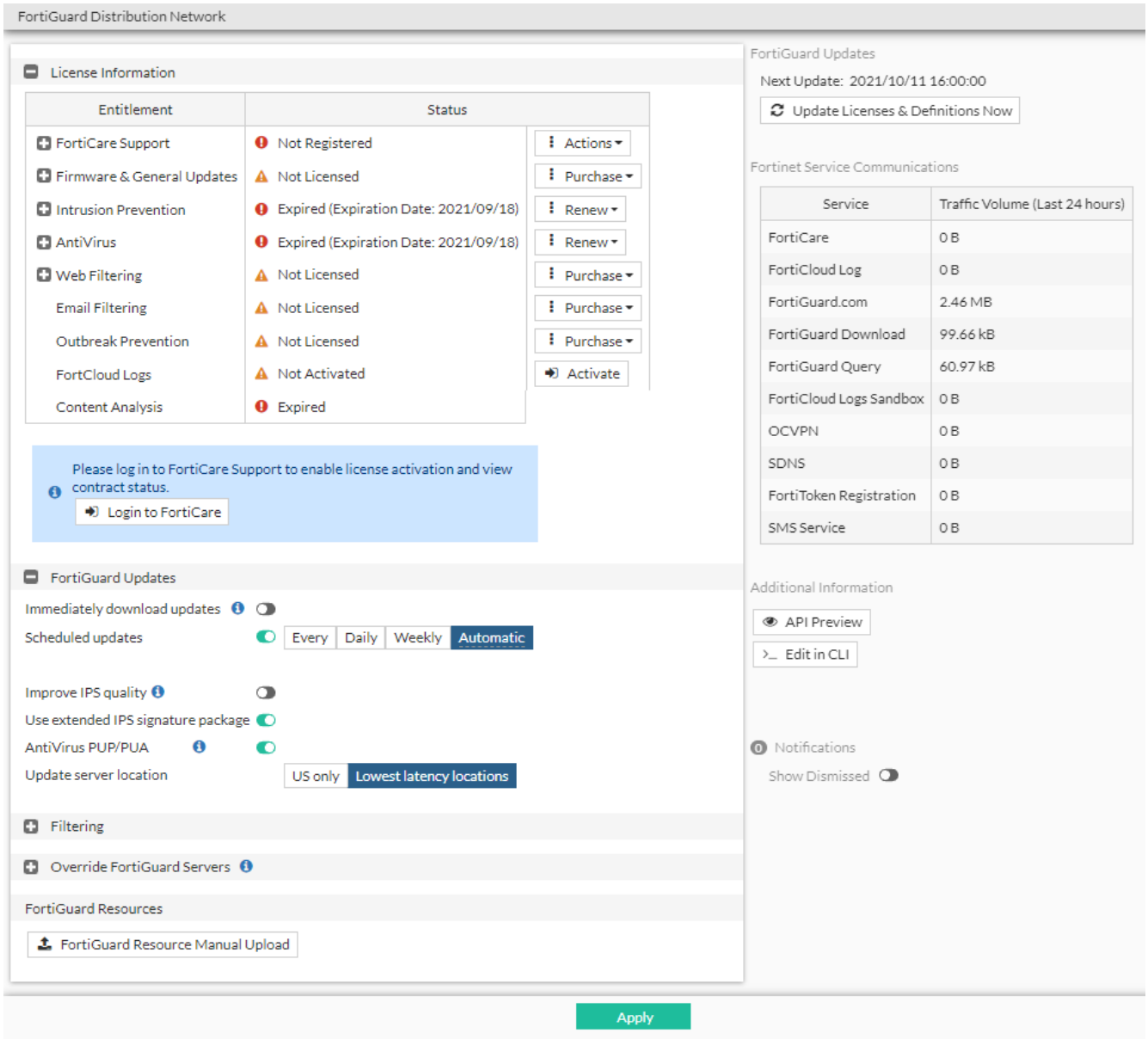
2. Apply the replacement message group to a virtual host:

```
config firewall access-proxy-virtual-host
    edit "test"
        set host "10.1.200.102"
        set replacemsg-group "test-vhost"
    next
end
```

FortiGuard

The *FortiGuard Distribution Network* page provides information and configuration settings for FortiGuard subscription services. For more information about FortiGuard services, see FortiGuard Labs.

To view and configure FortiGuard connections, go to *System* > *FortiGuard*.



Configure the following settings and select *Apply*:

FortiCare Support	The availability or status of your unit's support contract. The status can be *Unreachable*, *Not Registered*, or *Valid Contract*. Select *Launch Portal* to log in to FortiCloud. You can update your registration status by selecting *Register* and loading the license file from a location on your management computer.
Application Control Signatures	Application Control is a free FortiGuard service. Application Control allows you to identify and control applications on networks and endpoints regardless of port, protocol, and IP address used. It gives you unmatched visibility and control over application traffic, even traffic from unknown applications and sources. Although the Application Control profile can be used for free, signature database updates require a valid FortiGuard subscription. To update the database of Application Control signatures, select *Upgrade Database*.
IPS	The FortiGuard Intrusion Prevention System (IPS) uses a customizable database of more than 4000 known threats to stop attacks that evade conventional firewall defenses. It also provides behavior-based heuristics, enabling the system to recognize threats when no signature has yet been developed. It also provides more than 1000 application identity signatures for complete Application Control. To update the IPS database, select *Upgrade Database*.
AntiVirus	The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and protects against vulnerabilities. To update the antivirus database, select *Upgrade Database*.
Industrial DB	The FortiGuard Industrial Security Service provides in-line protection and proactive filtering of malicious and unauthorized network traffic; it enforces security policies tailored to industrial environments, protocols, and equipment. To update the industrial database, select *Upgrade Database*.
Web Filtering	Web Filtering provides Web URL filtering to block access to harmful, inappropriate, and dangerous web sites that may contain phishing/pharming attacks, malware such as spyware, or objectionable content that can expose your organization to legal liability. Based on automatic research tools and targeted research analysis, real-time updates enable you to apply highly-granular policies that filter web access based on 78 web content categories, over 45 million rated web sites, and more than two billion web pages—all continuously updated.
Virtual Machine	To upload or check your virtual machine license, select *FortiProxy VM License*.

Content Analysis	FortiGuard Content Analysis Service is a licensed feature for the real-time analysis of images to detect adult content. Detection of adult content in images uses various patented techniques (not just color-based), including limb and body part detection, body position, and so on. When adult content is detected, such content can be optionally blocked or reported.
Antivirus & IPS Updates	
Accept push updates	Enable to allow updates sent automatically to your FortiProxy. New definitions are added as soon as they are released by FortiGuard. If a specific override push IP address is required, select *Use override push IP* and enter an IP address and port number in the required fields.
Use override push	This option is available only when *Accept push updates* is enabled. Enable to configure an override server if you cannot connect to the FDN or if your organization provides updates using their own FortiGuard server. Enter the IP address and port of the NAT device in front of your FortiProxy. FDN connects to this device when attempting to reach the FortiProxy. The NAT device must be configured to forward the FDN traffic to the FortiProxy unit on UDP port 9443.
Scheduled Updates	Enable to receive scheduled updates and then select when the updates occur: *Every* 1-23 hours, *Daily* at a specific hour, or *Weekly* on a specific day at a specific hour.
Improve IPS quality	Enable to help Fortinet maintain and improve IPS signatures. The information sent to the FortiGuard servers when an attack occurs and can be used to keep the database current as variants of attacks evolve.
Use extended IPS signature package	Some models have access to an extended IPS database.
Update AV & IPS Definitions	Select to manually initiate an FDN update.
Update Server Location	
US only/Lowest latency locations	Select whether to access FortiGuard servers within the United States or the quickest FortiGuard servers.
Filtering	
Web Filter Cache	Enable the web filter cache. Enter the number of minutes the FortiProxy unit stores blocked IP addresses or URLs locally, saving time and network access traffic by not checking the FortiGuard server. After the specified time, the FortiProxy unit contacts the FDN server to verify a web address.
Clear Web Filter Cache	Select to manually delete the contents of the web filter cache.

FortiGuard Filtering Protocol	Select the protocol to use to contact the FortiGuard servers, either *HTTPS* or *UDP*.
FortiGuard Filtering Port	Select the port assignments for contacting the FortiGuard servers, either the default port (53) or the alternate port (8888).
Filtering Services Availability	Indicates the status of filtering service. Select *Check Again* if the filtering service is not available and then click *OK* in the confirmation dialog box. A warning is displayed if the FortiProxy unit does not have a valid license.
Request re-evaluation of a URL's category	Select to re-evaluate a URL's category rating using the Fortinet Live URL Rating Support (opens in a new browser window).
Override FortiGuard Servers	By default, the FortiProxy unit updates signature packages and queries rating servers using public FortiGuard servers. You can override this list of servers. You can also disable communication with public FortiGuard servers.
Create New	Select to display the *Create New Override FortiGuard Server* page.
Edit	Select a server in the list and click *Edit* to display the *Edit Override FortiGuard Server* page.
Delete	Select a server in the list and select *Delete* to remove one of the servers in the list. To remove multiple servers, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.

Setting automatic updates for FortiGuard packages

The default auto-update schedule for FortiGuard packages has been updated. Previously, the frequency was a reoccurring random interval within two hours. You can select an update frequency of `automatic`, and the update interval is calculated based on the model and percentage of valid subscriptions. The update interval is within one hour.

```
config system autoupdate schedule
    set frequency {every | daily | weekly | automatic}
end
```

FortiGuard Outbreak Prevention

FortiGuard Virus Outbreak Protection Service (VOS) allows the FortiProxy antivirus database to be subsidized with third-party malware hash signatures curated by FortiGuard. The hash signatures are obtained from FortiGuard's Global Threat Intelligence database. The antivirus database queries FortiGuard with the hash of a scanned file. If FortiGuard returns a match, the scanned file is deemed to be malicious. Enabling the AV engine scan is not required to use this feature.

NOTE: The FortiProxy unit must be registered with a valid FortiGuard outbreak prevention license.

To verify FortiGuard antivirus license information:

Go to *System > FortiGuard* and locate the *Outbreak Prevention* section in the *License Information* table.

To enable FortiGuard outbreak prevention:

1. Go to *Security Profiles > AntiVirus*.
2. Edit an antivirus profile or create a new one.
3. Under *Outbreak Protection*, enable *Block* or *Monitor* for each protocol.
4. Click *OK*.

Antiphish pattern database

To update the antiphish pattern database:

1. Go to *System > FortiGuard* and in the right-side pane, click *Update Licenses & Definitions Now*.
2. Enter the following in the CLI:

```
# diagnose autoupdate versions
...
AntiPhish Pattern DB
---------
Version: 0.00000
Contract Expiry Date: n/a
Last Updated using manual update on Tue Nov 30 00:00:00 1999
Last Update Attempt: Wed Sep 29 14:00:11 2021
Result: No Updates
```

Licensing in air-gap environments

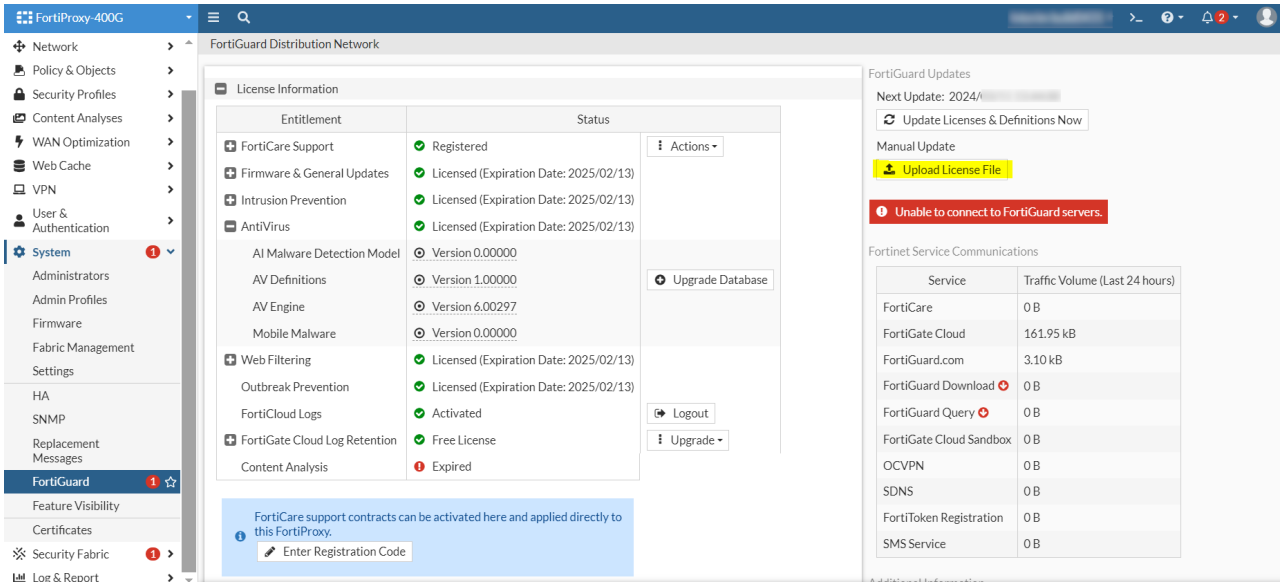
In the Operational Technology industry, industrial equipment is critical and must not be connected to the Internet. However, the equipment is still required to be protected by a firewall in this air-gap environment. Without a gateway to FortiGuard in air-gap environments, FortiGuard packages, such as AntiVirus and IPS, must be manually uploaded to the FortiProxy. FortiProxy licenses can be downloaded from FortiCloud and uploaded manually to the FortiProxy.

To manually upload FortiProxy licenses in the GUI:

1. Register the FortiGuard license on FortiCloud. See FortiCloud documentation for more information.
2. Download the product entitlement file in FortiCloud:
   a. Go to *Products > Product List*.
   b. Select the serial number of the FortiProxy. The product page opens.
   c. In the *License & Key* section, click *Get The License File*. The file downloads to your device in the format `FPX**********.lic`.
3. In FortiProxy, go to *System > FortiGuard*.

4. Click *Upload License File*. The file explorer opens.
5. Navigate to the product entitlement file and click *Open*.

   The license file uploads to the FortiProxy. Once the upload is complete, the FortiProxy shows that it is registered and licensed.



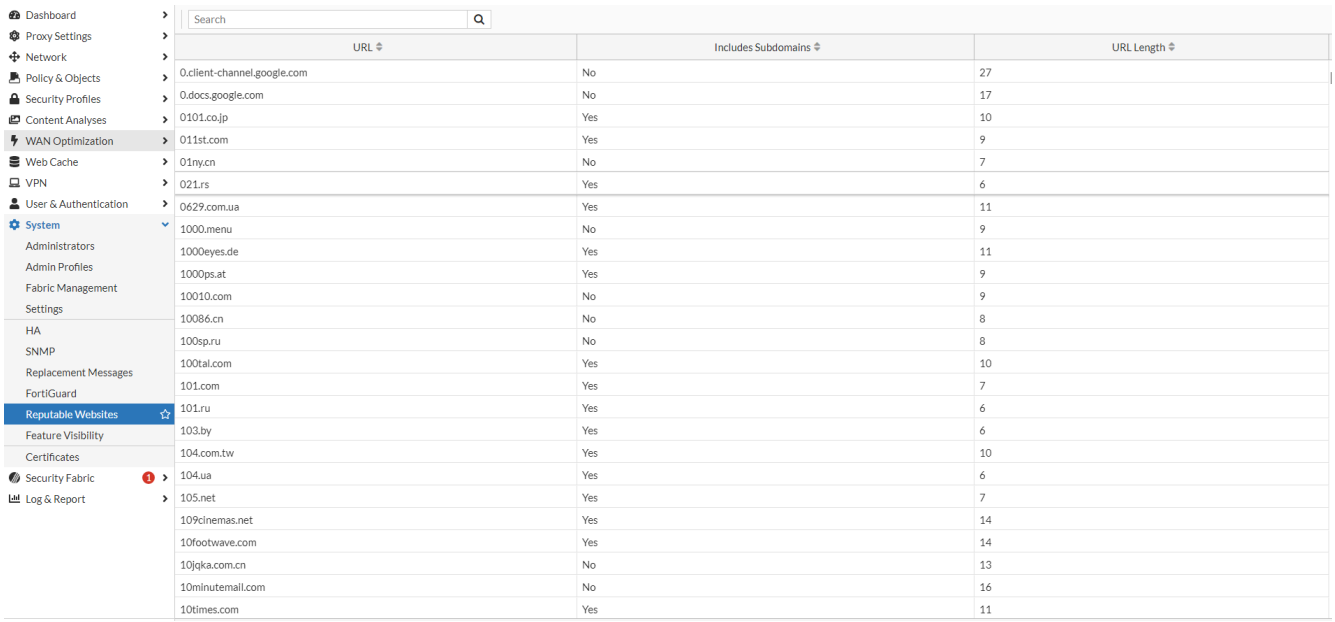
6. Click *Apply*.

To manually upload FortiProxy licenses in the CLI:

```
# execute restore manual-license {ftp | tftp} <license file name> <server> [args]
```

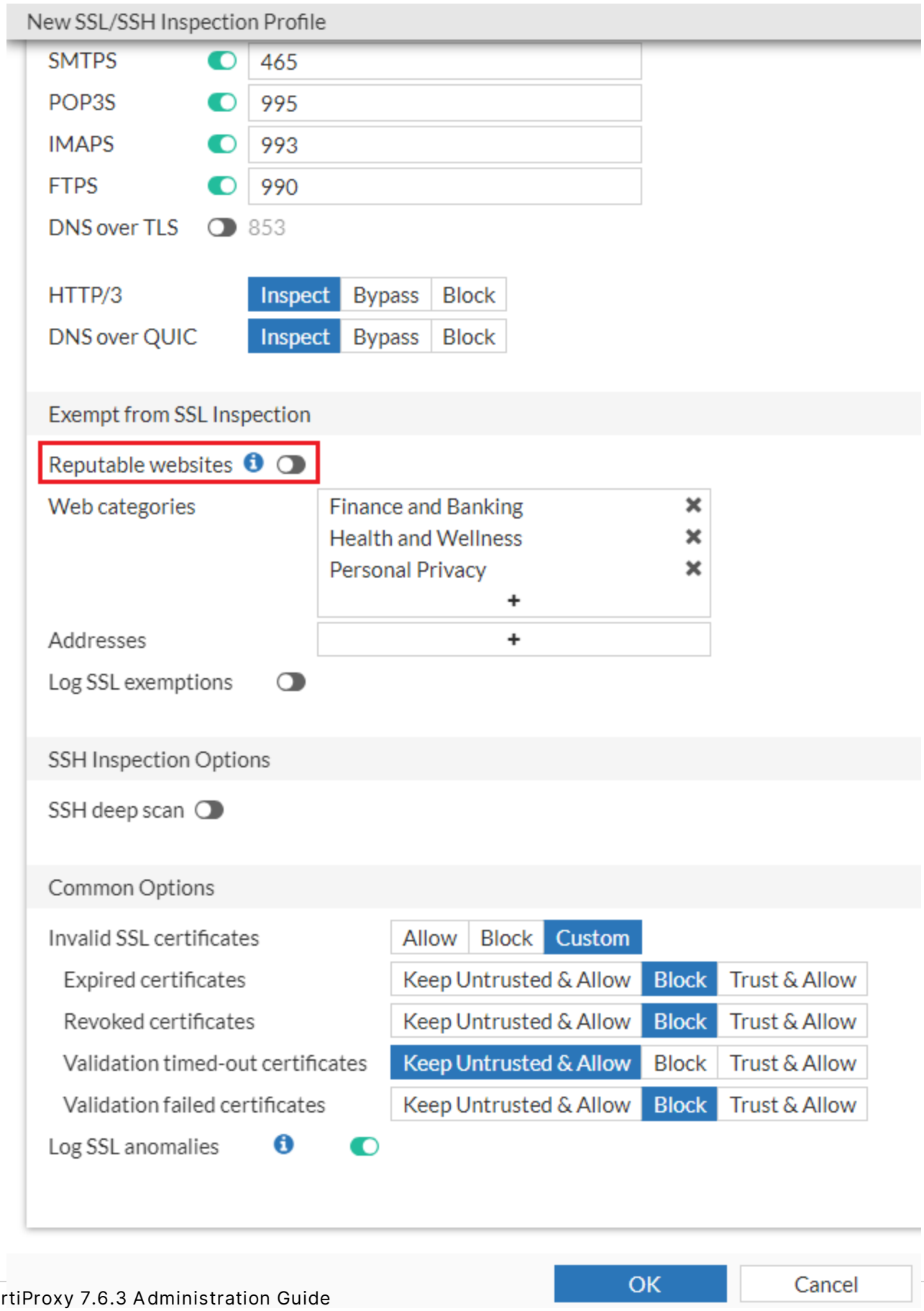
Reputable Websites

Use the *System* > *Reputable Websites* page to view the list of trusted URLs by FortiProxy. The list is synchronized from FortiGuard. You can search the list for an IP or domain.



URL	Includes Subdomains	URL Length
0.client-channel.google.com	No	27
0.docs.google.com	No	17
0101.co.jp	Yes	10
011st.com	Yes	9
01ny.cn	No	7
021.rs	Yes	6
0629.com.ua	Yes	11
1000.menu	No	9
1000eyes.de	Yes	11
1000ps.at	Yes	9
10010.com	No	9
10086.cn	No	8
100sp.ru	No	8
100tal.com	Yes	10
101.com	Yes	7
101.ru	Yes	6
103.by	Yes	6
104.com.tw	Yes	10
104.ua	Yes	6
105.net	Yes	7
109cinemas.net	Yes	14
10footwave.com	Yes	14
10jqka.com.cn	No	13
10minutemail.com	No	16
10times.com	Yes	11

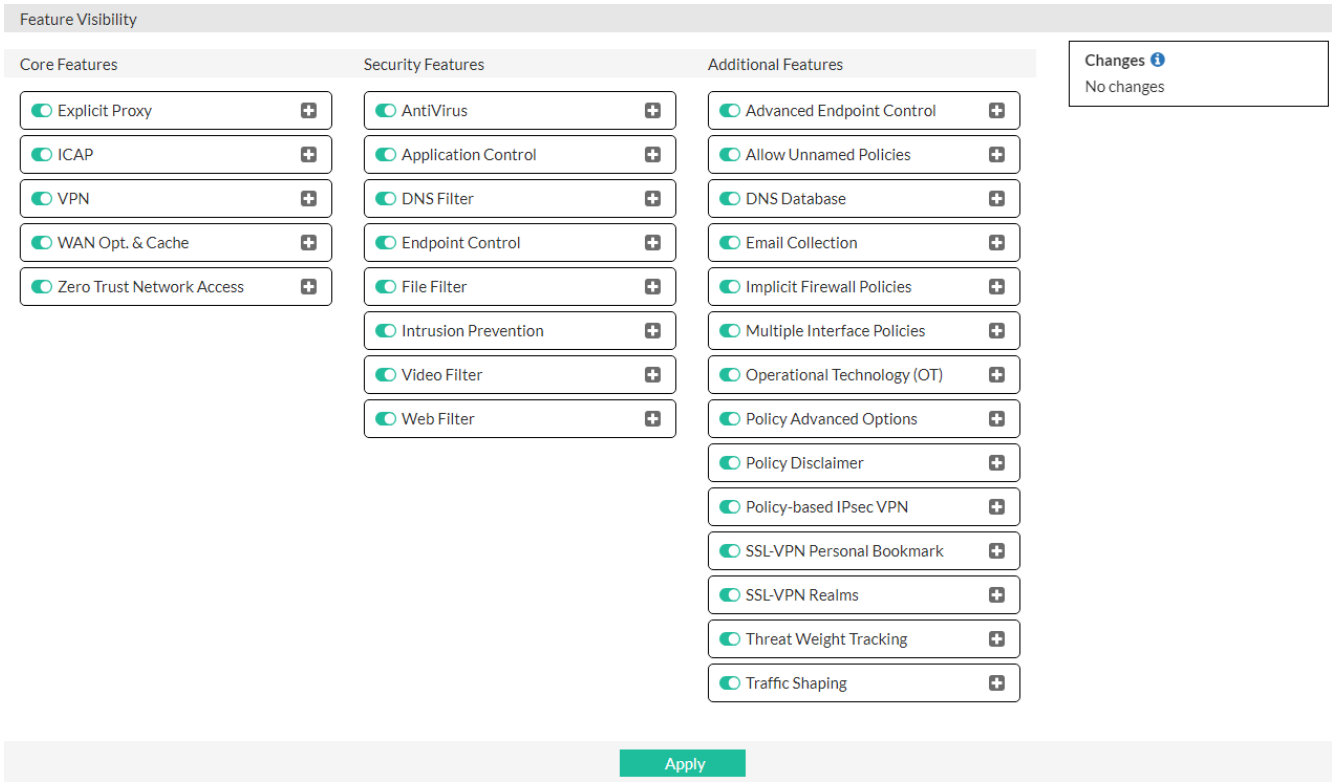
To exclude reputable websites from SSL deep inspection, enable the *Reputable websites* option under SSL/SSH Inspection.


New SSL/SSH Inspection Profile
SMTPS
465
POP3S
995
IMAPS
993
FTPS
990
DNS over TLS
853
HTTP/3
Inspect
Bypass
Block
DNS over QUIC
Inspect
Bypass
Block
Exempt from SSL Inspection
Reputable websites
Web categories
Finance and Banking
Health and Wellness
Personal Privacy
Addresses
Log SSL exemptions
SSH Inspection Options
SSH deep scan
Common Options
Invalid SSL certificates
Allow
Block
Custom
Expired certificates
Keep Untrusted & Allow
Block
Trust & Allow
Revoked certificates
Keep Untrusted & Allow
Block
Trust & Allow
Validation timed-out certificates
Keep Untrusted & Allow
Block
Trust & Allow
Validation failed certificates
Keep Untrusted & Allow
Block
Trust & Allow
Log SSL anomalies
OK
Cancel

Feature Visibility

Various FortiProxy features can be enabled or disabled as required. Disable features are not shown in the GUI.

Go to *System* > *Feature Visibility* to configure which features are available.



The following options can be turned on or off by toggling the sliders:

Explicit Proxy	Controls the visibility of the *Proxy Settings* > *Explicit Proxy* menu, which allows you to enable an HTTP, HTTPS, or FTP proxy for your network and add the proxy to one or more FortiProxy interfaces. Users on your network must configure their browsers to use the proxy. Create policies to control access to the proxy and apply UTM and other features to proxy traffic.
ICAP	Controls the visibility of the *Content Analyses* > *ICAP Profile*, *Content Analyses* > *ICAP Remote Servers*, and *Content Analyses* > *ICAP Local Servers* pages, which allow you to offload services to an external server. These services can include: ad insertion, virus scanning, content and language translation, HTTP header or URL manipulation, and content filtering. You can also use this feature to set up profiles and add them to security policies.

VPN	Controls the visibility of the *VPN on page 768* menu, which allow you to create secure communication channels between networks and allows remote users to safely connect to secure private networks using IPsec VPN and FortiClient.
WAN Opt. & Cache	Controls the visibility of the *WAN Optimization* and *Web Cache* menus. The *WAN Optimization* menu allows you to add WAN optimization to improve traffic performance and efficiency as it crosses the WAN. The *Web Cache* menu allows you to cache web pages from any web server. All traffic between a client network and one or more web servers is then intercepted by a web cache policy. This policy causes the FortiProxy unit to cache pages from the web servers on the FortiProxy unit and makes the cached pages available to users on the client network. Web caching can be configured for standard and reverse web caching.
Zero Trust Network Access	Controls the visibility of the *Policy & Objects* > *ZTNA* menu, which allows you to uses client device identification, authentication, and Zero Trust tags to provide role-based application access. It gives administrators the flexibility to manage network access for On-net local users and Off-net remote users. Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using Zero Trust tags.
AntiVirus	Controls the visibility of the *Security Profiles* > *AntiVirus* menu, which allows you to remove viruses, analyze suspicious files with FortiSandbox, and apply botnet protection to network traffic. Set up antivirus profiles and add them to policies. This feature requires a subscription to FortiGuard AntiVirus.
Application Control	Controls the visibility of the *Security Profiles* > *Application Control* menu, which allows you to visualize and control the applications on your network. Set up application sensors and add them to policies. This feature requires a subscription to Application Control Signatures.
DNS Filter	Controls the visibility of the *Security Profiles* > *DNS Filter* men, which allows you to apply DNS category filtering, URL filtering to control a user's access to web resources. Set up DNS filter profiles and add them to policies or add them to a DNS server on a FortiProxy interface. Some features require a subscription to FortiGuard Web Filtering.

Endpoint Control	Allows access block for endpoints (PCs, iOS devices, Android devices) through the FortiProxy unit unless they meet security requirements. Enforces the use of FortiClient on the endpoints. Sends non-compliant endpoints to the FortiClient download portal to install the latest version. Setup Endpoint Control on FortiClient EMS. Requires FortiClient licenses.
File Filter	Controls the visibility of the *Security Profiles* > *File Filter* menu, which allows you to block files passing through based on file type based on the file's metadata only and not on file size or file content. A DLP profile must be configured to block files based on size or content, such as SSN numbers, credit card numbers, or regular expression pattern. The file filter can be applied directly to policies.
Intrusion Prevention	Controls the visibility of the *Security Profiles* > *Intrusion Prevention* menu, which allows you to detect and block network-based attacks. You can set up IPS sensors and add them to policies. This feature requires a subscription to FortiGuard IPS.
Video Filter	Controls the visibility of the *Security Profiles* > *Video Filter* menu, which allows you to apply video filter rules to policies to control user's access to videos from different sources.
Web Filter	Controls the visibility of the *Security Profiles* > *Web Filter* menu, which allows you to apply web category filtering, URL filtering, and content filtering to control user's access to web resources. You can set up web filter profiles and add them to policies. Some features require a subscription to FortiGuard Web Filtering.
Advanced Endpoint Control	Allows FortiClient Device quarantine by enabling the display of On-Net options and status on GUI pages.
Allow Unnamed Policies	Relaxes the requirement for every policy to have a name when created in GUI.
DNS Database	Controls the visibility of the *Network* > *DNS Service* menu, which allows you to set up the FortiProxy unit as the DNS server for your network. You can add local DNS entries to the DNS database and forward other DNS lookups to external DNS servers. An alternative way to set up a DNS server is to set up DNS Filter Profiles (under *Security Profiles* > *DNS Filter*) and add them to DNS Server on a FortiProxy interface.
Implicit Firewall Policies	Firewall policy lists end with an implicit policy that denies all traffic. Enable this feature to see these policies on firewall policy lists in the GUI. You can edit an implicit policy and enable logging to record log messages when the implicit policy denies a session.
Multiple Interface Policies	Allows the configuration of policies with multiple source/destination interfaces. See Create or edit a policy on page 387.

Operational Technology (OT)	Controls the visibility of the *Security Fabric > Asset Identity Center > OT View* tab, which provides an OT mapping layout to browse assets by Purdue level.
Policy Advanced Options	Controls the visibility of advanced options when you create a policy in the GUI, such as the *Negate Destination* option. See Create or edit a policy on page 387.
Policy Disclaimer	Controls the visibility of the *Policy Disclaimer* option, which allows the user to enable a disclaimer on an allow policy, or a block notification on a deny policy. See Create or edit a policy on page 387.
Threat Weight Tracking	Controls the visibility of the *Log & Report > Log Settings > Threat Weight* tab, which includes the Threats option for FortiView and shows UTM events sorted using a weighted severity system.
Traffic Shaping	Controls the visibility of the *Policy & Objects > Traffic Shaping* menu, which allows you to configure policies to define how specific types of traffic are shaped by the FortiProxy unit.

Certificates

FortiProxy uses three types of certificates:

- **Local**: Local certificates are issued for a specific server or web site. They are usually very specific, and often for an internal enterprise network.
- **CA**: External CA certificates are similar to local certificates, but apply to a broader range of addresses or to whole company. A CA certificate would be issued for an entire web domain, instead of just a single web page.
- **Remote**: Remote certificates are public certificates without private keys.

The FortiProxy unit generates a certificate request based on the information entered to identify the FortiProxy unit. After generating a certificate request, it can be downloaded and then forward to a CA.

The certificate page also enables you to export certificates for authentication, importing, and viewing.

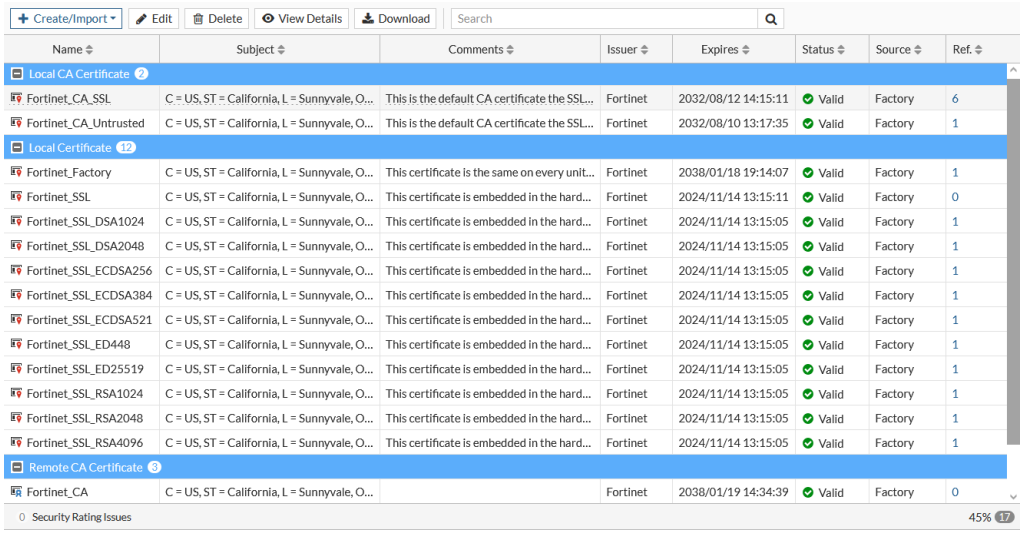
The certificates feature is hidden by default in FortiProxy. In the GUI, go to *System > Feature Visibility* and enable *Certificates*.

The following topics provide information about certificates:

- Certificate list on page 974
- Certificate Signing Requests on page 975
- Import a local certificate on page 978
- Import a CA certificate on page 982
- Upload a remote certificate on page 982
- Import a CRL on page 982
- View certificate details on page 983
- Default certificate authority on page 983
- Enrollment over Secure Transport for automatic certificate management on page 984

Certificate list

To see a list of certificates that have been imported, go to *System* > *Certificates*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create Import	• Create or import a local certificate (see Import a local certificate on page 978) • Generate a CSR (see Certificate Signing Requests on page 975) • Import a CA certificate (see Import a CA certificate on page 982) • Upload a remote certificate (see Upload a remote certificate on page 982) • Import a CRL (see Import a CRL on page 982)
Edit	Highlight a certificate and select to edit the certificate comments. This command is only available on some certificates.
Delete	Select a certificate and select *Delete* to remove the selected certificate or CSR. Click *OK* in the confirmation dialog box to proceed with the delete action. To remove multiple certificates or CSRs, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
View Details	View a certificate. See View certificate details on page 983.
Download	Select a certificate or CSR and then select *Download* to download that certificate or CSR to your management computer.
Search	Enter a search term to search the certificate list.
Name	The name of the certificate.

Subject	The subject of the certificate.
Comments	Comments.
Issuer	The issuer of the certificate.
Expires	Displays the certificate's expiration date and time.
Status	The status of the certificate or CSR. • *OK*: the certificate is okay. • *NOT AVAILABLE*: the certificate is not available, or the request was rejected. • *PENDING*: the certificate request is pending.
Source	The source of a certificate can be *Factory*, *User*, or *FortiGuard*.
Ref.	Displays the number of times the certificate or CSR is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.

Certificate Signing Requests

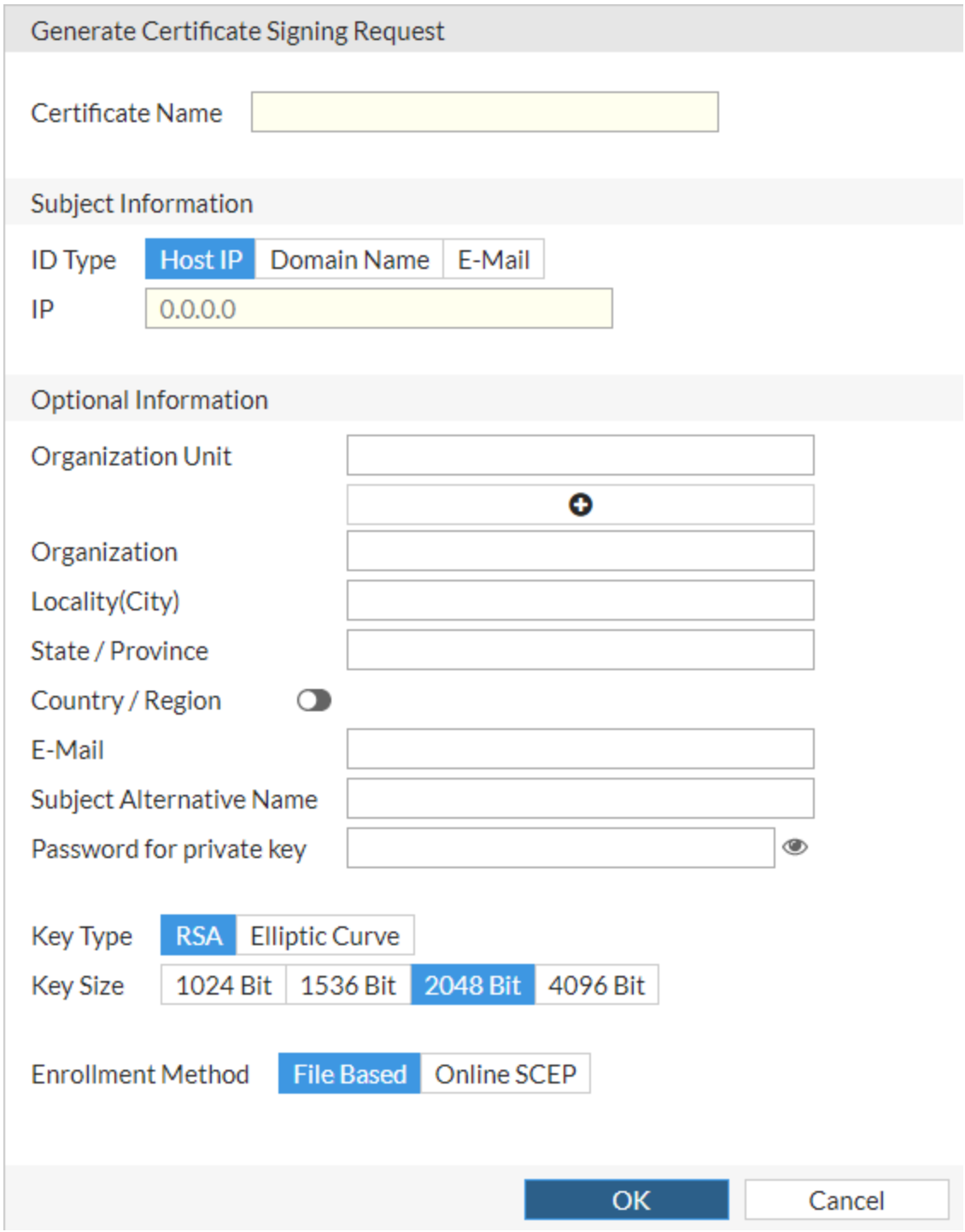
Whether you create certificates locally or obtain them from an external certificate service, you need to generate a Certificate Signing Request (CSR).

When a CSR is generated, a private and public key pair is created for the FortiProxy unit. The generated request includes the public key of the device, and information such as the unit's public static IP address, domain name, or email address. The device's private key remains confidential on the unit.

After the request is submitted to a CA, the CA verifies the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA then signs the certificate, after which you can install the certificate on the FortiProxy device.

To generate a CSR:

1. Go to *System* > *Certificates* and click *Create/Import* > *Generate CSR*. The *Generate Certificate Signing Request* page opens.



2. Enter the following information:

Certificate Name	Enter a unique name for the certificate request, such as the host name or the serial number of the device. Do not include spaces in the certificate to ensure compatibility as a PKCS12 file.

Subject Information	Select the ID type: • *Host IP*: Select if the unit has a static IP address. Enter the device's IP address in the *IP* field. • *Domain Name*: Enter the device's domain name or FQDN in the *Domain Name* field. • *E-mail*: Enter the email address of the device's administrator in the *E-mail* field.
Optional Information	Optional information to further identify the device.
Organization Unit	Enter the name of the department. Up to 5 OUs can be added.
Organization	Enter the legal name of the company or organization.
Locality (City)	Enter the name of the city where the unit is located.
State/Province	Enter the name of the state or province where the unit is located.
Country/Region	Enable and then enter the country where the unit is located. Select from the drop-down list.
E-Mail	Enter the contact email address.
Subject Alternative Name	Enter one or more alternative names, separated by commas, for which the certificate is also valid. An alternative name can be: email address, IP address, URI, DNS name, or a directory name. Each name must be preceded by its type, for example: IP:1/2/3/4, or URL: http://your.url.here/.
Password for private key	Enter a password for the private key.
Key Type	Select *RSA* or *Elliptic Curve*. The default is *RSA*.
Key Size	If you selected *RSA* for the *Key Type*, select the key size: *1024 Bit*, *1536 Bit*, *2048 Bit*, or *4096 Bit*. The default is *2048 Bit*. Larger key sizes are more secure but slower to generate.
Curve Name	If you selected *Elliptic Curve* for the *Key Type*, select the curve name: *secp256r1*, *secp384r1*, or *secp521r1*.
Enrollment Method	Select the enrollment method. The default is *File Based*. • *File Based*: Generate the certificate request. • *Online SCEP*: Obtain a signed, Simple Certificate Enrollment Protocol (SCEP) based certificate automatically over the network. Enter the CA server URL and challenge password in their respective fields.

3. Click *OK* to generate the CSR.

Import a local certificate

Local certificates are issued for a specific server, or web site. Generally they are very specific, and often for an internal enterprise network. For example, a personal web site for John Smith at www.example.com (such as http://www.example.com/home/jsmith) would have its own local certificate.

These can optionally be just the certificate file or also include a private key file and PEM passphrase for added security.

Signed local certificates can be imported to the FortiProxy unit.

To import a local certificate:

1. Go to *System* > *Certificates* and click *Create/Import* > *Certificate*. The *Import Certificate* page opens.
2. Select the *Type*:
   - If the *Type* is *Local Certificate*, select *Upload* and locate the certificate file on your computer.
   - If the *Type* is *PKCS #12 Certificate*, select *Upload* and locate the certificate with key file on your computer. Select *Change* to enter the password in the *Password* field.
   - If the *Type* is *Certificate*, select *Upload* and locate the certificate file on your computer. Select *Upload* and locate the key file on your computer. Select *Change* to enter the password in the *Password* field.
3. Click *OK* to import the certificate.

ACME certificate support

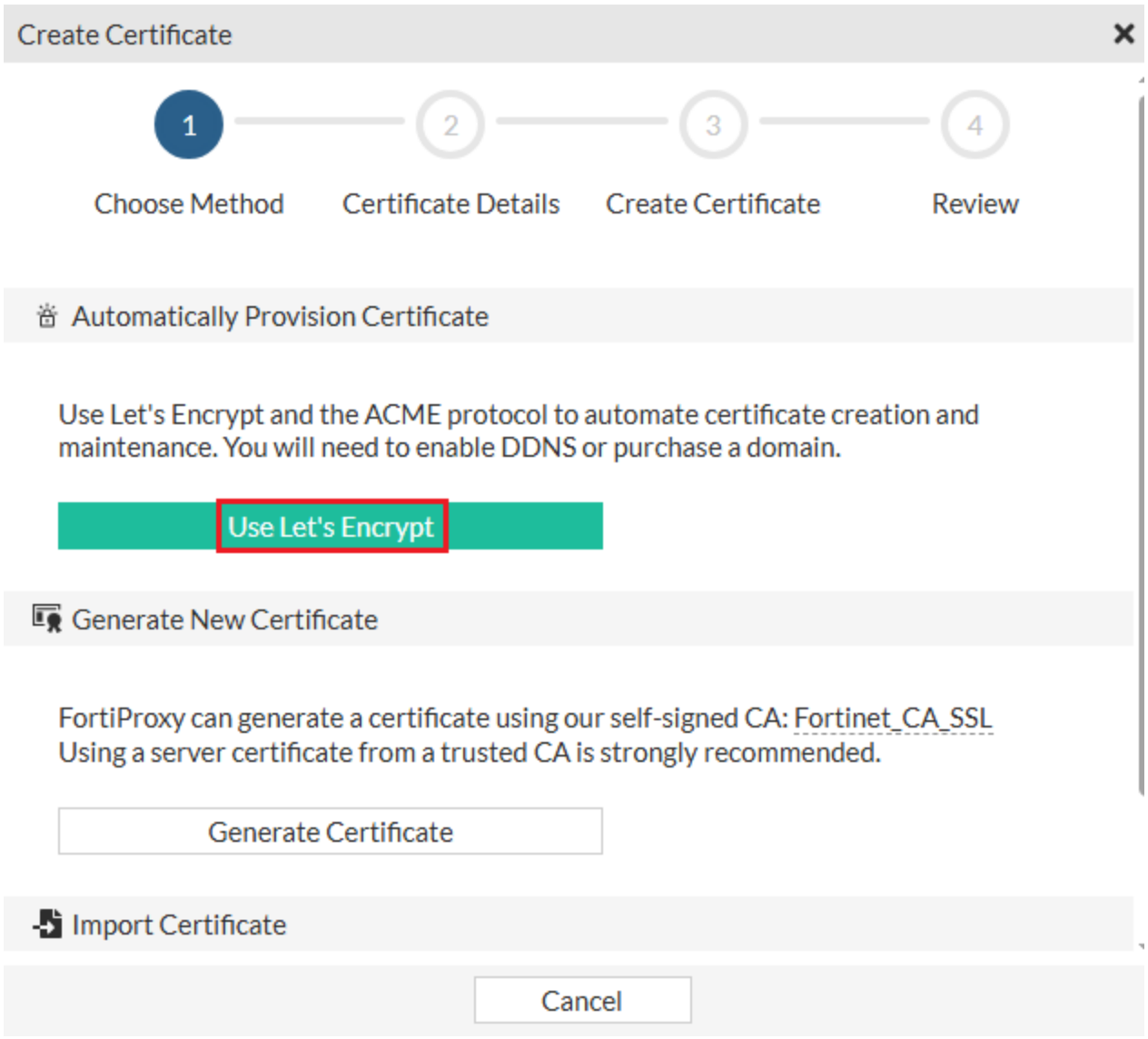
The Automated Certificate Management Environment (ACME), as defined in RFC 8555, is used by the public Let's Encrypt certificate authority (https://letsencrypt.org) to provide free SSL server certificates. The FortiProxy unit can be configured to use certificates that are manged by Let's Encrypt, and other certificate management services, that use the ACME protocol. The server certificates can be used for secure administrator log in to the FortiProxy unit.

- The FortiProxy unit must have a public IP address and a hostname in DNS (FQDN) that resolves to the public IP address.
- The configured ACME interface must be public facing so that the FortiProxy unit can listen for ACME update requests. It must not have any VIPs, or port forwarding on port 80 (HTTP) or 443 (HTTPS).
- The Subject Alternative Name (SAN) field is automatically filled with the FortiProxy DNS hostname. It cannot be edited, wildcards cannot be used, and multiple SANs cannot be added.

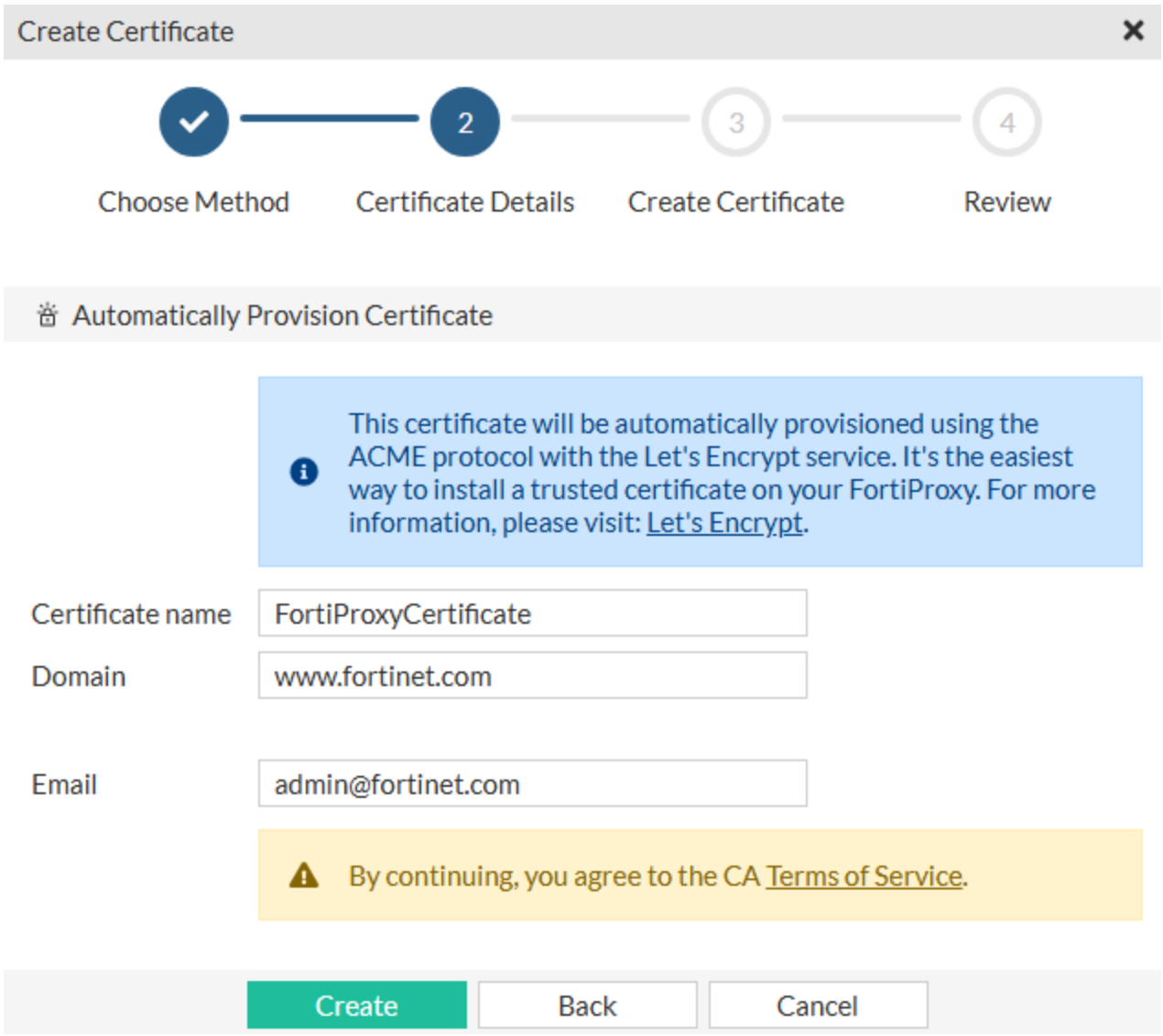
NOTE: To configure certificates in the GUI, go to *System* > *Feature Visibility* and enable *Certificates*.

To import an ACME certificate in the GUI:

1. Go to *System* > *Certificates* and click *Create/Import* > *Certificate*.
2. Click *Use Let's Encrypt*.



3. Set *Certificate name* to an appropriate name for the certificate.



4. Set *Domain* to the public FQDN of the FortiProxy unit.
5. Set *Email* to a valid email address. The email is not used during the enrollment process.
6. Click *Create*.
7. Select the interface that the FortiProxy unit communicates with.
   The ACME interface can later be changed in *System > Settings*.
8. Enable or disable *ACME Log* as needed.
9. Wait for the provisioning of the certificate to complete and click *OK*.
10. Select the new server certificate in the *Local Certificate* list and then click *View Details*to verify that the FortiProxy unit's FQDN is in the certificate's Subject: Common Name (CN).
    The *Remote CA Certificate* list includes the issuing Let's Encrypt intermediate CA, issued by the public CA DST Root CA X3 from Digital Signature Trust Company.

To exchange the default FortiProxy administration server certificate for the new public Let's Encrypt server certificate in the GUI:

1. Go to *System* > *Settings*.
2. Set the HTTPS server certificate to the new certificate.
3. Click *Apply*.
4. Log in to the FortiProxy unit using an administrator account from any Internet browser. There should be no warnings related to nontrusted certificates, and the certificate path should be valid.

To import an ACME certificate in the CLI:

1. Set the interface that the FortiProxy unit communicates with Let's Encrypt on:
```
config system acme
   set interface port1
end
```
2. Make sure that the FortiProxy unit can contact the Let's Encrypt enrollment server:
```
FortiProxy-400E # execute ping acme-v02.api.letsencrypt.org
PING ca80a1adb12a4fbdac5ffcbc944e9a61.pacloudflare.com (172.65.32.248): 56 data bytes
64 bytes from 172.65.32.248: icmp_seq=0 ttl=56 time=4.8 ms
64 bytes from 172.65.32.248: icmp_seq=1 ttl=56 time=4.5 ms
64 bytes from 172.65.32.248: icmp_seq=2 ttl=56 time=4.5 ms
64 bytes from 172.65.32.248: icmp_seq=3 ttl=56 time=4.5 ms
64 bytes from 172.65.32.248: icmp_seq=4 ttl=56 time=4.5 ms

--- ca80a1adb12a4fbdac5ffcbc944e9a61.pacloudflare.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.5/4.5/4.8 ms
```
3. Configure the local certificate request:
```
config vpn certificate local
   edit "acme-test"
      set enroll-protocol acme2
      set acme-domain "test.ftntlab.de"
      set acme-email "techdoc@fortinet.com"
      next
      By enabling this feature you declare that you agree to the Terms of Service at
      https://acme-v02.api.letsencrypt.org/directory
      Do you want to continue? (y/n)y
end
```
4. Verify that the enrollment was successful:
```
# get vpn certificate local details acme-test
```

To exchange the default FortiProxy administration server certificate for the new public Let's Encrypt server certificate in the CLI:

```
config system global
   set admin-server-cert "acme-test"
end
```

When you log in to the FortiProxy unit using an administrator account, there should be no warnings related to nontrusted certificates, and the certificate path should be valid.

Import a CA certificate

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to whole company; they are one step higher up in the organizational chain. Using the local certificate example, a CA root certificate would be issued for all of www.example.com instead of just the smaller single web page.

CA certificates can be imported to the FortiProxy unit.

To import a CA certificate:

1. From the Certificates page, select *Import* > *CA Certificate*. The *Import CA Certificate* page opens.
2. Select the *Type*:
   - If you select *Online SCEP* (Simple Certificate Enrollment Protocol), enter the URL of the SCEP server and optional CA identifier.
   - If you select *File*, select *Upload* and locate the certificate file on your computer.
3. Click *OK* to import the certificate.

Upload a remote certificate

Remote certificates are public certificates without a private key. Remote certificates can be uploaded to the FortiProxy unit.

To upload a remote certificate:

1. From the Certificates page, select *Import* > *Remote Certificate*. The *Upload Remote Certificate* page opens.
2. Select *Upload* and locate the certificate file on your computer.
3. Click *OK* to upload the certificate.

Import a CRL

Certificate revocation list (CRL) is a list of certificates that have been revoked and are no longer usable. This list includes certificates that have expired, been stolen, or otherwise compromised. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

CRLs can be imported to the FortiProxy unit.

To import a certificate revocation list:

1. From the Certificates page, select *Import* > *CRL*. The *Import CRL* page opens.
2. Select *File Based* or *Online Updating*.

If you select *File Based*, select *Upload* and locate the certificate file on your computer. If you select *Online Updating*, configure the following settings:

- *HTTP:* If you enable HTTP updating, enter the URL of the HTTP server.
- *LDAP:* If you enable LDAP updating, select or search for the LDAP server, enter the user name, and select *Change* to enter the password in the *Password* field.
- *SCEP:* If you enable SCEP updating, select a local certificate for SCEP communication for the online CRL and enter the URL of the SCEP server.

3. Click *OK* to import the CRL.

View certificate details

Certificate details can be viewed by selecting a certificate and then selecting *View Details* from the toolbar.

The following information is displayed:

Certificate Name	The name of the certificate.
Serial Number	The serial number of the certificate.
Subject Information	The subject information of the certificate, including: • *Common Name (CN)* • *Organization (O)* • *Organization Unit (OU)* • *Locality (L)* • *State (ST)* • *Country (C)* • *Email Address*
Issuer	The issuer information of the certificate, including most of the information from *Subject Information*.
Validity Period	Displays the *Valid From* and the expiration *Valid To* date of the certificate. The certificate should be renewed before this expiration date.
Fingerprints	The identifying fingerprint of the certificate.
Extension	The certificate extension information.

Select *Close* to return to the certificate list.

Default certificate authority

The default certificate authorities (CA) can be configured. By default, web-proxy and ssl-ssh-profile use the default CAs:

```
config firewall ssl default-certificate
    set default-ca "Fortinet_CA_SSL"
```

```
    set default-untrusted-ca "Fortinet_CA_Untrusted"
    set default-server-cert "Fortinet_Factory"
end
```

```
config web-proxy global
    set ssl-cert "default-server-cert"
    set ssl-ca-cert "default-ca"
end
```

```
confir firewall ssl-ssh-profile
    edit 1
        set caname "default-ca"
        set untrusted-caname "default-untrusted-ca"
    next
end
```

The CA can be changed by either changing the default, or by setting a specific CA for the web-proxy or ssl-ssh-profile. For example, to change the web-proxy CAs, but not the defaults:

```
config web-proxy global
    set ssl-cert "Personal_Server_CA"
    set ssl-ca-cert "Personal_CA"
end
```

Enrollment over Secure Transport for automatic certificate management

The FortiProxy supports Enrollment over Secure Transport (EST) and the RFC 7030 standards when generating a new CSR request, performing automatic renewals, or manually regenerating a certificate. EST provides more security for automatic certificate management than Simple Certificate Enrollment Protocol (SCEP), which is commonly used for certificate enrollment.

Background

SCEP helps automate and simplify the process for obtaining a digital certificate from a certificate authority (CA). However, SCEP does not natively support secure connections, and instead relies on the underlying transport protocol to provide security. EST was developed, which uses TLS to establish a secure communication channel over which subsequent certificate management protocol messages like initial certificate enroll and certificate renewal messages are exchanged.

On the FortiProxy, when generating a certificate signing request (CSR), you can use the SCEP method to send the request to an SCEP server, or use EST to send the request to an EST server to be signed by a CA.

To configure the enrollment protocol settings for a local certificate:

```
config vpn certificate local
    edit <name>
        set enroll-protocol est
        set est-server <string>
        set est-ca-id <string>
        set est-http-username <string>
        set est-http-password <string>
        set est-client-cert <certificate>
        set est-server-cert <certificate>
        set est-srp-username <string>
        set est-srp-password <string>
    next
end
```

`est-server <string>`	Enter the address and port for EST server (such as https://example.com:1234).
`est-ca-id <string>`	Enter the CA identifier of the CA server for signing with EST.
`est-http-username <string>`	Enter the HTTP Authentication username for signing with EST.
`est-http-password <string>`	Enter the HTTP Authentication password for signing with EST.
`est-client-cert <certificate>`	Enter the certificate used to authenticate this FortiProxy to the EST server.
`est-server-cert <certificate>`	Enter the EST server's certificate that has to be verifiable by the specified certificate on the FortiProxy.
`est-srp-username <string>`	Enter the EST SRP authentication username.
`est-srp-password <string>`	Enter the EST SRP authentication password.

To manually generate a CSR for the EST server to be signed by a CA:

```
# execute vpn certificate local generate est {reqired_1} {reqired_2} {reqired_3} [options]
```

option 1 (required)	Name of the local server certificate.
option 2 (required)	Cryptography algorithm: `rsa-1024`, `rsa-1536`, `rsa-2048`, `rsa-4096`, `ec-secp256r1`, `ec-secp384r1`, or `ec-secp521r1`.
option 3 (required)	URL and listening port of the remote EST responder.
option 4 (optional)	Server certificate subject in the certificate enroll request. Separate fields by a comma (,).
option 5 (optional)	Subject Alternative Name (SAN). This can be an FQDN and/or IP. Use DNS:<FQDN>,IP:<IP_address> for example. If the issuing CA does not support SAN, this option will be ignored. Separate fields by a comma (,).

option 6 (optional)	HTTP authentication username.
option 7 (optional)	HTTP authentication password.
option 8 (optional)	CA identifier.
option 9 (optional)	CA certificate used to verify the remote EST responder server certificate and certificates issued by a remote PKI.
option 10 (optional)	Password for the private key.
option 11 (optional)	Client certificate.
option 12 (optional)	Source IP for communications to the CA server.
option 13 (optional)	TLS-SRP username.
option 14 (optional)	TLS-SRP password.

Example 1: enrolling for a new FortiProxy server certificate with EST

To enroll for a new FortiProxy server certificate with EST:

1. Verify that the FortiProxy can communicate with remote EST responder (testrfc7030.com):

```
# execute ping testrfc7030.com
PING testrfc7030.com (54.70.32.33): 56 data bytes
64 bytes from 54.70.32.33: icmp_seq=0 ttl=31 time=13.6 ms
64 bytes from 54.70.32.33: icmp_seq=1 ttl=31 time=19.1 ms
64 bytes from 54.70.32.33: icmp_seq=2 ttl=31 time=16.5 ms
^C
--- testrfc7030.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 13.6/16.4/19.1 ms
```

2. Start running debugs to track the progress of the enrollment:

```
# diagnose debug application est -1
# diagnose debug enable
```

3. Create a new server CSR file locally and send it to the remote EST responder:

```
# execute vpn certificate local generate est est-test101 ec-secp256r1
https://testrfc7030.com:8443 CN=firewall-portal1,DC=local,DC=COM DNS:firewall-
portal1.local.ca,IP:172.18.60.184 estuser estpwd G_CA_Cert_1
```



The CA certificate (G_CA_Cert_1) is used to verify the remote EST responder server certificate and certificates issued by a remote PKI.

testrfc7030.com is a self-signed CA, which by default is not in the local trusted root store and must be imported prior to enrollment.

If the CA that issues the server certificate is not in the local root store, an error would appear in the debug messages:

```
# diagnose debug application est -1
# diagnose debug enable
...
[1795] est_curl_req: Error buf: SSL certificate problem: self-signed
certificate in certificate chain,
[2402] est_simple_enroll: Failed to get ca certs: -1.
...
```

4. If the enrollment was successful, in a few seconds, a Done message appears. Verify the debugs to view the enrollment process.
   a. The remote CA's certificate is retrieved and stored locally in the EST configuration after being verified with the CA in the trusted root store:

```
[1962] __est_curl_set_auth: trace
[2046] __est_curl_set_auth: HTTP Authentication username is set
[2050] __est_curl_set_auth: HTTP Authentication password is set
[2075] __est_get_ca_certs: ============STARTED============
[1728] est_curl_req: URL: https://testrfc7030.com:8443/.well-known/est/cacerts
[1776] est_curl_req: HTTP GET
[143] __curl_ssl_ctx_finalizer: global CAs are loaded.
[165] __curl_ssl_ctx_finalizer: SSL_CTX ex data is set.
[1651] curl_header_debug_func: Header received:HTTP/1.1 200 OK
```

   b. The debug displays the CA used by the remote EST responder:

```
[1191] save_pkcs7_certs: Saving pkcs7 response
[505] est_print_pkcs7: Certs: (1 in total)
[507] est_print_x509: Cert 1:
[427] est_print_x509:         Version: 3 (0x2)
        Serial Number:
            ab:e8:32:e1:f6:6a:6b:43
        Issuer: CN=estExampleCA
        Subject: CN=estExampleCA
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Subject Key Identifier:
                1A:DF:39:84:C2:56:E6:6C:CF:2A:B4:26:A5:FD:0C:D2:43:F5:3D:3E

[1220] save_pkcs7_certs: Received 1 certs
[1228] save_pkcs7_certs: Saving cert(s):
        is_global:1
        est_url:https://testrfc7030.com:8443
```

```
        source_ip:NULL
        ca_identifier:NULL
```

c. The CA certificate is imported. FortiProxy sends a query to learn about the attributes supported by the CA in the certificate request and will then create the CSR accordingly:

```
[1288] save_pkcs7_certs: CA certs imported!
[2101] __est_get_csr_attrs: ============STARTED============
[1728] est_curl_req: URL: https://testrfc7030.com:8443/.well-known/est/csrattrs
[1776] est_curl_req: HTTP GET
[1651] curl_header_debug_func: Header received:HTTP/1.1 200 OK
[1651] curl_header_debug_func: Header received:Status: 200 OK
[1651] curl_header_debug_func: Header received:Content-Type: application/csrattrs
[1651] curl_header_debug_func: Header received:Content-Transfer-Encoding: base64
[1651] curl_header_debug_func: Header received:Content-Length: 57
[1651] curl_header_debug_func: Header received:
[1787] est_curl_req: Response 200
[1788] est_curl_req: Buffer:MCYGBysGAQEBARYGCSqGSIb3DQEJAQYFK4EEACIGCWCGSAFlAwQCAg==
[1439] decode_csrattrs_callback: Decoding csrattrs, resp->len: 57
[1474] decode_csrattrs_callback: Object: 1.3.6.1.1.1.1.22 undefined
[1474] decode_csrattrs_callback: Object: 1.2.840.113549.1.9.1 emailAddress
[1474] decode_csrattrs_callback: Object: 1.3.132.0.34 secp384r1
[1474] decode_csrattrs_callback: Object: 2.16.840.1.101.3.4.2.2 sha384
```

d. The CSR information is generated, which is sent to the remote EST responder:

```
        est_ctx: is_global:1
        vfid:0
        svr_original_url:https://testrfc7030.com:8443
        svr_hostinfo:Exists
        ca_identifier:(null)
        http_username:estuser
        http_password:estpwd
        clt_cert:(null)
        svr_cert:(null)
        srp_username:(null)
        srp_password:(null)
        source_ip:(null)
        need_pop:0
        newcert_name:est-test101
        passwd:(null)
        rsa_keysize:0
        ec_curvename:secp256r1
        subject:CN=firewall-portal1,DC=local,DC=COM
        sub_alt_name:DNS:firewall-portal1.local.ca,IP:172.18.60.184
        svr_cert_x509:NULL
        csr_attrs:Exists
        csr:NULL
        pkey:NULL
        header_ptr:NULL
        tmp_p10:NULL
[2259] __est_simple_enroll: ============STARTED============
```

e. The CSR is sent to the EST responder:

```
[1728] est_curl_req: URL: https://testrfc7030.com:8443/.well-known/est/simpleenroll
[1753] est_curl_req: HTTP POST
[1651] curl_header_debug_func: Header received:HTTP/1.1 200 OK
[1651] curl_header_debug_func: Header received:Status: 200 OK
[1651] curl_header_debug_func: Header received:Content-Type: application/pkcs7-mime;
smime-type=certs-only
[1651] curl_header_debug_func: Header received:Content-Transfer-Encoding: base64
[1651] curl_header_debug_func: Header received:Content-Length: 585
[1651] curl_header_debug_func: Header received:
```

f. The CA issues the certificate and sends it back in a PKCS #7 structure:

```
[1787] est_curl_req: Response 200
[1788] est_curl_req:
Buffer:MIIBqwYJKoZIhvcNAQcCoIIBnDCCAZgCAQExADALBgkqhkiG9w0BBwGgggGAMIIB
fDCCASOgAwIBAgIDB0aXMAoGCCqGSM49BAMCMBcxFTATBgNVBAMTDGVzdEV4YW1w
...
```

g. The FortiProxy decodes and displays the attributes of the certificate, then saves the certificate:

```
[1191] save_pkcs7_certs: Saving pkcs7 response
[505] est_print_pkcs7: Certs: (1 in total)
[507] est_print_pkcs7: Cert 1:
[427] est_print_x509:         Version: 3 (0x2)
        Serial Number: 476823 (0x74697)
        Issuer: CN=estExampleCA
        Subject: CN=firewall-portal1
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature
            X509v3 Subject Key Identifier:
                9B:F8:39:D5:21:E6:FF:49:FF:AC:02:57:5B:FC:4C:1A:8B:1E:5D:8F
            X509v3 Authority Key Identifier:
                1A:DF:39:84:C2:56:E6:6C:CF:2A:B4:26:A5:FD:0C:D2:43:F5:3D:3E

[1220] save_pkcs7_certs: Received 1 certs
[1228] save_pkcs7_certs: Saving cert(s):
        is_global:1
        est_url:https://testrfc7030.com:8443
        source_ip:NULL
        ca_identifier:NULL

[1246] save_pkcs7_certs: Received 1 cert(s)
[427] est_print_x509:         Version: 3 (0x2)
        Serial Number: 476823 (0x74697)
        Issuer: CN=estExampleCA
        Subject: CN=firewall-portal1
        X509v3 extensions:
```

```
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature
            X509v3 Subject Key Identifier:
                9B:F8:39:D5:21:E6:FF:49:FF:AC:02:57:5B:FC:4C:1A:8B:1E:5D:8F
            X509v3 Authority Key Identifier:
                1A:DF:39:84:C2:56:E6:6C:CF:2A:B4:26:A5:FD:0C:D2:43:F5:3D:3E

[827] est_cmdb_update_cert: Cert est-test101 updated in CMDB
[1276] save_pkcs7_certs: The cert is saved!
[592] est_ctx_clear_tmp_data: trace
[2408] est_simple_enroll: POST ret:0
[592] est_ctx_clear_tmp_data: trace
Done.
```

Example 2: automatically renewing a FortiProxy server certificate with EST

When the time for certificate renewal is up, the FortiProxy will use the existing EST parameters to perform an automatic renewal. This example demonstrates the renewal process through debugs.

To automatically renew a FortiProxy server certificate with EST:

1. Verify the current local certificate configuration:

```
config vpn certificate local
(local) # get est-test101
name                : est-test101
password            : *
comments            :
private-key         : *
certificate         :
        Subject:     CN = firewall-portal1
        Issuer:      CN = estExampleCA
        Valid from:  2023-04-06 22:37:34  GMT
        Valid to:    2024-04-05 22:37:34  GMT
        Fingerprint: AE:67:11:CF:7D:F9:57:A4:09:8B:55:0A:F1:B1:7A:CF
...
state               : OK
range               : global
source              : user
source-ip           : 0.0.0.0
ike-localid-type    : asn1dn
enroll-protocol     : est
est-server          : https://testrfc7030.com:8443
est-ca-id           :
est-http-username   : estuser
est-http-password   : estpwd
est-client-cert     :
```

```
est-server-cert     :
est-srp-username    :
est-srp-password    :
auto-regenerate-days: 0
auto-regenerate-days-warning: 0
```

Note that the current `Valid to` date and time is `2024-04-05 22:37:34 GMT`, which is one year from the issue date.

2. Start running debugs to track the progress of the renewal:

```
# diagnose debug application est -1
# diagnose debug enable
```

3. For demonstration purposes, update the `auto-regenerate-days` setting to 364 days to trigger the automatic renewal on the FortiProxy:

```
config vpn certificate local
    edit est-test101
        set auto-regenerate-days 364
    next
end
```

4. Verify the debugs to confirm that the certificate was renewed.
   a. The FortiProxy uses the content of the current certificate to create a new CSR. User credentials used for the initial enrollment are stored in local certificate configuration, but they are not used for renewal:

```
[1024] reconstruct_est_ctx: Reconstruction succeeded
est_ctx:        is_global:1
        vfid:0
        svr_original_url:https://testrfc7030.com:8443
        svr_hostinfo:NULL
        ca_identifier:
        http_username:estuser
        http_password:estpwd
        clt_cert:
        svr_cert:
        srp_username:
        srp_password:
        source_ip:(null)
        need_pop:0
        newcert_name:est-test101
        passwd:f51da8548af5fef820edfe6267b0c178e76f7c3eae40ee0900318fc77ab6bd
        rsa_keysize:0
        ec_curvename:(null)
        subject:(null)
        sub_alt_name:(null)
        svr_cert_x509:NULL
        csr_attrs:NULL
        csr:NULL
        pkey:NULL
```

```
        header_ptr:NULL
        tmp_p10:NULL
```

b. The FortiProxy sends the current server certificate for authentication/authorization and not the username/password used for initial enrollment:

```
[2453] est_simple_reenroll: Try to use est-test101 as client cert to authenticate
[1962] __est_curl_set_auth: trace
[2011] __est_curl_set_auth: Warning: cert est-test101 may not have the correct key usage
for TLS client authentication
[2014] __est_curl_set_auth: Will use cert est-test101 to prove my identity
...
[1651] curl_header_debug_func: Header received:
[1787] est_curl_req: Response 200
[1788] est_curl_req: Buffer:MCYGBysGAQEBARYGCSqGSIb3DQEJAQYFK4EEACIGCWCGSAFlAwQCAg==
[1439] decode_csrattrs_callback: Decoding csrattrs, resp->len: 57
[1474] decode_csrattrs_callback: Object: 1.3.6.1.1.1.1.22 undefined
[1474] decode_csrattrs_callback: Object: 1.2.840.113549.1.9.1 emailAddress
[1474] decode_csrattrs_callback: Object: 1.3.132.0.34 secp384r1
[1474] decode_csrattrs_callback: Object: 2.16.840.1.101.3.4.2.2 sha384
est_ctx:        is_global:1
        vfid:0
        svr_original_url:https://testrfc7030.com:8443
        svr_hostinfo:Exists
        ca_identifier:
        http_username:estuser
        http_password:estpwd
        clt_cert:est-test101
        svr_cert:
        srp_username:
        srp_password:
        source_ip:(null)
        need_pop:0
        newcert_name:est-test101
        passwd:f51da8548af5fef820edfe6267b0c178e76f7c3eae40ee0900318fc77ab6bd
        rsa_keysize:0
        ec_curvename:(null)
        subject:(null)
        sub_alt_name:(null)
        svr_cert_x509:NULL
        csr_attrs:Exists
        csr:NULL
        pkey:NULL
        header_ptr:NULL
        tmp_p10:NULL
[2274] __est_simple_reenroll: ============STARTED============
```

c. The CSR for renewal is successfully generated:

```
[965] est_generate_csr_from_cert: Successfully generated CSR for est-test101
[2200] __est_simple_post: Data to be posted:
|||MIIBQDCB5gIBAjAbMRkwFwYDVQQDDBBmaXJld2FsbC1wb3J0YWwxMFkwEwYHKoZI
zj0CAQYIKoZIzj0DAQcDQgAEQoJQmPedxPNUcfCyRvpqyt1oiiJX/me+TdButUSu
```

```
8hg+9nPF6+xNf+5LmtG/YKHeXyCKG6xB9OmJf255Zmx+5qBpMGcGCSqGSIb3DQEJ
DjFaMFgwCQYDVR0TBAIwADALBgNVHQ8EBAMCB4AwHQYDVR0OBBYEFJv4OdUh5v9J
/6wCV1v8TBqLHl2PMB8GA1UdIwQYMBaAFBrfOYTCVuZszyq0JqX9DNJD9T0+MAoG
CCqGSM49BAMCA0kAMEYCIQCK3Li51F7fXsyKZwtIcYMFvDobY3cKKTTDixtN7QZ2
jwIhAKUkqfWPAzwcxQaNQw6pyYvo18ymB9aEheeIXZfGI+tV
|||

[1728] est_curl_req: URL: https://testrfc7030.com:8443/.well-known/est/simplereenroll
[1753] est_curl_req: HTTP POST
[1651] curl_header_debug_func: Header received:HTTP/1.1 200 OK
[1651] curl_header_debug_func: Header received:Status: 200 OK
[1651] curl_header_debug_func: Header received:Content-Type: application/pkcs7-mime;
smime-type=certs-only
[1651] curl_header_debug_func: Header received:Content-Transfer-Encoding: base64
[1651] curl_header_debug_func: Header received:Content-Length: 590
[1651] curl_header_debug_func: Header received:
[1787] est_curl_req: Response 200
```

d. The new certificate is received in PKCS #7 and is saved:

```
[1788] est_curl_req:
Buffer:MIIBrQYJKoZIhvcNAQcCoIIBnjCCAZoCAQExADALBgkqhkiG9w0BBwGgggGCMIIB
fjCCASOgAwIBAgIDB0aYMAoGCCqGSM49BAMCMBcxFTATBgNVBAMTDGVzdEV4YW1w
...
[1191] save_pkcs7_certs: Saving pkcs7 response
[505] est_print_pkcs7: Certs: (1 in total)
...
[1220] save_pkcs7_certs: Received 1 certs
[1228] save_pkcs7_certs: Saving cert(s):
        is_global:1
        est_url:https://testrfc7030.com:8443
        source_ip:NULL
        ca_identifier:

[1246] save_pkcs7_certs: Received 1 cert(s)
[427] est_print_x509:         Version: 3 (0x2)
        Serial Number: 476824 (0x74698)
        Issuer: CN=estExampleCA
        Subject: CN=firewall-portal1
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature
            X509v3 Subject Key Identifier:
                9B:F8:39:D5:21:E6:FF:49:FF:AC:02:57:5B:FC:4C:1A:8B:1E:5D:8F
            X509v3 Authority Key Identifier:
                1A:DF:39:84:C2:56:E6:6C:CF:2A:B4:26:A5:FD:0C:D2:43:F5:3D:3E

[827] est_cmdb_update_cert: Cert est-test101 updated in CMDB
[1276] save_pkcs7_certs: The cert is saved!
[592] est_ctx_clear_tmp_data: trace
```

```
[2477] est_simple_reenroll: POST ret:0
[592] est_ctx_clear_tmp_data: trace
```

5. Verify the renewed local certificate configuration:

```
config vpn certificate local
(local) # get est-test101
name                : est-test101
password            : *
comments            :
private-key         : *
certificate         :
        Subject:     CN = firewall-portal1
        Issuer:      CN = estExampleCA
        Valid from:  2023-04-06 22:55:09  GMT
        Valid to:    2024-04-05 22:55:09  GMT
        Fingerprint: D9:51:6C:EF:04:E9:79:8D:A0:EE:10:23:4A:F4:46:B7
        Root CA:     No
        Version:     3
        Serial Num:
                07:46:a5
        Extensions:
                Name:     X509v3 Basic Constraints
                Critical: no
                Content:
```

Note that the `Valid to` date and time is now `2024-04-05 22:55:09 GMT`.

Example 3: manually regenerating a local certificate with EST

Note that manually regenerating the certificate will not generate a new server key pair.

To manually regenerate a local certificate with EST:

1. Run the following command:

```
# execute vpn certificate local generate est est-test101
Certificate 'est-test101' already exists, re-generate will ignore all the options you have
provided.
Are you sure to re-generate the certificate?
Do you want to continue? (y/n) y
```

2. Verify the debugs to confirm that the certificate was generated:

```
# diagnose debug application est -1
# diagnose debug enable
...
[1024] reconstruct_est_ctx: Reconstruction succeeded
est_ctx:        is_global:1
        vfid:0
        svr_original_url:https://testrfc7030.com:8443
```

```
        svr_hostinfo:NULL
        ca_identifier:
        http_username:estuser
        http_password:estpwd
        clt_cert:
        svr_cert:
        srp_username:
        srp_password:
        source_ip:(null)
        need_pop:0
        newcert_name:est-test101
        passwd:f51da8548af5fef820edfe6267b0c178e76f7c3eae40ee0900318fc77ab6bd
        rsa_keysize:0
        ec_curvename:(null)
        subject:(null)
        sub_alt_name:(null)
        svr_cert_x509:NULL
        csr_attrs:NULL
        csr:NULL
        pkey:NULL
        header_ptr:NULL
        tmp_p10:NULL
[2453] est_simple_reenroll: Try to use est-test101 as client cert to authenticate
[1962] __est_curl_set_auth: trace
...
```

3. Once the certificate is saved, verify the local certificate configuration:

```
config vpn certificate local
(local) # get est-test101
name                : est-test101
password            : *
comments            :
private-key         : *
certificate         :
        Subject:     CN = firewall-portal1
        Issuer:      CN = estExampleCA
        Valid from:  2023-04-13 17:23:40  GMT
        Valid to:    2024-04-12 17:23:40  GMT
        Fingerprint: 4A:96:E1:73:6D:D3:64:FE:A3:A8:28:56:1D:39:05:37
        Root CA:     No
        Version:     3
        Serial Num:
                07:47:02
        Extensions:
                Name:     X509v3 Basic Constraints
                Critical: no
                Content:
                CA:FALSE

                Name:     X509v3 Key Usage
                Critical: no
```

```
                Content:
                Digital Signature

                Name:     X509v3 Subject Key Identifier
                Critical: no
                Content:
                9B:F8:39:D5:21:E6:FF:49:FF:AC:02:57:5B:FC:4C:1A:8B:1E:5D:8F

                Name:     X509v3 Authority Key Identifier
                Critical: no
                Content:
                1A:DF:39:84:C2:56:E6:6C:CF:2A:B4:26:A5:FD:0C:D2:43:F5:3D:3E


state               : OK
range               : global
source              : user
source-ip           : 0.0.0.0
ike-localid-type    : asn1dn
enroll-protocol     : est
est-server          : https://testrfc7030.com:8443
est-ca-id           :
est-http-username   : estuser
est-http-password   : estpwd
est-client-cert     :
est-server-cert     :
est-srp-username    :
est-srp-password    :
auto-regenerate-days: 0
auto-regenerate-days-warning: 0
```

The Subject Key Identifier is the same, so no new key pair was generated.

FortiProxy encryption algorithm cipher suites

FortiProxies use SSL/TLS encryption for HTTPS and SSH administrative access. When establishing an SSL/TLS or SSH connection, you can control the encryption level and the ciphers that are used in order to control the security level.

HTTPS access

HTTP administrative access encryption is controlled using the following commands:

```
config system global
    set strong-crypto {enable | disable}
    set admin-https-ssl-versions {tlsv1-1 tlsv1-2 tlsv1-3}
    set admin-https-ssl-ciphersuites {<cipher_1> ... <cipher_n>}
```

```
    set admin-https-ssl-banned-ciphers {<cipher_1> ... <cipher_n>}
end
```

- When strong encryption is enabled, only TLS 1.2 and TLS 1.3 are allowed. If strong encryption is then disabled, TLS 1.1 has to be manually enabled.
- Setting `admin-https-ssl-ciphersuites` controls which cipher suites are offered in TLS 1.3. TLS 1.2 and lower are not affected by this command. To disable all TLS 1.3 cipher suites, remove TLS1-3 from `admin-https-ssl-versions`.
- Setting `admin-https-ssl-banned-ciphers` controls which cipher technologies will not be offered for TLS 1.2 and lower.

The following table lists cipher suites supported by each TLS version:

TLS version	Supported cipher suites	
TLS 1.1[1]	ECDHE-RSA-AES256-SHA[1]	AES256-SHA[1]
	ECDHE-RSA-AES128-SHA[1]	AES128-SHA[1]
TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384	AES256-GCM-SHA384[1]
	ECDHE-RSA-AES128-GCM-SHA256	AES128-GCM-SHA256[1]
	ECDHE-RSA-CHACHA20-POLY1305	AES256-SHA256
	ECDHE-RSA-AES256-SHA384	AES128-SHA256
	ECDHE-RSA-AES128-SHA256	AES256-SHA[1]
	ECDHE-RSA-AES256-SHA[1]	AES128-SHA[1]
	ECDHE-RSA-AES128-SHA[1]	
TLS 1.3	TLS-AES-128-GCM-SHA256	TLS-AES-128-CCM-8-SHA256
	TLS-AES-256-GCM-SHA384	TLS-CHACHA20-POLY1305-SHA256
	TLS-AES-128-CCM-SHA256	

[1] Disabled if strong encryption (`strong-crypto`) is enabled. You must manually enable TLS 1.1 in this case.

SSH access

SSH access encryption is controlled using the following command:

```
config system ssh-config
    set admin-ssh-v1 {enable | disable}
    set strong-crypto {enable | disable}
    set ssh-enc-algo <algo_1> [<algo_2> ... <algo_n>]
    set ssh-kex-algo <algo_1> [<algo_2> ... <algo_n>]
    set ssh-mac-algo <algo_1> [<algo_2> ... <algo_n>]
end
```

The algorithms available when configuring `set ssh-enc-algo` are affected by `set strong-crypto` as follows:

Strong encryption setting	Supported ciphers	
Enabled	aes256-gcm@openssh.com	aes256-ctr
Disabled	chacha20-poly1305@openssh.com	aes128-ctr
	aes192-ctr	aes256-ctr
	arcfour256	arcfour128
	aes128-cbc	3des-cbc
	blowfish-cbc	cast128-cbc
	aes192-cbc	aes256-cbc
	arcfour	rijndael-cbc@lysator.liu.se
	aes128-gcm@openssh.com	aes256-gcm@openssh.com

The following options are available for the `ssh-kex-algo` algorithm based on the strong encryption setting:

Strong encryption setting	Supported ciphers	
Enabled	diffie-hellman-group-exchange-sha256	curve25519-sha256@libssh.org
	ecdh-sha2-nistp256	ecdh-sha2-nistp384
	ecdh-sha2-nistp521	
Disabled	diffie-hellman-group14-sha1	diffie-hellman-group-exchange-sha1
	diffie-hellman-group-exchange-sha256	curve25519-sha256@libssh.org
	ecdh-sha2-nistp256	ecdh-sha2-nistp384
	ecdh-sha2-nistp521	

The following options are available for the `ssh-mac-algo` algorithm based on the strong encryption setting:

Strong encryption setting	Supported ciphers	
Enabled	hmac-sha2-256	hmac-sha2-256-etm@openssh.com
	hmac-sha2-512	hmac-sha2-512-etm@openssh.com

Strong encryption setting	Supported ciphers	
Disabled	hmac-md5	hmac-md5-etm@openssh.com
	hmac-md5-96	hmac-md5-96-etm@openssh.com
	hmac-sha1	hmac-sha1-etm@openssh.com
	hmac-sha2-256	hmac-sha2-256-etm@openssh.com
	hmac-sha2-512	hmac-sha2-512-etm@openssh.com
	hmac-ripemd160	hmac-ripemd160@openssh.com
	hmac-ripemd160-etm@openssh.com	umac-64@openssh.com
	umac-128@openssh.com	umac-64-etm@openssh.com
	umac-128-etm@openssh.com	

Additional features

Security hardening for other FortiProxy features can also be achieved by managing the encryption level or ciphers. See SSL algorithm security level on page 1001 for more information about different levels of security.



An asterisk (*) represents the default values for each feature.

Some of these features are described next.

WAN optimization

For WAN optimization tunnel connections, the encryption algorithm is controlled using the following commands:

```
config wanopt settings
    set tunnel-ssl-algorithm {high* | medium | low}
end
```

Explicit FTP proxy

For explicit FTP proxy, the encryption algorithm is controlled using the following commands:

```
config ftp-proxy explicit
    set ssl-algorithm { high* | medium | low}
end
```

Explicit web proxy

For explicit web proxy, the encryption algorithm is controlled using the following commands:

```
config web-proxy explicit
  edit 1
    set ssl-algorithm {high | medium | low*}
end
```

SSL Server

For SSL server, the TLS versions and the encryption algorithm are controlled using the following commands:

```
config firewall ssl-server
    edit <name>
        set ssl-mode {half | full}
        set ssl-algorithm {high* |medium | low}
        set ssl-max-version {tls-1.0* |tls-1.1 | tls-1.2 | tls-1.3}
        set ssl-min-version {tls-1.0 |tls-1.1 | tls-1.2 | tls-1.3*}
    next
end
```

VIP

For VIP, the TLS versions and the encryption algorithm are controlled using the following commands:

```
config firewall vip
        set ssl-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls1-2 | tls-1.3*}
        set ssl-min-version {ssl-3.0 | tls-1.0 | tls-1.1* | tls1-2 | tls-1.3 | client}
        set ssl-algorithm {high* | medium | low | custom}
        config ssl-cipher-suites
            edit <priority>
                set cipher {TLS-AES-128-GCM-SHA256 | TLS-AES-256-GCM-SHA384|...}
                set versions {option1}, {option2}, ...
            next
        end
        set ssl-server-max-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls1-2 | tls-1.3 | client*}

        set ssl-server-min-version {ssl-3.0 | tls-1.0 | tls-1.1 | tls1-2 | tls-1.3 | client*}

        set ssl-server-algorithm {high | medium | low | custom | client* }
        config ssl-server-cipher-suites
            edit <priority>
                set cipher {TLS-AES-128-GCM-SHA256 | TLS-AES-256-GCM-SHA384|...}
                set versions {option1}, {option2}, ...
            next
        end
```

```
    next
end
```



The command `config ssl-cipher-suites` is available only under certain conditions:

- When `set type` is set to either `server-load-balance` or `access-proxy`
- When `set ssl-algorithm` is set to `custom`

Similarly, the command `config ssl-server-cipher-suites` is available only under certain conditions:

- When `set type` is set to `server-load-balance`
- When `set ssl-mode` is set to `full`
- When `set ssl-algorithm` is set to `custom`

SSL algorithm security level

Option	Description
high	High encryption. Allow only AES and ChaCha.
medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.
low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
*custom	Custom encryption. Use `ssl-server-cipher-suites` to select the cipher suites that are allowed.
*client	Use the same encryption algorithms for both client and server sessions.



The SSL algorithm security levels marked with an asterisk (*) are not supported across different FortiProxy features.

Other Products

The security level of communication to and from FortiProxy can be managed by controlling the encryption level and ciphers used. See Encryption algorithm security level on page 1003for more information about different levels of security.



An asterisk (*) represents the default value for each product.

Some products that commonly interact with the FortiProxy device are listed next.

syslog server

For syslog server, the TLS versions and the encryption algorithm are controlled using the following commands:

```
config log syslogd setting
    set enc-algorithm {high-medium | high | low | disable*}
    set ssl-min-proto-version {default* | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2}
end
config log syslogd override-setting
    set enc-algorithm {high-medium | high | low | disable*}
    set ssl-min-proto-version {default* | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2}
end
```



The command `ssl-min-proto-version` set to `default` means that the system global setting will be followed.

FortiCloud

For logging to FortiCloud, the TLS versions and the encryption algorithm are controlled using the following commands:

```
config log fortiguard setting
    set enc-algorithm {high-medium | high* | low}
    set ssl-min-proto-version {default* | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2}
end
```

FortiAnalyzer Cloud

For FortiAnalyzer Cloud, the TLS versions and the encryption algorithm are controlled using the following commands:

```
config log fortianalyzer-cloud setting
    set enc-algorithm {high-medium | high* | low}
    set ssl-min-proto-version {default* | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2 | TLSv1-3}
end
```

FortiAnalyzer

For FortiAnalyzer, the TLS versions and the encryption algorithm are controlled using the following commands:

```
config log fortianalyzer setting
    set enc-algorithm {high-medium | high* | low}
    set ssl-min-proto-version {default* | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2 | TLSv1-3}
```

```
end
config log fortianalyzer override-setting
    set enc-algorithm {high-medium | high* | low}
    set ssl-min-proto-version {default* | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2 | TLSv1-3}
end
```

FortiSandbox

For FortiSandbox, the TLS versions and the encryption algorithm are controlled using the following commands:

```
config system fortisandbox
    set enc-algorithm {default* | high | low}
    set ssl-min-proto-version {default* | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2}
end
```

FortiManager

For central management, the TLS versions and the encryption algorithm are controlled using the following commands:

```
config system central-management
    set enc-algorithm {default | high* | low}
end
```

Encryption algorithm security level

Option	Description
*high-medium/ default	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithm
low	SSL communication with low encryption algorithms.
*disable	Disable SSL communication.



Encryption algorithm security levels marked with an asterisk (*) are not supported across different products.

Integrating FortiProxy with SafeNet Luna Network HSM

A hardware security module (HSM) is a dedicated device for managing digital keys and performing cryptographic operations. An HSM can be a plug-in card or an external device directly connected to a computer or network server. Purposefully designed to protect the crypto-key life cycle, HSMs have been used by some of the world's most security-conscious entities to protect their cryptographic infrastructure by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device.

Because of their strengths in securing cryptographic keys and provisioning encryption, decryption, authentication, and digital signing services for a wide range of applications, HSMs have been used by enterprises worldwide to safeguard their online transactions, identities, and applications.

Starting from Version 2.0, FortiProxy has integrated with SafeNet Luna Network HSM. It enables you to retrieve a per-connection, SSL session key from the HSM server instead of loading the private key and certificate stored on FortiProxy. The HSM integration supports active-passive and active-active HA modes but not active-passive configuration synchronization (config-sync). You can sync local certificate using HSM to peer FortiProxy appliances but the local certificate may NOT function properly on peer FortiProxy appliances.

To integrate FortiProxy with SafeNet Luna Network HSM:

1. Check if the FortiProxy has already registered with the HSM by running the following command on HSM: `ssh admin@<hsm_ip>`.
   If the FortiProxy IP is listed under the HSM client list, clear up existing configuration by running the following commands:
   - `client revokePartition -client <fortiproxy_ip> -partition fortiproxy`
   - `client delete -client <fortiproxy_ip> –force`
2. Create and initialize a new HSM partition that uses password authentication using the `partition create` command on HSM. HSM partition is a global configuration that can be used from individual VDOMs.

   This is the partition FortiProxy uses on the HSM server. You can create more than one partition, but all the partitions are assigned to the same client. For more information, see SafeNet Luna Network HSM documentation.

3. Retrieve the server certificate file from the HSM server using the SCP utility and the following command:
   `scp <hsm_username>@<hsm_ip>:server.pem /usr/lunasa/bin/server_<hsm_ip>.pem`
4. Configure the HSM by running the `config system nethsm` command on the FortiProxy. You need to specify the HSM server certificate and the partition name/password. See config

```
config system nethsm
   set status enable
   set interface "port1"
   config servers
      edit "us_hsm"
         set server "172.30.30.13"
```

```
            set server-cert "copy over the HSM server certificate from previous step"
            set htl disable
        next
    end
        config slots
            edit "fortiproxy"
                set id <partition name on the HSM server>
                set password <partition password on the HSM server>
            next
        end
    end
```

The HSM configuration also generates a default FortiProxy client certificate, which can be displayed by running the `execute nethsm client-cert-show` command. To re-generate the client certificate, run the `execute nethsm client-cert-create` command.

5. Export the FortiProxy client certificate to local PC using the following command: `execute nethsm client-cert-export`.
6. Send the FortiProxy client certificate to the HSM using the SCP utility and the following command:
   `scp <fortiproxy_ip>.pem admin@<hsm_ip>:`
7. Connect to the HSM server using an admin account via SSH and register a client for FortiProxy on the HSM server using the following command:
   `lunash:> client register -c <client_name> -ip <fortiproxy_ip>`, where `<client_name>` is the name you specify that identifies the client.
   You can verify the client registration using the `exe nethsm diagnose`command.
8. Assign the client you registered to the partition you've created in step 2 above using the following command:
   `lunash:> client assignPartition -client <client_name> -partition <partition_name>`
   You can verify the assignment using the following command:
   `lunash:> client show -client <client_name>`
9. Repeat the client assignment process for any additional partitions you've created for FortiProxy.
10. In FortiProxy, generate a certificate-signing request that includes the HSM's configuration information.
    The CSR generation process creates a private key on both the HSM and FortiProxy. The private key on the HSM is the "real" key that secures communication when FortiProxy uses the signed certificate. The key found on the FortiProxy is to indicate the HSM server information when you upload the certificate to FortiProxy.
11. Download the certificate request (`.csr`) file under *System > Certificates > Local Certificates* in FortiProxy.
12. Upload the certificate request (`.csr`) file to your certificate authority (CA) under *System > Certificates > Create/Import > CA Certificate*. See Import a CA certificate on page 982.
13. Upload the HSM server certificate (that you obtained in step 3) under *System > Certificates > Create/Import > Certificate*. See Import a local certificate on page 978.
14. You can then use the HSM server in a policy or server pool configuration by referencing the HSM certificate.
15. In case of any server or client changes, you must re-configure the FortiProxy-HSM integration which involves deleting the intermediate CA, deleting the server and partitions, and then reset the configuration using the `exe nethsm reset`command on FortiProxy.

16. To configure FortiProxy HA with SafeNet Network HSM, follow the steps below:
    a. Enable HA with HSM by running the following command on the FortiProxy:
    ```
    config system nethsm
    set ha enable
    ```
    b. Disable Network Trust Links (NTLs) IP check (ntls ipcheck) on the HSM server.
    c. Configure multiple HSM servers with the same software version and multiple partitions with the same domain name and password. Refer to the steps above for instructions about creating one single HSM server or partition. Alternatively, use the `config system nethsm` command on the FortiProxy to set up the HA cluster with HSM:
    ```
    config system nethsm
       set ha enable
          config hagroups
             edit "hagroup1"
                set member "partition_1" "partition_2"
             next
          end
       end
    end
    config slots
       edit “partition_1”
          set id 0
          set password <password>
             next
             edit “partition_2”
                set id 1
                set password <password>
             next
             edit “hagroup1” <<<< virtual slot created by background process, which is used to
                   create the CSR>
          set id 5
          set password <password>
       next
    end
    ```
    d. Register each client to all HSM servers. Refer to the steps above for instructions about registering a client to an HSM server.

Configuration backups and reset

You can use the GUI or CLI to back up the configuration in FortiProxy or YAML format. You have the option to save the configuration file in FortiProxy format to various locations including the local PC, USB key, FTP, and TFTP server. FTP and TFTP are only configurable through the CLI. In YAML format, configuration files can be backed up or restored on an FTP or TFTP server through the CLI.



Administrators can back up a configuration file when using an admin profile with access permissions for *System* set to *Read/Write*. Therefore, administrators using admin profiles with access permissions for *System* set to *Read* cannot back up a config file from the FortiProxy or through SCP.

For more granularity within the admin profile, set access permission for *System* to *Custom* to access additional fields. When *System* is set to *Custom*, the *Administrator Users* field dictates whether the config file can be backed up in the GUI. Whereas the *Configuration* field dictates whether the config file can be backed up in the CLI.

This topic includes the following information:

- Backing up and restoring configurations from the GUI on page 1007
- Backing up and restoring configurations from the CLI on page 1009
- Configuration revision on page 1013
- Restore factory defaults on page 1014
- Secure file copy on page 1015

Backing up and restoring configurations from the GUI

Configurations can be backed up using the GUI to your PC or a USB disk.

Field	Description
Scope	When the FortiProxy is in multi-vdom mode and a user is logged in as a global administrator.
Backup to	You can choose where to save the configuration backup file. • *Local PC*: Save the configuration file to your PC. • *USB Disk*: Save the configuration file to an external USB disk. This option is not available if there is no USB drive inserted in the USB port. You can also back up to FortiManager using the CLI.
File format	The configuration file can be saved in FortiProxy or YAML format.
Password mask	Use password masking when sending a configuration file to a third party, such as Fortinet Inc. Support. When password masking is enabled, passwords and secrets will be replaced in the configuration file with `FortinetPasswordMask` to avoid information being unintentionally leaked.
Encryption	Enable *Encryption* to encrypt the configuration file. A configuration file cannot be restored on the FortiProxy without a set password. Encryption must be enabled on the backup file to back up VPN certificates. Encryption is performed using AES-GCM algorithm.

To mask passwords in the GUI:

1. Click on the username in the upper right-hand corner of the screen and select *Configuration* > *Backup*.
2. Select *YAML* as the *File format*.
3. Enable *Password mask*. A warning message is displayed.
4. Click *OK*. The configuration file is saved to your computer with passwords and secrets obfuscated.

The following is an example of output with password masking enabled:

```
config system admin
    edit "1"
        set accprofile "prof_admin"
        set vdom "root"
        set password FortinetPasswordMask
    next
end
config vpn ipsec phase1-interface
    edit "vpn-1"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: vpn-1 (Created by VPN wizard)"
        set wizard-type static-fortiproxy
        set remote-gw 172.16.200.55
        set psksecret FortinetPasswordMask
    next
end
config wireless-controller vap
    edit "ssid-1"
        set passphrase FortinetPasswordMask
        set schedule "always"
    next
end
```

Restoring configuration files from the GUI

Configuration files can be used to restore the FortiProxy to a previous configuration in the *Restore System Configuration* page.

To restore the FortiProxy configuration using the GUI:

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration* > *Restore*.
2. Identify the source of the configuration file to be restored: your *Local PC* or a *USB Disk*.
   The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.
3. Click *Upload*, locate the configuration file, and click *Open*.

4. Enter the password if required.
5. Click *OK*.

When restoring a configuration file that has password masking enabled, obfuscated passwords and secrets will be restored with the password mask.



Restoring the FortiProxy with a configuration with passwords obfuscated is not recommended.

To restore an obfuscated YAML configuration using the GUI:

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration* > *Restore*.
2. Click *Upload*. The File Explorer is displayed.
3. Navigate to the configuration file and click *Open*.
4. (Optional) Enter the file password in the *Password* field.
5. Click *OK*. The *Confirm* pane is displayed with a warning.
6. Toggle the acknowledgment.
7. Click *OK*.

Backing up and restoring configurations from the CLI

Configuration backups in the CLI are performed using the `execute backup` commands and can be backed up in FortiProxy and YAML format.

Configuration files can be backed up to various locations depending on the command:

- `flash`: Backup the configuration file to the flash drive.
- `ftp`: Backup the configuration file to an FTP server.
- `management-station`: Backup the configuration file to a management station, such as FortiManager or FortiGate Cloud.
- `sftp`: Backup the configuration file to a SFTP server.
- `tftp`: Backup the configuration file to a TFTP server.
- `usb`: Backup the configuration file to an external USB drive.
- `usb-mode`: Backup the configuration file for USB mode.

Command	Description
`# execute backup config`	Back up the configuration in FortiProxy format. Backup your configuration file to: • `flash` • `ftp` • `management-station` • `sftp`

Command	Description
	• tftp • usb • usb-mode
# execute backup full-config	Backup the configuration, including backups of default configuration settings. Backup your configuration file to: • ftp • sftp • tftp • usb • usb-mode
# execute backup yaml-config	Backup the configuration in YAML format. Backup your configuration file to: • ftp • tftp
# execute backup obfuscated-config	Backup the configuration with passwords and secrets obfuscated. Backup your configuration file to: • ftp • management-station • sftp • tftp • usb
# execute backup obfuscated-full-config	Backup the configuration (including default configuration settings) with passwords and secrets obfuscated. Backup your configuration file to: • ftp • sftp • tftp • usb
# execute backup obfuscated-yaml-config	Backup the configuration in YAML format with passwords and secrets obfuscated. Backup your configuration file to: • ftp • tftp

To back up the configuration in FortiProxy format using the CLI:

For FTP, note that port number, username are optional depending on the FTP site:

```
# execute backup config ftp <backup_filename> <ftp_server>[<:ftp_port>] [<user_name>] [<password>]
[<backup_password>]
```

or for TFTP:

```
# execute backup config tftp <backup_filename> <tftp_servers> [<backup_password>]
```

or for SFTP:

```
# execute backup config sftp <backup_filename> <sftp_server>[<:sftp_port>] <user> <password>
[<backup_password>]
```

or:

```
# execute backup config management-station <comment>
```

or:

```
# execute backup config usb <backup_filename> [<backup_password>]
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom
    edit <vdom_name>
```

See Backing up and restoring configurations in multi VDOM mode on page 900 for more information.

When backing up a configuration in YAML format, if it is not already specified in the file name, `.yaml` will be appended to the end. For example, if the file name entered is `301E.conf`, the name will become `301E.conf.yaml` after the configuration is backed up.

To back up the configuration in YAML format using the CLI:

```
# execute backup yaml-config {ftp | tftp} <filename> <server> [username] [password]
```

For example:

```
# execute backup yaml-config  tftp  301E.conf 172.16.200.55
    Please wait...
    The suffix '.yaml' will be appended to the filename if user does not add it specifically.
    Connect to tftp server 172.16.200.55 ...
    #
    Send config file to tftp server OK.
```

Configuration files can be configured with obfuscated passwords and secrets to not unintentionally leak information when sharing configuration files with third parties.

To mask passwords in a configuration backup in the CLI:

```
# execute backup obfuscated-config {ftp | management-station | sftp | tftp | usb}
```

To mask passwords in the full configuration backup in the CLI:

```
# execute backup obfuscated-full-config {ftp | sftp | tftp | usb}
```

To mask passwords in a configuration backup with YAML formatting in the CLI:

```
# execute backup obfuscated-yaml-config {ftp | tftp}
```



If a configuration is being backed up on a server, server information must be included with the command. Other information that may be required with an execute backup command includes file names, passwords, and comments.

Restoring configuration files from the CLI

Configuration files can be used to restore the FortiProxy using the CLI.

Command	Description
`# execute restore config`	Restore a configuration that is in FortiProxy or YAML format. The file format is automatically detected when it is being restored. Configurations can be loaded from: • `flash`: Load the configuration file from flash to firewall. • `ftp`: Load the configuration file from an FTP server. • `management-station`: Load the configuration from a management station. • `tftp`: Load the configuration from from a TFTP server. • `usb`: Load the configuration file from an external USB disk to firewall. • `usb-mode`: Load the configuration file from an external USB disk and reboot.

To restore the FortiProxy configuration using the CLI:

For FTP, note that port number, username are optional depending on the FTP site:

```
# execute restore config ftp <backup_filename> <ftp_server>[<:port>] [<user_name>] [<password>]
[<backup_password>]
```

or for TFTP:

```
# execute restore config tftp <backup_filename> <tftp_server> [<backup_password>]
```

For restoring the configuration from FortiManager or FortiGate Cloud:

```
# execute restore config management-station normal <revision ID>
```

or:

```
# execute restore config usb <backup_filename> [<backup_password>]
```

The FortiProxy will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored.

Troubleshooting

When restoring a configuration, errors may occur, but the solutions are usually straightforward.

Error message	Reason and Solution
Configuration file error	This error occurs when attempting to upload a configuration file that is incompatible with the device. This may be due to the configuration file being for a different model or being saved from a different version of firmware. **Solution**: Upload a configuration file that is for the correct model of FortiProxy device and the correct version of the firmware.
Invalid password	When the configuration file is saved, it can be protected by a password. The password entered during the upload process is not matching the one associated with the configuration file. **Solution**: Use the correct password if the file is password protected.

Configuration revision

You can manage multiple versions of configuration files on models that have a 512MB flash memory and higher. Revision control requires either a configured central management server or the local hard drive, if your FortiProxy has this feature. Typically, configuration backup to local drive is not available on lower-end models.

Central management server

The central management server can either be a FortiManager unit or FortiGate Cloud.

If central management is not configured on your FortiProxy, a message appears instructing you to either enable central management, or obtain a valid license.

To enable central management from the GUI:

1. Go to *Security Fabric* > *Fabric Connectors* and double-click the *Central Management* card.
2. Set the *Status* to *Enabled* and select a *Type*.
3. Click *OK*.

To enable central management from the CLI:

```
config system central-management
    set type {fortimanager | fortiguard}
    set mode backup
    set fmg <IP address>
end
```

To backup to the management server:

```
# execute backup config management-station <comment>
```

To view a backed up revision:

```
# execute restore config management-station normal 0
```

To restore a backed up revision:

```
# execute restore config management-station normal <revision ID>
```

Backing up to a local disk

When revision control is enabled on your FortiProxy unit, and configuration backups have been made, a list of saved revisions of those backed-up configurations appears.

Configuration backup occurs by default with firmware upgrades but can also be configured to occur every time you log out.

To configure configuration backup when logging out:

```
config system global
  set revision-backup-on-logout enable
end
```

To manually force backup:

```
# execute backup config flash <comment>
```

Configuration revisions are viewed by clicking on the user name in the upper right-hand corner of the screen and selecting *Configuration* > *Revisions*.

To view a list of revisions backed up to the disk from the CLI:

```
# execute revision list config
```

To restore a configuration from the CLI:

```
# execute restore config flash <revision ID>
```

Restore factory defaults

There may be a need to reset the FortiProxy to its original defaults; for example, to begin with a fresh configuration. There are two options when restoring factory defaults:

`# execute factoryreset`	Reset the device to factory default configuration. The firmware version and antivirus and IPS attack definitions are not changed.
`# execute factoryreset2`	Reset to factory default configuration without losing management access to the FortiProxy. Interface and VDOM configurations, as well as the firmware version and antivirus and IPS attack definitions, are not changed.

Secure file copy

You can also back up and restore your configuration using Secure File Copy (SCP). See How to download a FortiGate configuration file and upload firmware file using secure file copy (SCP).

You enable SCP support using the following command:

```
config system global
    set admin-scp enable
end
```

For more information about this command and about SCP support, see config system global.

Security Fabric

The Fortinet Security Fabric provides a visionary approach to security that allows your organization to deliver intelligent, powerful, and seamless security. Fortinet offers security solutions for endpoints, access points, network elements, the data center, applications, cloud, and data, designed to work together as an integrated security fabric that can be integrated, analyzed, and managed to provide end-to-end protection for your network. Your organization can also add third-party products that are members of the Fortinet Fabric-Ready Partner Program to the Security Fabric.

All elements in the Security Fabric work together as a team to share policy, threat intelligence, and application flow information. This collaborative approach expands network visibility and provides fast threat detection in real time and the ability to initiate and synchronize a coordinated response, no matter which part of the network is being compromised. The Security Fabric allows your network to automatically see and dynamically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware.

The Security Fabric is designed to cover the entire attack surface and provide you with complete visibility into your network. It allows you to collect, share, and correlate threat intelligence between security and network devices, centrally manage and orchestrate policies, automatically synchronize resources to enforce policies, and coordinate a response to threats detected anywhere across the extended network. The unified management interface provides you with cooperative security alerts, recommendations, audit reports, and full policy control across the Security Fabric that will give you confidence that your network is secure.

This section describes the following topics:

- Automation stitches on page 1016
- Fabric Connectors on page 1077
- External Connectors on page 1106
- Asset Identity Center on page 1132

Automation stitches

Automation stitches automate the activities between the different components in the Security Fabric, which decreases the response times to security events. Events from any source in the Security Fabric can be monitored, and action responses can be set up to any destination.



Automation stitches can also be used on FortiProxy devices that are not part of a Security Fabric.

An automation stitch consists of two parts: the trigger and the actions. The trigger is the condition or event on the FortiProxy that activates the action, for example, a specific log, or a failed log in attempt. The action is what the FortiProxy does in response to the trigger.

Automation stitches that use cloud-based actions (AWS Lambda, Azure Function, Google Cloud Function, and AliCloud Function) have the option to delay an action after the previous action is completed.

Diagnose commands are available in the CLI to test, log, and display the stitch history and settings.

Automation stitches can only be created on the root FortiProxy in a Security Fabric.

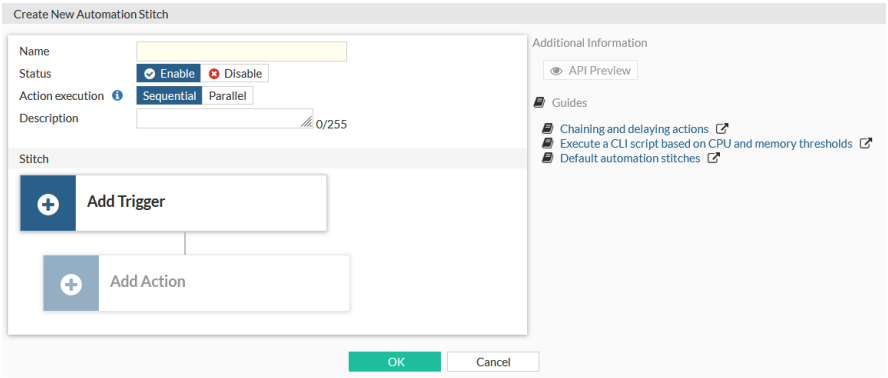
Creating automation stitches

To create an automation stitch, a trigger event and a response action or actions are selected. Automation stitches can be tested after they are created.

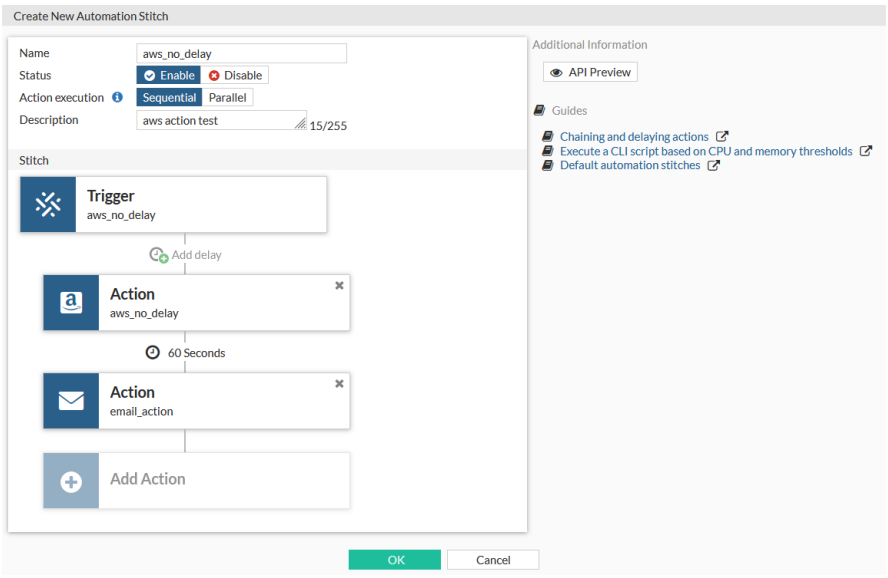
In the GUI, go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*. Automation stitches, actions, and triggers are configured in separate dialogs.

The stitch *Action execution* can be set to either *Sequential* or *Parallel*. In sequential execution, actions will execute one after another with a delay (if specified). If one action fails, then the action chain stops. This is the default setting. In parallel execution, all actions will execute immediately when the stitch is triggered.

When creating a stitch, clicking *Add Trigger* and *Add Action* displays the lists of available triggers and actions, and the option to create new ones.



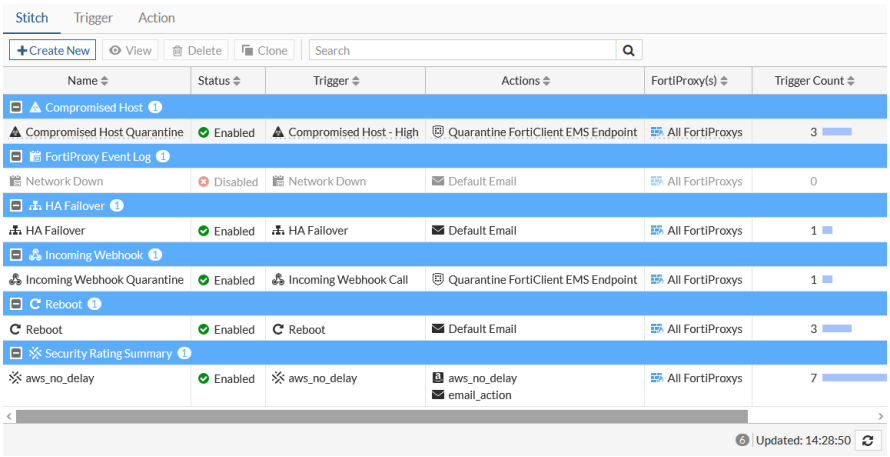
Once the stitch is configured, a process diagram of the trigger, actions, and delays is displayed. A delay can be added before an action if *Sequential* action execution is used. Executing the next action can be delayed by up to 3600 seconds (one hour).



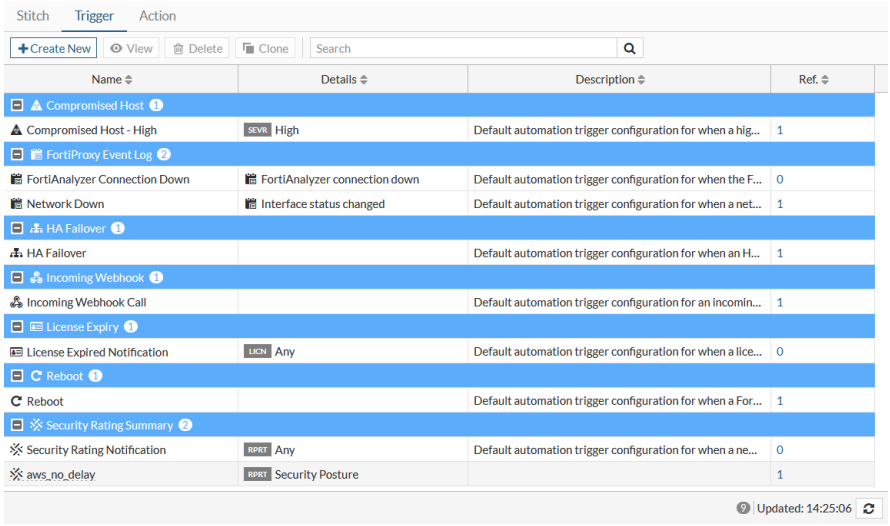
Triggers and actions can be configured separately, and then added to an automation stitch.

Tabs on the Automation page

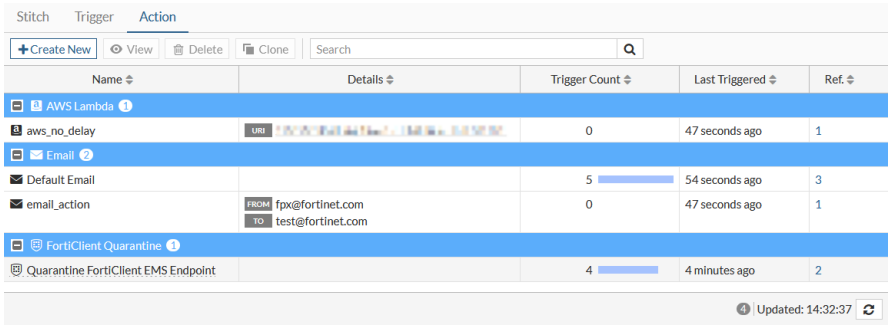
On the *Security Fabric* > *Automation* page, there are tabs for *Stitch*, *Trigger*, and *Action*. The *Stitch* tab is the default view that lists the trigger and actions used in each stitch. Individual triggers and actions can be created or edited in the corresponding tabs.



Click *Trigger* to view the list of triggers.



Click *Action* to view the list of actions.



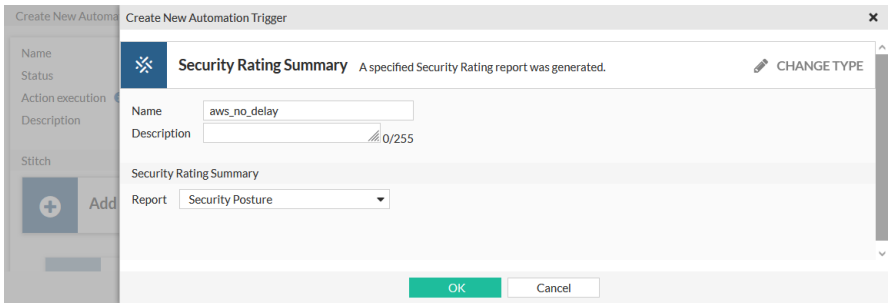
Sample configuration

The following example shows how to configure a Security Rating Summary automation stitch with AWS Lambda and Email actions. There is a 60-second delay before the Email action.

To configure the automation stitch in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name and description.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	*aws_no_delay*
Report	*Security Posture*



d. Click *OK*.

e. Select the trigger in the list and click *Apply*.

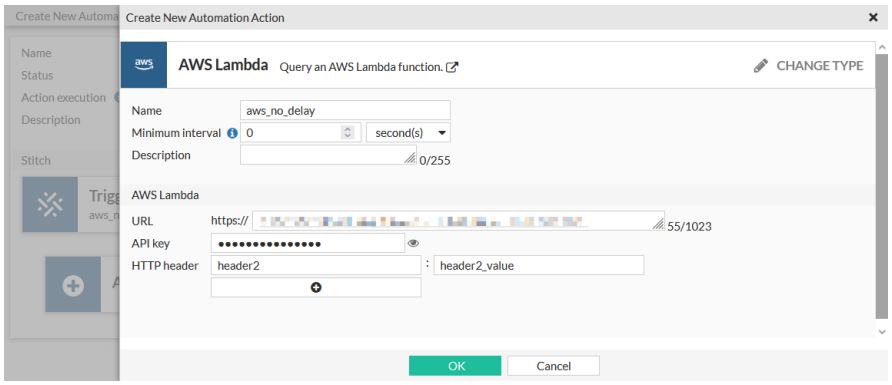
4. Configure the AWS Lambda function action:

a. Click *Add Action*.

b. Click *Create* and select *AWS Lambda*.

c. Enter the following:

Name	*aws_no_delay*
URL	Enter the request API URI
API key	Enter the API key
HTTP header	*header2 : header2_value*



d. Click *OK*.

e. Select the action in the list and click *Apply*.

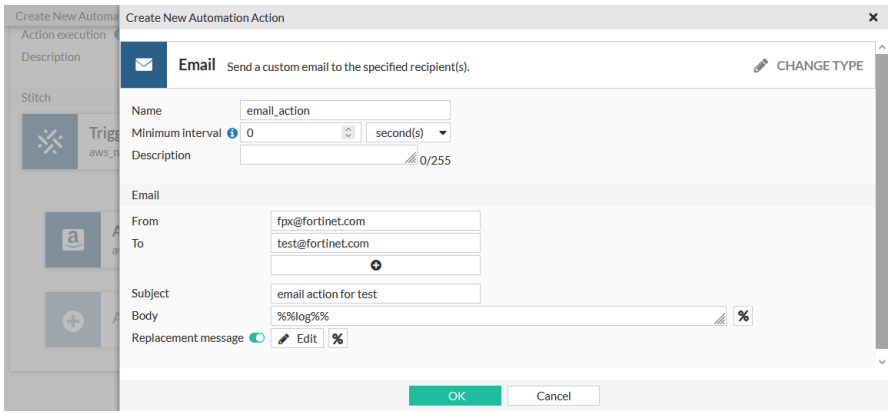
5. Configure the Email notification action:

a. Click *Add Action*.

b. Click *Create* and select *Email*.

c. Enter the following:

Name	*email_action*
To	Enter an email address
Subject	*email action for test*
Replacement message	Enable



d. Click *OK*.

e. Select the action in the list and click *Apply*.

6. Click the *Add delay* located between both actions. Enter *60* and click *OK*.
7. Click *OK*.

To configure the automation stitch in the CLI:

1. Configure the trigger:

```
config system automation-trigger
    edit "aws_no_delay"
        set event-type security-rating-summary
    next
end
```

2. Configure the actions:

```
config system automation-action
    edit "aws_no_delay"
        set action-type aws-lambda
        set aws-api-key xxxxxxxxxxxx
        set uri "xxxxxxxxxx.execute-api.us-east-1.amazonaws.com/xxxxxxxxxx"
        set headers "header2:header2_value"
    next
    edit "email_action"
        set action-type email
        set email-to "test@fortinet.com"
        set email-from "fpx@fortinet.com"
        set email-subject "email action for test"
        set replacement-message enable
    next
end
```

3. Configure the stitch:

```
config system automation-stitch
    edit "aws_no_delay"
        set description "aws action test"
        set trigger "aws_no_delay"
```

```
        config actions
            edit 1
                set action "aws_no_delay"
                set required enable
            next
            edit 2
                set action "email_action"
                set delay 60
                set required enable
            next
        end
    next
end
```

Testing automation stitches

In the GUI, go to *Security Fabric > Automation*, select the *Stitch* tab, right-click on the automation stitch, and select *Test Automation Stitch*.

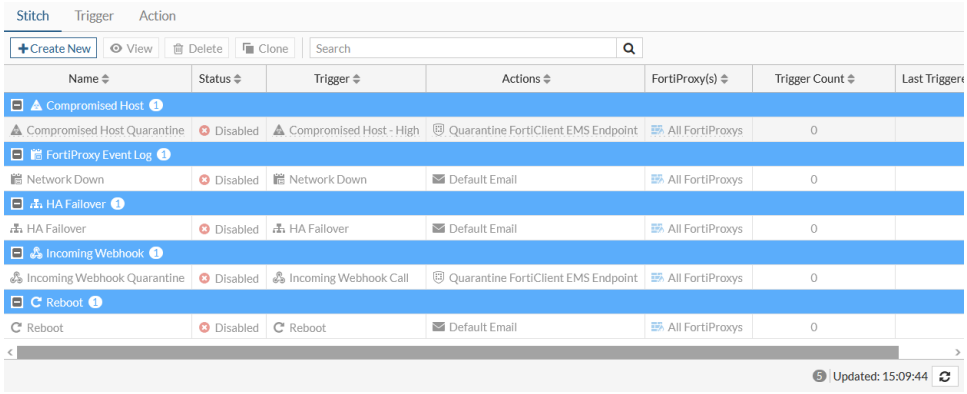
In the CLI, enter `diagnose automation test <automation-stitch name>`.

Default automation stitches

The following default automation stitches are included in FortiProxy:

- Compromised Host Quarantine
- Network Down
- HA Failover
- Incoming Webhook Quarantine
- Reboot

To view and edit the automation stitches in the GUI, go to *Security Fabric > Automation* and select the *Stitch* tab..



CLI configurations

Compromised Host Quarantine

```
config system automation-action
    edit "Quarantine FortiClient EMS Endpoint"
        set description "Default automation action configuration for quarantining a FortiClient
EMS endpoing device."
        set action-type quarantine-forticlient
    next
end
```

```
config system automation-trigger
    edit "Compromised Host - High"
        set description "Default automation trigger configuration for when a high severity
compromised host is detected."
    next
end
```

```
config system automation-stitch
    edit "Compromised Host Quarantine"
        set description "Default automation stitch to quarantine a high severity compromised host
on FortiClient EMS."
        set status disable
        set trigger "Compromised Host - High"
        config actions
            edit 1
                set action "Quarantine FortiClient EMS Endpoint"
            next
        end
    next
end
```

Network Down

```
config system automation-action
     edit "Default Email"
        set description "Default automation action configuration for sending an email with basic
information on the log event."
        set action-type email
        set email-subject "%%log.logdesc%%"
    next
end
```

```
config system automation-trigger
    edit "Network Down"
        set description "Default automation trigger configuration for when a network connection
goes down."
        set event-type event-log
        set logid 20099
```

```
        config fields
            edit 1
                set name "status"
                set value "DOWN"
            next
        end
    next
end
```

```
config system automation-stitch
    edit "Network Down"
        set description "Default automation stitch to send an email when a network goes down."
        set status disable
        set trigger "Network Down"
        config actions
            edit 1
                set action "Default Email"
            next
        end
    next
end
```

HA Failover

```
config system automation-action
    edit "Default Email"
        set description "Default automation action configuration for sending an email with basic
information on the log event."
        set action-type email
        set email-subject "%%log.logdesc%%"
    next
end
```

```
config system automation-trigger
    edit "HA Failover"
        set description "Default automation trigger configuration for when an HA failover occurs."
        set event-type ha-failover
    next
end
```

```
config system automation-stitch
    edit "HA Failover"
        set description "Default automation stitch to send an email when a HA failover is
detected."
        set status disable
        set trigger "HA Failover"
        config actions
            edit 1
                set action "Default Email"
            next
        end
```

```
    next
end
```

Incoming Webhook Quarantine

```
config system automation-action
    edit "Quarantine FortiClient EMS Endpoint"
        set description "Default automation action configuration for quarantining a FortiClient
EMS endpoing device."
        set action-type quarantine-forticlient
    next
end
```

```
config system automation-trigger
    edit "Incoming Webhook Call"
        set description "Default automation trigger configuration for an incoming webhook."
        set event-type incoming-webhook
    next
end
```

```
config system automation-stitch
    edit "Incoming Webhook Quarantine"
        set description "Default automation stitch to quarantine a provided MAC address on
FortiClient EMS using an Incoming Webhook."
        set status disable
        set trigger "Incoming Webhook Call"
        config actions
            edit 1
                set action "Quarantine FortiClient EMS Endpoint"
            next
        end
    next
end
```

Reboot

```
config system automation-action
    edit "Default Email"
        set description "Default automation action configuration for sending an email with basic
information on the log event."
        set action-type email
        set email-subject "%%log.logdesc%%"
    next
end
```

```
config system automation-trigger
    edit "Reboot"
        set description "Default automation trigger configuration for when a FortiProxy is
rebooted."
        set event-type reboot
```

```
    next
end
```

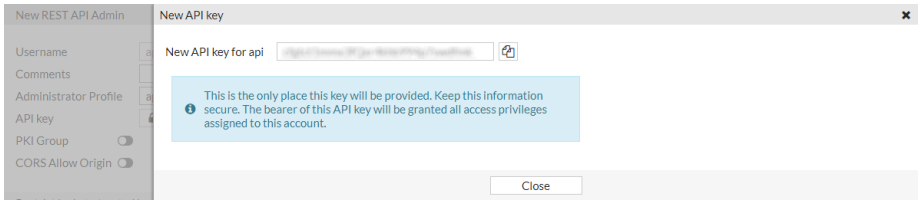
```
config system automation-stitch
    edit "Reboot"
        set description "Default automation stitch to send an email when a FortiProxy is
rebooted."
        set status disable
        set trigger "Reboot"
        config actions
            edit 1
                set action "Default Email"
            next
        end
    next
end
```

Incoming Webhook Quarantine stitch

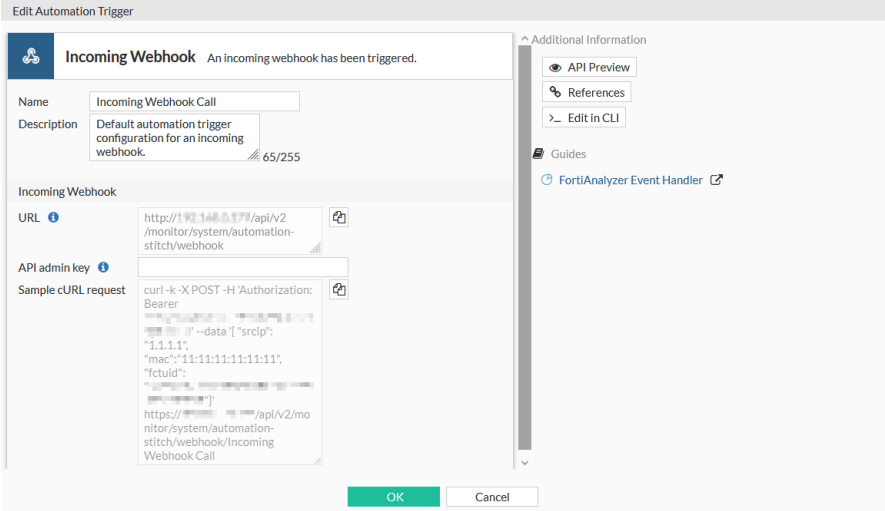
The Incoming Webhook Quarantine stitch for API calls to the FortiProxy accepts multiple parameters (MAC address and FortiClient UUID) from an Incoming Webhook trigger, which enacts either the Access Layer Quarantine action (MAC address) or the FortiClient Quarantine action (FortiClient UUID). This is a default automation stitch included in FortiOS.

To trigger the Incoming Webhook Quarantine stitch in the GUI:

1. Create a new API user:
   a. Go to *System > Administrators*.
   b. Click *Create New > REST API Admin*.
   c. Configure the *New REST API Admin* settings, and copy the API key to the clipboard.



2. Enable the stitch:
   a. Go to *Security Fabric > Automation* and select the *Stitch* tab.
   b. Under *Incoming Webhook*, right-click *Incoming Webhook Quarantine*, and select *Select Status > Enable*.
3. Get the sample cURL request:
   a. Go to the *Trigger* tab.
   b. Under *Incoming Webhook*, right-click *Incoming Webhook Call*, and select *Edit*.
   c. In the *API admin key* field, enter the API key you recorded previously. The *Sample cURL request* field updates.



d. Copy the *Sample cURL request* to the clipboard.

e. Click *OK*.

4. Execute the request:

a. Edit the sample cURL request you just copied.

b. Add parameters to the data field (`"mac"` and `"fctuid"`), and then execute the request.

```
root@pc:~# curl -k -X POST -H 'Authorization: Bearer cfgtct1mmx3fQxr4khb994p7swdfmk' --data
'{ "mac":"0c:0a:00:0c:ce:b0", "fctuid": "0000BB0B0ABD0D00B0D0A0B0E0F0B00B"}'
https://172.16.116.226/api/v2/monitor/system/automation-
stitch/webhook/Incoming%20Webhook%20Quarantine
{
   "http_method":"POST",
   "status":"success",
   "http_status":200,
   "serial":"FGT00E0Q00000000",
   "version":"v6.4.0",
   "build":1545
```

Encode spaces in the automation stitch name with `%20`. For example, `Incoming%20Webhook%20Quarantine`

Once the automation stitch is triggered, the MAC address is quarantined by the FortiProxy, and an event log is created. The FortiClient UUID is quarantined on the EMS server side.

To trigger the Incoming Webhook Quarantine stitch in the CLI:

1. Create a new API user and note the API key:

```
config system api-user
```

2. Enable the automation stitch:

```
config system api-user
    edit "api"
```

```
        set api-key ************
        set accprofile "api_profile"
        set vdom "root"
        config trusthost
            edit 1
                set ipv4-trusthost 10.6.30.0 200.200.200.0
            next
        end
    next
end
```

3. Edit the cURL request to include parameters in the data field ("mac" and "fctuid"), then execute the request:

```
root@pc56:~# curl -k -X POST -H 'Authorization: Bearer cfgtct1mmx0fQxr4khb000p70wdfmk' --
data '{ "mac":"0c:0a:00:0c:ce:b0", "fctuid": "3000BB0B0ABD0D00B0D0A0B0E0F0B00B"}'
https://100.10.100.200/api/v2/monitor/system/automation-
stitch/webhook/Incoming%20Webhook%20Quarantine
{
   "http_method":"POST",
   "status":"success",
   "http_status":200,
   "serial":"FGT80E0Q00000000",
   "version":"v6.4.0",
   "build":1545
```



Encode spaces in the automation stitch name with %20. For example, Incoming%20Webhook%20Quarantine.

Once the automation stitch is triggered, the MAC address is quarantined by the FortiProxy, and an event log is created. The FortiClient UUID is quarantined on the EMS server side.

Sample log

```
date=2020-02-14 time=15:37:48 logid="0100046600" type="event" subtype="system" level="notice"
vd="root" eventtime=1581723468644200712 tz="-0800" logdesc="Automation stitch triggered"
stitch="Incoming Webhook Quarantine" trigger="Incoming Webhook Quarantine"
stitchaction="Compromised Host Quarantine_quarantine,Compromised Host Quarantine_quarantine-
forticlient" from="log" msg="stitch:Incoming Webhook Quarantine is triggered."
```

Triggers

The following table outlines the available triggers.

Category	Trigger	Description
Security Fabric		

Category	Trigger	Description
	Compromised Host	An indicator of compromise (IoC) is detected on a host endpoint. The threat level must be selected and can be *Medium* or *High*. If *Medium* is selected, both medium and high level threats are included. Additional actions are available only for *Compromised Host* triggers: • Access Layer Quarantine • FortiClient Quarantine • VMware NSX Security Tag • IP Ban
	Security Rating Summary	A summary is available for a recently run Security Rating report. Options include: • Security Posture • Fabric Coverage • Optimization • Any
	FortiAnalyzer Event Handler	The specified FortiAnalyzer event handler has occurred.
	Fabric Connector Event	An event has occurred on a specific Fabric connector.
System		
	Reboot	A FortiProxy is rebooting.
	HA Failover	An HA failover has occurred.
	Conserve Mode	A FortiProxy entered conserve mode due to low memory. See Execute a CLI script based on CPU and memory thresholds on page 1062 for an example.
	Configuration Change	An administrator's session that changed a FortiProxy's configuration has ended.
	License Expiry	A FortiGuard license is expiring. The license type must be selected. Options include: • FortiCare Support • FortiGuard Web Filter • FortiGuard AntiSpam • FortiGuard AntiVirus • FortiGuard IPS • FortiGuard Management Service • FortiGate Cloud • Any
	AV & IPS DB Update	The antivirus and IPS database has been updated.

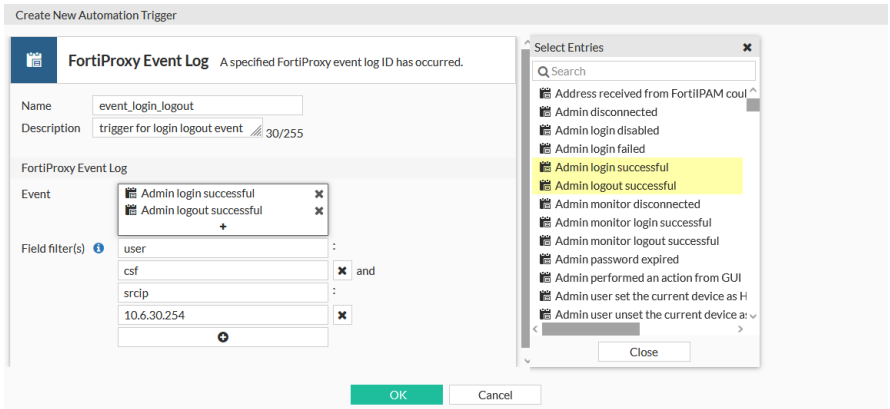
Category	Trigger	Description
	High CPU	A FortiProxy has high CPU usage. See Execute a CLI script based on CPU and memory thresholds on page 1062 for an example.
Miscellaneous		
	FortiProxy Event Log	A specified FortiProxy event log ID has occurred. Multiple event log IDs can be selected, and log field filters can be applied. See FortiProxy event log trigger on page 1030 for an example.
	Incoming Webhook	An incoming webhook has been triggered.
	Schedule	A scheduled monthly, weekly, daily, or hourly trigger. Set to occur on a specific minute of an specific hour on a specific day.

FortiProxy event log trigger

You can configure a FortiProxy event log trigger for when a specific event log ID occurs. You can select multiple event log IDs, and apply log field filters.

To configure a FortiProxy event log trigger in the GUI:

1. Go to *Security Fabric* > *Automation*, select the *Trigger* tab, and click *Create New*.
2. In the *Miscellaneous* section, click *FortiProxy Event Log*.
3. Enter a name and description.
4. In the *Event* field, click the *+* to select multiple event log IDs.
   The *Event* options correspond to the *Message Meaning* listed in the Log Message Reference. Hover over an entry to view the tooltip that includes the event ID and log name. In this example, the *Admin login successful* event in the GUI corresponds to log ID *32001*, which is *LOG_ID_ADMIN_LOGIN_SUCC*.
5. In the *Field filter(s)* field, click the *+* to add multiple field filters. The configured filters much match in order for the stitch to be triggered.



6. Click *OK*.

To configure a FortiProxy event log trigger in the CLI:

```
config system automation-trigger
    edit "event_login_logout"
        set description "trigger for login logout event"
        set event-type event-log
        set logid 32001 32003
        config fields
            edit 1
                set name "user"
                set value "csf"
            next
            edit 2
                set name "srcip"
                set value "10.6.30.254"
            next
        end
    next
end
```

Certificate expiration trigger

The local certificate expiry trigger (`local-certificate-near-expiry`) can be used in an automation stitch if a user-supplied local certificate used for deep inspection or other purpose is about to expire. This trigger relies on a VPN certificate setting in the CLI configuration setting for the certificate log expiring warning threshold:

```
config vpn certificate setting
    set cert-expire-warning <integer>
end
```

`cert-expire-warning <integer>`	Set the certificate log expiring warning threshold, in days (0 - 100, default = 14).

Example

In this example, the default local certificate expiry trigger is used with an email notification action to remind an administrator to re-sign or load a new local certificate to avoid any service interruptions. The local certificate, fw-cert-30-days, will expire in 30 days. The certificate log expiring warning threshold is set to 31 days.

To configure the certificate log expiring warning threshold:

```
config vpn certificate setting
    set cert-expire-warning 31
end
```

To configure an automation stitch with the local certificate expiry trigger in the GUI:

1. Configure the action:
   a. Go to *Security Fabric > Automation*, select the *Action* tab, and click *Create New*.
   b. In the *Notifications* section, click *Email*, and enter the following:

Name	*email_no_rep_message*
To	Enter an email address.
Subject	*CSF stitch alert*

   c. Click *OK*.
2. Configure the stitch:
   a. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
   b. Enter the name, *cert-expiry*.
   c. Click *Add Trigger*. Select *Local Certificate Expiry* and click *Apply*.
   d. Click *Add Action*. Select *email_no_rep_message* and click *Apply*.
   e. Click *OK*.

To configure an automation stitch with the local certificate expiry trigger in the CLI:

1. Configure the trigger:

```
config system automation-trigger
    edit "Local Certificate Expiry"
        set description "A local certificate is near expiration."
        set event-type local-cert-near-expiry
    next
end
```

2. Configure the action:

```
config system automation-action
    edit "email_no_rep_message"
        set action-type email
        set email-to "*******@fortinet.com"
        set email-subject "CSF stitch alert"
    next
end
```

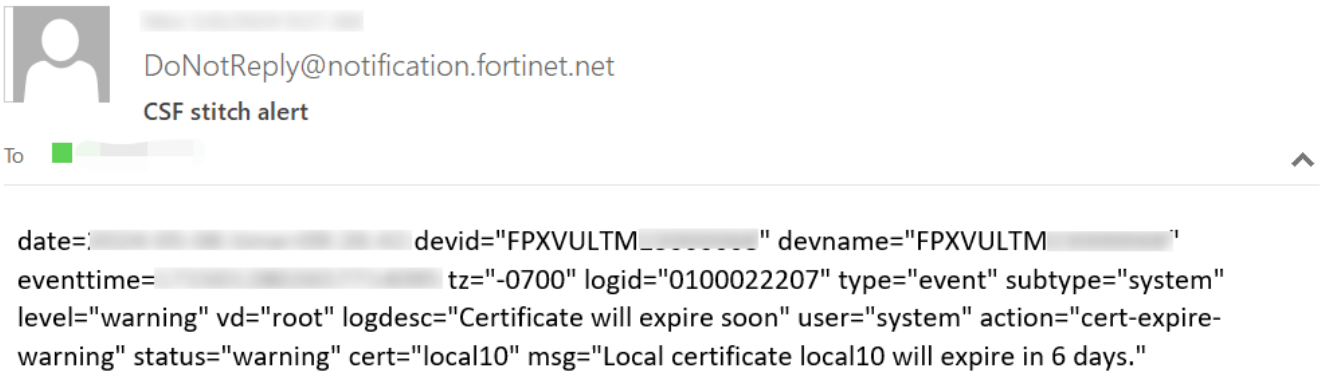
3. Configure the stitch:

```
config system automation-stitch
    edit "cert-expiry"
        set trigger "Local Certificate Expiry"
        config actions
            edit 1
                set action "email_no_rep_message"
                set required enable
            next
        end
```

```
    next
end
```

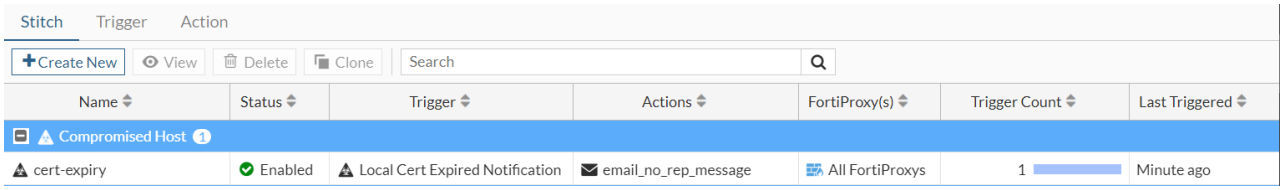
Verification

Once the event log is generated for the local certificate expiry, the automation stitch is triggered end the email notification is sent.



To confirm that the stitch was triggered in the GUI:

1. Go to *Security Fabric* > *Automation* and select the *Stitch* tab.
2. Verify the *Last Triggered* column.



To confirm that the stitch was triggered in the CLI:

```
# diagnose test application autod 3
alert mail log count: 0

stitch: cert-expiry

        local hit: 1 relayed to: 0 relayed from: 0
        last trigger:Thu May 23 09:32:21 2024
        last relay:
        actions:
                email_no_rep_message:
                        done: 1 relayed to: 0 relayed from: 0
                        last trigger:Thu May 23 09:32:21 2024
                        last relay:

logid to stitch mapping:
id:22207  local hit: 1 relayed hits: 0
        cert-expiry
```

Actions

The following table outlines the available actions. Multiple actions can be added to an automation stitch. Actions can be reorganized in the *Edit Automation Stitch* page by dragging and dropping the actions in the diagram.

Category	Action	Description
Security Response		
	Access Layer Quarantine	This option is only available for Compromised Host triggers. Quarantine the MAC address on access layer devices (FortiSwitch and FortiAP).
	FortiClient Quarantine	This option is only available for Compromised Host triggers. Use FortiClient EMS to block all traffic from the source addresses that are flagged as compromised hosts. Quarantined devices are flagged on the Security Fabric topology views.
	FortiNAC Quarantine	This option is only available for Compromised Host and Incoming Webhook triggers. Use FortiNAC to quarantine a client PC and disable its MAC address.
	VMware NSX Security Tag	This option is only available for Compromised Host triggers. If an endpoint instance in a VMware NSX environment is compromised, the configured security tag is assigned to the compromised endpoint. See VMware NSX security tag action on page 1036 and VMware NSX-T security tag action on page 1039 for details.
	IP Ban	This option is only available for Compromised Host triggers. Ban the IP address specified in the automation trigger event.
Notifications		
	Email	Send a custom email message to the selected recipients. At least one recipient and an email subject must be specified. The email body can use parameters from logs or previous action results. Wrapping the parameter with %% will replace the expression with the JSON value for the parameter, for example: *%%results.source%%* is the source property from the previous action.

Category	Action	Description
		Replacement messages can be enabled in the email body to create branded email alerts. See Replacement messages for email alerts on page 1043 for details.
	FortiExplorer Notification	Send push notifications to FortiExplorer. The FortiProxy must be registered to FortiCare on the mobile app that will receive the notification.
	Slack Notification	Send a notification to a Slack channel. See Slack Notification action on page 1046 for details.
	Microsoft Teams Notification	Send a notification to channels in Microsoft Teams. See Microsoft Teams Notification action on page 1049 for details.
Cloud Compute		
	AWS Lambda	AWS Lambda functions can be called when an automation stitch is triggered. See AWS Lambda action on page 1053 for details.
	Azure Function	Azure functions can be called when an automation stitch is triggered. See Azure Function action on page 1055 for details.
	Google Cloud Function	Google Cloud functions can be called when an automation stitch is triggered. See Google Cloud Function action on page 1056 for details.
	AliCloud Function	AliCloud functions can be called when an automation stitch is triggered. See AliCloud Function action on page 1058 for details.
General		
	CLI Script	Run one or more CLI scripts. See CLI script action on page 1059 for details, and Execute a CLI script based on CPU and memory thresholds on page 1062 for an example.
	Webhook	Send an HTTP request using a REST callback. See Webhook action on page 1068 for details, and Slack integration webhook on page 1073 and Microsoft Teams integration webhook on page 1075 for examples.
	Alert	Generate a FortiProxy dashboard alert. This option is only available in the CLI.
	Disable SSID	Disable the SSID interface. This option is only available in the CLI.

VMware NSX security tag action

If an endpoint instance in a VMware NSX environment is compromised, this action will assign the configured security tag to the compromised endpoint.

This action is only available when the automation trigger is set to compromised host.

To set up the NSX quarantine action, you need to:

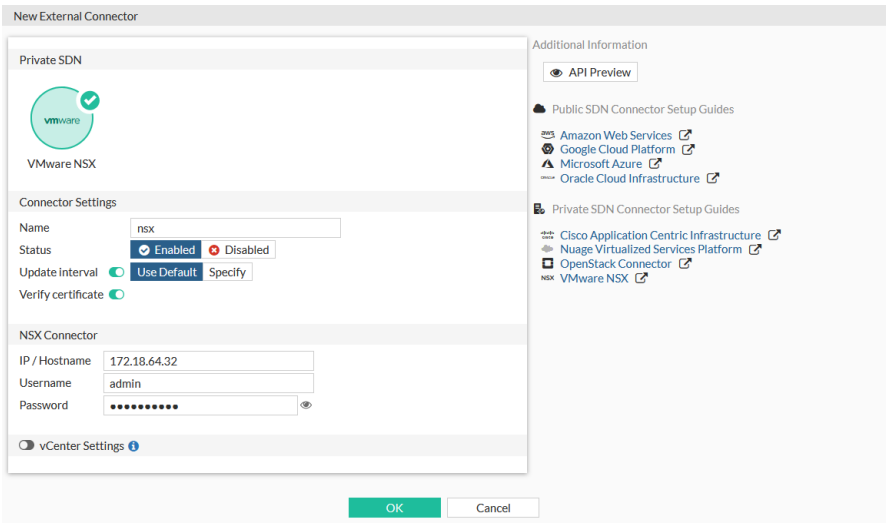
1. Configure a VMware NSX SDN connector
2. Configure an NSX security tag automation stitch
3. Configure FortiAnalyzer logging

Configure a VMware NSX SDN connector

The FortiPRoxy retrieves security tags from the VMware NSX server through the connector.

To configure a VMware NSX SDN connector in the GUI:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. Select *VMware NSX*.
3. Configure the settings as needed.



4. Click *OK*.

To configure a VMware NSX SDN connector in the CLI:

```
config system sdn-connector
    edit "nsx"
        set type nsx
        set server "172.18.64.32"
        set username "admin"
        set password xxxxxxxxxxxx
    next
end
```

Configure an NSX security tag automation stitch

Security tags are retrieved from the VMware NSX server through the NSX SDN connector.

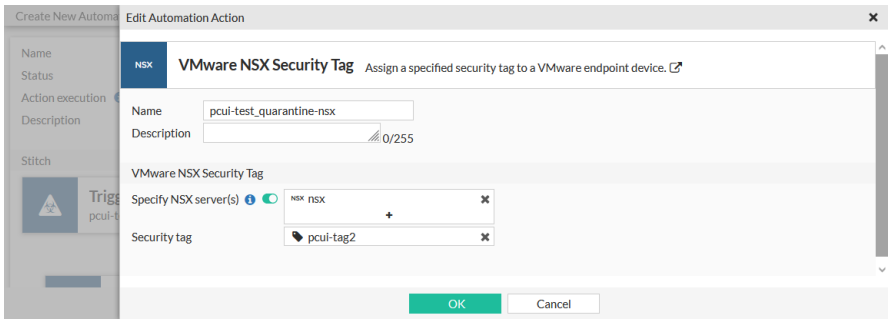
To configure an automation stitch with an NSX security tag in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name (*pcui-test*).
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Compromised Host*.
   c. Enter the following:

Name	pcui-test
Threat level threshold	High

   d. Click *OK*.
   e. Select the trigger from the list and click *Apply*.
4. Configure the VMware NSX Security Tag action:
   a. Click *Add Action*.
   b. Click *Create* and select *VMware NSX Security Tag*.
   c. Enter the following:

Name	pcui-test_quarantine-nsx
Specify NSX server(s)	Enable and select the SDN connector
Security tag	Select an existing tag, or create a new one



   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure an automation stitch with an NSX security tag in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "pcui-test"
```

```
        set ioc-level high
    next
end
```

2. Create an automation action:

```
config system automation-action
    edit "pcui-test_quarantine-nsx"
        set action-type quarantine-nsx
        set security-tag "pcui-tag2"
        set sdn-connector "nsx"
    next
end
```

3. Create the automation stitch:

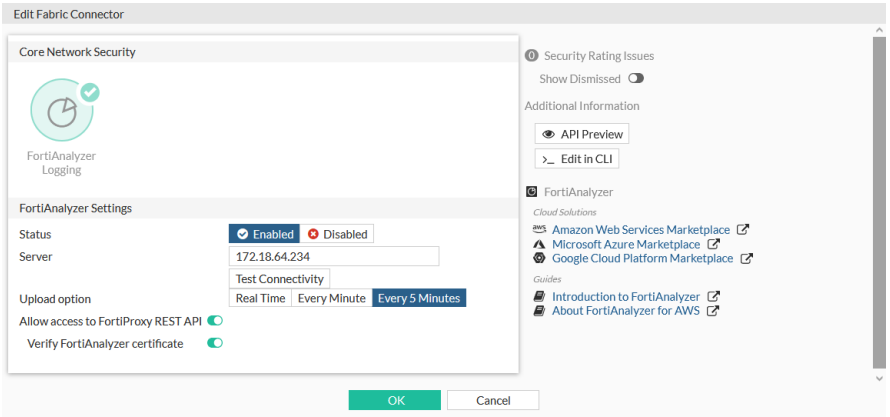
```
config system automation-stitch
    edit "pcui-test"
        set trigger "pcui-test"
        config actions
            edit 1
                set action "pcui-test_quarantine-nsx"
                set required enable
            next
        end
    next
end
```

Configure FortiAnalyzer logging

The FortiAnalyzer is used to send endpoint compromise notification to the FortiProxy.

To configure FortiAnalyzer logging in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *FortiAnalyzer Logging* card.
2. Ensure the *Status* is *Enabled*, and configure the settings as needed.



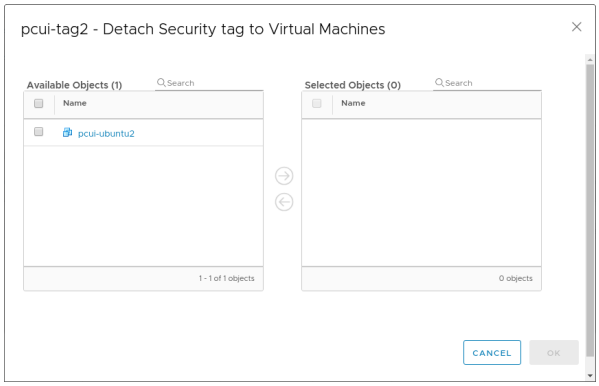
3. Click *OK*.

To configure FortiAnalyzer logging in the CLI:

```
config log fortianalyzer setting
    set status enable
    set server "172.18.64.234"
    set serial "FL-8HFT000000000"
    set upload-option realtime
    set reliable enable
end
```

When an endpoint instance is compromised

When an endpoint instance, such as *pcui-ubuntu2*, in the VMware NSX environment is compromised, the automation stitch is triggered. The FortiProxy then assigns the configured security tag, *pcui-tag2* in this example, to the compromised NSX endpoint instance.



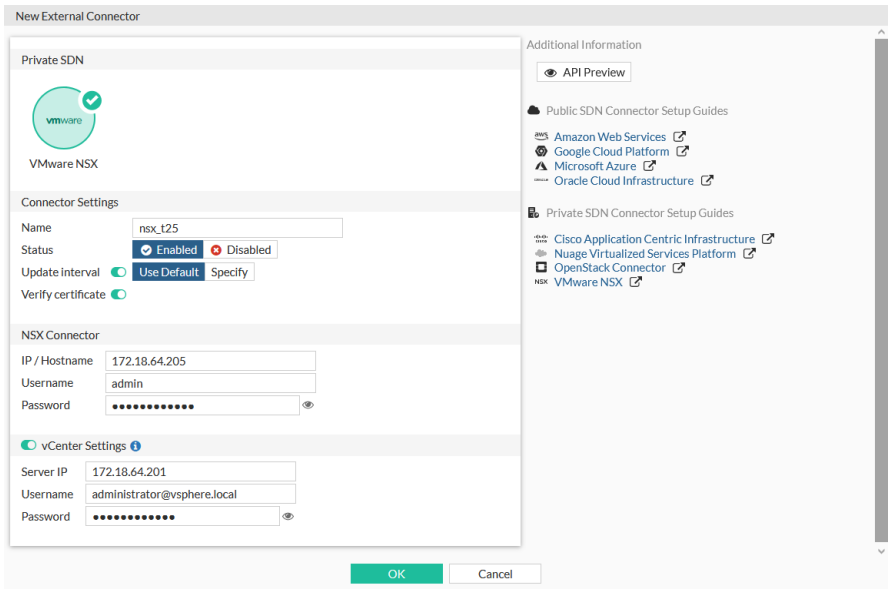
VMware NSX-T security tag action

VMware NSX SDN connectors' vCenter server and credentials can be configured so the FortiProxy resolves NSX-T VMs. The FortiProxy uses the VMWare NSX Security Tag automation action to assign a tag to the VM through an automation stitch.

The FortiProxy is notified of a compromised host on the NSX-T network by an incoming webhook or other means, such as FortiGuard IOC. An automation stitch can be configured to process this trigger and action it by assigning a VMware NSX security tag on the VM instance.

To configure an automation stitch to assign a security tag to NSX-T VMs in the GUI:

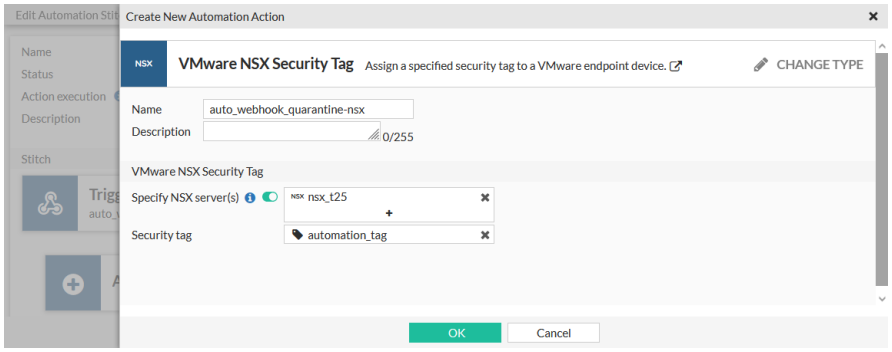
1. Configure the NSX SDN connector:
   a. Go to *Security Fabric > External Connectors* and click *Create New*.
   b. Select *VMware NSX*.
   c. Configure the connector settings.
   d. Enable *vCenter Settings* and configure as needed.



e. Click *OK*.

2. Configure the automation stitch trigger:
   a. Go to *Security Fabric* > *Automation*, select the *Stitch* tab, and click *Create New*.
   b. Enter the stitch name (*auto_webhook*).
   c. Click *Add Trigger*.
   d. Click *Create* and select *Incoming Webhook*.
   e. Enter a name (*auto_webhook*).
   f. Click *OK* to close the *Incoming Webhook URL* prompt.
   g. Select the trigger in the list and click *Apply*.
3. Configure the automation stitch action:
   a. Click *Add Action*.
   b. Click *Create* and select *VMware NSX Security Tag*.
   c. Enter the following:

Name	auto_webhook_quarantine-nsx
Specify NSX server(s)	Enable and select the SDN connector
Security tag	Select an existing tag, or create a new one



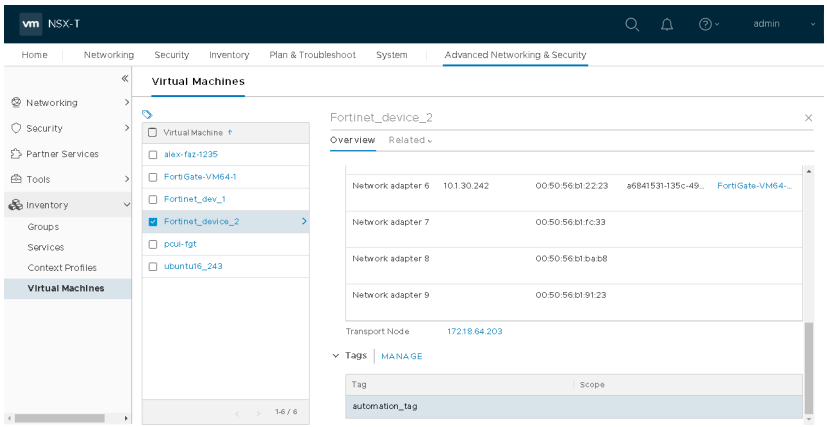
d. Click *OK*.

e. Select the action in the list and click *Apply*.

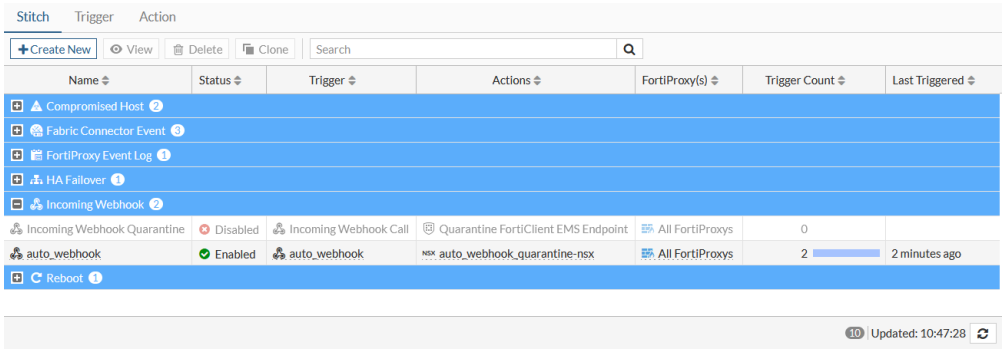
4. Click *OK*.
5. In NSX-T, create a cURL request to trigger the automation stitch on the FortiProxy:

```
root@pc56:/home# curl -k -X POST -H 'Authorization: Bearer 3fdxNG08mgNg0fh4NQ51g1NQ1QHcxx' --
data '{ "srcip": "10.1.30.242"}' https://172.16.116.230/api/v2/monitor/system/automation-
stitch/webhook/auto_webhook
{
  "http_method":"POST",
  "status":"success",
  "http_status":200,
  "serial":"FGVM08TM20000000",
  "version":"v6.4.0",
  "build":1608
}
```

The automation stitch is triggered and the configured tag is added to the NSX-T VM.



On the FortiProxy, the *Security Fabric > Automation* page shows the last trigger time.



To configure an automation stitch to assign a security tag to NSX-T VMs in the CLI:

1. Configure the NSX SDN connector:

```
config system sdn-connector
    edit "nsx_t25"
        set type nsx
        set server "172.18.64.205"
```

```
        set username "admin"
        set password xxxxxxxxxxxx
        set vcenter-server "172.18.64.201"
        set vcenter-username "administrator@vsphere.local"
        set vcenter-password xxxxxxxxxxxx
    next
end
```

2. Configure the automation stitch:

```
config system automation-trigger
    edit "auto_webhook"
        set trigger-type event-based
        set event-type incoming-webhook
    next
end
```

```
config system automation-action
    edit "auto_webhook_quarantine-nsx"
        set action-type quarantine-nsx
        set security-tag "automation_tag"
        set sdn-connector "nsx_t25"
    next
end
```

```
config system automation-stitch
    edit "auto_webhook"
        set trigger "auto_webhook"
        config actions
            edit 1
                set action "auto_webhook_quarantine-nsx"
                set required enable
            next
        end
    next
end
```

3. In NSX-T, create a cURL request to trigger the automation stitch on the FortiProxy:

```
root@pc56:/home# curl -k -X POST -H 'Authorization: Bearer 3fdxNG08mgNg0fh4NQ51g1NQ1QHcxx' --
data '{ "srcip": "10.1.30.242"}' https://172.16.116.230/api/v2/monitor/system/automation-
stitch/webhook/auto_webhook
{
  "http_method":"POST",
  "status":"success",
  "http_status":200,
  "serial":"FGVM08TM20000000",
  "version":"v6.4.0",
  "build":1608
}
```

To verify the automation stitch is triggered and the action is executed:

```
# diagnose test application autod 2

csf: enabled root:yes
version:1586883541 sync time:Tue Apr 14 11:04:05 2022

total stitches activated: 1

stitch: auto_webhook
        destinations: all
        trigger: auto_webhook
                type:incoming webhook

                field ids:
                        (id:15)service=auto_webhook

        local hit: 2 relayed to: 0 relayed from: 0
        actions:
                auto_webhook_quarantine-nsx type:quarantine-nsx interval:0
                        delay:0 required:yes
                        security tag:automation_tag
                        sdn connector:
        nsx_t25;
```

Replacement messages for email alerts

Automation stitches with an Email action can leverage the formatting options provided by replacement messages to create branded email alerts.

You can enable a replacement message and edit the message body or select a customized replacement message group when you configure the automation action. When the automation stitch is triggered, the FortiProxy will send the email with the defined replacement message.

In this example, a Security Rating report triggers an Email notification action. The email uses a customized replacement message group.

To configure the replacement message group in the GUI:

1. Go to *System* > *Replacement Message Groups* and click *Create New*.
2. Enter the following:

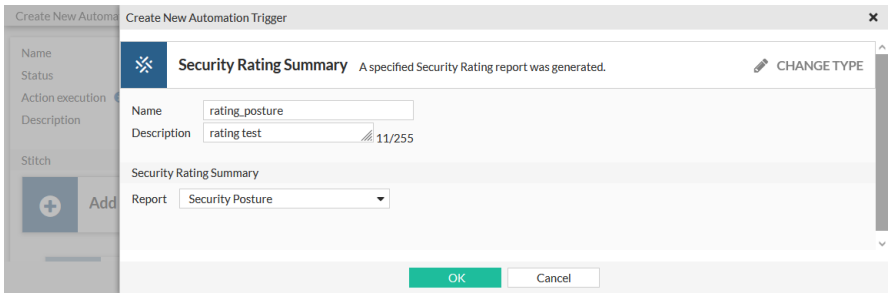
Name	group-sec1
Group Type	Security

3. Click *OK*.
4. Select the group in the list and click *Edit*.
5. Select *Automation Alert Email* and click *Edit*.
6. Edit the HTML code as needed, then click *Save*.

To configure the email action in the GUI:

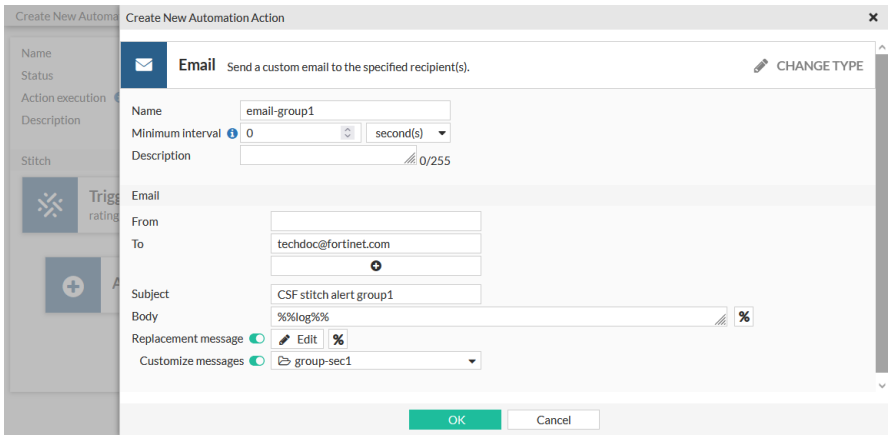
1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	rating_posture
Description	rating test
Report	Security Posture



   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the Email notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Email*.
   c. Enter the following:

Name	email-group1
To	Enter an email address
Subject	CSF stitch alert group1
Replacement message	Enable
Customize messages	Enable and select group-sec1 from the dropdown



d. Click *OK*.

e. Select the action in the list and click *Apply*.

5. Click *OK*.
6. Right-click the automation stitch, and click *Test Automation Stitch*.

   After the Security Rating report is finished, the automation is triggered, and the email is delivered with the customized replacement message in the email body.

To configure the replacement message group in the CLI:

```
config system replacemsg-group
    edit "group-sec1"
        set comment ""
        set group-type utm
        config automation
            edit "automation-email"
                set buffer "...<h1> Security Fabric Automation rating trigger </h1>..."
                ...
            next
        end
    next
end
```

To configure the email action in the CLI:

1. Configure the automation trigger:

```
config system automation-trigger
    edit "rating_posture"
        set description "rating test"
        set event-type security-rating-summary
    next
end
```

2. Configure the automation action:

```
config system automation-action
    edit "email-group1"
```

```
        set action-type email
        set email-to "admin@fortinet.com"
        set email-subject "CSF stitch alert group1"
        set replacement-message enable
        set replacemsg-group "group-sec1"
    next
end
```

3. Configure the automation stitch:

```
config system automation-stitch
    edit "auto_rating"
        set trigger "rating_posture"
        config actions
            edit 1
                set action "email-group1"
                set required enable
            next
        end
    next
end
```

4. To view the automation stitch information after it is triggered:

```
# diagnose test application autod 3
stitch: auto_rating
        local hit: 1 relayed to: 0 relayed from: 0
        last trigger:Tue Sep 13 11:25:01 2022
        last relay:
        actions:
                email-group1:
                        done: 1 relayed to: 0 relayed from: 0
                        last trigger:Tue Sep 13 11:25:01 2022
                        last relay:

logid2stitch mapping:
id:52000  local hit: 1 relayed hits: 0
        auto_rating
```

Slack Notification action

To configure an automation stitch with a Slack Notification action, you first need to configure an incoming webhook in Slack. Then you can enter the webhook URL when you configure the Slack Notification action.

This example uses a Security Rating Summary trigger in the automation stitch with two Slack Notification actions with different notification messages. One message is a custom message, and the other is for the Security Rating Summary log with a 90 second delay.

To create an Incoming Webhook in Slack:

1. Go to the Slack website, and create a workspace.
2. Create a Slack application for the workspace.
3. Add an Incoming Webhook to a channel in the workspace (see Sending messages using Incoming Webhooks for more details).
4. Activate the Incoming Webhook, and copy the *Webhook URL* to the clipboard.

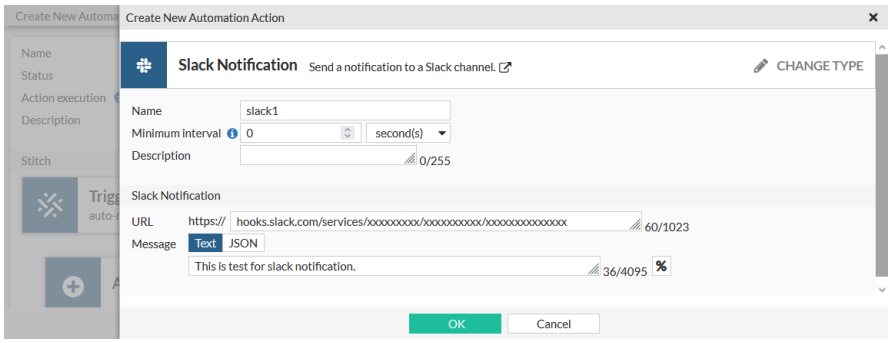
To configure an automation stitch with Slack Notification actions in the GUI:

1. Go to *Security Fabric* > *Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the Security Rating Summary trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	auto-rating
Report	Security Posture

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the first Slack Notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Slack Notification*.
   c. Enter the following:

Name	slack1
URL	Paste the webhook URL from the clipboard
Message	Text
Message text	This is test for slack notification.

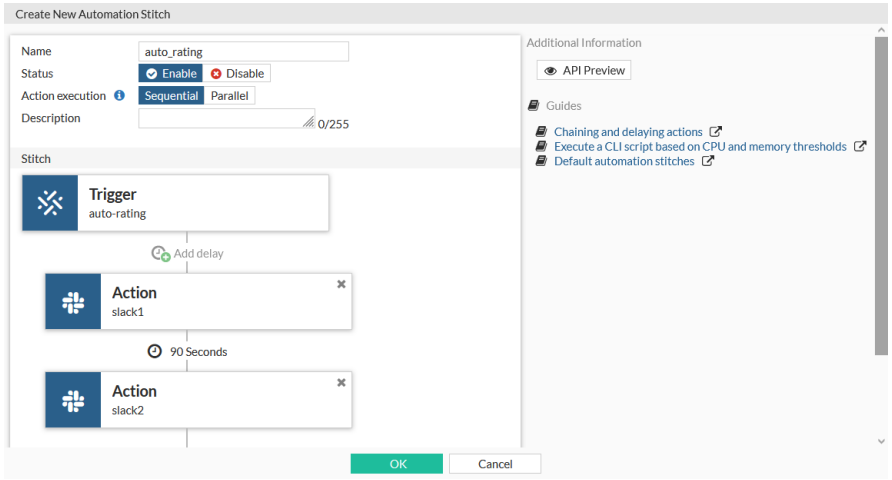


   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Configure the second Slack Notification action:

a. Click *Add Action*.
b. Click *Create* and select *Slack Notification*.
c. Enter the following:

Name	slack2
URL	Paste the webhook URL from the clipboard
Message	Text
Message text	%%log%%

d. Click *OK*.
e. Select the action in the list and click *Apply*.
f. Click the *Add delay* located between both actions. Enter *90* and click *OK*.



6. Click *OK*.
7. Trigger the automation stitch:
   a. Right-click the automation stitch and select *Test Automation Stitch*.
      After the Security Rating report is finished, the automation is triggered and an event log is created by the FortiProxy. The two notifications are sent to the Slack channel.

To configure an automation stitch with Slack Notification actions in the CLI:

1. Configure the automation trigger:

```
config system automation-trigger
    edit "auto-rating"
        set event-type security-rating-summary
    next
end
```

2. Configure the automation actions:

```
config system automation-action
    edit "slack1"
        set action-type slack-notification
```

```
        set message "This is test for slack notification."
        set uri "hooks.slack.com/services/xxxxxxxxx/xxxxxxxxx/xxxxxxxxxxxxxxxxxxxxxxx"
    next
    edit "slack2"
        set action-type slack-notification
        set uri "hooks.slack.com/services/xxxxxxxxx/xxxxxxxxx/xxxxxxxxxxxxxxxxxxxxxxx"
    next
end
```

3. Configure the automation stitch:

```
config system automation-stitch
    edit "auto_rating"
        set trigger "auto-rating"
        config actions
            edit 1
                set action "slack1"
                set required enable
            next
            edit 2
                set action "slack2"
                set delay 90
                set required enable
            next
        end
    next
end
```

4. Verify that the automation action was triggered:

```
# diagnose test application autod 3
stitch: auto-rating
    local hit: 1 relayed to: 0 relayed from: 0
    last trigger:Tue Sep 13 11:34:56 2022
    last relay:
    actions:
        slack1:
            done: 1 relayed to: 0 relayed from: 0
            last trigger:Tue Sep 13 11:34:56 2022
            last relay:
        slack2:
            done: 1 relayed to: 0 relayed from: 0
            last trigger:Tue Sep 13 11:34:56 2022
            last relay:
```

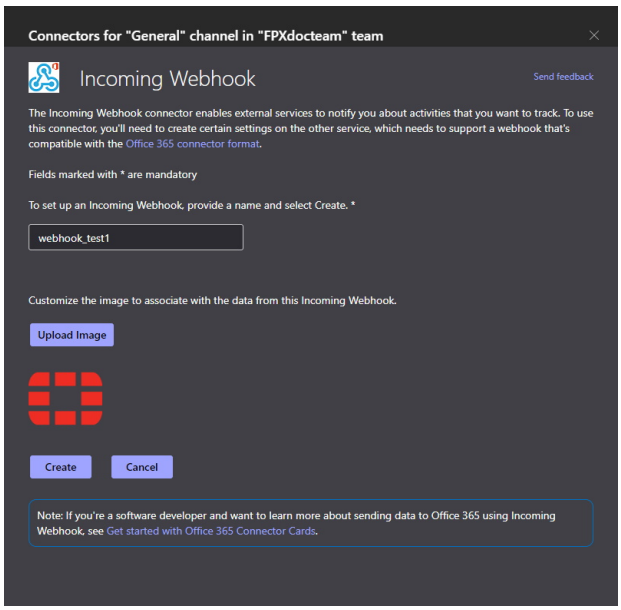
Microsoft Teams Notification action

Microsoft Teams Notification actions can be configured to send notifications to channels in Microsoft Teams. To trigger the notifications, you need to add an Incoming Webhook connector to a channel in Microsoft Teams, then you can configure the automation stitch with the webhook URL.

In the following example, you will configure an automation stitch with a Security Rating Summary trigger and two Microsoft Teams Notification actions with different notification messages. One message is for the Security Rating Summary log, and the other is a custom message with a ten second delay.

To add the Incoming Webhook connector in a Microsoft Teams channel:

1. In Microsoft Teams, click the ... (*More options*) beside the channel name, and select *Connectors*.
2. Find *Incoming Webhook* and click *Configure*.
3. Enter a name for the webhook, upload an image for the webhook, and click *Create*.

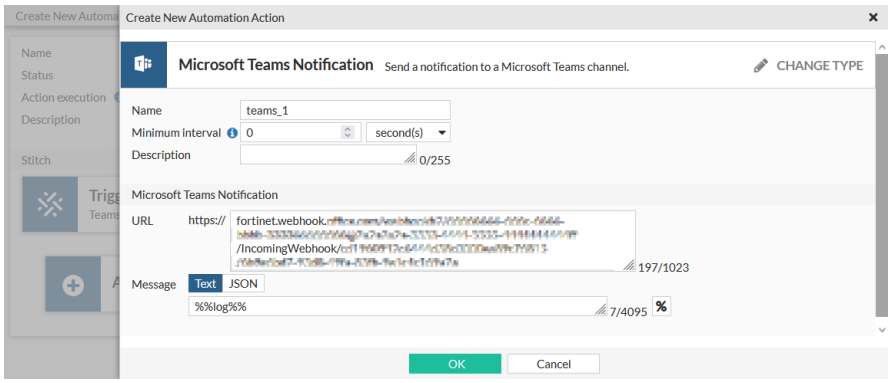


4. Copy the webhook to the clipboard and save it.
5. Click *Done*.

To configure an automation stitch with Microsoft Teams Notification actions in the GUI:

1. Go to *Security Fabric* > *Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the Security Rating Summary trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter a name, and for *Report*, select *Security Posture*.
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the first Microsoft Teams Notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Microsoft Teams Notification*.
   c. Enter the following:

Name	teams_1
URL	Paste the webhook URI from the clipboard
Message	Text
Message text	%%log%%



d. Click *OK*.

e. Select the action in the list and click *Apply*.

5. Configure the second Microsoft Teams Notification action:

a. Click *Add Action*.

b. Click *Create* and select *Microsoft Teams Notification*.

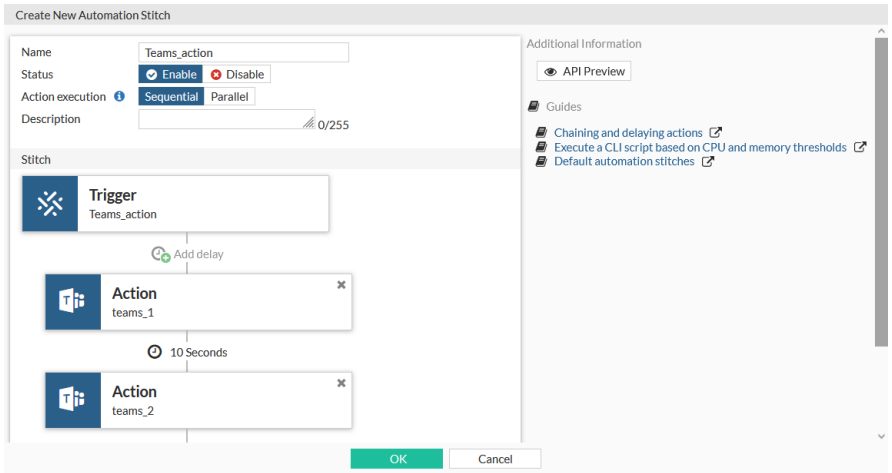
c. Enter the following:

Name	teams_2
URL	Paste the webhook URI from the clipboard
Message	Text
Message text	This is for test.

d. Click *OK*.

e. Select the action in the list and click *Apply*.

f. Click the *Add delay* located between both actions. Enter *10* and click *OK*.



6. Click *OK*.
7. Trigger the automation stitch:
   a. Right-click the automation stitch and select *Test Automation Stitch*.
      After the Security Rating report is finished, the automation is triggered and an event log is created by the FortiProxy. The two notifications are sent to the Microsoft Teams channel.

To configure an automation stitch with Microsoft Teams Notification actions in the CLI:

1. Configure the automation trigger:

```
config system automation-trigger
    edit "Teams_action"
        set event-type security-rating-summary
    next
end
```

2. Configure the automation actions:

```
config system automation-action
    edit "teams_1"
        set action-type microsoft-teams-notification
        set uri "outlook.office.com/webhook/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx@xxxxxxxx-
xxxx-xxxx-xxxx-xxxxxxxxxxxx/IncomingWebhook/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx"
    next
    edit "teams_2"
        set action-type microsoft-teams-notification
        set message "This is for test."
        set uri "outlook.office.com/webhook/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx@xxxxxxxx-
xxxx-xxxx-xxxx-xxxxxxxxxxxx/IncomingWebhook/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx"
    next
end
```

3. Configure the automation stitch:

```
config system automation-stitch
    edit "Teams_action"
        set trigger "Teams_action"
        config actions
            edit 1
                set action "teams_1"
                set required enable
            next
            edit 2
                set action "teams_2"
                set delay 10
                set required enable
            next
        end
    next
end
```

4. Verify that the automation action was triggered:

```
# diagnose test application autod 3
stitch: Teams_action

        local hit: 2 relayed to: 0 relayed from: 0
        last trigger:Tue Sep 13 12:09:12 2022
        last relay:
        actions:
                teams_1:
                        done: 2 relayed to: 0 relayed from: 0
                        last trigger:Tue Sep 13 12:09:12 2022
                        last relay:
                teams_2:
                        done: 2 relayed to: 0 relayed from: 0
                        last trigger:Tue Sep 13 12:09:12 2022
                        last relay:
         logid2stitch mapping:
         id:52000  local hit: 22 relayed hits: 0
         Teams_action
```

AWS Lambda action

AWS Lambda functions can be called when an automation stitch is triggered. This example uses a Security Rating Summary trigger in the automation stitch.

To configure an AWS Lambda function automation stitch in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	auto-aws
Report	Security Posture

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the AWS Lambda function action:
   a. Click *Add Action*.
   b. Click *Create* and select *AWS Lambda*.
   c. Enter the following:

Name	aws-action-1
URL	Enter the request API URI

API key	Enter the API key
HTTP header	header2 : header2_value

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure an AWS Lambda function automation stitch in the CLI:

1. Create the automation trigger:

```
config system automation-trigger
    edit "auto-aws"
        set event-type security-rating-summary
    next
end
```

2. Create the automation action:

```
config system automation-action
    edit "aws-action-1"
        set action-type aws-lambda
        set aws-api-key *************
        set uri "0100000000.execute-api.us-east-2.amazonaws.com/default/xxxxx-autobatoon-XXX-
lambdaXXX"
        config http-headers
            edit 1
                set key "header2"
                set value "header2_value"
            next
        end
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-aws"
        set trigger "auto-aws"
        config actions
            edit 1
                set action "aws-action-1"
                set required enable
            next
        end
    next
end
```

When the automation stitch is triggered, the *Security Fabric > Automation* page shows the stitch trigger time. In AWS, the log shows that the function was called, executed, and finished.

Azure Function action

Azure functions can be called when an automation stitch is triggered. This example uses a Security Rating Summary trigger in the automation stitch.

To configure an Azure function automation stitch in the GUI:

1. Go to *Security Fabric > Automation*, select the Stitch tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	auto-azure
Report	Security Posture

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the Azure Function action:
   a. Click *Add Action*.
   b. Click *Create* and select *Azure Function*.
   c. Enter the following:

Name	azure_function
URL	Enter the request API URI
Authorization	Function
API key	Enter the API key
HTTP header	header1 : value1

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure an Azure function automation stitch in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "auto-azure"
        set event-type security-rating-summary
    next
end
```

2. Create an automation action:

```
config system automation-action
    edit "azure_function"
        set action-type azure-function
        set azure-function-authorization function
        set azure-api-key **********
        set uri "xxxxx00-no-delete-xxxx.azurewebsites.net/api/headersResponse"
        config http-headers
            edit 1
                set key "header1"
                set value "value1"
            next
        end
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-azure"
        set trigger "auto-azure"
        config actions
            edit 1
                set action "azure_function"
                set required enable
            next
        end
    next
end
```

When the automation stitch is triggered, the *Security Fabric > Automation* page shows the stitch trigger time. In Azure, the function log shows that the function was called, executed, and finished.

Google Cloud Function action

Google Cloud functions can be called when an automation stitch is triggered. This example uses a Security Rating Summary trigger in the automation stitch.

To configure a Google Cloud function automation stitch in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	auto-google1
Report	Security Posture

   d. Click *OK*.

e. Select the trigger in the list and click *Apply*.

4. Configure the Google Cloud Function action:
   a. Click *Add Action*.
   b. Click *Create* and select *Google Cloud Function*.
   c. Enter the following:

Name	google-echo
URL	Enter the request API URI
HTTP header	echo-header : echo-value

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure a Google Cloud function automation stitch in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "auto-google1"
        set event-type security-rating-summary
    next
end
```

2. Create an automation action:

```
config system automation-action
    edit "google-echo"
        set action-type google-cloud-function
        set uri "us-central1-xxx-xxxxxxx-000-000000.cloudfunctions.net/xxxx-echo"
        config http-headers
            edit 1
                set key "echo-header"
                set value "echo-value"
            next
        end
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-google1"
        set trigger "auto-google1"
        config actions
            edit 1
                set action "google-echo"
                set required enable
            next
        end
```

```
    next
end
```

When the automation stitch is triggered, the *Security Fabric > Automation* page shows the stitch trigger time. In Google Cloud, go to *Logs* to see the function log showing that the configured function was called, executed, and finished.

AliCloud Function action

AliCloud functions can be called when an automation stitch is triggered. This example uses a Security Rating Summary trigger in the automation stitch.

To configure an AliCloud function automation stitch in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	auto-ali
Report	Security Posture

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the AliCloud Function action:
   a. Click *Add Action*.
   b. Click *Create* and select *AliCloud Function*.
   c. Enter the following:

Name	Ali-Action-1
URL	Enter the request API URI
Authorization	Function
AccessKey ID	Enter the access key ID
AccessKey Secret	Enter the access key secret

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure an AliCloud function automation stitch in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "auto-ali"
        set event-type security-rating-summary
    next
end
```

2. Create an automation action:

```
config system automation-action
    edit "Ali-Action-1"
        set action-type alicloud-function
        set alicloud-function-authorization function
        set alicloud-access-key-id "XXXXXxXXXXxxxxxx"
        set alicloud-access-key-secret xxxxxx
        set uri "0000000000000000.us-east-1.fc.aliyuncs.com/2099-99-99/proxy/test-
function/echoBodyAuth/"
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-ali"
        set trigger "auto-ali"
        config actions
            edit 1
                set action "Ali-Action-1"
                set required enable
            next
        end
    next
end
```

When the automation stitch is triggered, the *Security Fabric > Automation* page shows the stitch trigger time. In AliCloud, the function log shows that the function was called, executed, and finished.

CLI script action

CLI scripts can run when an automation stitch is triggered. The scripts can be entered manually, uploaded as a file, or recorded in the CLI console. The output of the script can be sent as an email action.



The maximum size of the CLI script action output is 16K characters.

In this example, the script sets the idle timeout value to 479 minutes, and sends an email with the script output.

To configure a stitch with a CLI script action in the GUI:

1. Go to *Security Fabric* > *Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name (*auto-cli-1*).
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

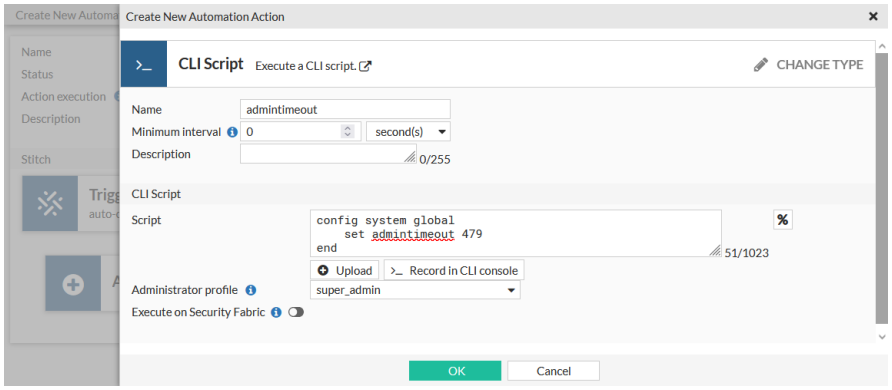
Name	auto-cli-1
Report	Security Posture

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the CLI Script action:
   a. Click *Add Action*.
   b. Click *Create* and select *CLI Script*.
   c. Enter the following:

Name	admintimeout

Script	`config system global`
	`  set admintimeout 479`
	`end`
	
	Alternatively, click *Upload* to upload a file, or click *>_Record in CLI console* and enter the CLI commands.

Administrator profile	Select a profile



   d. Click *OK*.
   e. Select the action in the list and click *Apply*.

5. Configure the Email notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Email*.
   c. Enter the following:

Name	auto-cli-1_email
To	Enter an email address
Subject	CSF stitch alert
Body	%%results%%

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
6. Click *OK*.

To configure a stitch with a CLI script action in the CLI:

1. Create the automation trigger:

```
config system automation-trigger
    edit "auto-cli-1"
        set event-type security-rating-summary
    next
end
```

2. Create the automation actions:

```
config system automation-action
    edit "admintimeout"
        set action-type cli-script
        set script "config system global
            set admintimeout 479
            end"
        set accprofile "super_admin"
    next
    edit "auto-cli-1_email"
        set action-type email
        set email-to "admin@fortinet.com"
        set email-subject "CSF stitch alert"
        set message "%%results%%"
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-cli-1"
        set trigger "auto-cli-1"
        config actions
            edit 1
                set action "admintimeout"
```

```
                set required enable
            next
            edit 2
                set action "auto-cli-1_email"
                set required enable
            next
        end
    next
end
```

Execute a CLI script based on CPU and memory thresholds

Automation stitches can be created to run a CLI script and send an email message when CPU or memory usage exceeds specified thresholds.

In this example, two automation stitches are created that run a CLI script to collect debug information, and then email the results of the script to a specified email address when the CPU usage threshold is exceeded, or memory usage causes the FortiProxy to enter conserve mode.



The maximum size of the CLI script action output is 16K characters.

To define CPU and memory usage thresholds:

```
config system global
    set cpu-use-threshold <percent>
    set memory-use-threshold-extreme <percent>
    set memory-use-threshold-green <percent>
    set memory-use-threshold-red <percent>
end
```

Where:

`cpu-use-threshold`	Threshold at which CPU usage is reported, in percent of total possible CPU utilization (default = 90).
`memory-use-threshold-extreme`	Threshold at which memory usage is considered extreme, and new sessions are dropped, in percent of total RAM (default = 95).
`memory-use-threshold-green`	Threshold at which memory usage forces the FortiProxy to exit conserve mode, in percent of total RAM (default = 82).
`memory-use-threshold-red`	Threshold at which memory usage forces the FortiProxy to enter conserve mode, in percent of total RAM (default = 88).

Configuring the automation stitches

High CPU usage stitch

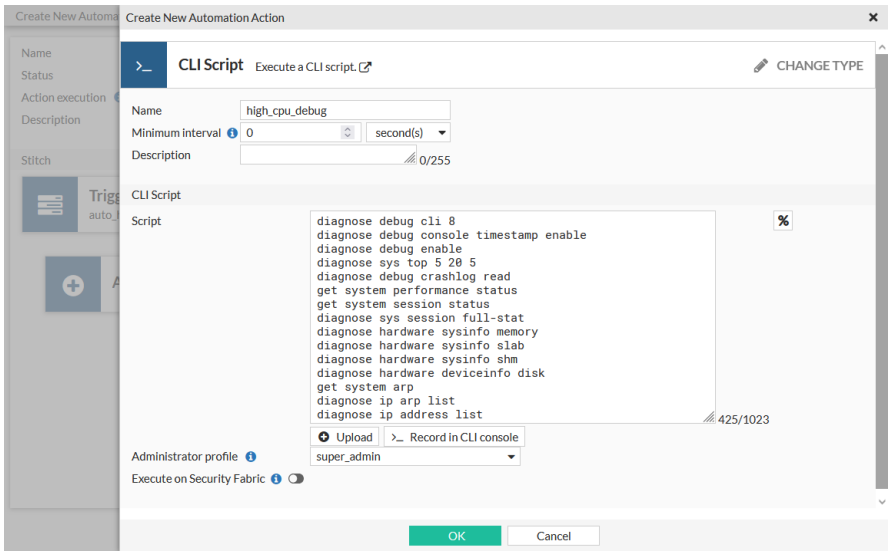
To create an automation stitch for high CPU usage in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name (*auto_high_cpu*).
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *High CPU*.
   c. Enter the name, *auto_high_cpu*.
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the CLI Script action:
   a. Click *Add Action*.
   b. Click *Create* and select *CLI Script*.
   c. Enter the following:

Name	high_cpu_debug

Script	`diagnose debug cli 8`
	`diagnose debug console timestamp enable`
	`diagnose debug enable`
	`diagnose sys top 5 20 5`
	`diagnose debug crashlog read`
	`get system performance status`
	`get system session status`
	`diagnose sys session full-stat`
	`diagnose firewall iprope state`
	`diagnose sys flash list`
	`diagnose hardware sysinfo memory`
	`diagnose hardware sysinfo slab`
	`diagnose hardware sysinfo shm`
	`diagnose hardware deviceinfo disk`
	`get system arp`
	`diagnose ip arp list`
	`diagnose ip address list`
	`get router info routing-table all`
	`get router info kernel`

Administrator profile	Select a profile



d. Click *OK*.
e. Select the action in the list and click *Apply*.

5. Configure the Email notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Email*.
   c. Enter the following:

Name	auto_high_cpu_email
To	Enter an email address
Subject	CSF stitch alert: high_cpu
Body	%%results%%

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
6. Click *OK*.

To create an automation stitch for high CPU usage in the CLI:

1. Create the automation trigger:

```
config system automation-trigger
    edit "auto_high_cpu"
        set event-type high-cpu
    next
end
```

2. Create the automation actions:

```
config system automation-action
    edit "high_cpu_debug"
        set action-type cli-script
```

```
        set script "diagnose debug cli 8
diagnose debug console timestamp enable
diagnose debug enable
diagnose sys top 5 20 5
diagnose debug crashlog read
get system performance status
get system session status
diagnose sys session full-stat
diagnose hardware sysinfo memory
diagnose hardware sysinfo slab
diagnose hardware sysinfo shm
diagnose hardware deviceinfo disk
get system arp
diagnose ip arp list
diagnose ip address list"
        set accprofile "super_admin"
    next
    edit "auto_high_cpu_email"
        set action-type email
        set email-to "person@fortinet.com"
        set email-subject "CSF stitch alert: high_cpu"
        set message "%%results%%"
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto_high_cpu"
        set trigger "auto_high_cpu"
        config actions
            edit 1
                set action "high_cpu_debug"
                set required enable
            next
            edit 2
                set action "auto_high_cpu_email"
                set required enable
            next
        end
    next
end
```

High memory usage stitch

To create an automation stitch for high memory usage in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name (*auto_high_memory*).
3. Configure the trigger:

   a. Click *Add Trigger*.
   b. Click *Create* and select *Conserve Mode*.
   c. Enter the name, *auto_high_memory*.
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the CLI Script action:
   a. Click *Add Action*.
   b. Click *Create* and select *CLI Script*.
   c. Enter the following:

Name	high_memory_debug

Script	`diagnose debug cli 8`
	`diagnose debug console timestamp enable`
	`diagnose debug enable`
	`diagnose sys top 5 20 5`
	`diagnose debug crashlog read`
	`get system performance status`
	`get system session status`
	`diagnose sys session full-stat`
	`diagnose hardware sysinfo memory`
	`diagnose hardware sysinfo slab`
	`diagnose hardware sysinfo shm`
	`diagnose hardware deviceinfo disk`
	`get system arp`
	`diagnose ip arp list`
	`diagnose ip address list`

Administrator profile	Select a profile

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Configure the Email notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Email*.
   c. Enter the following:

Name	auto_high_memory_email
To	Enter an email address
Subject	CSF stitch alert: high_memory
Body	%%results%%

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
6. Click *OK*.

To create an automation stitch for high memory usage in the CLI:

1. Create the automation trigger:

```
config system automation-trigger
    edit "auto_high_memory"
        set event-type low-memory
    next
end
```

2. Create the automation actions:

```
config system automation-action
    edit "high_memory_debug"
        set action-type cli-script
        set script "diagnose debug cli 8
diagnose debug console timestamp enable
diagnose debug enable
diagnose sys top 5 20 5
diagnose debug crashlog read
get system performance status
get system session status
diagnose sys session full-stat
diagnose hardware sysinfo memory
diagnose hardware sysinfo slab
diagnose hardware sysinfo shm
diagnose hardware deviceinfo disk
get system arp
diagnose ip arp list
diagnose ip address list"
        set accprofile "super_admin"
    next
    edit "auto_high_memory_email"
        set action-type email
        set email-to "person@fortinet.com"
        set email-subject "CSF stitch alert: high_memory"
        set message "%%results%%"
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto_high_memory"
        set trigger "auto_high_memory"
        config actions
            edit 1
                set action "high_memory_debug"
                set required enable
            next
            edit 2
                set action "auto_high_memory_email"
                set required enable
```

```
            next
        end
    next
end
```

Results

When the FortiProxy enters conserve mode due to the `memory-use-threshold-red` being exceeded, the GUI displays a notice, and the *auto_high_memory* automation stitch is triggered. This causes the CLI script to run and the script results are emailed to the specified address.

Here is sample text from the email message:

```
CSF stitch alert: high_memory
noreply@notification.fortinet.net
Thu 11/21/2019 11:06 AM
John Doe
FPX[FPXM16TM11111111] Automation Stitch:auto_high_memory is triggered.
########## script name: autod.47 ##########
========== #1, 2019-11-21 11:07:24 ==========
FPXM16TM11111111 $  diag deb cli 8
Debug messages will be on for 25 minutes.
FPXM16TM11111111 $  diag deb console timestamp enable
FPXM16TM11111111 $  diag deb enable
FPXM16TM11111111 $  diag deb crashlog read
1: 2019-08-08 11:35:25 the killed daemon is /bin/dhcpcd: status=0x0
2: 2019-08-08 17:52:47 the killed daemon is /bin/pyfcgid: status=0x0
3: 2019-08-23 11:32:31 from=license status=INVALID
4: 2019-08-23 11:32:32 from=license status=INVALID
5: 2019-11-21 09:53:31 from=license status=VALID
...
```

Webhook action

The webhook automation stitch action makes HTTP and HTTPS requests to a specified server, with custom headers, bodies, ports, and methods. It can be used to leverage the ubiquity of HTML requests and APIs to integrate with other tools.



The URI and HTTP body can use parameters from logs or previous action results. Wrapping the parameter with %% will replace the expression with the JSON value for the parameter, for example: *%%results.source%%* is the source property from the previous action.

In this example, a specific log message (failed administrator log in attempt) triggers the FortiProxy to send the contents of the log to a server. The server responds with a generic reply. This example assumes that the server is already configured and able to communicate with the FortiProxy.

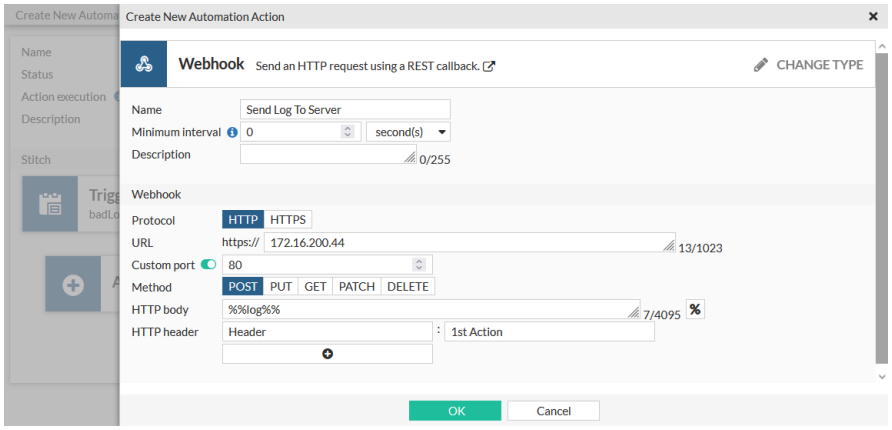
To configure the webhook automation stitch in the GUI:

1. Go to *Security Fabric* > *Automation* and click *Create New*.
2. Enter the stitch name (*badLogin*).
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *FortiProxy Event Log*.
   c. Enter the following:

Name	badLogin
Event	Admin login failed

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the automation stitch action:
   a. Click *Add Action*.
   b. Click *Create* and select *Webhook*.
   c. Enter the following:

Name	Send Log To Server
Protocol	HTTP
URL	172.16.200.44
Custom port	Enable and enter 80
Method	POST
HTTP body	%%log%%
HTTP header	Header : 1st Action



   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure the webhook automation stitch in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "badLogin"
        set event-type event-log
        set logid 32002
    next
end
```

2. Create the automation action:

```
config system automation-action
    edit "Send Log To Server"
        set action-type webhook
        set uri "172.16.200.44"
        set http-body "%%log%%"
        set port 80
        config http-headers
            edit 1
                set key "Header"
                set value "1st Action"
            next
        end
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "badLogin"
        set trigger "badLogin"
        config actions
            edit 1
                set action "Send Log To Server"
                set required enable
            next
        end
    next
end
```

To test the automation stitch:

1. Attempt to log in to the FortiProxy with an incorrect username or password.
2. On the server, check the log to see that its contents were sent by the FortiProxy.
   The body content is replaced with the log from the trigger.
3. On the FortiProxy, go to *Log & Report > Events* and select *System Events* to confirm that the stitch was activated.
4. Go to *Security Fabric > Automation* to see the last time that the stitch was triggered.

Diagnose commands

To enable log dumping:

```
# diagnose test application autod 1
autod dumped total:1 logs, num of logids:1
autod log dumping is enabled

vdom:root(0) logid:32002 len:408 log:
date=2019-05-30 time=17:41:03 logid="0100032002" type="event" subtype="system" level="alert"
vd="root" eventtime=1559263263858888451 tz="-0700" logdesc="Admin login failed" sn="0"
user="admin" ui="http(10.6.30.254)" method="http" srcip=10.6.30.254 dstip=10.6.30.5 action="login"
status="failed" reason="passwd_invalid" msg="Administrator admin login failed from http
(10.6.30.254) because of invalid password"
autod log dumping is disabled

autod logs dumping summary:
        logid:32002 count:1

autod dumped total:1 logs, num of logids:1
```

To show the automation settings:

```
# diagnose test application autod 2
csf: enabled   root:yes
total stitches activated: 2

stitch: badLogin
       destinations: all
       trigger: badLogin

       local hit: 6 relayed to: 6 relayed from: 6
       actions:
               Send Log To Server type:webhook interval:0
                       delay:0 required:no
                       proto:0 method:0 port:80
                       uri: 172.16.200.44
                       http body: %%log%%
                       headers:
                       0. Header:1st Action
```

To show the automation statistics:

```
# diagnose test application autod 3

stitch: badLogin

       local hit: 1 relayed to: 1 relayed from: 1
       last trigger:Tue Sep 13 13:25:09 2022
       last relay:Tue Sep 13 13:25:09 2022
```

```
       actions:
               Send Log To Server:
                       done: 1 relayed to: 1 relayed from: 1
                       last trigger:Tue Sep 13 13:25:09 2022
                       last relay:Tue Sep 13 13:25:09 2022

logid2stitch mapping:
id:32002  local hit: 3 relayed to: 3 relayed from: 3
       badLogin

action run cfg&stats:
total:55 cur:0 done:55 drop:0
       email:
               flags:10
               stats: total:4 cur:0 done:4 drop:0
       fortiexplorer-notification:
               flags:1
               stats: total:0 cur:0 done:0 drop:0
       alert:
               flags:0
               stats: total:0 cur:0 done:0 drop:0
       disable-ssid:
               flags:7
               stats: total:0 cur:0 done:0 drop:0
       quarantine:
               flags:7
               stats: total:0 cur:0 done:0 drop:0
       quarantine-forticlient:
               flags:4
               stats: total:0 cur:0 done:0 drop:0
       quarantine-nsx:
               flags:4
               stats: total:0 cur:0 done:0 drop:0
       ban-ip:
               flags:7
               stats: total:0 cur:0 done:0 drop:0
       aws-lambda:
               flags:11
               stats: total:21 cur:0 done:21 drop:0
       webhook:
               flags:11
               stats: total:6 cur:0 done:6 drop:0
       cli-script:
               flags:10
               stats: total:4 cur:0 done:4 drop:0
       azure-function:
               flags:11
               stats: total:0 cur:0 done:0 drop:0
       google-cloud-function:
               flags:11
               stats: total:0 cur:0 done:0 drop:0
```

```
        alicloud-function:
                flags:11
                stats: total:20 cur:0 done:20 drop:0
```

Slack integration webhook

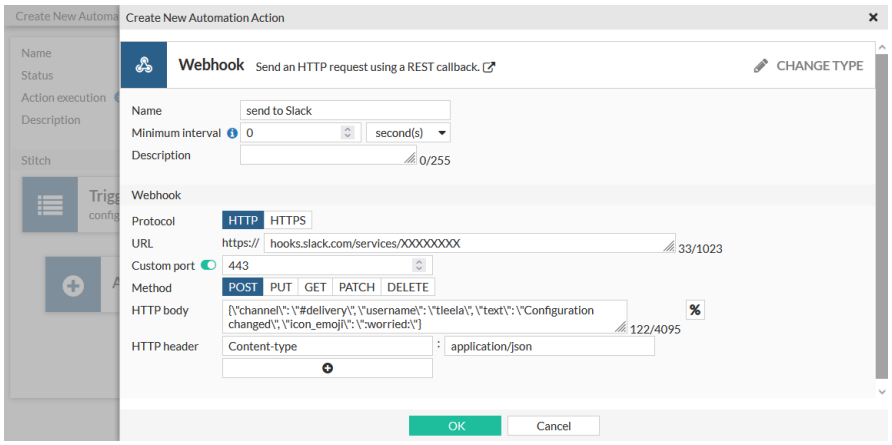
A webhook can be created to post messages and notifications to Slack.

In this example, a configuration change triggers the FortiProxy to post a message to Slack.

To create a webhook automation stitch for Slack integration in the GUI:

1. Create an incoming webhook in Slack. See Sending messages using Incoming Webhooks for more information.
2. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
3. Enter the stitch name.
4. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Configuration Change*.
   c. Enter a name (*config change*).
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
5. Configure the action:
   a. Click *Add Action*.
   b. Click *Create* and select *Webhook*.
   c. Enter the following:

Name	send to Slack
Protocol	HTTPS
URL	Enter the incoming webhook URL created in Slack
Custom port	Enable and enter 443
Method	POST
HTTP body	{\"channel\": \"#delivery\", \"username\": \"tleela\", \"text\": \"Configuration changed\", \"icon_emoji\": \":worried:\"}
HTTP header	Content-type : application/json



d. Click *OK*.

e. Select the action in the list and click *Apply*.

6. Click *OK*.

To create a webhook automation stitch for Slack integration in the CLI:

1. Create an incoming webhook in Slack. See Sending messages using Incoming Webhooks for more information.
2. Create the automation trigger:

```
config system automation-trigger
    edit "config change"
        set event-type config-change
    next
end
```

3. Create the automation action:

```
config system automation-action
    edit "send to Slack"
        set action-type webhook
        set protocol https
        set uri "hooks.slack.com/services/XXXXXXXX"
        set http-body "{\"channel\": \"#delivery\", \"username\": \"tleela\", \"text\":
\"Configuration changed\", \"icon_emoji\": \":worried:\"}"
        set port 443
        config http-headers
            edit 1
                set key "Content-type"
                set value "application/json"
            next
        end
    next
end
```

4. Create the automation stitch:

```
config system automation-stitch
    edit "Slack"
        set trigger "config change"
        config actions
            edit 1
                set action "send to Slack"
                set required enable
            next
        end
    next
end
```

Microsoft Teams integration webhook

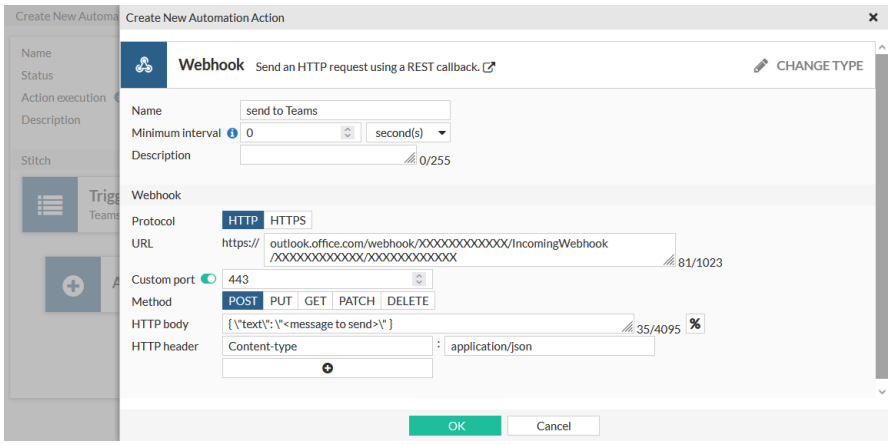
A webhook can be created to post messages and notifications to Microsoft Teams.

In this example, a configuration change triggers the FortiProxy to post a message to Teams.

To create a webhook automation stitch for Teams integration in the GUI:

1. Create an incoming webhook in Teams. See Create an incoming webhook for information.
2. Go to *Security Fabric > Automation* and click *Create New*.
3. Enter the stitch name.
4. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Configuration Change*.
   c. Enter a name (*Teams*).
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
5. Configure the action:
   a. Click *Add Action*.
   b. Click *Create* and select *Webhook*.
   c. Enter the following:

Name	send to Teams
Protocol	HTTPS
URL	Enter the incoming webhook URL created in Teams
Custom port	Enable and enter 443
Method	POST
HTTP body	{ \"text\": \"<message to send>\" }
HTTP header	Content-type : application/json



d. Click *OK*.

e. Select the action in the list and click *Apply*.

6. Click *OK*.

To create a webhook automation stitch for Teams integration in the CLI:

1. Create an incoming webhook in Teams. See Create an incoming webhook for information.
2. Create the automation trigger:

```
config system automation-trigger
    edit "Teams"
        set event-type config-change
    next
end
```

3. Create the automation action:

```
config system automation-action
    edit "send to Teams"
        set action-type webhook
        set protocol https
        set uri
"outlook.office.com/webhook/XXXXXXXXXXXX/IncomingWebhook/XXXXXXXXXXXX/XXXXXXXXXXXX"
        set http-body "{ \"text\": \"<message to send>\" }"
        set port 443
        config http-headers
            edit 1
                set key "Content-type"
                set value "application/json"
            next
        end
    next
end
```

4. Create the automation stitch:

```
config system automation-stitch
    edit "Teams"
```

```
        set trigger "Teams"
        config actions
            edit 1
                set action "send to Teams"
                set required enable
            next
        end
    next
end
```



For information about more advanced messages that can be configured and sent to the Teams incoming webhook, see Sending messages to connectors and webhooks.

Fabric Connectors

Fabric connectors provide integration with Fortinet products to automate the process of managing dynamic security updates without manual intervention.

Creating a Security Fabric Group

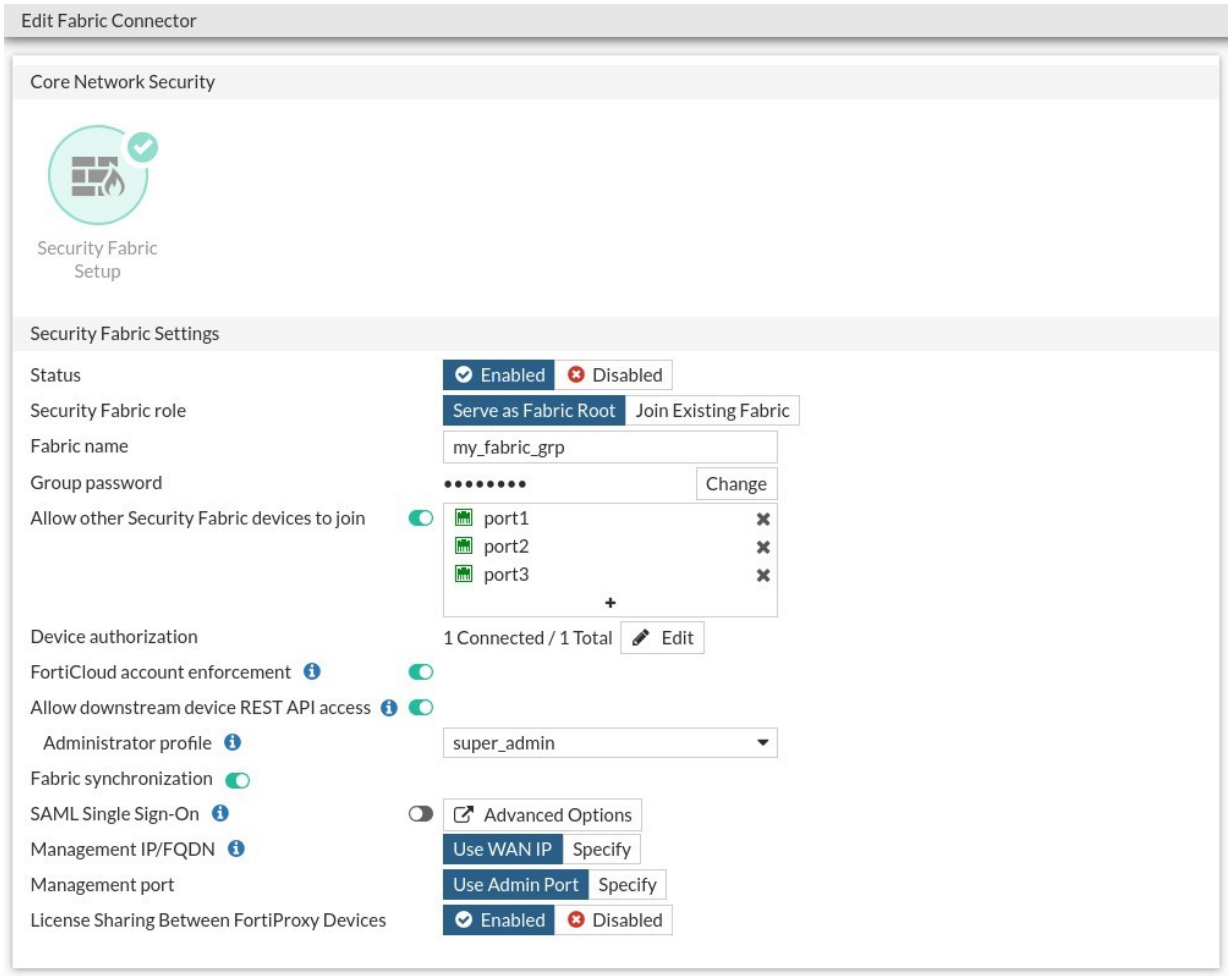
To create a Security Fabric group in the GUI:

1. Configure FortiAnalyzer or Cloud Logging. See Configuring logging and analytics on page 1082 for details.



This step is optional if the security fabric group is for license sharing purposes only.

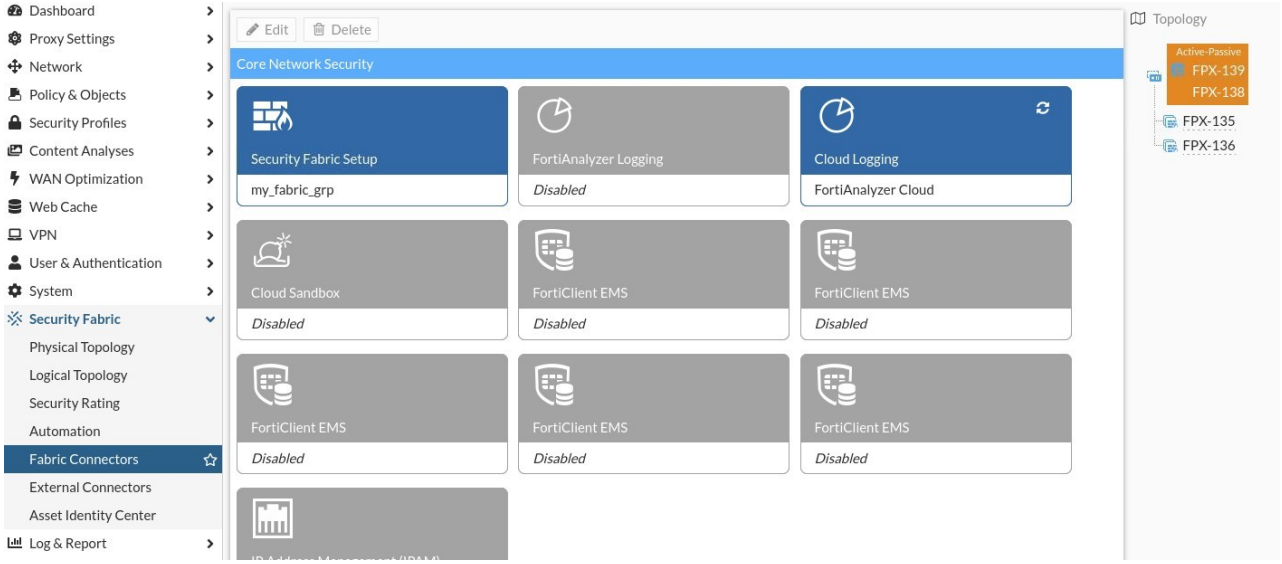
2. Configure the Security Fabric group root:
   a. Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.



   b. Change *Status* to *Enabled*.
   c. In *Security Fabric role*, select *Serve as Fabric Root* to configure a Security Fabric root.
   d. In the *Fabric name* and *Group password* fields, specify the group name and password, which are required for other devices to join the group. If the *Group password* field is unavailable, enable it using the `set legacy-authentication enable` option under `config system csf`.
   e. Enable *Allow other Security Fabric devices to join*.
   f. Add members to the trusted list by clicking *Edit* next to *Device authorization* and clicking *Create New* in the *Device Authorization* panel. Fill in the license serial number of the member and specify a name. The license serial number can be retrieved by running the `get system status` command in the member device.
   g. Configure other options as needed, such as *License Sharing Between FortiProxy Devices* which specifies whether to allow the root to share licenses with other devices within the group.
   h. Click *OK*.
3. **(Optional)** Add additional members to the group by editing the root you just configured and repeat step f. Alternatively, you can add additional members by configuring a new *Security Fabric Setup* card:

a. Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
b. Change *Status* to *Enabled*.
c. In *Security Fabric role*, select *Join Existing Fabric* to configure a Security Fabric member.
d. Fill in the root device address in *Upstream FortiProxy IP/FQDN*.
e. In the *Group password* field, enter the password you set in the root.
f. Configure other options as needed, such as *License Sharing Between FortiProxy Devices* which specifies whether to allow the device to share licenses with other devices within the group.

4. Verify the fabric group status using the fabric group topology in right-side menu on the *Security Fabric >> Fabric Connectors* page.



To create a Security Fabric group in the CLI:

1. Configure FortiAnalyzer logging:

```
config log fortianalyzer setting
    set status enable
    set server "172.18.64.234"
    set serial "FL-8HFT000000000"
    set upload-option realtime
    set reliable enable
end
```

Refer to the config log fortianalyzer setting topic in the CLI guide for more details about each option and a full list of available options.

2. Configure the security fabric group root:

```
config system csf
    set status enable
    set group-name <string>
    set downstream-access enable
    set license-sharing enable
    config trusted-list
    edit <MEMBER_DEVICE_NAME>
    set serial <LICENSE_SERIAL_OF_MEMBER_DEVICE>
```

```
    set guaranteed-seats <integer>
    next
    edit <MEMBER_DEVICE_2_NAME>
    set serial <LICENSE_SERIAL_OF_MEMBER_DEVICE_2>
    set guaranteed-seats <integer>
    next ...
end
```

When adding devices to the trusted list, you can retrieve the license serial number by running the `get system status` command in the member device.

Refer to the config system csf topic in the CLI guide for more details about each option and a full list of available options.

3. **(Optional)** Add additional members to the group you just configured in step 2 as needed. Alternatively, you can add additional members using the following command:

```
config system csf
    set status enable
    set upstream <IP_OF_FABRIC_ROOT>
    set group-name <FABRIC_GROUP_NAME>
    set group-password <FABRIC_GROUP_PASSWORD>
    set configuration-sync local
    set license-sharing enable
end
```

When license sharing is enabled, setting `configuration-sync` to `local` disables configuration synchronization with a management device, which is recommended for license sharing.

Refer to the config system csf topic in the CLI guide for more details about each option and a full list of available options.

4. Verify the fabric group status:
   - To check connected member devices to the root, run `diag system csf downstream`. All connected devices will be listed, regardless of the authorization status.
   - To check the root device status, run `diag system csf upstream`. The connection status should be `Authorized`. If the connection status is `Authorization Rejected`, check if the member device is added to the trusted list of the root device.
   - To check the fabric group setting, run `get system csf`. The following is an example of the results from a root device:

```
status : enable
upstream :
upstream-port : 8013
group-name : my_fabric_grp
group-password : *
accept-auth-by-cert : enable
log-unification : enable
authorization-request-type: serial
fabric-workers : 2
downstream-access : enable
license-sharing : enable
downstream-accprofile: super_admin
configuration-sync : local
fabric-object-unification: local
trusted-list:
== [ 1 ]
name: 1 serial: FPX*************
ha-members:
fabric-connector:
forticloud-account-enforcement: enable
```

Simplify EMS pairing with Security Fabric so one approval is needed for all devices

FortiClient EMS with Fabric authorization and silent approval capabilities is able to approve the root FortiProxy unit in a Security Fabric once and then silently approve remaining downstream FortiProxy units in the Fabric. Similarly in an HA scenario, an approval only needs to be made once to the HA primary unit. The remaining cluster members are approved silently.

To use EMS silent approval:

1. Configure the EMS entry on the root FortiProxy unit or HA primary:

```
config endpoint-control fctems
    edit "ems139"
        set fortinetone-cloud-authentication disable
        set server "172.16.200.139"
        set https-port 443
        set source-ip 0.0.0.0
        set pull-sysinfo enable
        set pull-vulnerabilities enable
        set pull-avatars enable
        set pull-tags enable
        set pull-malware-hash enable
        unset capabilities
        set call-timeout 30
        set websocket-override disable
    next
end
```

   When the entry is created, the capabilities are unset by default.
2. Authenticate the FortiProxy unit with EMS:

```
# execute fctems verify ems_139
...
```

   The FortiProxy unit enables the Fabric authorization and silent approval based on the EMS supported capabilities.

```
config endpoint-control fctems
    edit "ems139"
        set server "172.18.62.12"
        set capabilities fabric-auth silent-approval websocket
    next
end
```

3. Configure a downstream device in the Security Fabric. The downstream device is silently approved.
4. Configure a secondary device in an HA system. The secondary device is silently approved.

Configuring logging and analytics

FortiAnalyzer or Cloud Logging is a required component for the security fabric unless the security fabric group is for license sharing purposes only. Either FortiAnalyzer, FortiAnalyzer Cloud, or FortiGate Cloud can be used to meet this requirement. These settings are configured on the *Logging & Analytics* card on the *Security Fabric > Fabric Connectors* page. If there are multiple services enrolled on the FortiProxy, the preference is: FortiAnalyzer Cloud logging, FortiAnalyzer logging, then FortiGate Cloud logging.

The following topics provide more information about configuring the logging and analytics connector:

- Configuring FortiAnalyzer on page 1082
- Configuring cloud logging on page 1084

Logs Sent daily chart for remote logging sources

The *Logs Sent* widget displays a chart for a select remote logging source (FortiAnalyzer, FortiGate Cloud, and FortiAnalyzer Cloud). Once configured, the same data is available on the *FortiAnalyzer* and *Cloud Logging* tabs of the *Logging & Analytics* card.

To add the Logs Sent widget:

1. Go to *Dashboard > Status* and click *Add Widget*.
2. In the *Resource Usage* section, click the *+* beside *Logs Sent*.
3. Select a *Logging Source* (*FortiAnalyzer*, *FortiGate Cloud*, or *FortiAnalyzer Cloud*).
4. Click *Add Widget* and click *Close*. The *FortiAnalyzer Logs Sent Daily*, *FortiGate Cloud Logs Sent Daily*, or *FortiAnalyzer Cloud Logs Sent Daily* widget is displayed in the dashboard.

To view the chart on the Logging & Analytics card:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Logging & Analytics* card.
   The *Logging Settings* pane is displayed.
2. In the *Settings* tab, click either *FortiAnalyzer* or *Cloud Logging* to view the *Remote Logs Sent Daily* chart.
3. Click *OK* to close the pane.

Configuring FortiAnalyzer

FortiAnalyzer allows the Security Fabric to show historical data for the Security Fabric topology and logs for the entire Security Fabric. For more information about using FortiAnalyzer, see the FortiAnalyzer Administration Guide.

To authorize a FortiAnalyzer in the Security Fabric:

1. In FortiAnalyzer, configure the authorization address and port:
   a. Go to *System Settings > Admin > Admin Settings*.
   b. In the *Fabric Authorization* section, enter an *Authorization Address* and *Authorization Port*. This is used to access the FortiAnalyzer login screen.
   c. Click *Apply*.
2. In FortiProxy, go to *Security Fabric > Fabric Connectors* and double-click the *Logging & Analytics* card.
3. Select the *Settings* tab, select the *FortiAnalyzer* tab, and set the *Status* to *Enabled*.
4. Enter the FortiAnalyzer IP in the *Server* field.
5. Optionally, configure the remaining log settings:

Upload option	Select the frequency of log uploads to the remote device: • *Real Time*: logs are sent to the remote device in real time. • *Every Minute*: logs are sent to the remote device once every minute. This option is unavailable if the Security Fabric connection is configured. • *Every 5 Minutes*: logs are sent to the remote device once every five minutes. This is the default option. This option is unavailable if the Security Fabric connection is configured. • `store-and-upload`: store logs to a local disk before uploading to FortiAnalyzer or FortiManager at a scheduled time. This option is only available in the CLI.
Allow access to FortiGate REST API	Define access to FortiProxy REST API: • *Enable*: the REST API accesses the FortiProxy topology and shares data and results. • *Disable*: the REST API does not share data and results.
Verify FortiAnalyzer certificate	Define the FortiAnalyzer certificate verification process: • *Enable*: the FortiProxy will verify the FortiAnalyzer serial number against the FortiAnalyzer certificate. When verified, the serial number is stored in the FortiProxy configuration. • *Disable*: the FortiProxy will not verify the FortiAnalyzer certificate against the serial number.

6. Click *OK*. The FortiAnalyzer *Connection status* is *Unauthorized*.
7. Click *Authorize*. You are redirected to a login screen.
8. Enter the username and password, then click *Login*.
   The authorization dialog opens.
9. Select *Approve* and click *OK* to authorize the FortiProxy.
10. In FortiProxy, refresh the *FortiAnalyzer* page. The *Connection status* is *Authorized*.



FortiProxies with a FortiAnalyzer Cloud license can send all logs to FortiAnalyzer Cloud.

Configuring cloud logging

There are two options available in the *Cloud Logging* tab of the *Logging & Analytics* connector card: *FortiGate Cloud* and *FortiAnalyzer Cloud*. If there are multiple services enrolled on the FortiProxy, the preference is: FortiAnalyzer Cloud logging, FortiAnalyzer logging, then FortiGate Cloud logging.

This topic covers the following cloud logging aspects:

- Configuring FortiGate Cloud
  - Registration and activation
  - Enabling logging to FortiGate Cloud
  - Logging into the FortiGate Cloud portal
  - Configuring a Security Fabric with FortiGate Cloud logging
- Configuring FortiAnalyzer Cloud

Configuring FortiGate Cloud

FortiGate Cloud is a hosted security management and log retention service for FortiProxy devices. It provides centralized reporting, traffic analysis, configuration management, and log retention without the need for additional hardware or software.

FortiGate Cloud offers a wide range of features:

- **Simplified central management**
  FortiGate Cloud provides a central GUI to manage individual or aggregated FortiProxy and FortiWiFi devices. Adding a device to the FortiGate Cloud management subscription is straightforward. FortiGate Cloud has detailed traffic and application visibility across the whole network.
- **Hosted log retention with large default storage allocated**
  Log retention is an integral part of any security and compliance program, but administering a separate storage system is onerous. FortiGate Cloud takes care of this automatically and stores the valuable log information in the cloud. Different types of logs can be stored, including Traffic, System Events, Web, Applications, and Security Events.
- **Monitoring and alerting in real time**
  Network availability is critical to a good end-user experience. FortiGate Cloud enables you to monitor your FortiProxy network in real time with different alerting mechanisms to pinpoint potential issues. Alerting mechanisms can be delivered via email.
- **Customized or pre-configured reporting and analysis tools**
  Reporting and analysis are your eyes and ears into your network's health and security. Pre-configured reports are available, as well as custom reports that can be tailored to your specific reporting and compliance requirements. The reports can be emailed as PDFs, and can cover different time periods.
- **Maintain important configuration information uniformly**
  The correct configuration of the devices within your network is essential for maintaining optimum performance and security posture. In addition, maintaining the correct firmware (operating system) level allows you to take advantage of the latest features.
- **Service security**
  All communication (including log information) between the devices and the cloud is encrypted. Redundant data centers are always used to give the service high availability. Operational security

measures have been put in place to make sure your data is secure — only you can view or retrieve it.

For more information, refer to the FortiGate Cloud documentation.

Registration and activation



Before you can activate a FortiGate Cloud account, you must register your device first.

FortiGate Cloud accounts can be registered manually through the FortiGate Cloud website, https://www.forticloud.com, or you can easily register and activate your account directly from your FortiProxy.

To activate your FortiGate Cloud account:

1. On your device, go to *Dashboard* > *Status*.
2. In the *FortiGate Cloud* widget, click the *Not Activated* > *Activate* button in the *Status* field.
3. A pane will open asking you to register your FortiGate Cloud account. Click *Create Account*, enter your information, view and accept the terms and conditions, and then click *OK*.
4. A second dialogue window opens, asking you to enter your information to confirm your account. This sends a confirmation email to your registered email. The dashboard widget then updates to show that confirmation is required.
5. Open your email, and follow the confirmation link it contains.
   A FortiGate Cloud page will open, stating that your account has been confirmed. The *Activation Pending* message on the dashboard will change to state the type of account you have, and will provide a link to the FortiGate Cloud portal.

Enabling logging to FortiGate Cloud

To enable logging to FortiGate Cloud:

1. Go to *Security Fabric* > *Fabric Connectors* and double-click the *Logging & Analytics* card.
2. Select the *Settings* tab, select the *Cloud Logging* tab, and set the *Type* to *FortiGate Cloud*.
3. Select an upload option:
   - *Real Time*: logs are sent to the cloud device in real time.
   - *Every Minute*: logs are sent to the cloud device once every minute.
   - *Every 5 Minutes*: logs are sent to the cloud device once every five minutes (default).

   If the Security Fabric connection is configured, only the *Real Time* option is available.
4. Click *OK*.

Logging into the FortiGate Cloud portal

Once logging has been configured and you have registered your account, you can log into the FortiGate Cloud portal and begin viewing your logging results. There are two methods to reach the FortiGate Cloud portal:

- If you have direct network access to the FortiProxy:
  a. Go to *Dashboard > Status*.
  b. In the *FortiGate Cloud* widget, in the *Status* field, click *Activated > Launch Portal*, or, in the *Licenses* widget, click *FortiCare Support > Launch Portal*.
- If you do not have access to the FortiProxy's interface, visit the FortiGate Cloud website (https://www.forticloud.com) and log in remotely, using your email and password. It will ask you to confirm the FortiGate Cloud account you are connecting to and then you will be granted access.

Configuring a Security Fabric with FortiGate Cloud logging

A Security Fabric can be created on the root device using FortiGate Cloud for cloud logging. When the FortiCloud account enforcement is enabled (by default), members joining the Fabric must be registered to the same FortiCloud account. Devices that are not activated with FortiCloud are also allowed.

For example, the root FortiProxy is configured with FortiGate Cloud logging. In the Security Fabric settings, the *FortiCloud account enforcement* option is enabled by default. The downstream FortiProxy with the same FortiCloud account ID is able to join the Fabric.

To configure a Security Fabric with FortiCloud logging in the GUI:

1. Configure the Security Fabric settings on the root FortiProxy (see Fabric Connectors on page 1077). The *FortiCloud account enforcement* setting is enabled by default.
2. Configure FortiCloud logging on the root FortiProxy:
   a. Go to *Security Fabric > Fabric Connectors* and double-click the *Logging & Analytics* card.
   b. Select the *Settings* tab, select the *Cloud Logging* tab, and set the *Type* to *FortiGate Cloud*.
   c. Click *OK*.
3. Configure the FortiProxy to join the Security Fabric:
   a. Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
   b. Select the *Settings* tab, and set the *Security Fabric role* to *Join Existing Fabric*.
   c. Click *OK*. The FortiProxy is authorized and successfully joins the Security Fabric.
4. Check the FortiCloud logging settings:
   a. Go to *Security Fabric > Fabric Connectors* and double-click the *Logging & Analytics* card.
   b. Select the *Settings* tab, select the *Cloud Logging* tab. The settings are automatically retrieved from the root FortiProxy and the *Account* is the same.

To configure a Security Fabric with FortiCloud logging in the CLI:

```
config log fortiguard setting
    set status enable
```

```
    set upload-option realtime
end
```

The FortiCloud account enforcement setting is enabled by default in the Security Fabric settings:

```
show system csf
    config system csf
        set status enable
        set group-name "CSF_101"
        set forticloud-account-enforcement enable
    end
```

Configuring FortiAnalyzer Cloud

FortiAnalyzer Cloud differs from FortiAnalyzer in the following ways:

- You cannot enable FortiAnalyzer Cloud in `vdom override-setting` when global FortiAnalyzer Cloud is disabled.
- You must use the CLI to retrieve and display logs sent to FortiAnalyzer Cloud. The FortiProxy GUI is not supported.
- You cannot enable FortiAnalyzer Cloud and FortiGate Cloud at the same time.

For more information, see Licensing in the FortiAnalyzer Cloud Deployment Guide.

In the *Security Fabric > Fabric Connectors > Logging & Analytics* card settings, *FortiAnalyzer Cloud* is grayed out when you do not have a FortiAnalyzer Cloud entitlement. When you have a FortiAnalyzer Cloud entitlement, *FortiAnalyzer Cloud* is available and you can authenticate by the certificate.

In FortiAnalyzer Cloud, you can view logs from FortiProxy in the *Event > All Types* page.

To configure FortiAnalyzer Cloud logging in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *Logging & Analytics* card.
2. Select the *Settings* tab, select the *Cloud Logging* tab, and set the *Type* to *FortiAnalyzer Cloud*.
3. Optionally, configure the remaining log settings:

Upload option	Select the frequency of log uploads to the remote device: • *Real Time*: logs are sent to the remote device in real time. • *Every Minute*: logs are sent to the remote device once every minute. This option is unavailable if the Security Fabric connection is configured. • *Every 5 Minutes*: logs are sent to the remote device once every five minutes. This is the default option. This option is unavailable if the Security Fabric connection is configured.
Allow access to FortiGate REST API	Define access to FortiProxy REST API: • *Enable*: the REST API accesses the FortiProxy topology and shares data and results. • *Disable*: the REST API does not share data and results.

Verify FortiAnalyzer Cloud certificate	Define the FortiAnalyzer Cloud certificate verification process: • *Enable*: the FortiProxy will verify the FortiAnalyzer Cloud serial number against the FortiAnalyzer certificate. When verified, the serial number is stored in the FortiProxy configuration. • *Disable*: the FortiProxy will not verify the FortiAnalyzer Cloud certificate against the serial number.

4. Click *OK*. A prompt appears to verify the FortiAnalyzer Cloud serial number.
5. Click *Accept*.
6. The verified FortiAnalyzer Cloud certificate appears in the settings.

To enable FortiAnalyzer Cloud logging in the CLI:

1. Configure the FortiAnalyzer Cloud settings:

```
config log fortianalyzer-cloud setting
    set status enable
    set ips-archive disable
    set certificate-verification enable
    set serial "FAZVCLTM19000000"
    set access-config enable
    set enc-algorithm high
    set ssl-min-proto-version default
    set conn-timeout 10
    set monitor-keepalive-period 5
    set monitor-failure-retry-period 5
    set upload-option realtime
end
```

2. Configure the FortiAnalyzer Cloud filters:

```
config log fortianalyzer-cloud filter
    set severity information
    set forward-traffic disable
    set local-traffic disable
    set multicast-traffic disable
    set sniffer-traffic disable
    set anomaly disable
    set voip disable
    set dlp-archive disable
end
```

To disable FortiAnalyzer Cloud logging for a specific VDOM in the CLI:

1. Enable override FortiAnalyzer in the general log settings:

```
config log setting
    set faz-override enable
end
```

2. Disable the override FortiAnalyzer Cloud setting:

```
config log fortianalyzer-cloud override-setting
    set status disable
end
```

To set FortiAnalyzer Cloud logging to filter for a specific VDOM in the CLI:

1. Enable override FortiAnalyzer in the general log settings:

```
config log setting
    set faz-override enable
end
```

2. Enable the override FortiAnalyzer Cloud setting:

```
config log fortianalyzer-cloud override-setting
    set status enable
end
```

3. Configure the override filters for FortiAnalyzer Cloud:

```
config log fortianalyzer-cloud override-filter
    set severity information
    set forward-traffic disable
    set local-traffic disable
    set multicast-traffic disable
    set sniffer-traffic disable
    set anomaly disable
    set voip disable
    set dlp-archive disable
end
```

To display FortiAnalyzer Cloud logs in the CLI:

```
# execute log filter device fortianalyzer-cloud
# execute log filter category event
# execute log display
```

Sample log

```
date=2019-05-01 time=17:57:45 idseq=60796052214644736 bid=100926 dvid=1027 itime="2019-05-01
17:57:48" euid=3 epid=3 dsteuid=0 dstepid=3 logver=602000890 logid=0100032002 type="event"
subtype="system" level="alert" srcip=10.6.30.254 dstip=10.6.30.9 action="login" msg="Administrator
ddd login failed from https(10.6.30.254) because of invalid user name" logdesc="Admin login
failed" sn="0" user="ddd" ui="https(10.6.30.254)" status="failed" reason="name_invalid"
method="https" eventtime=1556758666274548325 devid="FG5H1E5818900000" vd="root" dtime="2019-05-01
17:57:45" itime_t=1556758668 devname="FortiProxy-501E"
```

```
date=2019-05-01 time=17:57:21 idseq=60796052214644736 bid=100926 dvid=1027 itime="2019-05-01
17:57:23" euid=3 epid=3 dsteuid=0 dstepid=3 logver=602000890 logid=0100044546 type="event"
```

```
subtype="system" level="information" action="Edit" msg="Edit log.fortianalyzer-cloud.filter "
logdesc="Attribute configured" user="admin" ui="ssh(10.6.30.254)" cfgtid=164757536
cfgpath="log.fortianalyzer-cloud.filter" cfgattr="severity[information->critical]"
eventtime=1556758642413367644 devid="FG5H1E5818900000" vd="root" dtime="2019-05-01 17:57:21"
itime_t=1556758643 devname="FortiProxy-501E"
```

Configuring FortiClient EMS

The FortiProxy Security Fabric root device can link to FortiClient Endpoint Management System (EMS) and FortiClient EMS Cloud (a cloud-based EMS solution) for endpoint connectors and automation. Up to seven EMS servers can be added to the Security Fabric, including a FortiClient EMS Cloud server. EMS settings are synchronized between all Fabric members.

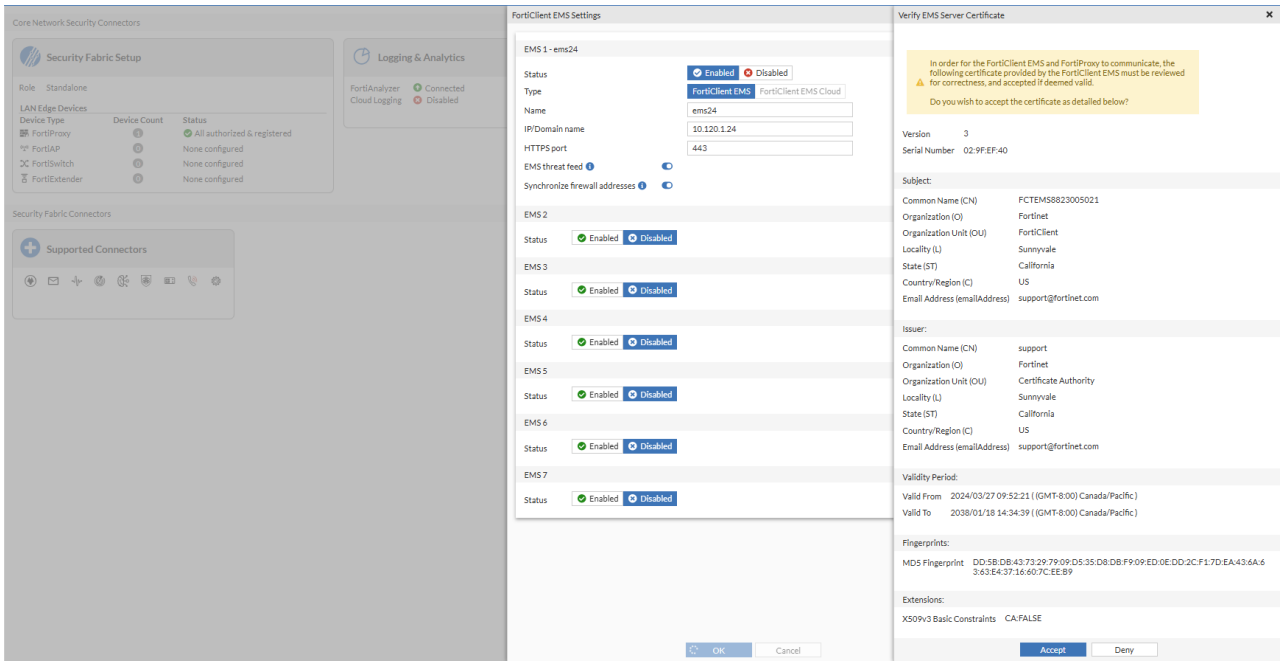
To enable cloud-based EMS services, the FortiProxy must be registered to FortiCloud with an appropriate user account. The following examples presume that the EMS certificate has already been configured.

To add an on-premise FortiClient EMS server to the Security Fabric in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *FortiClient EMS* card.
2. Enable an EMS, and set *Type* to *FortiClient EMS*.
3. Enter a name and IP address or FQDN.

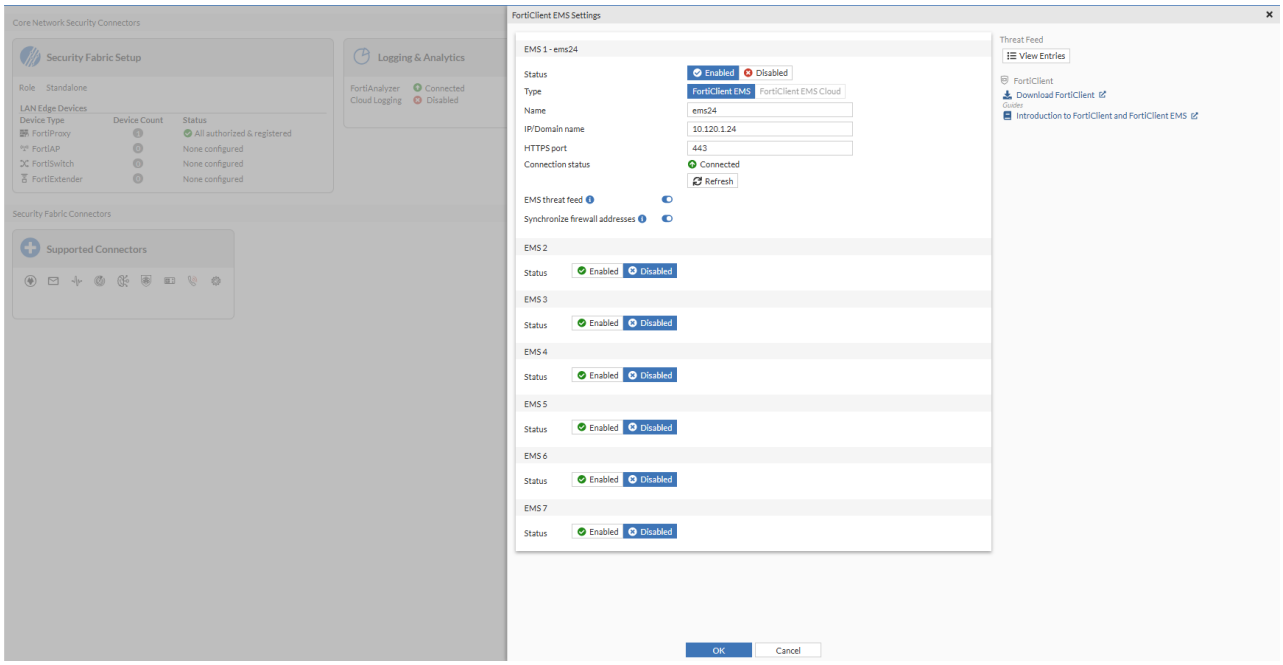
   When connecting to a multitenancy-enabled EMS, Fabric connectors must use an FQDN to connect to EMS, where the FQDN hostname matches a site name in EMS (including "Default"). The following are examples of FQDNs to provide when configuring the connector to connect to the default site and to a site named SiteA, respectively: default.ems.yourcompany.com, sitea.ems.yourcompany.com. See Multitenancy.
4. Optionally, enable *EMS Threat Feed*.
5. Click *OK*.

   A window appears to verify the EMS server certificate:



6. Click *Accept*.
7. Click *Accept*.

   The *Connection status* is now *Connected*:



8. If the device is not authorized, log in to the FortiClient EMS to authorize the FortiProxy under *Administration > Fabric Devices*.

To add a FortiClient EMS Cloud server to the Security Fabric in the GUI:



FortiClient EMS Cloud can only be configured when the FortiProxy is registered to FortiCloud and the EMS Cloud entitlement is verified.

If the FortiCloud account does not pass the FortiClient EMS Cloud entitlement check, the option is not selectable in the FortiClient EMS connector settings.

1. Go to *Security Fabric > Fabric Connectors* and double-click the *FortiClient EMS* card.
2. Set the *Type* to *FortiClient EMS Cloud*.
3. Enter a name.
4. Click *OK*.
   A window appears to verify the EMS server certificate.
5. Click *Accept*.
   The *Connection status* is now *Connected*.

To test connectivity with the EMS server:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *FortiClient EMS* card.
2. In the *Connection status* section, click *Refresh*.

To add an on-premise FortiClient EMS server to the Security Fabric in the CLI:

```
config endpoint-control fctems
    edit {1 | 2 | 3 | 4 | 5}
        set status {enable | disable}
        set name <string>
        set server <ip_address>
        set certificate <string>
        set https-port <integer>
        set source-ip <ip_address>
    next
end
```

The `https-port` is the EMS HTTPS access port number, and the `source-ip` is the REST API call source IP address.

To add a FortiClient EMS Cloud server to the Security Fabric in the CLI:

```
config endpoint-control fctems
    edit {1 | 2 | 3 | 4 | 5}
        set status {enable | disable}
        set name <string>
        set fortinetone-cloud-authentication enable
        set certificate <string>
    next
end
```

To verify the EMS Cloud entitlement in the CLI:

```
# diagnose test update info
```

To verify an EMS certificate in the CLI:

```
# fpx1-209 (root) (Interim)# execute fctems verify 1
```

```
EMS already verified.
```

Configuring FortiClient EMS and FortiClient EMS Cloud on a per-VDOM basis

FortiClient EMS and FortiClient EMS Cloud can be added on a per-VDOM basis. Override must be configured for each VDOM that connects to an EMS server. If override is enabled for a VDOM, the global configuration will not affect the VDOM.

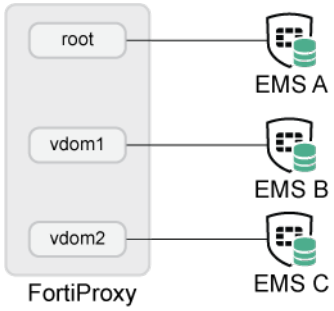
This feature requires FortiClient EMS 7.2.1 and later.

With this override configuration, the FortiProxy can connect to multiple on-premise FortiClient EMS instances per VDOM. However, with this same configuration, only one FortiClient EMS Cloud instance can be connected per FortiProxy.

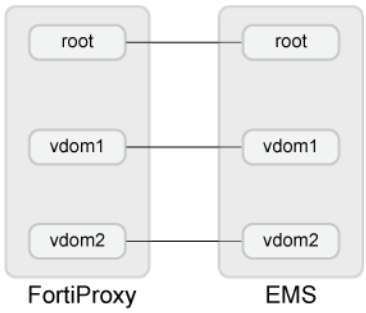
Each VDOM supports up to seven EMS servers, plus an additional seven in the global configuration. With override enabled on all ten VDOMs, a 10-VDOM contract would have up to 77 EMS servers. If override is enabled on only one VDOM, a 10-VDOM contract would have up to 14 EMS servers.

This functionality can be applied to MSSP (managed security service provider) configurations, and each VDOM has its own *FortiClient EMS* card for the EMS server or instance. For example:

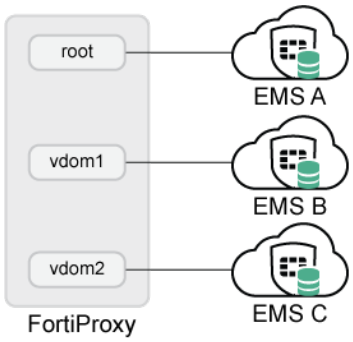
- Separate on-premise FortiClient EMS instances



- Single FortiClient EMS multi-tenant instance based on FQDN type



- Separate FortiClient EMS Cloud instances



To configure a FortiClient EMS server per VDOM in the GUI:

1. Enable override in the FortiProxy CLI on the required VDOMs:

```
config endpoint-control settings
    set override enable
end
```

2. Navigate to the desired VDOM, then go to *Security Fabric > Fabric Connectors* and double-click the *FortiClient EMS* card.
3. Configure the EMS server settings as needed (see the preceding examples for detailed steps).

To configure a FortiClient EMS server per VDOM in the CLI:

1. Enable override on the required VDOMs:

```
config endpoint-control settings
    set override enable
end
```

2. Configure the EMS server on the desired VDOM:

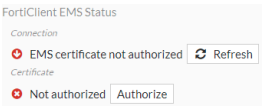
```
fpx1-209 (fctems-override) (Interim)# sh
config endpoint-control fctems-override
    edit 1
        set status enable
        set name "ems24"
        set server "10.120.1.24"
        set serial-number "FCTEMS8823005021"
```

```
        set tenant-id "00000000000000000000000000000000"
        set capabilities fabric-auth silent-approval websocket websocket-malware push-ca-certs
common-tags-api tenant-id client-avatars single-vdom-connector
        set verifying-ca "Fortinet_CA_Backup"
    next
end
```

Troubleshooting

Certificate not trusted

When configuring a new connection to an EMS server, the certificate might not be trusted.



When you click *Authorize*, a warning displays: *The server certificate cannot be authenticated with installed CA certificates. Please install its CA certificates on this FortiProxy*.

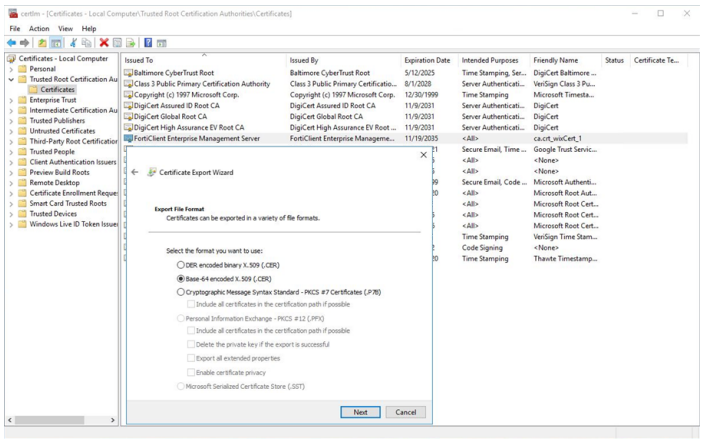
In the CLI, an error message displays when you try to verify the certificate:

```
# execute fctems verify Win2K16-EMS
certificate not configured/verified: 2
Could not verify server certificate based on current certificate authorities.
Error 1--92-60-0 in get SN call: EMS Certificate is not signed by a known CA.
```

The default FortiClient EMS certificate that is used for the SDN connection is signed by the CA certificate that is saved on the Windows server when FortiClient EMS is first installed. You can manually export and install it on the FortiProxy.

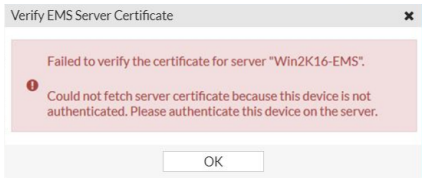
To manually export and install the certificate on to the FortiProxy:

1. Export the EMS certificate on the server that EMS is installed on:
   a. On the Windows server that EMS is installed on, go to *Settings > Manage computer certificates*.
   b. In the certificate management module, go to *Trusted Root Certification Authorities > Certificates*.
   c. Right click on the certificate issued by FortiClient Enterprise Management Server and select *All Tasks > Export*.
   d. The *Certificate Export Wizard* opens. Click *Next*.
   e. Select *Base-64 encoded X.509*, then click *Next*.



f. Enter a file name for the certificate and click *Browse* to select the folder where it will be located, then click *Next*.
g. Review the settings, then click *Finish*. The certificate is downloaded to the specified folder.

2. On the FortiProxy, import the certificate:
   a. Go to *System > Certificate*. By default, the *Certificate* option is not visible, see Feature Visibility on page 970 for information.
   b. Click *Import > CA Certificate*.
   c. Set *Type* to *File*, and click *Upload* to import the certificate from the management computer.
   d. Click *OK*. The imported certificate is shown in the *Remote CA Certificate* section of the certificate table.
3. Try to authorize the certificate on the FortiProxy:
   a. Go to *Security Fabric > Fabric Connectors* and edit the FortiClient EMS connector. The connection status should now say that the certificate is not authorized.
   b. Click *Authorize*. The following warning is shown:



   The warning can also be seen in the CLI:

```
# execute fctems verify Win2K16-EMS
failure in certificate configuration/verification: -4
Could not verify EMS. Error 1--94-0-401 in get SN call: Authentication denied.
```

4. Authorize the FortiProxy on EMS:
   a. Log in to the EMS server console and go to *Administration > Fabric Devices*.
   b. Select the serial number of the FortiProxy device, then click *Authorize*.
5. Try to authorize the certificate on the FortiProxy again:
   a. On the FortiProxy, go to *Security Fabric > Fabric Connectors* and edit the *FortiClient EMS* card.
   b. Click *Refresh*.
   c. When presented with the EMS server certificate, click *Accept* to accept the certificate.
   Your connection should now be successful and authorized.

d. Click *OK*.

Using EMS silent approval in the Security Fabric

FortiClient EMS with Fabric authorization and silent approval capabilities can approve the root FortiProxy in a Security Fabric once, and then silently approve remaining downstream FortiProxies in the Fabric. Similarly in an HA scenario, an approval only needs to be made once to the HA primary unit. The remaining cluster members are approved silently.

To use EMS silent approval:

1. Configure the EMS entry on the root FortiProxy or HA primary:

```
config endpoint-control fctems
    edit "ems139"
        set fortinetone-cloud-authentication disable
        set server "172.16.200.139"
        set https-port 443
        set source-ip 0.0.0.0
        set pull-sysinfo enable
        set pull-vulnerabilities enable
        set pull-avatars enable
        set pull-tags enable
        set pull-malware-hash enable
        unset capabilities
        set call-timeout 30
        set websocket-override disable
    next
end
```

   When the entry is created, the capabilities are unset by default.

2. Authenticate the FortiProxy with EMS:

```
# execute fctems verify ems_139
...
```

   The FortiProxy will enable the Fabric authorization and silent approval based on the EMS supported capabilities.

```
config endpoint-control fctems
    edit "ems139"
        set server "172.18.62.12"
        set capabilities fabric-auth silent-approval websocket
    next
end
```

3. Configure a downstream device in the Security Fabric. The downstream device will be silently approved.
4. Configure a secondary device in an HA system. The secondary device will be silently approved.

Allowing deep inspection certificates to be synchronized to EMS and distributed to FortiClient

On FortiClient EMS versions that support `push CA certs` capability, the FortiProxy will push CA certificates used in SSL deep inspection to the EMS server. On the EMS server, the CA certificates can be selected in the managed endpoint profiles so they can be installed on managed endpoints. FortiClient EMS 7.0.1 and later is required to use this feature.

To configure deep inspection certificate synchronization to EMS:

1. Configure the EMS Fabric connector:

```
config endpoint-control fctems
    edit "ems138"
        set fortinetone-cloud-authentication disable
        set server "172.16.200.138"
        set https-port 443
        set source-ip 0.0.0.0
        set pull-sysinfo enable
        set pull-vulnerabilities enable
        set pull-avatars enable
        set pull-tags enable
        set pull-malware-hash enable
        set capabilities fabric-auth silent-approval websocket websocket-malware push-ca-certs
        set call-timeout 30
        set websocket-override disable
        set preserve-ssl-session disable
    next
end
```

2. Apply the certificate to an SSL/SSH profile for deep inspection:

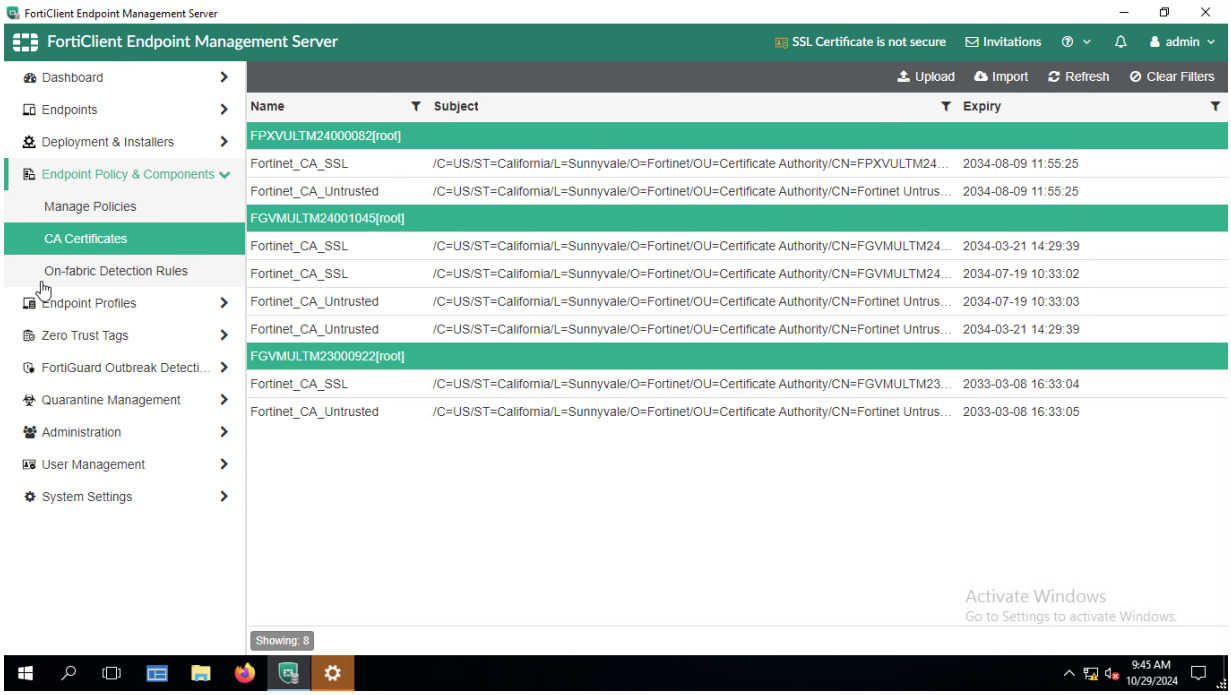
```
config firewall ssl-ssh-profile
    edit "deep-inspection"
        set comment "Read-only deep inspection profile."
        config https
            set ports 443
            set status deep-inspection
        end
        ...
        set server-cert-mode re-sign
        set caname "Fortinet_CA_SSL"
        set untrusted-caname "Fortinet_CA_Untrusted"
    next
end
```

   The default deep inspection profile, CA certificate, and untrusted CA certificates are used in this example.

3. Configure the firewall policy:

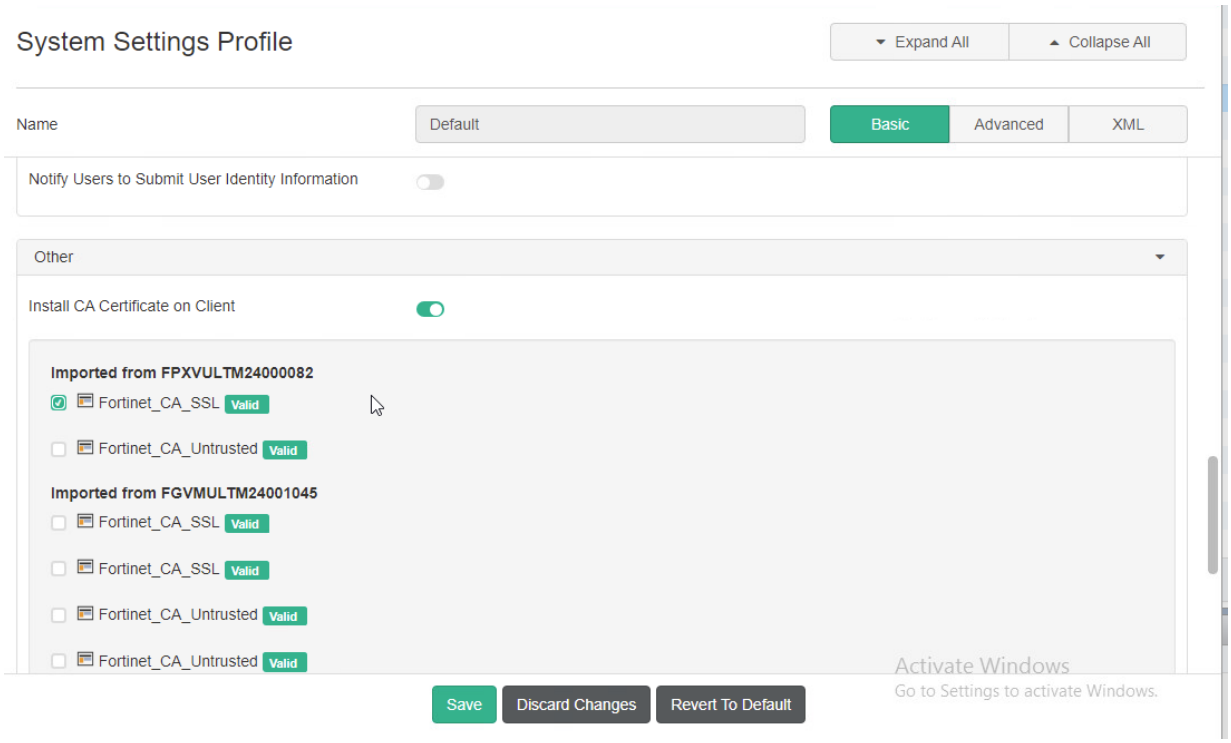
```
config firewall policy
    edit 1
        set name "deep-inspection"
        set srcintf "port14"
        set dstintf "port13"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "deep-inspection"
        set av-profile "default"
        set nat enable
    next
end
```

4. In EMS, verify that the CA certificate was pushed to EMS:
   a. Go to *Endpoint Policy & Components > CA Certificates*.



   b. Verify the certificate table to see that the EMS server received the CA certification from the different FortiProxies.

5. Select the CA certificate in the endpoint profile:
   a. Go to *Endpoint Profiles > System Settings* and edit a profile. The default profile is used in this example.
   b. In the *Other* section, enable *Install CA Certificate on Client* and select the *Fortinet_CA_SSL* certificate for the desired endpoint.



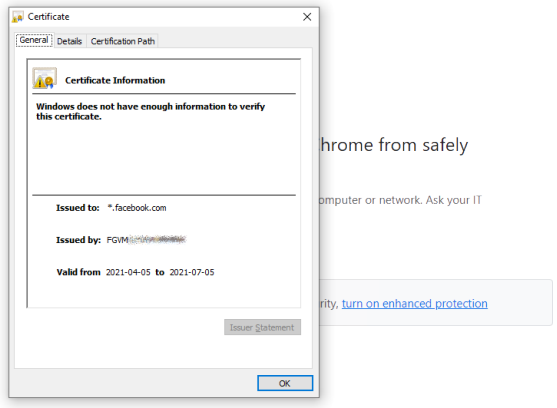
c. Click *Save*.

After the FortiClient endpoint is registered, it receives the CA certificate. When the FortiClient endpoint tries to access the internet through the FortiProxy with the firewall policy that has deep inspection, no warning message is displayed. The server certificate is trusted with the installed CA certificate to complete the certificate chain.

Verification

Before configuring deep inspection certificate synchronization, a warning message is displayed when a FortiClient endpoint accesses the internet through the FortiProxy with the firewall policy that has deep inspection. The FortiClient certificate store does not have the FortiProxy's CA that is used in the deep inspection SSL/SSH profile.

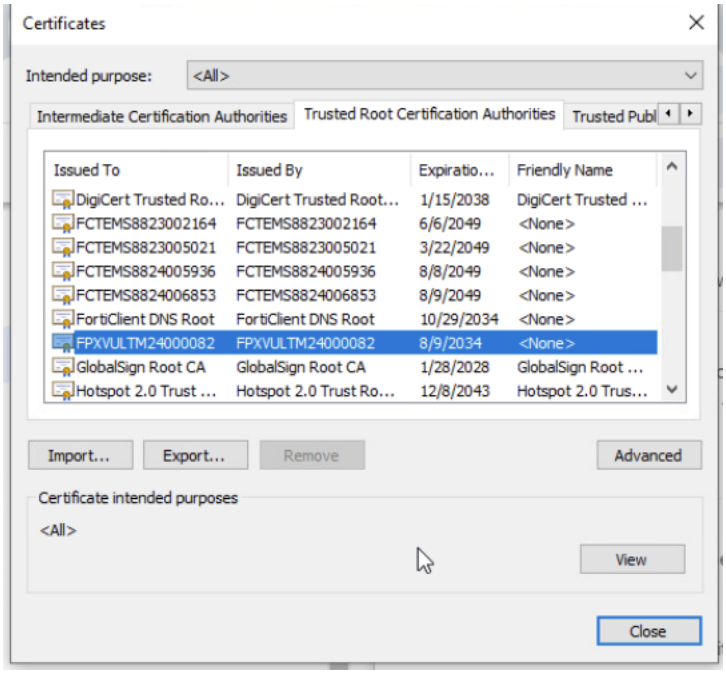
For example, accessing https://www.facebook.com in Chrome shows a warning. In the address bar, clicking *Not secure > Certificate* opens the *Certificate* dialog, which indicates that *Windows does not have enough information to verify the certificate.*



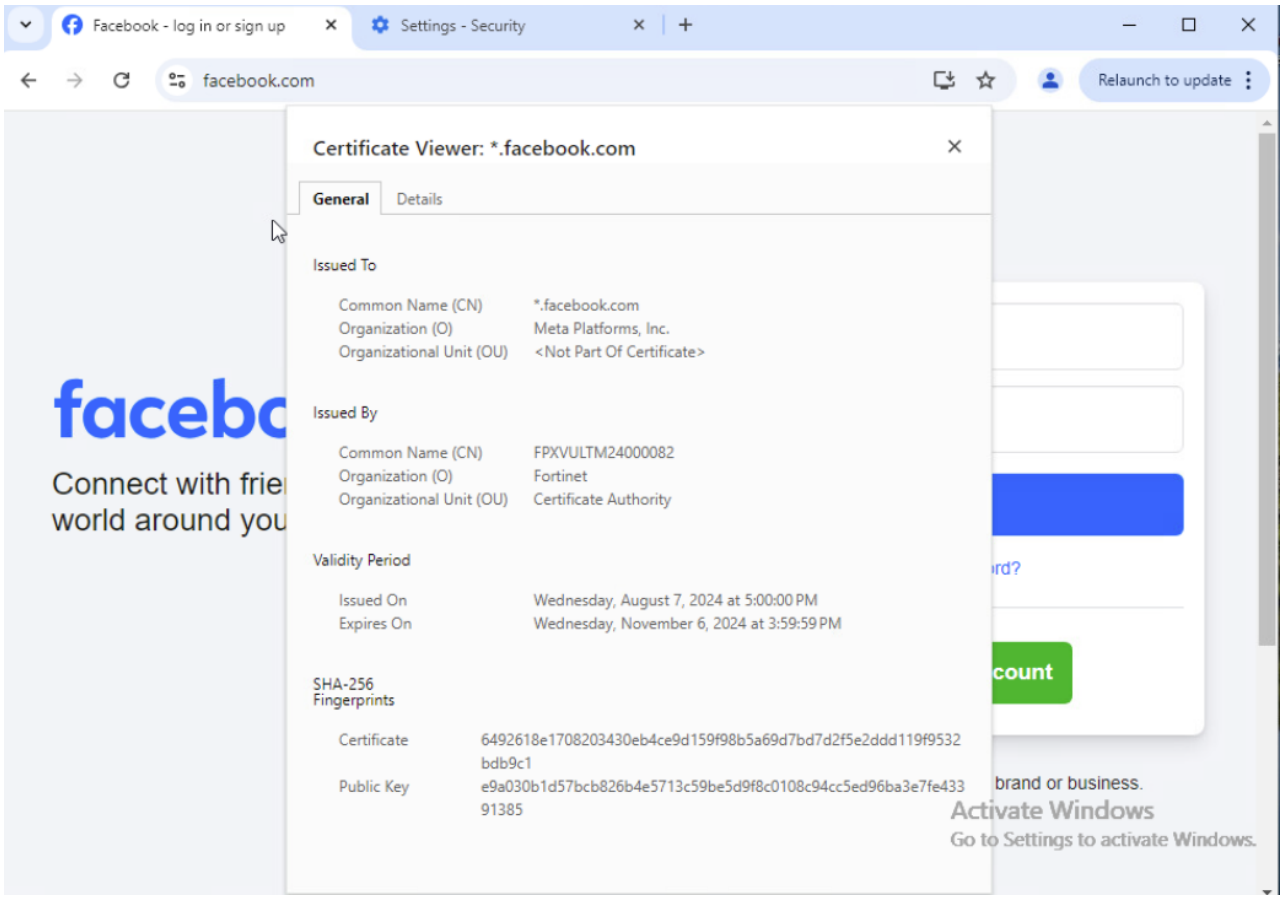
After the EMS profile is pushed to FortiClient endpoint, the expected FortiProxy's certificate is shown in its certificate store.

To verify the deep inspection certificate synchronization:

1. In Chrome, go to *Settings > Privacy and security* and open *Manage certificates*.
2. Click the *Trusted Root Certification Authorities* tab. The FortiProxy's certificate appears in the list.



3. On the FortiClient endpoint using Chrome, go to https://www.facebook.com. The website is displayed.
4. In the address bar, click the padlock, then click *Certificate*. The dialog displays the valid certificate information.



Diagnostics

Use the `diagnose endpoint fctems json deep-inspect-cert-sync` command in FortiProxy to verify the certificate information.

To verify the FortiProxy:

```
FGT_EC_Primary (global) # diagnose endpoint fctems json deep-inspect-cert-sync
JSON:
"""
{
  "fortiproxies":[
    "FPXVULTM24000082"
  ],
  "vdoms":[
    {
      "vdom":"root",
      "certs":[
        {
          "name":"Fortinet_CA_SSL",
          "cert":"-----BEGIN CERTIFICATE-----
\\nMIID8zCCAtugAwIBAgIIQ87QKgsf3EcwDQYJKoZIhvcNAQELBQAwgakxCzAJBgNV\\nBAYTAlVTMRMwEQYDVQQIDApDYWxp
```

```
Zm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUx\\nETAPBgNVBAoMCEZvcnRpbmV0MR4wHAYDVQQLDBVDZXJ0aWZpY2F0ZSBBdXR
ob3Jp\\ndHkxGTAXBgNVBAMMEEZQWFZVTFRNMjQwMDAwODIxIzAhBgkqhkiG9w0BCQEWFHN1\\ncHBvcnRAZm9ydGluZXQuY29
tMB4XDTI0MDgwODE4NTUyNVoXDTM0MDgwOTE4NTUy\\nNVowgakxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMR
IwEAYDVQQH\\nDAlTdW5ueXZhbGUxETAPBgNVBAoMCEZvcnRpbmV0MR4wHAYDVQQLDBVDZXJ0aWZp\\nY2F0ZSBBdXRob3JpdH
kxGTAXBgNVBAMMEEZQWFZVTFRNMjQwMDAwODIxIzAhBgkq\\nhkiG9w0BCQEWFHN1cHBvcnRAZm9ydGluZXQuY29tMIIBIjANB
gkqhkiG9w0BAQEF\\nAAOCAQ8AMIIBCgKCAQEAqB5rpjMxhcFUKCxU0FQ462UfkwIksm1+X96RyREsY2BP\\nhJtxlW+n5A0qR
3ptmQZEt\/uKozitm5cBI52yks2CkxsI9I8H18ba1dWlHkZW+Maq\\ntAegXNB3umJPHsIzist8LOuv2r3n9dAD8aNDSXP6S9x
rUxDZiGKDj5xuTnghVGk7\\nljl7YhnXqklDOyRBiF7TLstfUn5DbTEcT03LyZf+TUhDE1HNGO5LAk+rAgb0kDqF\\nkmihD8+
T3dLsQAzA\/eGl0hHlJHOBnh5\/mdM1jN0ObaacAwdaqvqOZQrTw0gFEtcE\\nL2XV6clqWIixHpScnwH+\/LBnlSCiMa+jmuQ
HMbzhLQIDAQABox0wGzAMBgNVHRME\\nBTADAQH\/MAsGA1UdDwQEAwICBDANBgkqhkiG9w0BAQsFAAOCAQEAnMrl0PuwKwoo\
\nxb9gKjkfZairHqanDGb19ergYUKm8uIaQ\/kHTi5RjHzdwos9NvGcr3oEjt9RUc2G\\nrrOKxRQwb4JjXsgo6mNxyOk6e3WK
grrUJxqIqoZWxRn4\/v1yZ4R\/BJAc7mEEccjI\\nhUGGDU\/CTsSW\/yfEk+UDIkrQZf9rCGNbY7H1o8BUBNEBWhnnC6itCFD
VDRB5E3vZ\\nrIoT6PP7VCWKzlpSYVp4fmS+vq4JzsnLMkBLSDkBV97F8EV8yyDxpUvl0OeaR7wf\\nOhyY8SZKMP2JTHuRuqZ
wRKh6y6N6jdMer11DpQPADniDtBLCFdVMQx1GXhNO3FTZ\\nDThv1haduw==\\n-----END CERTIFICATE-----\\n"
        },
        {
          "name":"Fortinet_CA_Untrusted",
          "cert":"-----BEGIN CERTIFICATE-----
\\nMIID\/TCCAuWgAwIBAgIIbq+nqfHMdW0wDQYJKoZIhvcNAQELBQAwga4xCzAJBgNV\\nBAYTAlVTMRMwEQYDVQQIDApDYWx
pZm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUx\\nETAPBgNVBAoMCEZvcnRpbmV0MR4wHAYDVQQLDBVDZXJ0aWZpY2F0ZSBBdX
Rob3Jp\\ndHkxHjAcBgNVBAMMFUZvcnRpbmV0IFVudHJ1c3RlZCBDQTEjMCEGCSqGSIb3DQEJ\\nARYUc3VwcG9ydEBmb3J0aW
5ldC5jb20wHhcNMjQwODA4MTg1NTI1WhcNMzQwODA5\\nMTg1NTI1WjCBrjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb
3JuaWExEjAQ\\nBgNVBAcMCVN1bm55dmFsZTERMA8GA1UECgwIRm9ydGluZXQxHjAcBgNVBAsMFUNl\\ncnRpZmljYXRlIEF1d
Ghvcml0eTEeMBwGA1UEAwwVRm9ydGluZXQgVW50cnVzdGVk\\nIENBMSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGZvcnRpbmV0
LmNvbTCCASIwDQYJ\\nKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIUqzXof0CxPYABddoAyHtTnxapeGt4p\\nQXh\/SFnsmdN
zlpNg3+pZr8vitYcDjKGKXBqGFK100bSuZ9mzeK3g5Zxgl\/CJcNsv\\naiTawXPF1V0nTVfujIOxK5ThABiAuacszhuZ3UAQC
VrWogvHiDv63bioJxnNBtEw\\nQB1v0F2W5bTaiAN8CpEUyGnZo+qdvgU+C0t21urdA2wuhEBju7E9nW2OTG\/\/62G2\\nF98
uVE5dBzXFx9HZoY6Ra\/fGXFdYugKsmINoagNtKL2nDG9DHzBk\/vtjKAFfCJwl\\nvy797znw\/7+tfKDBP\/aeLpw99Y9zyM
iAAjhntd4hwUNNXTSKAxBWul0CAwEAAaMd\\nMBswDAYDVR0TBAUwAwEB\/zALBgNVHQ8EBAMCAgQwDQYJKoZIhvcNAQELBQAD
ggEB\\nAHV4pMDNvvhqQ627Czy6+OXa2PLlGNS\/j4AKtMF2450rqPkjmnSi8glPBQ\/7Isrz\\ne4lxdNQcpvTX6Kd\/KKw4g
I2Io2rdXb1udlCZwXkm4eTOnIGs\/24L2BPmWRyo\/WSy\\nX9OyAQ+pprUMXWFvrZ6g5jzmaFKVHz09ytKNnOufeCH4c4NlHx
7srlQYJt6udZfF\\ng6sWzhY6qxAKJf56GcdGJDk2l7is9l52P6NOhpCgLnvnEnaADYExKKmswP57MAGZ\\n0\/2FFLPwxobWm
AJjvZCixgecDTlEQ4giEM9gCp8LjOTdNgee\/m7JSFRQUMm+K5LF\\nKVFl3KuRqdOyf+hwbxGn1bY=\\n-----END
CERTIFICATE-----\\n"
        }
      ]
    },
    {
      "vdom":"vd1",
      "certs":[
      ]
    },
    {
      "vdom":"vd2",
      "certs":[
      ]
    }
  ]
}
"""
```

Allowing FortiClient EMS connectors to trust EMS server certificate renewals based on the CN field

When a FortiProxy establishes a Fabric connection with FortiClient EMS, the FortiProxy must trust the CA that signed the server certificate. Upon the approval of the EMS certificate, the FortiProxy saves the CN field and will trust future certificates that are signed by the same CA and have the same CN field. This allows EMS servers to update their certificates at regular intervals without requiring re-authorization on the FortiProxy side, as long as the CN field matches. This prevents interruptions to the EMS Fabric connection when a certificate is updated. Previously, upon the user's approval of the certificate, the certificate fingerprint was saved on the FortiProxy, and this required the FortiProxy to re-authorize the EMS connection each time the server certificate is updated.

```
config endpoint-control fctems
    edit <id>
        set trust-ca-cn {enable | disable}
    next
end
```

This feature is supported for EMS on-premise and cloud connections, and is the default setting. To authorize based on the certificate fingerprint, disable the `trust-ca-cn` setting. If the setting is changed back to be enabled at a later time, the user will have to re-approve the EMS certificate.

To configure the EMS Fabric connector to trust EMS server certificate renewals based on the CN field:

```
config endpoint-control fctems
    edit 1
        set status enable
        set name "ems133"
        set dirty-reason none
        set fortinetone-cloud-authentication disable
        set server "172.18.62.35"
        set https-port 443
        set serial-number "FCTEMS8822000000"
        set tenant-id "00000000000000000000000000000000"
        set source-ip 0.0.0.0
        set pull-sysinfo enable
        set pull-vulnerabilities enable
        set pull-avatars enable
        set pull-tags enable
        set pull-malware-hash enable
        set capabilities fabric-auth silent-approval websocket websocket-malware push-ca-certs
common-tags-api tenant-id
        set call-timeout 30
        set out-of-sync-threshold 180
        set websocket-override disable
        set preserve-ssl-session disable
        set interface-select-method auto
        set trust-ca-cn enable
```

```
    next
end
```

To verify the configuration:

1. Download the FortiProxy configuration file.

```
config endpoint-control fctems-override
    edit 1
        set status enable
        set name "ems26"
        set server "10.120.1.26"
        set serial-number "FCTEMS8824006853"
        set tenant-id "00000000000000000000000000000000"
        set capabilities fabric-auth silent-approval websocket websocket-malware push-ca-certs
common-tags-api tenant-id client-avatars single-vdom-connector
        set certificate-fingerprint
"D7:2A:AB:25:75:DA:D6:DB:C7:5A:47:5C:C0:5F:5A:80:27:32:06:5E:B7:3C:25:48:E9:E9:14:DB:52:F6:22:
5E:06:19:D2:7C:95:28:2D:40:B9:0F:39:55:58:82:71:41:05:E3:BC:9C:85:50:32:E4:C0:48:22:BA:F1:69:8
2:40"
        set trust-ca-cn disable
    next
end
```

```
# diagnose test application fcnacd 96
ems_id 1, certificate authority and common name: C = CA, ST = BC, L = VANCOUVER, O = FTNT, OU
= ReleaseQA, CN = Release_QA, emailAddress = ********@fortinet.comRelease_QA
ems_id 1, fingerprint_sha512:
ems_id 2, certificate authority and common name:
ems_id 2, fingerprint_sha512:
18:51:76:67:EB:4C:31:A1:51:3F:74:F7:8E:1D:47:5C:18:0F:FE:45:DF:52:91:52:37:0B:27:E7:F1:85:5B:0
1:8C:7D:FB:2D:C7:D2:CC:FE:4A:E3:0E:A9:2A:1C:27:4D:D2:A6:C5:87:B8:97:98:57:75:10:15:28:EF:A2:23
:7C
```

2. Run diagnostics to view the certificate information:

```
fpx1-209 (global) (Interim)# diagnose test application fcnacd 96
global:

ems_id: 1
Verified CN: FCTEMS8824005936
Verifying CA: Fortinet_CA_Backup

ems_id: 1, fingerprint_sha512:


vdom root:

ems_id: 1
Verified CN: FCTEMS8823005021
Verifying CA: Fortinet_CA_Backup
```

```
ems_id: 1, fingerprint_sha512:


vdom vd1:

ems_id: 1
Verified CN:
Verifying CA:

ems_id: 1, fingerprint_sha512:
D7:2A:AB:25:75:DA:D6:DB:C7:5A:47:5C:C0:5F:5A:80:27:32:06:5E:B7:3C:25:48:E9:E9:14:DB:52:F6:22:5
E:06:19:D2:7C:95:28:2D:40:B9:0F:39:55:58:82:71:41:05:E3:BC:9C:85:50:32:E4:C0:48:22:BA:F1:69:82
:40
```

External Connectors

You can use external connectors to connect your FortiProxy unit to public and private cloud solutions. By using an external connector, you can ensure that changes to cloud environment attributes are automatically updated in the Security Fabric. You can use external connector address objects to create policies that provide dynamic access control based on cloud environment attribute changes. There is no need to manually reconfigure addresses and policies whenever changes to the cloud environment occur.

There are four steps to creating and using an external connector:

1. Gather the required information. The required information depends on which public or private cloud solution SDN connector you are configuring.
2. Create the external connector.
3. Create an external connector address.
4. Add the address to a firewall policy.

The following provides general instructions for creating an external connector and using the dynamic address object in a firewall policy.

To create an SDN connector in the GUI:

1. Go to *Security Fabric* > *External Connectors*.
2. Click *Create New*.
3. Click the desired public or private cloud.
4. Enter the *Name*, *Status*, and *Update interval* for the connector.
5. Enter the previously collected information for the connector as needed.
6. Click *OK*.

To create an SDN connector in the CLI:

```
config system sdn-connector
    edit <name>
```

```
        set status {enable | disable}
        set type {connector type}
        ...
        set update-interval <integer>
    next
end
```

The available CLI commands vary depending on the selected SDN connector type.

Threat feeds

FortiProxy can dynamically import external threat intelligence lists from an HTTP/HTTPS server as plain text files. Once imported, these threat feeds can be used to enforce specific security policies, such as long-term policies to always allow or block access to certain websites, or short-term requirements to dynamically block access to known compromised locations as threat intelligence updates. Threat feeds are regularly synchronized with the external server. Any changes on the remote server will be imported into FortiProxy based on the configured update interval.



If the FortiProxy loses connectivity with the external server, the threat feed will continue to function despite the *Connection Status* error or reboot. However, the threat feed will not be updated and no new entries will be added until the connection is restored.

FortiProxy supports the following types of threat feeds:

FortiGuard Category	Dynamically imports a text file from an external server, which contains one URL per line. See FortiGuard category threat feed on page 1109 for more information.
IP Address	Dynamically imports a text file from an external server, which contains one IP/IP range/subnet per line. See IP address threat feed on page 1113 for more information.
Domain Name	Dynamically imports a text file from an external server, which contains one domain per line. Simple wildcards are supported. See Domain name threat feed on page 1115 for more information.
Malware Hash	Dynamically imports a text file from an external server, which contains one hash per line (MD5, SHA1, or SHA256) in the format `<hex hash> [optional hash description]`. See Malware hash threat feed on page 1118 for more information.
URL List	Dynamically imports a text file containing one URL per line, supporting wildcards. See URL list threat feed on page 1120 for details.



FortiProxy does not support MAC address feeds or EMS-integrated feeds.

FortiManager can host threat feeds. See External resources in the FortiManager Administration Guide.

External resources file format

All HTTP/HTTPS external resources files must meet the following format requirements:

- The file is in plain text format with each entry on its own line.
  Comments can be added by using the number sign, for example: `# This is a test`.
- The file size and the number of entries are subject to device model limitations. See External resource entry limit on page 1109.
- The external resources update period can be set to 1 minute, hourly, daily, weekly, or monthly (43200 min, 30 days).
- The external resources types "FortiGuard Category" and "Domain Name" share the category number range 192 to 221 (total of 30 categories).
- No duplicate entry validation is performed. Duplicate entries will appear multiple times.
- If the number of entries exceed the limit, a warning is displayed. Additional entries beyond the threshold will not be loaded.

The following table lists format guidelines specific to each threat feed type:

Threat feed type	Format requirements
FortiGuard Category / URL List (type = category)	• Each line contains a single URL entry. • The scheme is optional, and will be truncated if found; https:// and http:// are not required. • Wildcards are allowed at the beginning or end or the URL, for example: *.domain.com or domain.com.*. • IDN and UTF encoding URL are supported . • The URL can be an IPv4 or IPv6 address. An IPv6 URL must be in [ ] format.
IP Address (type = address):	• Each line can contain a single IP address, IP subnet, or IP range. • The IP address can be a single IP address, subnet address, or address range. For example, 192.168.1.1, 192.168.10.0/24, or 192.168.100.1-192.168.100.254. • The address can be an IPv4 or IPv6 address. An IPv6 address does not need to be in [ ] format.
Domain Name (type = domain)	• Each line contains a single domain name. • Simple wildcards are allowed in the domain name list, for example: *.test.com. • IDN (international domain name) is supported.

Malware Hash (type = malware)	Malware hash signature entries must be separated into each line. Each line can contain one MD5, SHA1, or SHA256 hash, with an optional description separated by spaces. Valid examples:
	`# MD5 Entry with hash description`
	`aa67243f746e5d76f68ec809355ec234  md5_sample1`

Threat feed type	Format requirements
	# SHA1 Entry with hash description a57983cb39e25ab80d7d3dc05695dd0ee0e49766 sha1_sample2 # SHA256 Entry with hash description ae9bc0b4c5639d977d720e4271da06b50f7c60d1e2070e9c75cc59ab30e49379 sha256_sample1 # Entry without hash description 0289b0d967cb7b1fb1451339c7b9818a621903090e0020366ab415c549212521 # Invalid entries 7688499dc71b932feb126347289c0b8a_md5_sample2 7614e98badca10b5e2d08f8664c519b7a906fbd5180ea5d04a82fce9796a4b87sha256_sample3

External resource entry limit

The number of entries is globally limited to 200,000 and the file size is globally limited to 16 MB for all external resource entries. If Virtual Domains (VDOMs) are enabled, global entries are counted first, followed by VDOM entries in alphabetical order of VDOM names.

When the maximum number of entries is exceeded, the most recently considered entries are truncated unless you manually reorder the entries using the `move` CLI command. For example:

```
config system external-resource
    move "entry2" before "entry1"
end
```

FortiGuard category threat feed

A FortiGuard category threat feed is a dynamic list that contains URLs and is periodically updated from an external server. The list is stored in text file format on an external server. After the FortiProxy imports this list, it becomes available as a category in the *Remote Categories* group of web filter profiles that can be used to block or monitor URLs matching this category. A category threat feed can also be used solely or grouped with other categories to be used for exemptions within an SSL/SSH profile that performs full SSL inspection.

Multiple custom categories can be defined by creating a FortiGuard Category threat feed for each category.

Text file example:

```
http://example/com.url
https://example.com/url
http://example.com:8080/url
https://www.facebook.com
```

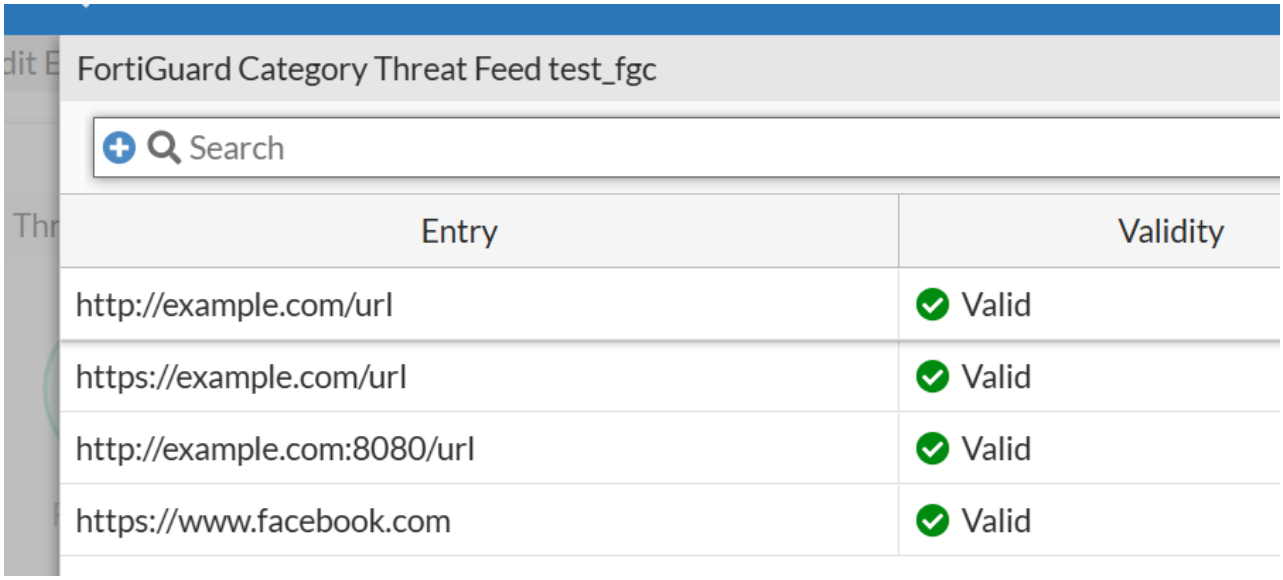
The file contains one URL per line. See External resources file format on page 1108 for more information about the URL list formatting style.

Example configuration

In this example, a list of URLs is imported using the FortiGuard category threat feed. The newly created threat feed is set to block in the web filter profile, and the web filter profile is applied to a policy. Any traffic that passes through the FortiProxy and matches the URLs in the threat feed list will be dropped.

To configure a FortiGuard category threat feed in the GUI:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *FortiGuard Category*.
3. Set the *Name* to *test_fgc*.
4. Set the *Update method* to *External Feed*.
5. Set the *URL of external resource* to *https://172.18.20.80:8443/Override_URLs.txt*.
6. Configure the remaining settings as needed, then click *OK*.
7. Edit the connector, then click *View Entries* to view the URL in the feed, which is https://www.facebook.com.



To configure a FortiGuard category threat feed in the CLI:

```
config system external-resource
    edit "test_fgc"
       set uuid 0a142726-d852-51ef-dea0-fa28469f772f
       set type category
        set category 192
        set resource "https://172.18.20.80:8443/Override_URLs.txt"
        set refresh-rate 1
```

```
    next
end
```

To apply a FortiGuard category threat feed in a web filter profile:

1. Go to *Security Profiles > Web Filter* and create a new web filter profile, or edit an existing one.
2. Enable *FortiGuard Category Based Filter*.
3. In the *Remote Categories* group, set the action for the *test_fgc* category to *Block*.



Selecting the *Allow* action for the *FortiGuard Category Based Filter* does not actually allow the category. It merely implies that no filter has been applied.

We recommend avoid using the *Allow* action for remote categories, as it will not override the original action specified in the *FortiGuard Category Based Filter*.

The *Monitor* and *Block* actions for remote categories can override the original action specified in the *FortiGuard Category Based Filter*.

4. Configure the remaining settings as needed, then click *OK*.

To apply the web filter profile in a policy:

1. Go to *Policy & Objects > Policy* and create a new policy, or edit an existing one.
2. Configure the policy fields as required.
3. Under *Security Profiles*, enable *Web Filter* and select the profile used in the previous procedure.
4. Enable *Log Allowed Traffic*.
5. Click *OK*.

URLs that match the FortiGuard category threat feed list are rated as the FortiGuard category threat feed, overriding their original domain rating. Use the FortiGuard Web Filter Lookup to check the original category of a URL.

To view the web filer logs:

1. Go to *Log & Report > Security Events* and select *Web Filter*.
2. View the log details in the GUI, or download the log file:

```
date=2025-01-21 time=15:52:52 eventtime=1737503572081488023 tz="-0800" logid="0316013056"
type="utm" subtype="webfilter" eventtype="ftgd_blk" level="warning" vd="root" policyid=10
poluuid="8e08c7a4-6b5c-51ed-cb01-295931c9eeb5" policytype="policy" sessionid=859743810
transid=16777395 srcip=10.100.1.1 srcport=48026 srccountry="Reserved" srcintf="port1"
srcintfrole="undefined" dstip=157.240.3.35 dstport=443 dstcountry="United States"
dstintf="port1" dstintfrole="undefined" proto=6 httpmethod="GET" service="HTTPS"
hostname="www.facebook.com" agent="curl/7.68.0" profile="test" action="blocked"
reqtype="direct" url="https://www.facebook.com/" sentbyte=898 rcvdbyte=3255
direction="outgoing" msg="URL belongs to a denied category in policy" ratemethod="domain"
cat=192 catdesc="test_fgc"
```

Note that facebook.com, which was originally in the Social Networking category with a default action set to allow in the *FortiGuard Category Based Filter*, has been overridden by the block

action of the remote category.

The log shows that the access attempt to `facebook.com` was blocked because it matched the custom category "test_fgc" (category ID 192) defined in our external resource configuration. The connection attempt was made using HTTPS (port 443) from a client with IP 10.100.1.1 using curl as the user agent.

Applying a FortiGuard category threat feed in an SSL/SSH profile

A FortiGuard category threat feed can be applied in an SSL/SSH profile where full SSL inspection mode is used. The threat feed category can be selected in the exempt category list. HTTPS requests that match the URLs in the threat feed list will be exempted from SSL deep inspection. This example uses the *test_fgc* threat feed configured in the previous example.

To configure the SSL/SSH profile:

1. Go to *Security Profiles > SSL/SSH Inspection* and create a new profile, or edit an existing one.
2. Set the *Inspection method* to *Full SSL Inspection*.
3. In the *Exempt from SSL Inspection* section, locate *Web categories*. Click the *+* and add *test_fgc* in the *FORTIGUARD CATEGORY THREAT FEED* section.
4. Enable *Log SSL exemptions*.
5. Click *OK*.

To apply the SSL/SSH inspection profile in a policy:

1. Go to *Policy & Objects > Policy* and create a new policy, or edit an existing one.
2. Configure the policy fields as required.
3. Under *Security Profiles*, set *SSL Inspection* to the profile used in the previous procedure.
4. Enable *Log Allowed Traffic*.
5. Click *OK*.

URLs that match the FortiGuard category threat feed list are rated as the FortiGuard category threat feed, overriding their original domain rating. Use the FortiGuard Web Filter Lookup to check the original category of a URL.

To view the SSL logs:

1. Go to *Log & Report > Security Events* and select *SSL*.
2. View the log details in the GUI, or download the log file:

```
date=2025-01-30 time=07:11:02 eventtime=1738177862164729643 tz="+1200" logid="1701062009"
type="utm" subtype="ssl" eventtype="ssl-exempt" level="notice" vd="root" action="exempt"
policyid=4 poluuid="13930d7e-ddb3-51ef-9d0f-ca3105dfd757" policytype="policy"
sessionid=1350861449 transid=16777219 service="HTTPS" profile="custom-deep-inspection"
srcip=10.100.1.1 srcport=40002 srccountry="Reserved" dstip=23.192.228.80 dstport=443
dstcountry="United States" srcintf="port1" srcintfrole="undefined" dstintf="port1"
dstintfrole="undefined" srcuuid="5d6e5070-5d80-51ee-053f-cc6d87753d9d" proto=6
eventsubtype="user-category" cat=192 catdesc="test_ext_cate" hostname="example.com" msg="SSL
connection is exempted based on user category rating."
```

IP address threat feed

An IP address threat feed is a dynamic list that contains IPv4 and IPv6 addresses, address ranges, and subnets. The list is periodically updated from an external server and stored in text file format on an external server. After the FortiProxy imports this list, it can be used as a source or destination in policies, access control rules, and DNS filter profiles. It can also function as an external IP block list to enhance security measures.

Text file example:

```
23.192.228.80
23.215.0.138
96.7.128.198
96.7.128.175
23.192.228.84
23.215.0.136
2600:1406:3a00:21::173e:2e66
2600:1408:ec00:36::1736:7f31
2600:1406:3a00:21::173e:2e65
2600:1406:bc00:53::b81e:94ce
2600:1408:ec00:36::1736:7f24
2600:1406:bc00:53::b81e:94c8
```

The file contains one IPv4 or IPv6 address, address range, or subnet per line. See External resources file format on page 1108 for more information about the IP list formatting style.

Example configuration

In this example, a list of destination IP addresses is imported using the IP address threat feed. The newly created threat feed is then used as a destination in a policy with the action set to deny. Any traffic that passes through the FortiProxy and matches the defined policy will be dropped. This setup ensures that FortiProxy can efficiently utilize an external IP threat feed to enhance network security.

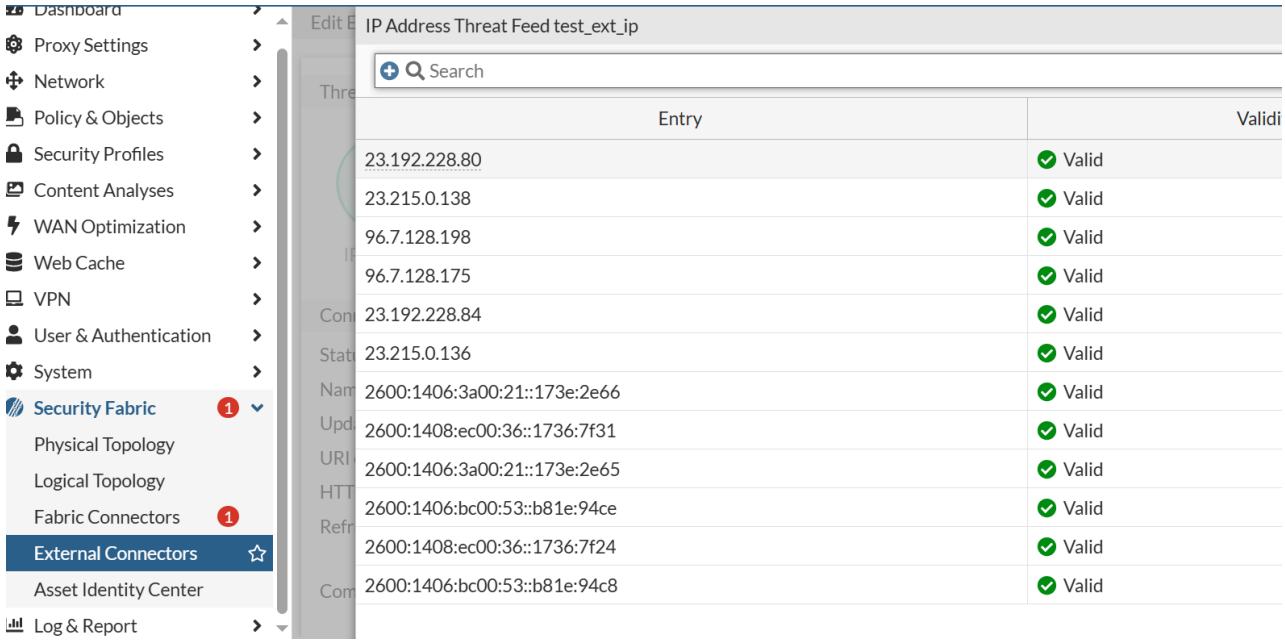


Please note that the URI provided in the example is solely for demonstration purposes and does not represent a reliable list of well-maintained IP addresses. It is recommended that you utilize a URI of a reputable external IP list that is regularly updated.

To configure an IP address threat feed in the GUI:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *IP Address*.
3. Set the *Name* to *test_ext_ip*.
4. Set the *Update method* to *External Feed*.
5. Set the *URL of external resource* to *http://172.18.20.80:8443/blocklist.txt*.
6. Configure the remaining settings as required, then click *OK*.

7. Edit the connector, then click *View Entries* to view the IP addresses in the feed.



To configure an IP address threat feed in the CLI:

```
config system external-resource
   edit "test_ext_ip"
      set uuid 1d44eb56-de78-51ef-ffe0-8004ef4724c2
       set type address
      set resource "http://172.18.20.80:8443/blocklist.txt"
   next
end
```

To improve the security of the connection, it is recommended to enable server certificate validation (`server-identity-check`) either in basic or full mode. By default, it is set to none.

To apply an IP address threat feed in a policy:

1. Go to *Policy & Objects* > *Policy* and create a new policy, or edit an existing one.
2. Configure the policy fields as required.
3. In the *Destination* field, click the *+* and select *test_ext_ip* from the list (in the *IP ADDRESS FEED* section).
4. Set *Action* to *DENY*.
5. Enable *Log Allowed Traffic*.
6. Click *OK*.

Applying an IP address threat feed as an external IP block list in a DNS filter profile

An IP address threat feed can be applied by enabling *External IP Block Lists* in a DNS filter profile. Any DNS query that passes through the FortiProxy and resolves to any of the IP addresses in the threat feed list will be dropped.

To configure the DNS filter profile:

1. Go to *Security Profiles* > *DNS Filter* and create a new profile, or edit an existing one.
2. Enable *External IP Block Lists*.
3. Click the *+* and select *test_ext_ip* from the list.
4. Click *OK*.

To apply the DNS filter profile in a policy:

1. Go to *Policy & Objects* > *Policy* and create a new policy, or edit an existing one.
2. Configure the policy fields as required.
3. Under *Security Profiles*, enable *DNS Filter* and select the profile used in the previous procedure.
4. Enable *Log Allowed Traffic*.
5. Click *OK*.

IP addresses that match the IP address threat feed list will be blocked.

To view the DNS query logs:

1. Go to *Log & Report* > *Security Events* and select *DNS Query*.
2. View the log details in the GUI, or download the log file:

```
date=2025-02-03 time=13:54:49 eventtime=1738619688720896953 tz="-0800" logid="1501054400"
type="utm" subtype="dns" eventtype="dns-response" level="warning" vd="root" policyid=3
sessionid=0 user="unknown" dstuser="unknown" srcip=10.100.1.45 srcport=49711
srccountry="Reserved" srcintf="port1" srcintfrole="undefined" dstip=8.8.8.8 dstport=53
dstcountry="United States" dstintf="port1" dstintfrole="undefined" proto=17 profile="test_ip_
feed" xid=6535 qname="example.com" qtype="A" qtypeval=1 qclass="IN" ipaddr="208.91.112.55"
msg="Domain was blocked because it is in the domain-filter list" action="redirect"
domainfilteridx=0 domainfilterlist="test_ext_ip" rcode=0
```

Domain name threat feed

A domain name threat feed is a dynamic list that contains domains and periodically updates from an external server. The list is stored in a text file format on an external server. After the FortiProxy imports this list, it becomes available as a category in the *Remote Categories* group of DNS filter profiles that can be used to block or monitor domains matching this category. Multiple custom categories can be defined by creating a domain name threat feed for each category.

Text file example:

```
mail.*.example.com
*-special.example.com
```

```
www.*example.com
example.com
```

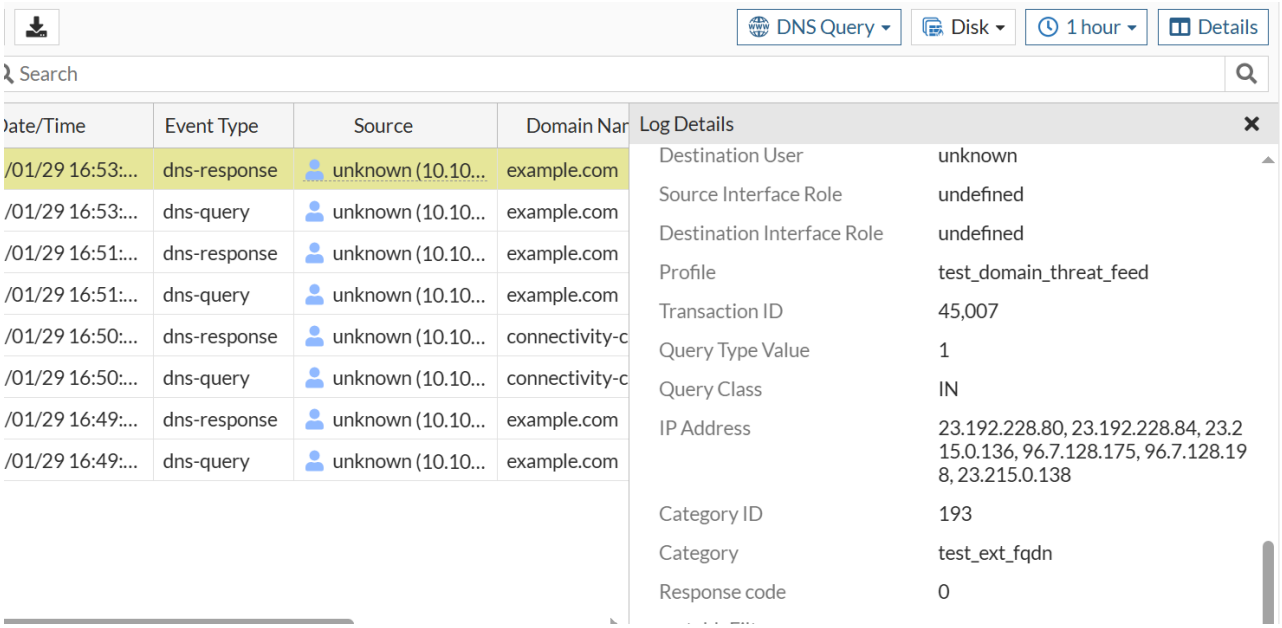
The file contains one domain name per line. See External resources file format on page 1108 for more information about the domain list formatting style.

Example configuration

In this example, a list of domain names is imported using the domain name threat feed. The newly created threat feed is set to monitor in the DNS filter profile, and the DNS filter profile is applied to a policy. Any traffic that passes through the FortiProxy and matches any of the domain names in the threat feed list will be monitored.

To configure a domain name threat feed in the GUI:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *Domain Name*.
3. Set the *Name* to *test_ext_fqdn*.
4. Set the *Update method* to *External Feed*.
5. Set the *URL of external resource* to *http://172.18.20.80:8443*.
6. Configure the remaining settings as required, then click *OK*.
7. Edit the connector, then click *View Entries* to view the domain names in the feed.



To configure a domain name threat feed in the CLI:

```
config system external-resource
    edit "test_ext_fqdn”
        set uuid c1de2236-dea0-51ef-04aa-286146d757e1
        set type domain
        set category 193
```

```
        set resource "http://172.18.20.80:8443"
    next
end
```



To improve the security of the connection, it is recommended to enable server certificate validation (`server-identity-check`) either in basic or full mode. By default, it is set to none.

To apply a domain name threat feed in a DNS filter profile:

1. Go to *Security Profiles* > *DNS Filter* and create a new DNS filter profile, or edit an existing one.
2. Enable *FortiGuard Category Based Filter*.
3. In the *Remote Categories* group, set the action for the *Domain_monitor_list* category to *Monitor*.



Selecting the *Allow* action for the *FortiGuard Category Based Filter* does not actually allow the category. It merely implies that no filter has been applied.

We recommend avoid using the *Allow* action for remote categories, as it will not override the original action specified in the *FortiGuard Category Based Filter*.

The *Monitor* and *Block* actions for remote categories can override the original action specified in the *FortiGuard Category Based Filter*.

4. Configure the remaining settings as needed, then click *OK*.

To apply the DNS filter profile in a policy:

1. Go to *Policy & Objects* > *Policy* and create a new policy, or edit an existing one.
2. Configure the policy fields as required.
3. Under *Security Profiles*, enable *DNS Filter* and select the profile used in the previous procedure.
4. Enable *Log Allowed Traffic*.
5. Click *OK*.

Domains that match the domain threat feed list are rated as domain threat feed, overriding their original domain rating. Use the FortiGuard Secure DNS Service to check the original category of a domain name.

To view the DNS query logs:

1. Go to *Log & Report* > *Security Events* and select *DNS Query*.
2. View the log details in the GUI, or download the log file:

```
date=2025-01-29 time=16:53:26 eventtime=1738198405841358280 tz="-0800" logid="1501054802"
type="utm" subtype="dns" eventtype="dns-response" level="notice" vd="root" policyid=3
sessionid=0 user="unknown" dstuser="unknown" srcip=10.100.1.45 srcport=57717
srccountry="Reserved" srcintf="port1" srcintfrole="undefined" dstip=8.8.4.4 dstport=53
dstcountry="United States" dstintf="port1" dstintfrole="undefined" proto=17 profile="test_
domain_threat_feed" xid=45007 qname="example.com" qtype="A" qtypeval=1 qclass="IN"
```

```
ipaddr="23.192.228.80, 23.192.228.84, 23.215.0.136, 96.7.128.175, 96.7.128.198, 23.215.0.138"
msg="Domain is monitored" action="pass" cat=193 catdesc="test_ext_fqdn" rcode=0
```

Note that example.com, which was originally in the Information Technology category with a default action set to allow in the *FortiGuard Category Based Filter*, has been overridden by the monitor action of the remote category.

Malware hash threat feed

A malware hash threat feed is a dynamic list that contains malware hashes and periodically updates from an external server. The list is stored in text file format on an external server. After the FortiProxy imports this list, it is automatically used for virus outbreak prevention on antivirus profiles when *Use external malware block list* is enabled. Similar to FortiGuard outbreak prevention, the malware hash threat feed is not supported in AV quick scan mode.

Text file example:

```
292b2e6bb027cd4ff4d24e338f5c48de
dda37961870ce079defbf185eeeef905 Trojan-Ransom.Win32.Locky.abfl
3fa86717650a17d075d856a41b3874265f8e9eab Trojan-Ransom.Win32.Locky.abfl
c35f705df9e475305c0984b05991d444450809c35dd1d96106bb8e7128b9082f Trojan-Ransom.Win32.Locky.abfl
```

The file contains one malware hash per line. See External resources file format on page 1108 for more information about the malware hash list formatting style.



For optimal performance, do not mix different hashes in the list. Only use one MD5, SHA1, or SHA256.

Example configuration

In this example, a list of malware hashes is imported using the malware threat feed. The newly created threat feed is applied to an antivirus profile, and the antivirus profile is applied to a policy. Any traffic that passes through the FortiProxy and matches the malware hashes in the threat feed list will be dropped.

To configure a malware hash threat feed in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *Malware Hash*.
3. Set the *Name* to *test_malware_ext*.
4. Set the *Update method* to *External Feed*.
5. Set the *URL of external resource* to *"http://172.18.20.80:8080/malware.txt*.
6. Configure the remaining settings as required, then click *OK*.
7. Edit the connector, then click *View Entries* to view the hash list.

To configure a malware hash threat feed in the CLI:

```
config system external-resource
    edit "test_malware_ext"
        set type malware
        set resource ""http://172.18.20.80:8080/malware.txt"
        set server-identity-check {none | basic | full}
    next
end
```



To improve the security of the connection, it is recommended to enable server certificate validation (`server-identity-check`) either in basic or full mode. By default, it is set to none.

To apply a malware hash threat feed in an antivirus profile (CLI only):

```
config antivirus profile
   edit "test_ext_feed"
      config http
         set external-blocklist enable
      end
      set external-blocklist "test_malware_ext"
   next
end
```

To apply the antivirus profile in a policy in the GUI:

1. Go to *Policy & Objects > Policy* and create a new policy, or edit an existing one.
2. Configure the policy fields as required.
3. Under *Security Profiles*, enable *AntiVirus* and select the profile used in the previous procedure.
4. Set *SSL Inspection* to *deep-inspection* to inspect HTTPS traffic.
5. Enable *Log Allowed Traffic*.
6. Click *OK*.

To apply the antivirus profile in a policy in the CLI:

```
config firewall policy
   edit 4
      set name "Malware Test Policy"
      set srcintf "port1"
      set dstintf "port1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set logtraffic all
      set utm-status enable
      set av-profile "test_ext_feed"
   next
end
```

To view the antivirus logs:

1. Go to *Log & Report > Security Events* and select *AntiVirus* in the GUI or run `diagnose log display` in the CLI.
2. View the log details in the GUI, or download the log file:

```
date=2025-01-31 time=14:58:56 eventtime=1738364335833075192 tz="-0800" logid="0207008212"
type="utm" subtype="virus" eventtype="malware-list" level="warning" vd="root" policyid=4
poluuid="13930d7e-ddb3-51ef-9d0f-ca3105dfd757" policytype="policy" msg="Blocked by local
malware list." action="blocked" service="HTTPS" sessionid=424501225 srcip=10.100.1.1
dstip=104.22.58.173 srcport=52341 dstport=443 srccountry="Reserved" dstcountry="United States"
srcintf="port1" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined"
srcuuid="5d6e5070-5d80-51ee-053f-cc6d87753d9d" proto=6 direction="incoming"
filename="example.txt" quarskip="Quarantine-disabled" virus="1f-51ef-d2a5-8921d8954279"
viruscat="File Hash" dtype="cached" filehash="51ce4dcef1fa486499b8b50dcfd91c33"
filehashsrc="test_malware_ext" url="https://example-files.online-
convert.com/document/txt/example.txt" profile="test_ext_feed" agent="Mozilla/5.0 (Windows NT
10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0" httpmethod="GET"
analyticssubmit="false" crscore=10 craction=2 crlevel="medium"
```

To verify the scanunit daemon:

```
# diagnose sys scanunit file-hash list
malware '51ce4dcef1fa486499b8b50dcfd91c33' vf_id 0 uuid 15750 profile 'test_malware_ext'
description '1f-51ef-d2a5-8921d8954279'
```

The list of external hashes has been updated.

URL list threat feed

A URL threat feed is a dynamic list that contains URLs and periodically updates from an external server. The list is stored in a text file format on an external server. After the FortiProxy imports this list, it becomes available for use in proxy address configurations as a URL list. This allows you to create policies that specifically target URLs in the external list. Multiple custom URL lists can be defined by creating a URL threat feed for each list.

Example:

```
example.com/page1
*.example.com/login
www.example.com/admin/*
```

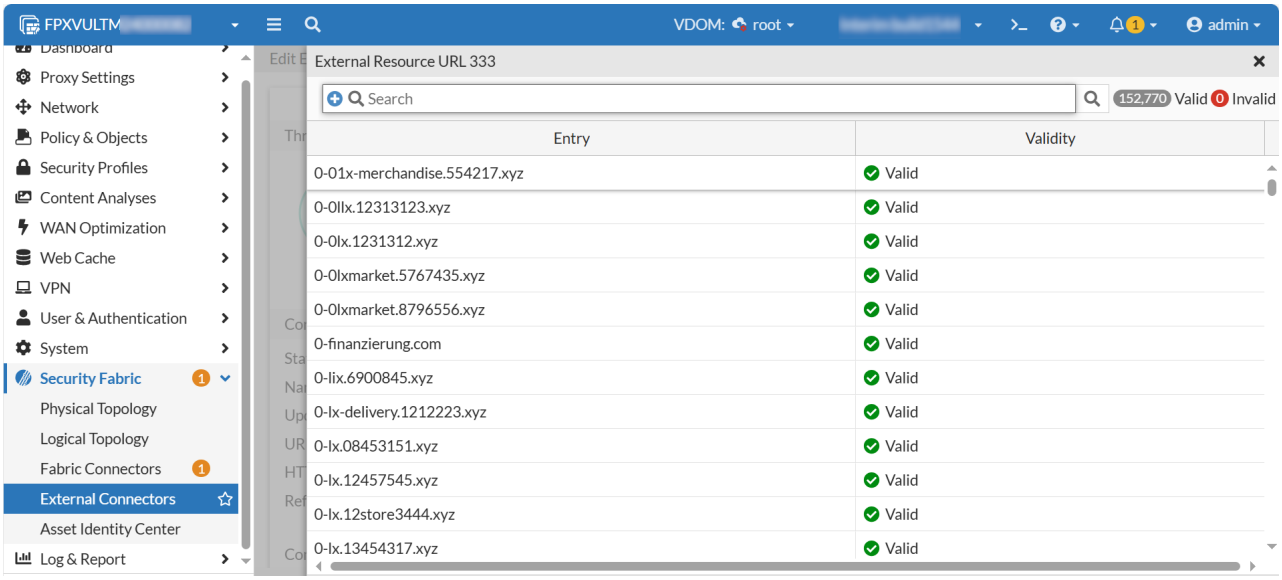
The file contains one URL pattern per line. See External resources file format on page 1108 for more information about the URL list formatting style.

Example configuration

In this example, a list of URLs is imported using the URL threat feed. The newly created URL threat feed is configured as a proxy address, which is then applied to a policy. Any traffic that passes through the FortiProxy and matches any of the URLs in the threat feed list will be controlled according to the policy action.

To configure a URL threat feed in the GUI:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *URL List*.
3. Set the *Name* to *test_ext_url*.
4. Set the *Update method* to *External Feed*.
5. Set the *URL of external resource* to *http://172.18.20.80:8443/urllist.txt*.
6. Configure the remaining settings as required, then click *OK*.
7. Edit the connector, then click *View Entries* to view the URLs in the feed.



To configure a URL threat feed in the CLI:

```
config system external-resource
   edit "test_ext_url"
      set uuid c2de3337-dea0-52ef-05bb-387246d858e2
      set type url
      set resource "http://172.18.20.80:8443/urllist.txt"
   next
end
```

To improve the security of the connection, it is recommended to enable server certificate validation (`server-identity-check`) either in basic or full mode. By default, it is set to none.

To use the URL list threat feed in a proxy address in the GUI:

1. Go to *Policy & Objects* > *Addresses* and create a new proxy address, or edit an existing one.
2. Set *Name* to *test_ext_urllist*.
3. Set *Type* to *URL List*.
4. Set *Host* to *all*.
5. Set *URL List* to the external resource you created (*test_ext_url*).

6. Click *OK*.

To configure a proxy address with URL list threat feed in the CLI:

```
config firewall proxy-address
   edit "test_ext_urllist"
      set uuid ad22888a-0378-51f0-a888-78c0ec22fa35
      set type url-list
      set host "all"
      set url-list "test_ext_url"
   next
end
```

To configure a policy with the URL proxy address in the GUI:

1. Go to *Policy & Objects* > *Policy* and create a new policy, or edit an existing one.
2. Configure the policy fields as required.
3. Set *Destination* to the proxy address you created (*test_ext_urllist*).
4. Configure security profiles as needed.
5. Enable *Log Allowed Traffic*.
6. Click *OK*.

To configure a policy with the URL proxy address in the CLI:

```
config firewall policy
   edit 15
      set type explicit-web
      set name "111"
      set uuid 9f066e76-0376-51f0-4298-db6db18529a3
      set dstintf "any"
      set srcaddr "all"
      set dstaddr "test_ext_urllist"
      set action accept
      set schedule "always"
      set service "webproxy"
      set explicit-web-proxy "web-proxy"
      set utm-status enable
      set logtraffic all
      set logtraffic-start enable
      set log-http-transaction enable
      set extended-log enable
      set ssl-ssh-profile "deep-inspection"
      set dnsfilter-profile "test"
   next
end
```

To view the Web Filter logs:

1. Go to *Log & Report* > *Security Events* and select *Web Filter*.
2. View the log details in the GUI, or download the log file:

```
date=2025-03-19 time=15:02:30 eventtime=1742421749460287753 tz="-0700" logid="0010000099"
type="traffic" subtype="http-transaction" level="notice" vd="root" srcip=10.120.1.1
dstip=172.18.20.213 clientip=10.120.1.1 scheme="http" srcport=61609 dstport=80
hostname="wwww.amazonnow.vip" url="http://wwww.amazonnow.vip/" prefetch=0 policyid=15
sessionid=1281393107 transid=1586 reqlength=136 resplength=350 rcvdbyte=350 sentbyte=136
resptype="normal" httpmethod="GET" agent="curl/8.0.1" statuscode="301" rawdata="Time=-
1741961ms|[REQ] Host=wwww.amazonnow.vip" reqtime=1742421749 resptime=1742421749
respfinishtime=0 duration=0 appcat="unscanned"
```

Threat feed connectors per VDOM

When multi-VDOM mode is enabled, a threat feed external connector can be defined in global or within a VDOM. Global threat feeds can be used in any VDOM, but cannot be edited within the VDOM. FortiGuard category and domain name-based external feeds have an added category number field to identify the threat feed. The threat feed name in global must start with `g-`. Threat feed names in VDOMs cannot start with `g-`.

FortiGuard category and domain name-based external feed entries must have a number assigned to them that ranges from 192 to 221. This number can be assigned to both external feed types. However, when a category number is used under a global entry, such as 192 with the name `g-cat-192`, this category number cannot be used in any other global or VDOM entries. If a category is used under a VDOM entry, such as 192 under VDOM1 with the name `cat-192`, the category 192 can be used in another VDOM or root with the name `cat-192`.

A threat feed connector can only be used in profiles in the VDOM that it was created in. Global connectors can be used in all VDOMs.

Each VDOM can have a maximum of 256 threat feed entries. But in total, a FortiProxy can only have 511 threat feed entries.

To improve the security of the connection, it is recommended to enable server certificate validation (`server-identity-check`) either in basic or full mode.

To configure a FortiGuard category threat feed connector under global in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *FortiGuard Category*.
3. Enter a name that begins with `g-`.
4. Configure the other settings as needed.
5. Click *OK*.

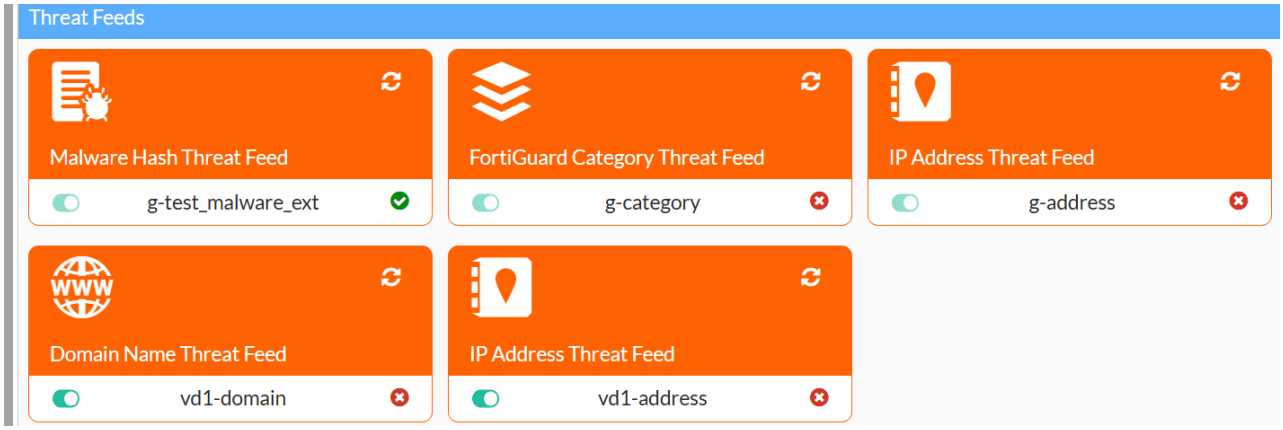
To configure a FortiGuard category threat feed connector under global in the CLI:

```
config global
    config system external-resource
        edit "g-category"
            set status enable
            set type category
            set category 195
            set comments ''
```

```
            set resource "http://172.18.20.80:8443/external-resource-test/513-FDGCategory.txt"
            set server-identity-check {none | basic | full}
            set refresh-rate 5
        next
    end
end
```

To configure a domain name threat feed connector under a VDOM in the GUI:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *Domain Name*.
3. Enter a name that does not begin with g-.
4. Configure the other settings as needed.
5. Click *OK*. The threat feed connector created under global also appears, but it is not editable.



To configure a domain name threat feed connector under a VDOM in the CLI:

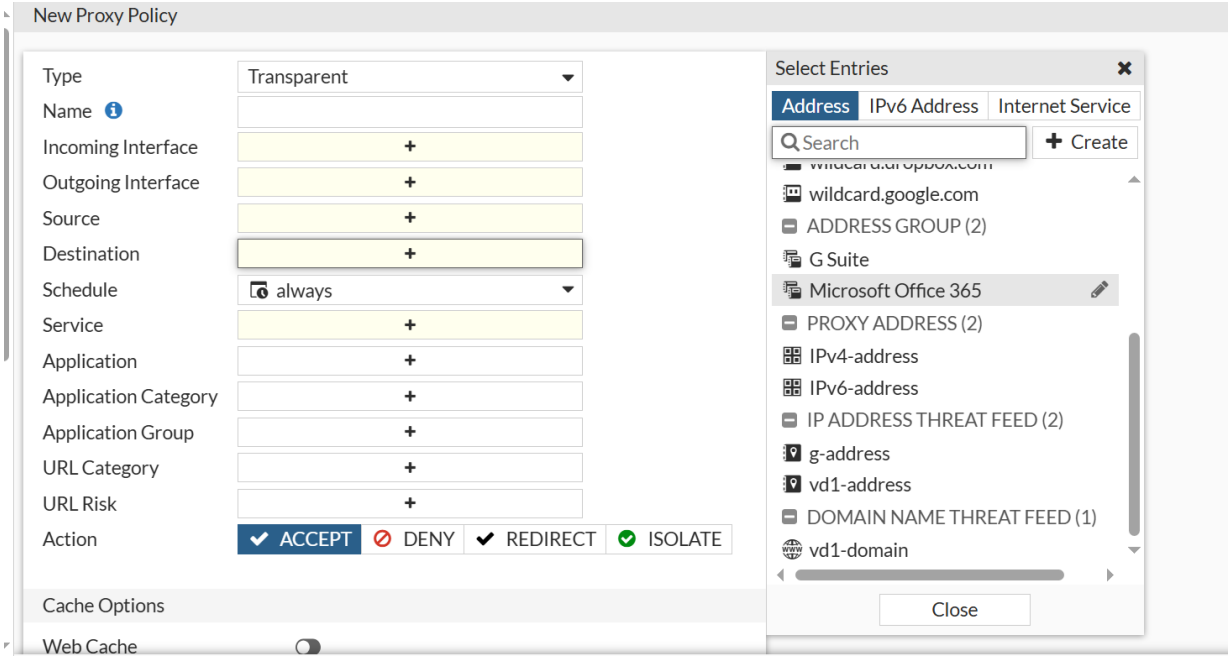
```
config vdom
    edit vd1
        config system external-resource
            edit "vd1-domain"
                set status enable
                set type domain
                set category 196
                set comments ''
                set resource "http://172.18.20.80:8443/external-resource-test/513-Domain.txt"
                set server-identity-check {none | basic | full}
                set refresh-rate 5
            next
        end
    next
end
```

To use an IP address threat feed in a policy in the GUI:

1. Configure an IP address connector in global:
   a. Go to *Security Fabric > External Connectors* and click *Create New*.
   b. In the *Threat Feeds* section, click *IP Address*.
   c. Enter a name that begins with g-.
   d. Configure the other settings as needed.
   e. Click *OK*.
2. Configure an IP address connector in the VDOM (vd1):
   a. Go to *Security Fabric > External Connectors* and click *Create New*.
   b. In the *Threat Feeds* section, click *IP Address*.
   c. Enter a name that does not begin with g-.
   d. Configure the other settings as needed.
   e. Click *OK*. The threat feed connectors created under global also appear, but they are not editable.



3. Configure the policy in the VDOM (vd1):
   a. Go to *Policy & Objects > Policy* and click *Create New*.
   b. For *Destination*, select *vd1-address*. Since this policy is configured under vd1, *g-address* can also be set as the destination.



c. Configure the other settings as needed.
d. Click *OK*.

To use an IP address threat feed in a policy in the CLI:

1. Configure the IP address connectors:

```
config global
    config system external-resource
        edit "g-address"
            set status enable
            set type address
            set username ''
            set comments ''
            set resource "172.18.20.80:8443/external-resource-test/513-IP.txt"
            set server-identity-check {none | basic | full}
            set refresh-rate 5
        next
    end
end
```

```
config vdom
    edit vd1
        config system external-resource
            edit "vd1-address"
                set status enable
                set type address
                set comments ''
                set resource "http://172.18.20.80:8443/external-resource-test/513-IP.txt"
                set user-agent "curl/7.58.0"
                set server-identity-check {none | basic | full}
                set refresh-rate 5
            next
        end
    next
end
```

2. In the VDOM, configure a policy with the external address as the destination address:

```
config vdom
    edit vd1
        config firewall policy
            edit 1
                set name "test"
                set srcintf "port10"
                set dstintf "port9"
                set srcaddr "all"
                set dstaddr "vd1-address"
                set action accept
                set schedule "always"
                set service "ALL"
                set profile-protocol-options "protocol"
```

```
                set nat enable
            next
        end
    next
end
```



Since this policy is configured under `vd1`, `g-address` can also be set as the `dstaddr`.

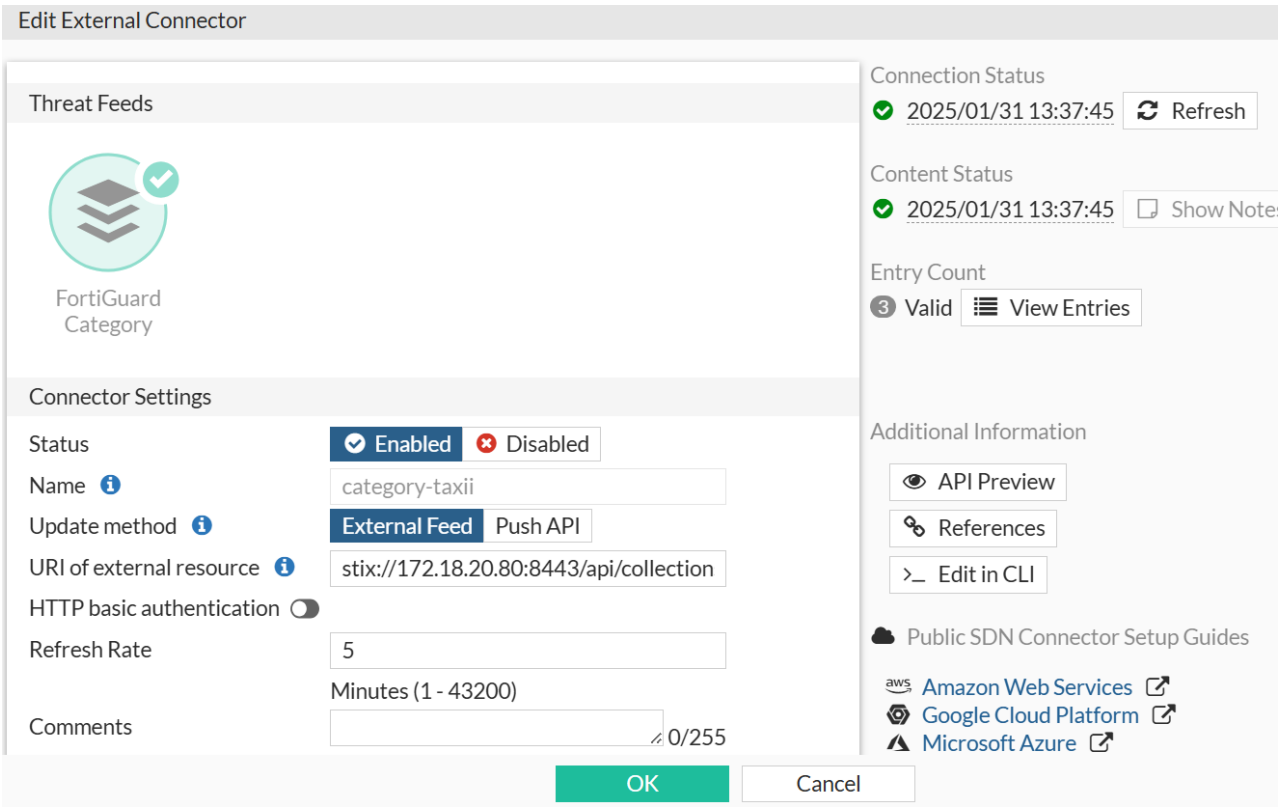
STIX format for external threat feeds

The FortiProxy supports external threat feeds that use the STIX/TAXII format. Use the `stix://` prefix in the URI to denote the protocol.

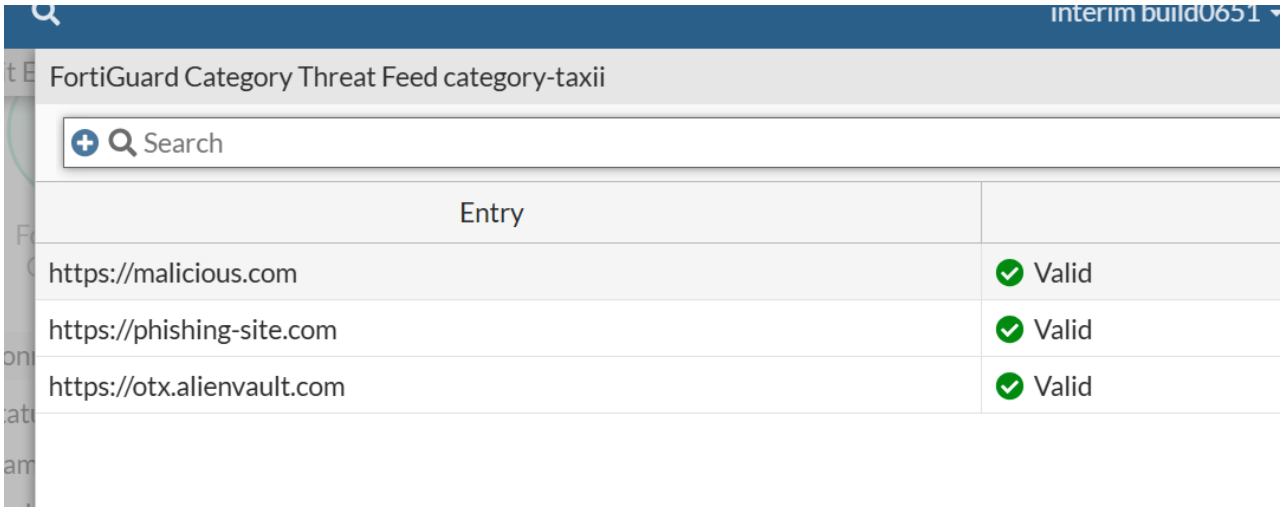
All external threat feeds support the STIX format. In this example, a FortiGuard Category threat feed in the STIX format is configured.

To configure a FortiGuard Category threat feed in the STIX format in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. Select *FortiGuard Category* from the *Threat Feeds* section.
3. Configure the connector:
   - *Name*: *category-taxii*
   - *Update method*: *External Feed*
   - *URL of external resource*: *stix://172.18.20.80:8443/api/collections/*
   - *HTTP basic authentication*: Enable and enter the username and password, such as *guest* and *guest*.



4. Click *OK*.
5. Edit the connector, and click *View Entries* in the right side bar to view the retrieved entries.



To configure a FortiGuard Category threat feed in the STIX format in the CLI:

```
config system external-resource
    edit "category-taxii"
        set uuid afb6111c-e00e-51ef-5ea4-ed01d4143c21
        set category 194
        set resource "stix://172.18.20.80:8443/api/collections/"
```

```
    next
end
```



To improve the security of the connection, it is recommended to enable server certificate validation (`server-identity-check`) either in basic or full mode. By default, `server-identity-check` is set to `none`.

- **none**: No certificate validation.
- **basic**: Validates certificate against a CA but does not verify hostname.
- **full**: Full validation, including CA and hostname check **(Recommended for security)**.

If the connector is used in webfilter that blocks category 194, the traffic that matches the retrieved URLs is blocked.

Example log:

```
date=2025-01-31 time=13:46:42 eventtime=1738360002401548826 tz="-0800" logid="0316013056"
type="utm" subtype="webfilter" eventtype="ftgd_blk" level="warning" vd="root" policyid=4
poluuid="13930d7e-ddb3-51ef-9d0f-ca3105dfd757" policytype="policy" sessionid=492580641
transid=16778026 srcip=10.100.1.1 srcport=61116 srccountry="Reserved" srcintf="port1"
srcintfrole="undefined" srcuuid="5d6e5070-5d80-51ee-053f-cc6d87753d9d" dstip=18.172.185.2
dstport=80 dstcountry="Canada" dstintf="port1" dstintfrole="undefined" proto=6 httpmethod="GET"
service="HTTP" hostname="otx.alienvault.com" agent="Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:134.0) Gecko/20100101 Firefox/134.0" profile="test-web-prof" action="blocked"
reqtype="referral" url="http://otx.alienvault.com/favicon.ico"
referralurl="http://otx.alienvault.com/" sentbyte=394 rcvdbyte=0 direction="outgoing" msg="URL
belongs to a denied category in policy" ratemethod="domain" cat=194 catdesc="category-taxii"
```

Configuring an external malicious URL feed with an API key

You can configure FortiProxy to consume an external malicious URL feed using API key authentication. This allows FortiProxy to integrate custom threat intelligence sources for automatically blocking malicious URLs in web traffic.

To configure the external malicious URL feed in FortiProxy GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *FortiGuard Category*.
3. Set the *Name* to *Custom_Malicious_URL_Feed*.
4. Set the *Update method* to *External Feed*.
5. Set the *URL of external resource* to *o http://172.18.20.80:8080/malicious-urls*.
6. Configure the remaining settings as needed, then click *OK*.

To configure the external malicious URL feed in FortiProxy CLI:

```
config system external-resource
    edit "Custom_Malicious_URL_Feed"
```

```
        set uuid a24fcf94-e00f-51ef-d901-d7632353620f
         set category 200
         set resource "http://172.18.20.80:8080/malicious-urls"
         set user-agent "Firefox\r\nAPI-Key:SECRETAPIKEY"
    next
end
```

Option	Description
`set category 200`	Ensures the category ID is unique (valid range: 192 - 221).
`set resource`	Points to your locally hosted threat feed.
`set user-agent`	Sends the required API key via User-Agent.

To apply a FortiGuard category threat feed in a web filter profile:

1. Go to *Security Profiles* > *Web Filter* and create a new web filter profile, or edit an existing one.
2. Enable *FortiGuard Category Based Filter*.
3. In the *Remote Categories* group, set the action for the *Custom_Malicious_URL_Feed* category to *Block*.



Selecting the *Allow* action for the *FortiGuard Category Based Filter* does not actually allow the category. It merely implies that no filter has been applied.

We recommend avoid using the *Allow* action for remote categories, as it will not override the original action specified in the *FortiGuard Category Based Filter*.

The *Monitor* and *Block* actions for remote categories can override the original action specified in the *FortiGuard Category Based Filter*.

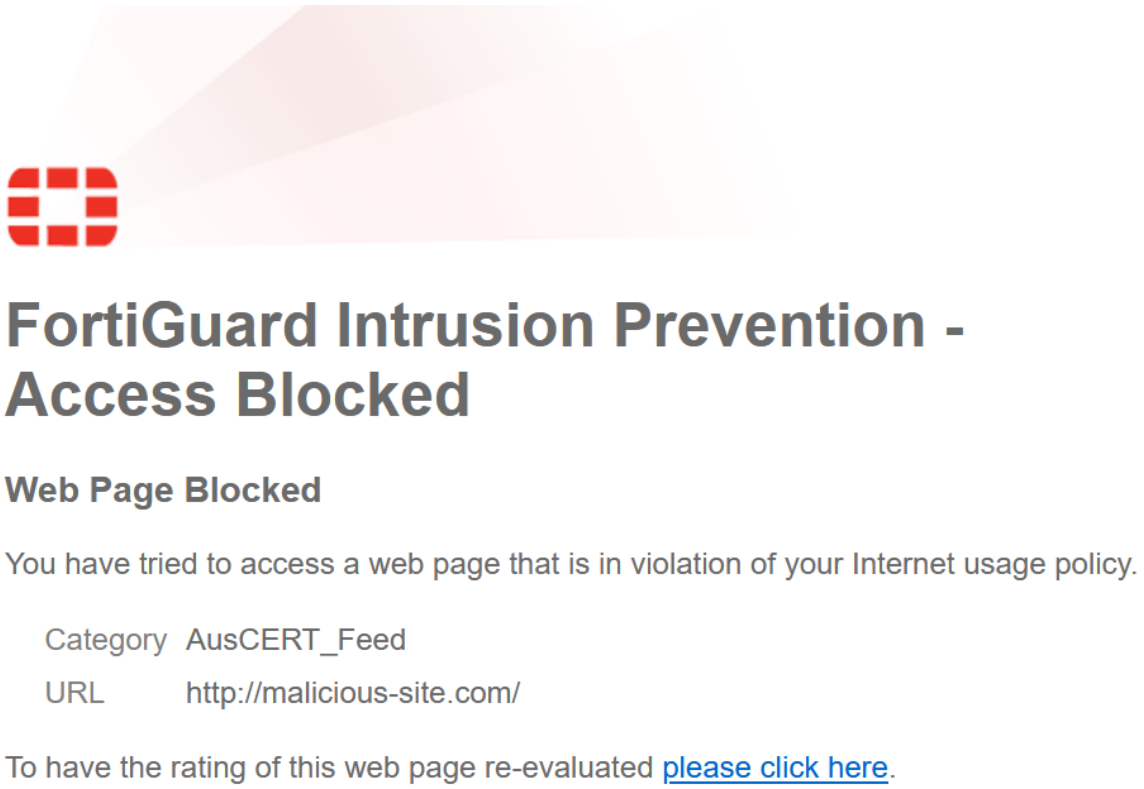
4. Configure the remaining settings as needed, then click *OK*.

To apply the web filter profile in a policy:

1. Go to *Policy & Objects* > *Policy* and create a new policy, or edit an existing one.
2. Configure the policy fields as required.
3. Under *Security Profiles*, enable *Web Filter* and select the profile used in the previous procedure.
4. Enable *Log Allowed Traffic*.
5. Click *OK*.

To verify that FortiProxy is blocking malicious URLs:

1. Visit a blocked URL from the feed, such as: *http://malicious-site.com*. A FortiProxy block page should appear.



2. Go to *Log & Report > Web Filter* to to find the log for blocked requests categorized as *Custom_Malicious_URL_Feed*.

   Example log:

```
date=2025-01-31 time=14:18:02 logid="0316013056" type="utm" subtype="webfilter"
eventtype="ftgd_blk" level="warning" policyid=1 srcip=192.168.1.100 dstip=45.77.89.10
service="HTTP" hostname="malicious-site.com" action="blocked" cat=200 catdesc="Custom_
Malicious_URL_Feed"
```

Troubleshooting

- If FortiProxy does not retrieve the feed, use these commands to check if FortiProxy can resolve and connect to the local server:
  - `diagnose debug app dnsproxy -1`
  - `diagnose debug app forticron -1`
  - `diagnose debug enable`

  Example output:

```
http_request_make()-2292: HTTP request: http
GET /malicious-urls HTTP/1.1
Host: 172.18.20.80
User-Agent: Firefox
API-Key:SECRETAPIKEY
Accept: */*
Connection: close
```

- If FortiProxy successfully connects, `diagnose debug app forticron -1` should return `HTTP 200 OK`.

  Example log:

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.10.12
Date: Fri, 31 Jan 2025 20:49:02 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 126
Connection: close
```

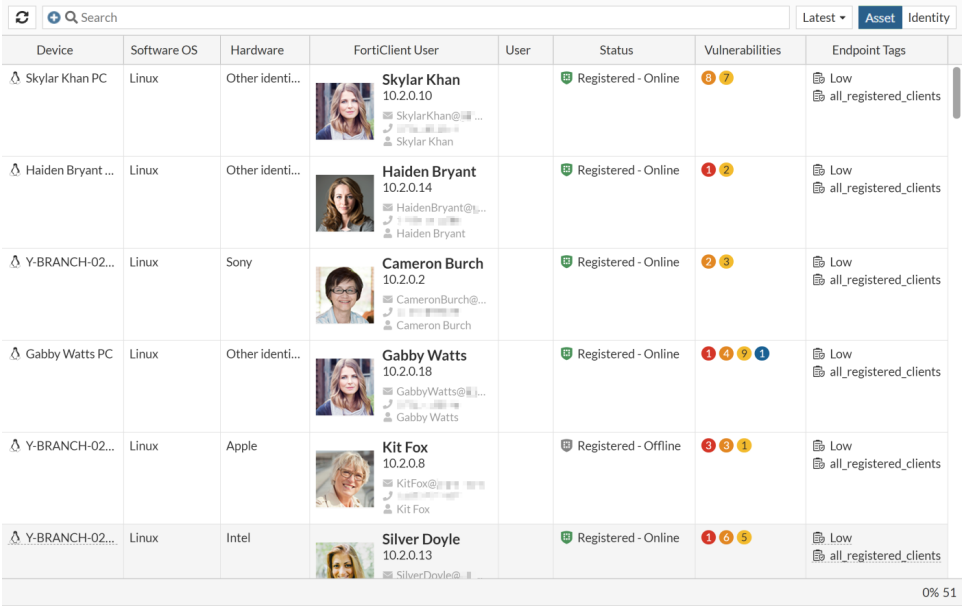
- If the feed is accessible, FortiProxy will successfully retrieve and update the entries. If you receive 403 Forbidden, check if the API key is correctly set in User-Agent. Different providers may require different authentication methods (User-Agent, Authorization headers, URL params). Ensure your external server correctly returns TXT format (one URL per line).

Asset Identity Center

The *Asset Identity Center* page unifies information from detected addresses, devices, and users into a single page, while building a data structure to store the user and device information in the backend. *Asset* view groups information by *Device*, while *Identity* view groups information by *User*. Hover over a device or a user in the GUI to perform different actions relevant to the object, such as adding a firewall device address, adding an IP address, banning the IP address, quarantining the host, and more.

To view the Asset Identity Center page:

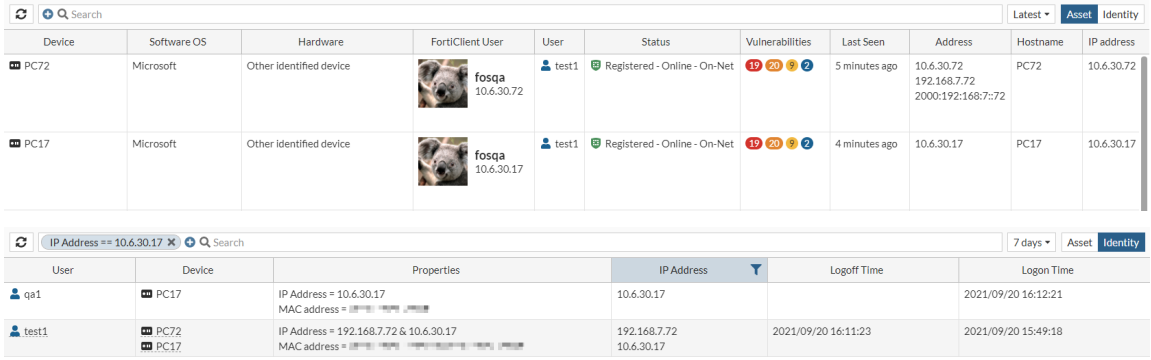
1. Go to *Security Fabric* > *Asset Identity Center*.
2. Click *Asset* to view information by device. The available columns are *Device*, *Software OS*, *Hardware*, *FortiClient User*, *User*, *Status*, *Vulnerabilities*, *Endpoint Tags*, and *Last Seen*. The optional columns are *Address*, *Firewall Address*, *Hostname*, *IP Address*, and *Server*.



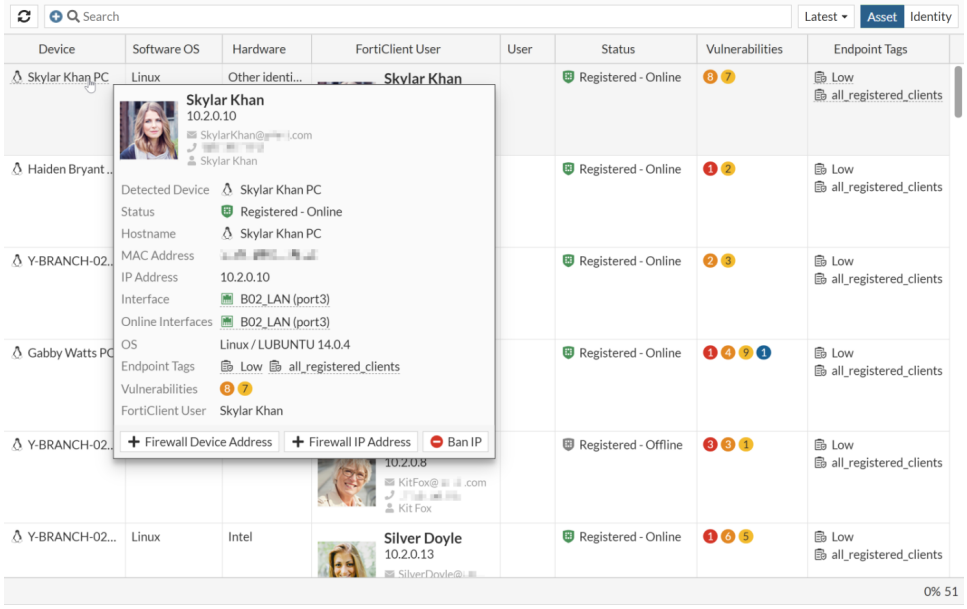
3. Click *Identity* to view information by user. The available columns are *User*, *Device*, and *Properties*. The optional columns are *IP Address*, *Logoff Time*, and *Logon Time*.



Each view has a dropdown option to view the information within different time frames (*Latest*, *1 hour*, *24 hours*, and *7 days*). Vulnerability information is displayed when applicable. The page displays user and device relationships, such as which users are logged in to multiple devices or if multiple users are logged in to single devices.



4. Hover over a device in the list to view the tooltip and possible actions. In this example, the available actions are add firewall device address, add firewall IP address, and ban the IP.



Diagnostics for the unified user device store

The following options are available for `diagnose user-device-store unified <option>`:

Option	Description
`device-memory-query`	Get device records and associated user records from memory.

Option	Description
`device-query`	Get device records and associated user records from memory and disk.
`user-memory-query`	Get user records and associated device records from memory.
`user-query`	Get user records and associated device records from memory and disk.
`re-query`	Retrieve query by `<query-id> <iteration-start> <iteration-count>` (takes 0-3 arguments).
`list`	List unified queries.
`clear`	Delete all unified queries.
`dump`	Dump unified query stats by `<query-id>` (takes 0-1 arguments).
`delete`	Delete unified query by `<query-id>` (takes 0-1 arguments).
`stats`	Get statistics for unified queries.
`debug`	Enable/disable debug logs for unified queries.

Log & Report

The *Log & Report* menu allows you to view and download reports and traffic, event, and security logs. Logging, archiving, and user interface settings can also be configured.

This section describes the following:

- Types of logs on page 1138
- System Events on page 1140
- Security Events on page 1143
- Reports on page 1145
- Log settings on page 1147
- Email Alert Settings on page 1152
- Port Exhaustion Alert on page 1155
- Logging to FortiAnalyzer on page 1156
- Log fields for long-live sessions on page 1163

The log messages are a record of all of the traffic that passes through the FortiProxy device, and the actions taken by the device while scanning said traffic.

After a log message is recorded, it is stored in a log file. The log files can be stored on the FortiProxy device itself, on a connected FortiManager or FortiAnalyzer device, or on a FortiGate Cloud server (you must have a FortiCloud subscription before you can configure the FortiProxy device to send logs to a FortiGate Cloud server). The FortiProxy device's system memory or local disk can be configured to store logs.



The HTTP response code returned by the upstream content server has been added to the FortiProxy logs to aid in the debugging of content failures.

Each page of log messages contains the following controls.

Refresh	Select *Refresh* to refresh the log list.
Download Log	Select *Download Log* to download the raw log file to your local computer. The log file can be viewed in any text editor.
Add Filter	When you select the *Add Filter* button, a drop-down list appears with a list of available filtering options. Available options differ based on which log is currently being viewed.
Log Location	The location where the displayed logs are stored.
Details	Details about the selected log message. The information displayed varies depending on the type of log message selected.
Log list	The log messages.

	The available columns vary depending on the type of log being viewed. Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.
Page navigation	Navigate to different pages of the log list. The total number of log messages are also shown.

Debug logs

Customer Support might request a copy of your debug logs for troubleshooting.

To download the debug logs:

1. Go to *System* > *Settings*.
2. In the *Debug Log* section, click *Download*.

Logs for the execution of CLI commands

The `cli-audit-log` option records the execution of CLI commands in system event logs (log ID 44548). In addition to `execute` and `config` commands, `show`, `get`, and `diagnose` commands are recorded in the system event logs.

The `cli-audit-log` data can be recorded on memory or disk and can be uploaded to FortiAnalyzer or a syslog server.

To enable the CLI audit log option:

```
config system global
    set cli-audit-log enable
end
```

To display the logs:

```
# execute log filter device disk
# execute log filter category event
# execute log filter field subtype system
# execute log filter field logid 0100044548
# execute log display
```

Filter WAD log messages by process types or IDs

WAD log messages can be filtered by process types or IDs. Multiple process type filters can be configured, but only one process ID filter can be configured.

```
# diagnose wad filter process-type <integer>
# diagnose wad filter process-id <integer>
```

`diagnose wad filter process-type <integer>`	Select process type to filter by (0 - 17, 0 = disable): • 1 = manager • 2 = dispatcher • 3 = worker • 4 = algo • 5 = informer • 6 = user-info • 7 = cache-service-cs • 8 = cache-service-db • 9 = cert-inspection • 10 = YouTube-filter-cache-service • 11 = user-info-history • 12 = debug • 13 = config-notify • 14 = object-cache • 15 = byte-cache • 16 = traffic aggregator • 17 = preload daemon
`diagnose wad filter process-id <integer>`	Select process id to filter by (0 = disable).

To configure multiple filters:

```
# diagnose wad filter process-type 1
# diagnose wad filter process-type 3
# diagnose wad filter process-type 16
# diagnose wad filter process-id 1115
```

To view the configured filters:

```
# diagnose wad filter list
        drop unknown sessions: disabled
        process type:
                manager
                worker
```

```
               traffic aggregator
      process id: 1115
```

Types of logs

The *Log & Report* menu allows you to view traffic logs, event logs, and security logs:

Traffic logs		
	Forward Traffic	The forward traffic log includes log messages for traffic that passes through the FortiProxy device. It includes both traffic and security log messages so that messages about security events can be viewed alongside messages about the traffic at the time of the event. See also Logging client IP for forward traffic and HTTP transaction on page 144.
	HTTP Transaction	HTTP transaction-related traffic log. To allow HTTP transaction log to appear here, make sure the *Log HTTP Transaction* option is not disabled when you Create or edit a policy on page 387. See also Logging client IP for forward traffic and HTTP transaction on page 144.
	Correlation Log	Correlation log of forward traffic log(s) and HTTP transaction log (s) that have a common session ID.
	Sniffer Traffic	The sniffer log records all traffic that passes through a particular interface that has been configured to act as a One-Armed Sniffer, so it can be examined separately from the rest of the traffic logs.
	ZTNA Traffic	
System Event logs		
	System Events	General system events.
	Router Events	Events relating to layer-3 routing.
	VPN Events	Events relating to VPN.
	User Events	Events relating to users.
	HA Events	Events relating to HA
	Security Rating Events	Events relating to Security Rating.
	WAN Opt. & Cache Events	Events relating to WAN optimization and cache.

	SDN Connector Events	Events relating to Fabric connectors.
	CIFS Events	Events relating to CIFS.

	REST API Events	The REST API events log subtype logs POST, PUT, DELETE, and GET REST API requests. They can be enabled or disabled in the CLI:
		`config log setting`
		`set rest-api-set {enable | disable}`
		`set rest-api-get {enable | disable}`
		`end`

Security Event logs		
	AntiVirus	The antivirus log records when, during the antivirus scanning process, the FortiProxy unit finds a match within the antivirus profile, which includes the presence of a virus or grayware signature.
	Web Filter	The web filter log records HTTP log rating errors, including web content blocking actions that the FortiProxy device performs. It also includes how long it takes to scan the HTTP request, the client request host header, the client request host inside of the request line, and the server response code.
	SSL	Records detected and blocked malicious SSL connections.
	DNS Query	The DNS query log messages include details of each DNS query and response. DNS log messages are recorded for all DNS traffic though the FortiProxy unit and originated by the FortiProxy unit. The detailed DNS log can be used for low-impact security investigation. Most network activity involves DNS activity of some kinds. Analyzing the DNS log can provide a lot of details about the activity on your network without using resource-intensive techniques.
	File Filter	Records file filter events.
	Data Loss Prevention	The data loss prevention (DLP) log provides valuable information about the sensitive data trying to get through to your network as well as any unwanted data trying to get into your network. The DLP log can record the following traffic types: • email (SMTP, POP3, or IMAP; if SSL content, SMTPS, POP3S, and IMAPS) • HTTP • HTTPS • FTP • NNTP • IM

	Application Control	The Application Control log provides detailed information about the traffic that internet applications such as Skype are generating. The Application Control feature controls the flow of traffic from a specific application, and the FortiProxy unit examines this traffic for signatures that the application generates. The log messages that are recorded provide information such as the type of application being used (such as P2P software), and what type of action the FortiProxy unit took. These log messages can also help you to determine the top ten applications that are being used on your network. This feature is called Application Control monitoring and you can view the information from a widget on the Executive Summary page. The Application Control list that is used must have logging enabled within the list, as well as logging enabled within each application entry. Each application entry can also have packet logging enabled. Packet logging for Application Control records the packet when an application type is identified, similar to IPS packet logging. Logging of Application Control activity can only be recorded when an Application Control list is applied to a firewall policy, regardless of whether or not logging is enabled within the Application Control list.
	Intrusion Prevention	The Intrusion Prevention log, also referred to as the attack log, records attacks that occurred against your network. Attack logs contain detailed information about whether the FortiProxy unit protected the network using anomaly-based defense settings or signature-based defense settings, as well as what the attack was. The Intrusion Prevention or attack log file is especially useful because the log messages that are recorded contain a link to the FortiGuard Center, where you can find more information about the attack. This is similar to antivirus logs, where a link to the FortiGuard Center is provided as well that informs you of the virus that was detected by the FortiProxy unit. An Intrusion Prevention sensor with log settings enabled must be applied to a firewall policy so that the FortiProxy unit can record the activity.
	SSH	
Content Analyses		

System Events

The *Log & Report* > *System Events* page includes:

- A *Summary* tab that displays the top five most frequent events in each type of event log and a line chart to show aggregated events by each severity level. Clicking on a peak in the line chart will display the specific event count for the selected severity level. You can also filter the log viewer with specific time frames.
- A *Logs* tab that displays individual, detailed log views for event type. You can change the type of event log in the top-right, dropdown list. You can apply a custom time frame using the *Date/Time* filter. When the *Date/Time* filter is applied, the time frame will be disabled and set to *custom*. To select a new time frame, you must first remove the existing filter by clicking the *X* in the search bar or selecting *Remove* in the *Filter* dialog.

Clicking on an event in the *Summary* tab will automatically bring users to the *Logs* tab with the appropriate filters applied.

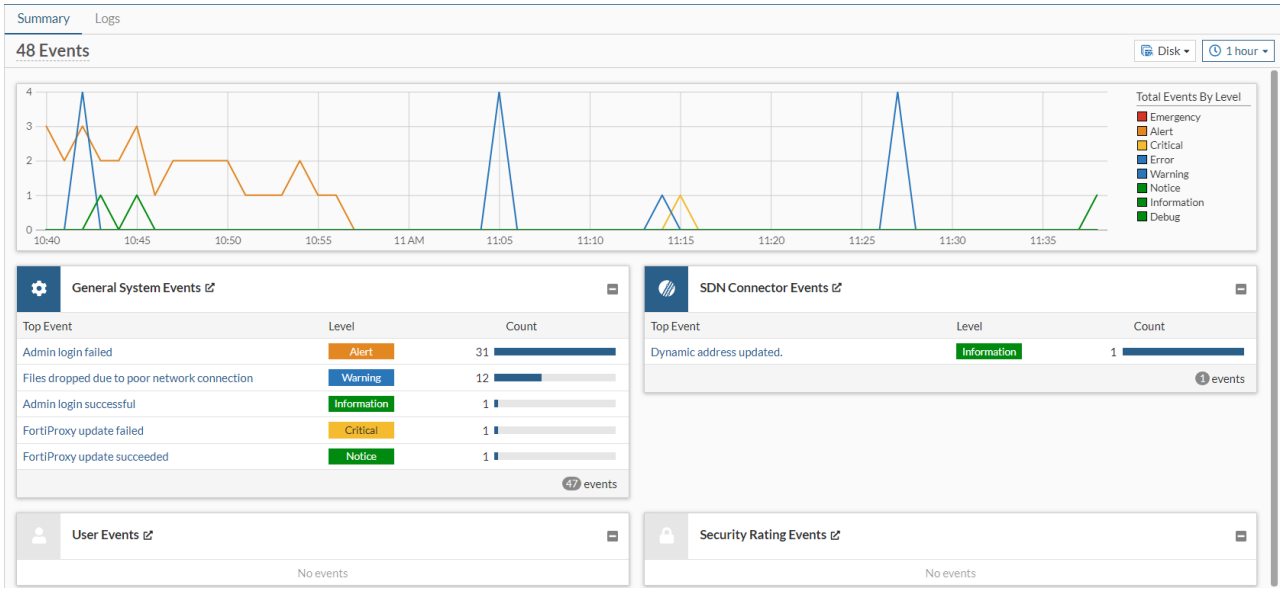
Disk logging and historical FortiView must be enabled for the *Summary* tab to display valid data.

To review system events in the GUI:

1. Go to *Log & Report* > *System Events*. The *Summary* tab opens.
2. On the right-side of the screen, select the time range from the dropdown list.

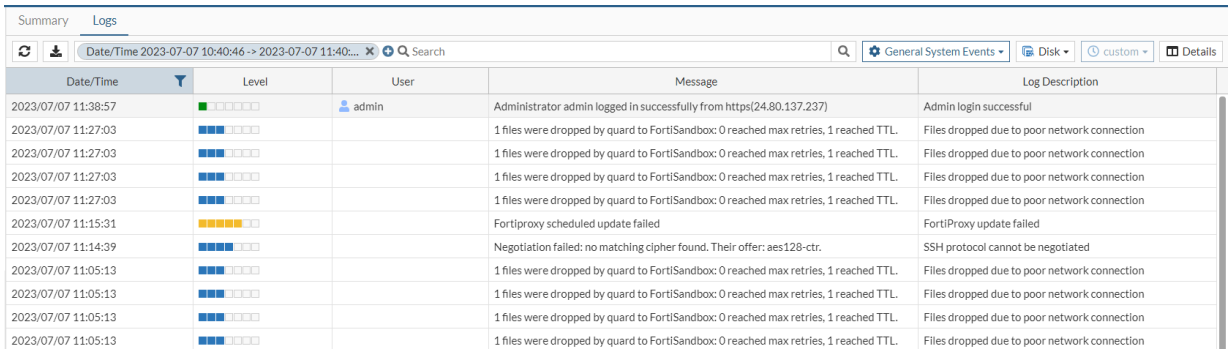
   The line chart will display all of the system events, and the non-empty event cards will list up to five *Top Event* entries within the time range set.

   Data is retrieved from FortiView with the *5 minutes* range updated first. When selecting either the *1 hour* or *24 hours* time range, there may be a delay to update *Top Event* entries.



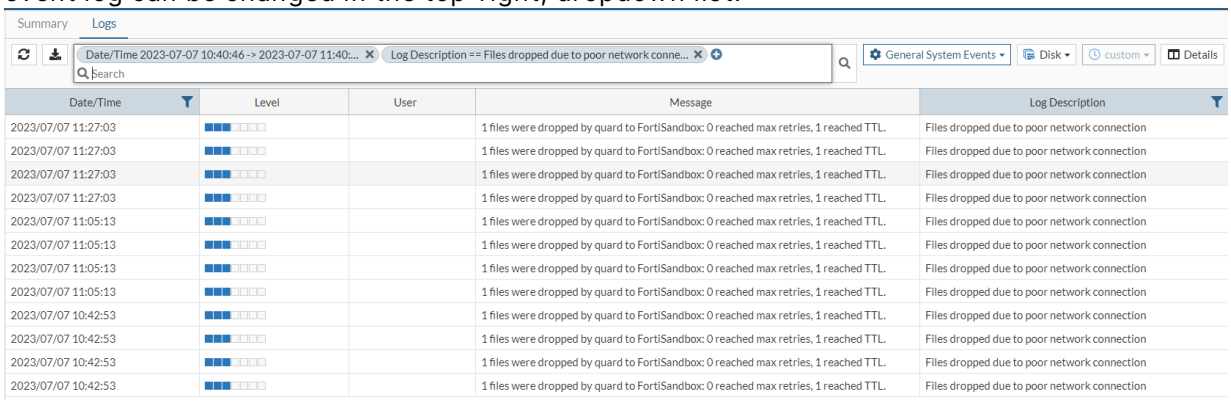
3. Review the details of system events:
   - Clicking on any event type title opens the *Logs* page for that event type filtered by the selected time span.

For example, on the *System Events > Summary* page, clicking *General System Events* opens the following page. The type of event log can be changed in the top-right, dropdown list.



- Clicking on any event entry opens the *Logs* page for that event type filtered by the selected time span and log description.

  For example, on the *System Events > Summary* page in the *General System Events* box, clicking *Files dropped due to poor network connection* opens the following page. The type of event log can be changed in the top-right, dropdown list.



  A custom time frame can be applied using the *Date/Time* filter. If the *Date/Time* filter is applied, the time frame will be disabled and set to *custom*. To select a new time frame, you must first remove the existing filter by clicking the *X* in the search bar or selecting *Remove* in the *Filter* dialog.

Up to 100 *Top Event* entries can be listed in the CLI using the `diagnose fortiview result event-log` command.

To list system events in the CLI:

```
# diagnose fortiview result event-log

    data(1646760000-1646846401):
    0). subtype-ha | eventname-HA device interface failed | level-warning | count-1 |
    1). subtype-system | eventname-DHCP statistics | level-information | count-40 |
    2). subtype-system | eventname-Super admin left VDOM | level-information | count-13 |
    3). subtype-system | eventname-Admin performed an action from GUI | level-warning | count-5 |
    4). subtype-system | eventname-Super admin entered VDOM | level-information | count-4 |
    5). subtype-system | eventname-Global setting changed | level-notice | count-3 |
    6). subtype-system | eventname-Attribute configured | level-information | count-2 |
    7). subtype-system | eventname-Clear active sessions | level-warning | count-2 |
```

```
    8). subtype-system | eventname-Disk log rolled | level-notice | count-2 |
    9). subtype-system | eventname-Log rotation requested by FortiCron | level-notice | count-1 |
    10). subtype-system | eventname-Report generated successfully | level-notice | count-1 |
    11). subtype-system | eventname-Test | level-warning | count-1 |
    12). subtype-system | eventname-VDOM added | level-notice | count-1 |
    13). subtype-user | eventname-Authentication failed | level-notice | count-1 |
    14). subtype-user | eventname-Authentication lockout | level-warning | count-1 |
    15). subtype-user | eventname-FortiGuard override failed | level-warning | count-1 |
```

The data is collected from FortiView for the last 24 hours by default. To specify a specific time range, customize the time filter using the `diagnose fortiview time` command.

To filter the time range of system events in the CLI:

```
# diagnose fortiview time <arg1> <arg2>
```

Where `<arg1>` is the start time in YYYY-MM-DD HH:MM:SS and `<arg2>` is the end time in YYYY-MM-DD HH:MM:SS.

Security Events

The *Log & Report > Security Events* log page includes:

- A *Summary* tab that displays the five most frequent events for all of the enabled UTM security events. Clicking on a peak in the line chart will display the specific event count for the selected severity level. You can also filter the log viewer with specific time frames.
- A *Logs* tab that displays individual, detailed logs for each UTM type. You can change the type of event log in the top-right, dropdown list. You can apply a custom time frame using the *Date/Time* filter. When the *Date/Time* filter is applied, the time frame will be disabled and set to *custom*. To select a new time frame, you must first remove the existing filter by clicking the *X* in the search bar or selecting *Remove* in the *Filter* dialog.

Clicking on an event in the *Summary* tab will bring users to the *Logs* tab with the appropriate filters automatically applied.



Disk logging and historical FortiView must be enabled for the *Summary* tab to display valid data.

To review security events in the GUI:

1. Go to *Log & Report > Security Events*.
   The *Summary* tab displays up to five top events for each enabled, non-empty security event cards.
2. On the right-side of the screen, select the time range from the dropdown list.
   The non-empty security event cards will list up to five top entries within the time range set.



Data is retrieved from FortiView with the *5 minutes* range updated first. When selecting either the *1 hour* or *24 hours* time range, there may be a delay to update top security event entries.

3. Review the details of security events:
   - Click the security event card name.

     The *Logs* tab displays all event entries for the selected type of security event. You can change the type of event log in the top-right, dropdown list.
   - Click a top event entry in a security event card.

     The *Logs* tab displays security events with filters for the selected event entry and time filter. The security event type can be changed in the top-right dropdown list. A custom time frame can be applied using the *Date/Time* filter. If the *Date/Time* filter is applied, the time frame will be disabled and set to *custom*. To select a new time frame, you must first remove the existing filter by clicking the *X* in the search bar or selecting *Remove* in the *Filter* dialog.

Up to 100 top security event entries can be listed in the CLI using the `diagnose fortiview result security-log` command.

To list security events in the CLI:

```
# diagnose fortiview result security-log [<filters>]
```

To list security events in the CLI with no filters applied:

```
# diagnose fortiview result security-log

    data(1646862300-1646948701):
    0). logcat-2 | logcatname-virus | logid-0211008192 | eventname-EICAR_TEST_FILE | eventname_
field-virus | action-blocked | count-1 |
    1). logcat-2 | logcatname-virus | logid-0211008192 | eventname-virus_test3 | eventname_field-
virus | action-passthrough | count-1 |
    2). logcat-2 | logcatname-virus | logid-0212008448 | eventname-filename | eventname_field-
virus | action-passthrough | count-1 |
    3). logcat-3 | logcatname-webfilter | logid-0318012800 | eventname- | eventname_field-catdesc
| action-blocked | count-2 |
    4). logcat-3 | logcatname-webfilter | logid-0316013056 | eventname-Information Technology |
eventname_field-catdesc | action-blocked | count-1 |
    5). logcat-3 | logcatname-webfilter | logid-0316013056 | eventname-Malicious Websites |
eventname_field-catdesc | action-blocked | count-1 |
    6). logcat-4 | logcatname-ips | logid-0419016384 | eventname-Eicar.Virus.Test.File |
eventname_field-attack | action-dropped | count-3 |
    7). logcat-4 | logcatname-ips | logid-0422016400 | eventname-test_botnet | eventname_field-
attack | action-detected | count-1 |
    8). logcat-7 | logcatname-anomaly | logid-0720018432 | eventname-tcp_syn_flood | eventname_
field-attack | action-clear_session | count-1 |
    9). logcat-10 | logcatname-app-ctrl | logid-1059028704 | eventname-Storage.Backup | eventname_
field-appcat | action-pass | count-9 |
    10). logcat-10 | logcatname-app-ctrl | logid-1059028704 | eventname-Video/Audio | eventname_
field-appcat | action-pass | count-3 |
```

```
    11). logcat-10 | logcatname-app-ctrl | logid-1059028672 | eventname-im | eventname_field-
appcat | action-pass | count-1 |
    12). logcat-10 | logcatname-app-ctrl | logid-1059028704 | eventname-P2P | eventname_field-
appcat | action-pass | count-1 |
    13). logcat-15 | logcatname-dns | logid-1501054400 | eventname-Domain blocked because it is in
the domain-filter list | eventname_field-logid | action-block | count-1 |
    14). logcat-17 | logcatname-ssl | logid-1700062300 | eventname-SSL connection is blocked due
to the server certificate is blocklisted | eventname_field-logid | action-blocked | count-1 |
    15). logcat-16 | logcatname-ssh | logid-1600061002 | eventname-SSH shell command is detected |
eventname_field-logid | action-passthrough | count-1 |
    16). logcat-16 | logcatname-ssh | logid-1601061010 | eventname-SSH channel is blocked |
eventname_field-logid | action-blocked | count-1 |
    17). logcat-12 | logcatname-waf | logid-1200030248 | eventname-Web application firewall
blocked application by signature | eventname_field-logid | action-blocked | count-1 |
    18). logcat-8 | logcatname-voip | logid-0814044032 | eventname-Logid_44032 | eventname_field-
logid | action-permit | count-1 |
    19). logcat-5 | logcatname-emailfilter | logid-0513020480 | eventname-SPAM notification |
eventname_field-logid | action-blocked | count-1 |
```

To list blocked security events in the CLI:

```
# diagnose fortiview result security-log action=blocked

    data(1646862600-1646949001):
    0). logcat-2 | logcatname-virus | logid-0211008192 | eventname-EICAR_TEST_FILE | eventname_
field-virus | action-blocked | count-1 |
    1). logcat-3 | logcatname-webfilter | logid-0318012800 | eventname- | eventname_field-catdesc
| action-blocked | count-2 |
    2). logcat-3 | logcatname-webfilter | logid-0316013056 | eventname-Information Technology |
eventname_field-catdesc | action-blocked | count-1 |
    3). logcat-3 | logcatname-webfilter | logid-0316013056 | eventname-Malicious Websites |
eventname_field-catdesc | action-blocked | count-1 |
    4). logcat-17 | logcatname-ssl | logid-1700062300 | eventname-SSL connection is blocked due to
the server certificate is blocklisted | eventname_field-logid | action-blocked | count-1 |
    5). logcat-16 | logcatname-ssh | logid-1601061010 | eventname-SSH channel is blocked |
eventname_field-logid | action-blocked | count-1 |
    6). logcat-12 | logcatname-waf | logid-1200030248 | eventname-Web application firewall blocked
application by signature | eventname_field-logid | action-blocked | count-1 |
    7). logcat-5 | logcatname-emailfilter | logid-0513020480 | eventname-SPAM notification |
eventname_field-logid | action-blocked | count-1 |
```

Reports

The *Log & Report* > *Reports* page consolidates FortiAnalyzer and local log reports. Administrators can generate, delete, and edit report schedules, and view and download generated reports. The *Reports* page is organized into dedicated tabs:

- FortiAnalyzer reports on page 1146
- Local reports on page 1146

FortiAnalyzer reports

FortiAnalyzer reports can be viewed in the GUI on the *Log & Report > Reports > FortiAnalyzer* page. Administrators can generate, delete, and edit report schedules, and view and download generated reports. The *Generated* report data is displayed by default. You can review scheduled report data by selecting *Scheduled*.



FortiAnalyzer must be configured in FortiProxy. If the FortiProxy is unauthorized on FortiAnalyzer, or the connection to FortiAnalyzer is down, the *FortiAnalyzer Reports* page loads with *No results*.

When the Security Fabric is enabled, only the root FortiProxy can run, edit, and delete FortiAnalyzer reports. Downstream FortiProxies can only view the generated reports.

To edit a report schedule:

1. Go to *Log & Report > Reports > FortiAnalyzer* and select the *Scheduled* tab.
2. Select a report and click *Edit Schedule*. The *Edit Schedule* pane opens. In this example, the schedule for the Bandwidth and Applications report is changed to run from every week to every two weeks.
3. In the *Schedule* section, set the values for *Generate report every* to *2 week(s)*.
4. Click *OK*.
   The schedule is also updated automatically in FortiAnalyzer for the same report (go to *Reports > Report Definitions > All Reports* and edit the report to view the settings).

To view and download reports:

1. Go to *Log & Report > Reports > FortiAnalyzer* and select the *Generated* tab.
   A pie chart displays the total count of FortiAnalyzer reports, categorized by report title. Generated reports are listed below and arranged by title, which includes reports from all VDOMs.
2. In the pie chart, click a segment to filter the category of reports.
3. In the filtered results, select a report, right-click it, and select *Download*.
4. Select a file format. The report is saved to the default download location.

Local reports

Local reports provide a clear, concise overview of what is happening on your network based on log data and can be customized to serve different purposes. Local reports are created from logs stored on the FortiProxy unit's hard drive. These reports, generated by the FortiProxy unit itself, provide a central overview of traffic and security features on the FortiProxy unit. The default report compiles security feature activity from various security-related logs, such as virus and attack logs.

On the *Log & Report > Reports > Local* page, you can generate, schedule, view, and download local reports. You can also set the frequency and timing of auto-generated reports.



To create local reports, you need to enable disk logging and local reports in *Log settings on page 1147*.

To generate a local report:

1. Go to *Log & Report > Reports* and select the *Local* tab.
2. Select *Generate Now*. The *Confirm* pane opens.
3. Click *OK*.

Local reports are marked as *On-Demand-default* if created by selecting *Generate Now*.

To view a local report:

1. Go to *Log & Report > Reports* and select the *Local* tab.
2. Select the report.
3. Click *View*. The report is displayed.

To download a report:

1. Go to *Log & Report > Reports* and select the *Local* tab.
2. Select the report.
3. Click *Download*. The report is saved to the default download location.

To schedule local reports:

1. Go to *Log & Report > Reports* and select the *Local* tab.
2. Click *Report Schedule*. The *Report Schedule* pane opens.
3. Set the schedule details.
4. Click *OK*.

Local reports are marked as *Schedule-default* if created automatically.

Log settings

Log settings determine what information is recorded in logs, where the logs are stored, and how often storage occurs. Log settings can be configured in the GUI and CLI. In the GUI, *Log & Report > Log Settings* provides the settings for local and remote logging.

Log & Report > Log Settings is organized into tabs:

- Global Settings on page 1148
- Local Logs on page 1148

- Threat Weight on page 1149

Global Settings

Settings available in the *Global Settings* tab include:

UUIDs in Traffic Log		
	Policy	Define the use of policy UUIDs in traffic logs: • *Enable*: Policy UUIDs are stored in traffic logs. UUIDs can be matched for each source and destination that match a policy in the traffic log. • *Disable*: Policy UUIDs are excluded from the traffic logs.
	Address	Define the use of address UUIDs in traffic logs: • *Enable*: Address UUIDs are stored in traffic logs. When viewing *Forward Traffic* logs, a filter is automatically set based on UUID. • *Disable*: Address UUIDs are excluded from traffic logs.
Log Settings		
	Event Logging	Define the allowed set of event logs to be recorded: • *All*: All event logs will be recorded. • *Customize*: Select specific event log types to be recorded. Deselect all options to disable event logging.
	Local Traffic Log	Define the allowed set of traffic logs to be recorded: • *All*: All traffic logs to and from the FortiProxy will be recorded. • *Customize*: Select specific traffic logs to be recorded. Deselect all options to disable traffic logging. Local traffic logging is disabled by default due to the high volume of logs generated.
GUI Preferences		
	Resolve Hostnames	Define the translation of IP addresses to host names: • *Enable*: IP addresses are translated to host names using reverse DNS lookup. If the DNS server is not available or is slow to reply, requests may time out. • *Disable*: IP addresses are not translated to host names.
	Resolve Unknown Applications	Define the resolution of unknown applications: • *Enable*: Unknown applications are resolved using the Internet Service Database. • *Disable*: Unknown applications are not resolved.

Local Logs

Settings available in the *Local Logs* tab include:

Local Logs		
	Disk logging	Define local log storage on the FortiProxy: • *Enable*: Logs will be stored on a local disk. • *Disable*: Logs will be stored remotely to FortiAnalyzer/FortiManager or to a Cloud logging device.
	Local Reports	Define log reporting on the FortiProxy: • *Enable*: Local reports will be available on the FortiProxy. Reports can be reviewed in *Log & Report > Reports* in the *Local* tab. • *Disable*: Local reports will not be available on the FortiProxy.
	Historical FortiView	Define the presentation of log information on FortiView: • *Enable*: Historical log data will be available on a FortiView monitor. By default, logs older than seven days are deleted. Disk logging must be enabled. • *Disable*: Historical log data will not be available on FortiView.
	Disk Usage	Presents the disk space used and the total disk space available on the disk.

Threat Weight

Threat weight helps aggregate and score threats based on user-defined severity levels. It adds several fields such as threat level (`crlevel`), threat score (`crscore`), and threat type (`craction`) to traffic logs. Threat weight logging is enabled by default and the settings can be customized. Threats can be viewed from the *Top Threats* FortiView dashboard.

To configure threat weight settings:

1. Go to *Log & Report > Log Settings* and select the *Threat Weight* tab.
2. Adjust the settings as needed, such as individual weights per threat type and risk level values.
3. Click *Apply*.

To add the Top Threats monitor to the dashboard:

1. In the tree menu, click *Dashboard* and in the FortiView section, click the *+* sign (*Add Monitor*).
2. In the *Security* section, enable *Show More* and click *Top Threats*.
3. Configure the settings as needed.
4. Click *Add Monitor*.
5. Go to *Dashboard > Top Threats*. The *Top Threats* monitor displays threats based on the scores in the traffic logs.
6. Double-click a threat to view the summary.
7. Click *Sources*, *Destinations*, *Countries/Regions*, or *Sessions* to view more information. Double-click an entry to view the log details.

Configuring logs in the CLI

The FortiProxy can store logs locally to its system memory or a local disk. Logs can also be stored externally on a storage device, such as FortiAnalyzer, FortiAnalyzer Cloud, FortiGate Cloud, or a syslog server.

Disk logging

Disk logging must be enabled for logs to be stored locally on the FortiProxy. By default, logs older than seven days are deleted from the disk. Log age can be configured in the CLI. Approximately 75% of disk space is available for log storage. Log storage space can be determined using the `diagnose sys logdisk usage` command.

To configure local disk logging:

```
config log disk setting
    set status enable
    set maximum-log-age <integer>
    set max-log-file-size <integer>
end
```

Remote logging

The process to configure FortiProxy to send logs to FortiAnalyzer or FortiManager is identical. Remote logging to FortiAnalyzer and FortiManager can be configured using both the GUI and CLI. When using the CLI, use the `config log fortianalyzer setting` command for both FortiAnalyzer and FortiManager.

If VDOMs are configured on the FortiProxy, multiple FortiAnalyzers and syslog servers can be added globally. See Configuring multiple FortiAnalyzers (or syslog servers) per VDOM on page 1158 and Configuring multiple FortiAnalyzers on a FortiProxy in multi-VDOM mode on page 1160 for more information.

To configure remote logging to FortiAnalyzer:

```
config log fortianalyzer setting
    set status enable
    set server <server_IP>
    set upload option {store-and-upload | realtime | 1-minute | 5-minute}
end
```

Remote logging can also be configured to FortiGate Cloud, FortiSIEM, and syslog servers. Up to four syslog servers or FortiSIEM devices can be configured using the `config log syslogd` command and can send logs to syslog in CSV and CEF formats.

To configure remote logging to FortiGate Cloud:

```
config log fortiguard setting
    set status enable
    set source-ip <source IP used to connect FortiGate Cloud>
end
```

To configure remote logging to a syslog server:

```
config log syslogd setting
    set status enable
    set server <syslog_IP>
    set format {default | cev | cef}
end
```

Log filters

Log filter settings can be configured to determine which logs are recorded to the FortiAnalyzer, FortiManager, and syslog servers. This allows certain logging levels and types of logs to be directed to specific log devices.

To configure log filters for FortiAnalyzer:

```
config log fortianalyzer filter
    set severity <level>
    set forward-traffic {enable | disable}
    set local-traffic {enable | disable}
    set multicast-traffic {enable | disable}
    set sniffer-traffic {enable | disable}
end
```

To configure log filters for a syslog server:

```
config log syslogd filter
    set severity <level>
    set forward-traffic {enable | disable}
    set local-traffic {enable | disable}
    set multicast-traffic {enable | disable}
    set sniffer-traffic {enable | disable}
end
```

Email alerts

FortiProxy events can be monitored at all times using email alerts. Email alerts send notifications to up to three recipients and can be triggered based on log event and severity level. Email alerts will be sent every five minutes by default but this can be configured in the CLI.

To configure email alerts:

```
config alertemail setting
    set username <name>
    set mailto1 <email>
    set filter-mode {category | threshold}
    set email-interval <integer>
    set IPS-logs {enable | disable}
    set HA-logs {enable | disable}
    set antivirus-logs {enable | disable}
    set webfilter-logs {enable | disable}
    set log-disk-usage-warning {enable | disable}
end
```

Email Alert Settings

Alert email messages provide notification about activities or events logged, including the log severity level, such as a critical or emergency. You can send alert email messages to up to three email addresses. Alert messages are also logged and can be viewed from the System Events log file.

You can use the alert email feature to monitor logs for log messages, and to send email notification about a specific activity or event logged. For example, if you require notification about administrators logging in and out, you can configure an alert email that is sent whenever an administrator logs in and out. You can also base alert email messages on the severity levels of the logs.

To configure email notifications:

1. Configure email service:
   a. Go to *System* > *Setting*.
   b. Under *Email Service*, configure the SMTP server so that FortiProxy knows exactly where the email will be sent from and who to send it to.
      - If you have an active FortiCare support contract, the default SMTP server (*fortinet-notifications.com*) is automatically selected and used.
      - If you do not have an active FortiCare support contract or if your environments has specific email routing requirements, enable *Use Custom Email Server* and configure a custom SMTP server.

      FortiProxy does not currently support SSL/TLS connections for SMTP servers. If the configured SMTP server requires SSL/TLS connections, the alert email configuration will not work.

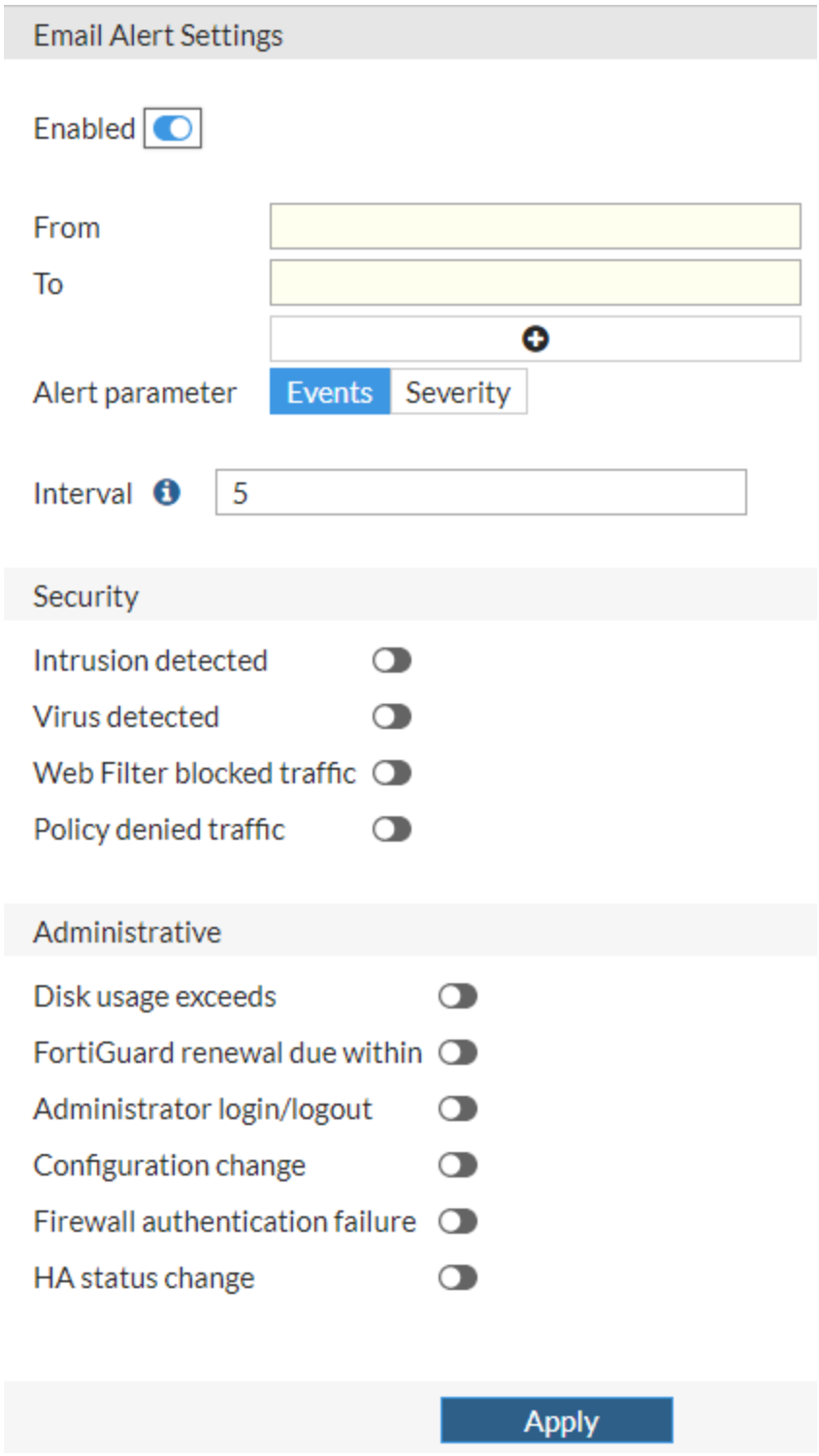
2. Configure at least one DNS server if you are configuring with an Fully Qualified Domain Server (FQDN). The FortiProxy unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server. You can also specify an IP address.
3. Configure alert email for IPsec tunnel errors, firewall authentication failure, configuration changes and FortiGuard license expiry:

a. In *Log & Report* > *Email Alert Settings*, toggle *Enabled*.

b. Configure the email alert settings as described in the table.

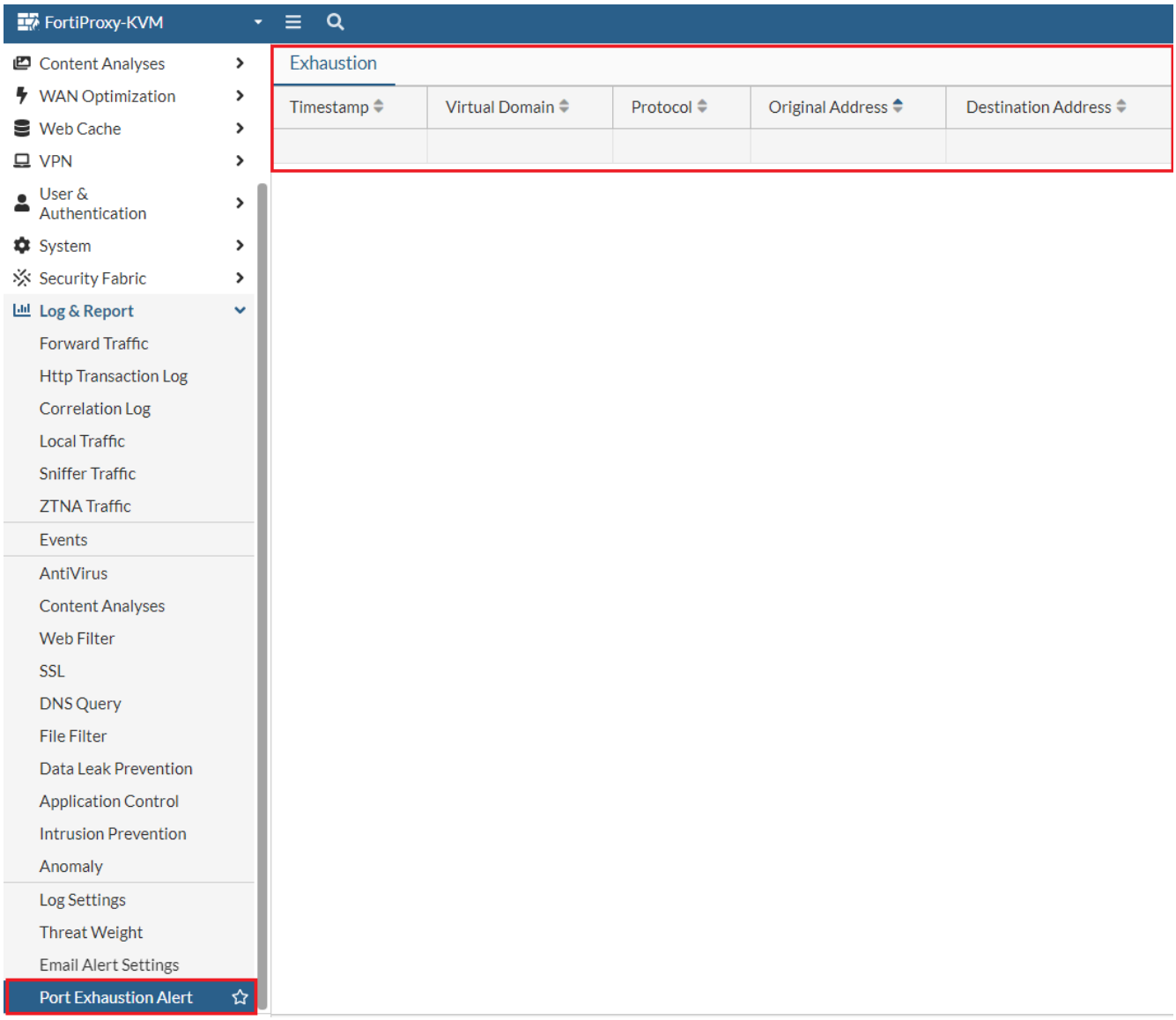
From	Enter the source email address.
To	Enter up to three target email addresses.
Alert parameter	If you select *Events*, enter the number of minutes in *Interval* and enable the events that will cause email alerts to be sent. If you select *Severity*, select the event priority level for email alerts to be sent in the *Minimum level* drop-down list. The priority level indicates the immediacy and the possible repercussions of the event. There are eight priority levels from *Debug* (lowest priority) to *Emergency* (highest priority). The default priority level is *Alert*.
Interval	Select the number of minutes between email alerts, from 1 to 99,999 minutes. The default is 5 minutes. If the FortiProxy unit collects more than one log message before an interval is reached, the FortiProxy unit combines the messages and sends out one alert email.
Intrusion detected	Enable to send an email alert when an intrusion is detected.
Virus detected	Enable to send an email alert when a virus is detected.
Web Filter blocked traffic	Enable to send an email alert when a web filter blocked traffic.
Policy denied traffic	Enable to send an email alert when a policy denied traffic.
Disk usage exceeds	Enable and enter a percentage to send an email alert when the disk usage exceeds the specified level. The default is 75%.
FortiGuard renewal due within	Enable and enter the number of days to send an email alert before FortiGuard must be renewed.
Administrator login/logout	Enable to send an email alert when an administrator logs in or out of the FortiProxy unit.
Configuration change	Enable to send an email alert when the FortiProxy configuration has been changed.
Firewall authentication failure	Enable to send an email when traffic fails authentication.
HA status change	Enable to send an email when there is a change in the HA status.

c. Click *Apply* to save your changes.



Port Exhaustion Alert

The *Port Exhaustion Alert* tab displays port exhaustion events with timestamp, virtual domain, protocol, and address information of the exhaustion. When a port exhaustion occurs, an alert appears next to *Log & Report* and *Port Exhaustion Alert* until the event expires.



You can also use the following logs to learn about source port usage:

- High source port usage—This log is recorded when more than half of the available source ports on an IP is in use during the last few consecutive attempts of the FortiProxy to get a source port.
- Source port exhaustion—This log is recorded when no available source port can be found for a source IP.

Logging to FortiAnalyzer

The following topics provide instructions on logging to FortiAnalyzer:

- FortiAnalyzer log caching on page 1156
- Configuring multiple FortiAnalyzers (or syslog servers) per VDOM on page 1158
- Configuring multiple FortiAnalyzers on a FortiProxy in multi-VDOM mode on page 1160

FortiAnalyzer log caching

Reliable logging to FortiAnalyzer prevents lost logs when the connection between FortiProxy and FortiAnalyzer is disrupted. When reliable mode is enabled:

1. Logs are cached in a FortiProxy memory queue.
2. FortiProxy sends logs to FortiAnalyzer, and FortiAnalyzer uses `seq_no` to track received logs.
3. After FortiProxy sends logs to FortiAnalyzer, logs are moved to a confirm queue in FortiProxy.
4. FortiProxy periodically queries FortiAnalyzer for the latest `seq_no` of the last log received, and clears logs from the confirm queue up to the `seq_no`.
5. If the connection between FortiProxy and FortiAnalyzer is disrupted, FortiProxy resends the logs in the confirm queue to FortiAnalyzer when the connection is reestablished.



FortiAnalyzer 7.2.0 and later is required.

To enable reliable mode:

```
config log fortianalyzer setting
    set reliable enable
end
```

To view the memory and confirm queues:

1. Verify that log synchronization is enabled for FortiAnalyzer:

```
# diagnose test application fgtlogd 1
vdom-admin=0
mgmt=root

fortilog:
faz: global , enabled
    server=172.16.200.251, realtime=1, ssl=1, state=connected
    server_log_status=Log is allowed.,
    src=, mgmt_name=FGh_Log_root_172.16.200.251, reliable=1, sni_prefix_type=none,
    required_entitlement=none, region=ca-west-1,,
```

```
    logsync_enabled:1, logsync_conn_id:65535, seq_no:790
...
```

2. When a network disruption disconnects FortiProxy from FortiAnalyzer and FortiProxy continues to generate logs, the logs are cached in the memory queue.
   - View the number of logs in the cache and queue:

```
# diagnose test application fgtlogd 41

cache maximum: 189516595(180MB) objects: 40 used: 27051(0MB) allocated: 29568(0MB)

VDOM:root
Memory queue for: global-faz
    queue:
        num:9 size:6976(0MB) total size:26068(0MB) max:189516595(180MB) logs:28
Confirm queue for: global-faz
    queue:
        num:29 size:19092(0MB) total size:27051(0MB) max:189516595(180MB) logs:7
```

```
# diagnose test application fgtlogd 30
VDOM:root
Memory queue for: global-faz
        queue:
                num:9 size:6976(0MB) total size:26068(0MB) max:189516595(180MB)
                        type:3, cat=1, log_count=1, seq_no=0, data len=359 size:435
                        type:3, cat=1, log_count=1, seq_no=0, data len=307 size:383
                        ......
                        type:3, cat=0, log_count=4, seq_no=0, data len=1347 size:1423
                        type:3, cat=4, log_count=1, seq_no=0, data len=653 size:729
                'total log count':28,  'total data len':6292

Confirm queue for: global-faz
        queue:
                num:29 size:19092(0MB) total size:26068(0MB) max:189516595(180MB)
                        type:3, cat=1, log_count=1, seq_no=1, data len=290 size:366
                        type:3, cat=1, log_count=1, seq_no=2, data len=233 size:309
                        ......
                        type:3, cat=0, log_count=1, seq_no=28, data len=524 size:600
                        type:3, cat=1, log_count=1, seq_no=29, data len=307 size:383
                'total log count':76,  'total data len':16888
```

   There are nine OFTP items cached to the memory queue, and 29 OFTP items to send from FortiOS to FortiAnalyzer that are waiting for confirmation from FortiAnalyzer.
   - Go to *Log & Report > Log Settings* to view the queue in the GUI:
3. Re-establish the connection between FortiProxy and FortiAnalyzer and confirm that the queue has cleared by checking the `seq_no`, which indicates the latest confirmation log from FortiAnalyzer:

```
# diagnose test application fgtlogd 30
VDOM:root
Memory queue for: global-faz
    queue:
```

```
        num:0 size:0(0MB) total size:0(0MB) max:189516595(180MB)
        'total log count':0,  'total data len':0

Confirm queue for: global-faz
    queue:
        num:0 size:0(0MB) total size:0(0MB) max:189516595(180MB)
        'total log count':0,  'total data len':0
```

The queue has been cleared, meaning that FortiProxy received confirmation from FortiAnalyzer and cleared the confirm queue.

```
# diagnose test application fgtlogd 1
vdom-admin=0
mgmt=root

fortilog:
faz: global , enabled
        server=172.16.200.251, realtime=1, ssl=1, state=connected
        server_log_status=Log is allowed.,
        src=, mgmt_name=FGh_Log_root_172.16.200.251, reliable=1, sni_prefix_type=none,
        required_entitlement=none, region=ca-west-1,
        logsync_enabled:1, logsync_conn_id:65535, seq_no:67
            status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_verified=Y
            SNs: last sn update:38 seconds ago.
                Sn list:
               (FAZ-VMTM21000000,age=38s)
            queue: qlen=0.
```

OFTP items with a seq_no lower than 67 have been sent to FortiAnalyzer and were confirmed.

Configuring multiple FortiAnalyzers (or syslog servers) per VDOM

In a VDOM, multiple FortiAnalyzer and syslog servers can be configured as follows:

- Up to three override FortiAnalyzer servers
- Up to four override syslog servers

If the VDOM faz-override and/or syslog-override setting is enabled or disabled (default) before upgrading, the setting remains the same after upgrading.

If the override setting is disabled, the GUI displays the global FortiAnalyzer1 or syslog1 setting. If the override setting is enabled, the GUI displays the VDOM override FortiAnalyzer1 or syslog1 setting.

You can only use CLI to enable the override to support multiple log servers.

To enable FortiAnalyzer and syslog server override under VDOM:

```
config log setting
    set faz-override enable
```

```
    set syslog-override enable
end
```

When `faz-override` and/or `syslog-override` is enabled, the following CLI commands are available for configuring VDOM override:

To configure VDOM override for FortiAnalyzer:

1. Configure the FortiAnalyzer override settings:

```
config log fortianalyzer/fortianalyzer2/fortianalyzer3 override-setting
    set status enable
    set server "123.12.123.123"
    set reliable enable
end
```

2. Configure the override filters:

```
config log fortianalyzer/fortianalyzer2/fortianalyzer3 override-filter
    set severity information
    set forward-traffic enable
    set local-traffic enable
    set multicast-traffic enable
    set sniffer-traffic enable
    set anomaly enable
    set voip enable
    set dlp-archive enable
    set dns enable
    set ssh enable
    set ssl enable
end
```

To configure VDOM override for a syslog server:

1. Configure the syslog override settings:

```
config log syslogd/syslogd2/syslogd3/syslogd4 override-setting
    set status enable
    set server "123.12.123.12"
    set facility local1
end
```

2. Configure the override filters:

```
config log syslogd/syslogd2/syslogd3/syslogd4 override-filter
    set severity information
    set forward-traffic enable
    set local-traffic enable
    set multicast-traffic enable
    set sniffer-traffic enable
    set anomaly enable
    set voip enable
```

```
    set dns enable
    set ssh enable
    set ssl enable
end
```

Configuring multiple FortiAnalyzers on a FortiProxy in multi-VDOM mode

This topic shows a sample configuration of multiple FortiAnalyzers on a FortiProxy in multi-VDOM mode.

In this example:

- The FortiProxy has three VDOMs:
  - Root (management VDOM)
  - VDOM1
  - VDOM2
- There are four FortiAnalyzers.
  These IP addresses are used as examples in the instructions below.
  - FAZ1: `172.16.200.55`
  - FAZ2: `172.18.60.25`
  - FAZ3: `192.168.1.253`
  - FAZ4: `192.168.1.254`
- Set up FAZ1 and FAZ2 under global.
  - These two collect logs from the root VDOM and VDOM2.
  - FAZ1 and FAZ2 must be accessible from management VDOM root.
- Set up FAZ3 and FAZ4 under VDOM1.
  - These two collect logs from VDOM1.
  - FAZ3 and FAZ4 must be accessible from VDOM1.

To set up FAZ1 as global FortiAnalyzer 1 from the GUI:

Prerequisite: FAZ1 must be reachable from the management root VDOM.

1. Go to *Global > Log & Report > Log Settings*.
2. Enable *Send logs to FortiAnalyzer/FortiManager*.
3. Enter the FortiAnalyzer IP.
   In this example: `172.16.200.55`.
4. For *Upload option*, select *Real Time*.
5. Click *Apply*.

To set up FAZ2 as global FortiAnalyzer 2 from the CLI:

Prerequisite: FAZ2 must be reachable from the management root VDOM.

```
config log fortianalyzer2 setting
    set status enable
    set server "172.18.60.25"
    set upload-option realtime
end
```

To set up FAZ3 and FAZ4 as VDOM1 FortiAnalyzer 1 and FortiAnalyzer 2:

Prerequisite: FAZ3 and FAZ4 must be reachable from VDOM1.

```
config log setting
   set faz-override enable
end

config log fortianalyzer override-setting
   set status enable
   set server "192.168.1.253"
   set upload-option realtime
end

config log fortianalyzer2 override-setting
   set status enable
   set server "192.168.1.254"
   set upload-option realtime
end
```

Checking FortiAnalyzer connectivity

To use the diagnose command to check FortiAnalyzer connectivity:

1. Check the global FortiAnalyzer status:

```
FGTA(global) # diagnose test application fgtlogd 1
vdom-admin=1
mgmt=root
faz: global , enabled
        server=172.16.200.55, realtime=1, ssl=1, state=connected
        server_log_status=Log is allowed.,
        src=, mgmt_name=FGh_Log_root_172.16.200.55, reliable=0, sni_prefix_type=none,
        required_entitlement=none, region=ca-west-1,
        logsync_enabled:1, logsync_conn_id:65535, seq_no:0
                status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_verified=Y
                SNs: last sn update:383 seconds ago.
                        Sn list:
                        (FAZ-VMTM2200****,age=383s)
                queue: qlen=0.
filter: severity=6, sz_exclude_list=0
         traffic virus webfilter ips emailfilter anomaly voip dlp app-ctrl waf dns ssh ssl
file-filter icap sctp-filter
subcategory:
```

```
        traffic: forward local multicast sniffer ztna
        anomaly:all subcategories are enabled.
        server: global, id=0, ready=1, name=172.16.200.55 addr=172.16.200.55:514
        oftp-state=connected
faz2: global , enabled
        server=172.18.60.25, realtime=3, ssl=1, state=connected
        server_log_status=Log is allowed.,
        src=, mgmt_name=FGh_Log_root_172.18.60.25, reliable=0, sni_prefix_type=none,
        required_entitlement=none, region=ca-west-1,
        logsync_enabled:1, logsync_conn_id:131071, seq_no:0
                status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_verified=Y
                SNs: last sn update:383 seconds ago.
                        Sn list:
                        (FAZ-VMTM2201****,age=383s)
                queue: qlen=0.
filter: severity=6, sz_exclude_list=0
         traffic virus webfilter ips emailfilter anomaly voip dlp app-ctrl waf dns ssh ssl
file-filter icap sctp-filter
subcategory:
        traffic: forward local multicast sniffer ztna
        anomaly:all subcategories are enabled.
        server: global, id=1, ready=1, name=172.18.60.25 addr=172.18.60.25:514
        oftp-state=connected
```

2. Check the VDOM1 override FortiAnalyzer status:

```
FGTA(global) # diagnose test application fgtlogd 3101
vdom VDOM1: id=3
event filter:
         event
system vpn user router wireless wanopt endpoint ha security-rating fortiextender connector
sdwan cifs-auth-fail switch-controller rest-api webproxy
faz: vdom, enabled, override
        server=192.168.1.253, realtime=3, ssl=1, state=connected
        server_log_status=Log is allowed.,
        src=, mgmt_name=FGh_Log_VDOM1_192.168.1.253, reliable=0, sni_prefix_type=none,
        required_entitlement=none, region=ca-west-1,
        logsync_enabled:1, logsync_conn_id:3, seq_no:0
                status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_verified=Y
                SNs: last sn update:16 seconds ago.
                        Sn list:
                        (FAZ-VMTM2200****,age=16s)
                queue: qlen=0.
filter: severity=6, sz_exclude_list=0
         traffic virus webfilter ips emailfilter anomaly voip dlp app-ctrl waf dns ssh ssl
file-filter icap sctp-filter
subcategory:
        traffic: forward local multicast sniffer ztna
        anomaly:all subcategories are enabled.
        server: vdom, id=0, ready=1, name=192.168.1.253 addr=192.168.1.253:514
        oftp-state=connected
faz2: vdom, enabled, override
```

```
        server=192.168.1.254, realtime=3, ssl=1, state=connected
        server_log_status=Log is allowed.,
        src=, mgmt_name=FGh_Log_VDOM1_192.168.1.254, reliable=0, sni_prefix_type=none,
        required_entitlement=none, region=ca-west-1,
        logsync_enabled:1, logsync_conn_id:65539, seq_no:0
                status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_verified=Y
                SNs: last sn update:16 seconds ago.
                        Sn list:
                        (FAZ-VMTM2201****,age=16s)
                queue: qlen=0.
filter: severity=6, sz_exclude_list=0
         traffic virus webfilter ips emailfilter anomaly voip dlp app-ctrl waf dns ssh ssl
file-filter icap sctp-filter
subcategory:
        traffic: forward local multicast sniffer ztna
        anomaly:all subcategories are enabled.

        server: vdom, id=1, ready=1, name=192.168.1.254 addr=192.168.1.254:514
        oftp-state=connected
faz3: vdom, disabled, override
```

Log fields for long-live sessions

Logging of long-live session statistics can be enabled or disabled in traffic logs.

```
config log setting
     set long-live-session-stat {enable | disable}
end
```

When enabled, traffic logs include the following fields of statistics for long-live sessions:

Duration delta (durationdelta)	Displays the time in seconds between the last session log and the current session log.
Sent packet delta (sentpktdelta)	Displays the number of sent packets. When the number of packets reported in the sentpktdelta field matches the number of bytes reported in the sentpkt field, it shows no missing logs.
Received packet delta (rcvdpktdelta)	Displays the number of received packets. When the number of packets reported in the rcvdpktdelta field matches the number of bytes reported in the rcvdpkt field, it shows no missing logs.

The long-live session fields enhance the granularity and accuracy of traffic longs to aid troubleshooting and analysis.

Example

In this example, logging is enabled for long-live session statistics. Log ID 20 includes the new fields for long-live sessions.

To log long-live session statistics:

1. Enable logging of long-live session statistics:

```
config log setting
     set long-live-session-stat enable
end
```

2. View information in the logs:

   In the following example, log fields are filtered for log ID 0000000020 to displays the new fields of data.

   The `sentpkt` field displays `205` bytes, and the `rcvdpkt` field displays `1130` bytes. The new fields (`sentpktdelta=205` and `rcvdpktdelta=1130`) display the same number of packets, which shows no logs have been lost. The `durationdelta` shows `120` seconds between the last session log and the current session log.

```
# execute log filter device Disk

# execute log filter category 0

# execute log filter field subtype forward

# execute log filter field logid 0000000020

# execute log display

1 logs found.

1 logs returned.
1: date=2023-12-07 time=14:19:59 eventtime=1701987599439429340 tz="-0800" logid="0000000020"
type="traffic" subtype="forward" level="notice" vd="vdom1" srcip=10.1.100.22 srcport=53540
srcintf="wan2" srcintfrole="undefined" dstip=172.16.200.55 dstport=80 dstintf="wan1"
dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=296 proto=6
action="accept" policyid=1 policytype="policy" poluuid="e538d622-53eb-51ee-8adc-f8fbb0f22fdd"
policyname="B-out" service="HTTP" trandisp="snat" transip=172.16.200.2 transport=53540
appcat="unscanned" duration=120 sentbyte=10855 rcvdbyte=1397640 sentpkt=205 rcvdpkt=1130
sentdelta=10855 rcvddelta=1397640 durationdelta=120 sentpktdelta=205 rcvdpktdelta=1130
```

Appendices

- Perl regular expressions on page 1166
- Preload cache content and web crawler on page 1168
- Automatic backup to an FTP or TFTP server on page 1170
- Custom signature keywords on page 1175
- FortiProxy bypass mode on page 1199

Perl regular expressions

The following table lists and describes some examples of Perl regular expressions.

Expression	Matches
abc	“abc” (the exact character sequence but anywhere in the string).
^abc	“abc” at the beginning of the string.
abc$	“abc” at the end of the string.
a|b	Either “a” or “b”.
^abc|abc$	The string “abc” at the beginning or at the end of the string.
ab{2,4}c	“a” followed by two, three, or four “b”s followed by a “c”.
ab{2,}c	“a” followed by at least two “b”s followed by a “c”.
ab*c	“a” followed by any number (zero or more) of “b”s followed by a “c”.
ab+c	“a” followed by one or more “b”s followed by a “c”.
ab?c	“a” followed by an optional “b” followed by a “c”; that is, either “abc” or “ac”.
a.c	“a” followed by any single character (not newline) followed by a “c”.
a\.c	“a.c” exactly.
[abc]	Any one of “a”, “b”, and “c”.
[Aa]bc	Either of “Abc” and “abc”.
[abc]+	Any (nonempty) string of “a”s, “b”s and “c”s (such as “a”, “abba”, “acbabcacaa”).
[^abc]+	Any (nonempty) string that does not contain any of “a”, “b”, and “c” (such as “defg”).
\d\d	Any two decimal digits, such as 42; same as \d{2}.
/i	Makes the pattern case insensitive. For example, /bad language/i blocks any instance of “bad language” regardless of case.
\w+	A “word”: A nonempty sequence of alphanumeric characters and low lines (underscores), such as “foo”, “12bar8”, and “foo_1”.
100\s*mk	The strings “100” and “mk” optionally separated by any amount of white space (spaces, tabs, and newlines).
abc\b	“abc” when followed by a word boundary (for example, in “abc!” but not in “abcd”).
perl\B	“perl” when not followed by a word boundary (for example, in “perlert” but not in “perl stuff”).

Expression	Matches
\x	Tells the regular expression parser to ignore white space that is neither preceded by a backslash character nor within a character class. Use this to break up a regular expression into slightly more readable parts.
/x	Used to add regular expressions within other text. If the first character in a pattern is forward slash "/", the "/" is treated as the delimiter. The pattern must contain a second "/". The pattern between the "/" is taken as a regular expression, and anything after the second "/" is parsed as a list of regular expression options ("i","x", and so on). An error occurs if the second "/" is missing. In regular expressions, the leading and trailing space is treated as part of the regular expression.

Block common spam phrases

Block common phrases found in spam messages with the following expressions:

```
/try it for free/i
/student loans/i
/you're already approved/i
/special[\+\-\*=<>\.\,;!\?%&~#§@\^°\$£€\{\}()\[\]\|\\_1]offer/i
```

Block purposely misspelled words

Random characters are often inserted between the letters of a word to bypass spam-blocking software. The following expressions can help to block those messages:

```
/^.*v.*i.*a.*g.*r.*o.*$/i
/cr[eéèêë][\+\-\*=<>\.\,;!\?%&§@\^°\$£€\{\}()\[\]\|\\_01]dit/i
```

Block any word in a phrase

Use the following expression to block any word in a phrase:

```
/block|any|word/
```

Preload cache content and web crawler

You can configure FortiProxy to pre-load cache content based on manually defined URL patterns with scheduled crawling function. This feature is useful for schools and hotels where popular content, such as video, can be predicted ahead of schedule, downloaded outside of peak hours, and viewed by customers using the cache.

The following `execute preload` CLI commands list and describe configurable preload caching and web crawler options.

execute preload list

Use this command to show currently active URLs and their run schedules:

```
execute preload list
```

For example:

```
URL's scheduled for preload:
http://google.com
    Depth: 0, runs every 1 minutes, next run at Dec 23 16:49
http://google.ca
    Depth: 5, runs every 2 minutes, next run at Dec 23 16:52
https://news.cnn.com
    Depth: 1, runs every 5 minutes, next run at Dec 23 18:47
```

execute preload show-log

Use this command to display all the completed operations and their status.

execute preload url

Use this command to schedule a crawl, preload, refresh, or pin request for a given URL:

```
execute preload url <url> <depth> <at_time> <repeat_after> <repetitions> <user-agent> <password>
```

- **<url>:** URL to preload.
- **<depth>:** Depth of preload.
- **<at_time>:** In the format of HHH:MM. HHH is hours from present (between 0-672), and MM is minutes from present (between 0-59). The default is set to 0:00.

- **<repeat_after>:** HHH:MM. Set HHH between 0-168 and MM between 0-59. The default is set to 168:59 (max).
- **<repetitions>:** End after this many repetitions (between 1-365). The default is set to 1.
- **<user-agent>:** Specify client type (free text) to identify as a user agent. The default is set to "Wget/1.17 (linux-gnu)".
- **<user>:** Specify user name.
- **<password>:** Password for the user (asked for in a separate prompt).

execute preload url-delete

Use this command to delete a scheduled crawl, preload, refresh, or pin request for a given URL:

```
execute preload url-delete <url>
```

Use the following command, for example, to delete all operations for `http://www.fortinet.com`:

```
execute preload url-delete http://www.fortinet.com/
```

To view a list of pending crawls, see execute preload list on page 1168.

Examples

The following command would fetch `http://www.fortinet.com` and do the following:

- preload cache immediately:

  ```
  execute preload url http://www.fortinet.com/
  ```

- crawl it to depth two immediately:

  ```
  execute preload url http://www.fortinet.com/ 2
  ```

- crawl it to depth two after ten minutes:

  ```
  execute preload url http://www.fortinet.com/ 2 00:10
  ```

- crawl it to depth two after ten minutes and after 24 hours 30 times (that is,fetch the URL in ten minutes and every day for 30 days):

  ```
  execute preload url http://www.fortinet.com/ 2 00:10 24:00 30
  ```

- crawl with the user agent “Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0”:

  ```
  execute preload url http://www.fortinet.com/ 0 00:00 00:01 1 "Mozilla/5.0 (Macintosh; Intel
  Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
  ```

Automatic backup to an FTP or TFTP server

You can schedule automatic FortiProxy backups to an FTP or TFTP server.

Manual backups to a remote FTP or TFTP using IPv4

To manually back up the full FortiProxy configuration to a remote FTP server:

```
execute backup full-config ftp <configuration_file_name> <FTP_server_IPv4_address> <user_name>
<password>
```

To manually back up the full FortiProxy configuration to a remote TFTP server:

```
execute backup full-config tftp <configuration_file_name> <TFTP_server_IPv4_address> <password>
```

Specifying a password is optional for backing up to a TFTP server.

Manual backups to a remote FTP or TFTP using IPv6

IPv6 addresses are supported in the `execute backup` and `execute restore` commands to TFTP and FTP servers.

To back up a configuration file to an IPv6 TFTP server:

```
# execute backup config tftp fpx.conf 2000:172:16:200::55
```

To restore a configuration file from an IPv6 TFTP server:

```
# execute restore config tftp fpx.conf 2000:172:16:200::55
```

To back up a configuration file to an IPv6 FTP server:

```
# execute backup config ftp fpx.conf 2000:172:16:200::55 root xxxxxxxxxx
```

To restore a configuration file from an IPv6 FTP server:

```
# execute restore config ftp fpx.conf 2000:172:16:200::55 root xxxxxxxxxx
```

Scheduled automatic backups with an auto script

Use an auto script to schedule a FortiProxy backup and to define how many times to repeat the backup. The auto script overrides the existing configuration file with the same name. Auto script does not support keeping all of the hourly configuration files. When using the %%PASSWD%% variable in the script, the variable is replaced by the password setting and encrypted.

The following example shows how to automate the hourly backup of the FortiProxy configuration to an FTP server.

FTP server: 10.1.5.241

FTP user: ftp_user

FTP user password: ftppassword

Name of the configuration file: FPX1_autoScript.conf

```
config system auto-script
    edit "hourly_config_backup"
        set interval 3600
        set repeat 0
        set start auto
        set script "execute backup full-config ftp FPX1_autoScript.conf 10.1.5.241 ftp_user
%%PASSWD%%"
        set password ftppassword
    next
end
```

If the FTP auto script was executed successfully, the following is the result:

```
FPX1 $  execute auto-script status
========== #1, 2019-07-29 09:00:01 ==========
FPX1 $  execute backup full-config ftp FPX1_autoScript.conf 10.1.5.241 ftp_user ftppassword

Connect to ftp server 10.1.5.241 ...
Please wait...
Send config file to ftp server OK.

========== #2, 2019-07-29 10:00:01 ==========
FPX1 $  execute backup full-config ftp FPX1_autoScript.conf 10.1.5.241 ftp_user ftppassword

Connect to ftp server 10.1.5.241 ...
Please wait...
Send config file to ftp server OK.
```

The following example shows to automate the hourly backup of the FortiProxy configuration to a TFTP server:

```
config system auto-script
    edit "hourly_config_backup"
        set interval 3600
        set repeat 0
        set start auto
```

```
        set script "execute backup full-config tftp FPX1_autoScript.conf 10.1.5.241"
    next
end
```

The following is the full syntax of the auto-script CLI commands:

```
config system auto-script
    edit <name>
        set name <string>
        set interval <integer>
        set repeat <integer>
        set start {manual | auto}
        set script <string>
        set password <string>
        set output-size <integer>
        set timeout <integer>
    next
end
```

`name <string>`	Auto script name. The size is 35 characters.
`interval <integer>`	Repeat interval, in seconds (0 - 31557600, default = 0).
`repeat <integer>`	Number of times to repeat this script (0 - 65535, 0 = infinite, default = 1).
`start {manual | auto}`	Script starting mode. • `manual`: Starting manually (default). • `auto`: Starting automatically.
`script <string>`	List of FortiProxy CLI commands to repeat. The maximum size is 1023 characters.
`password <string>`	Script password to replace %%PASSWD%% tag in the script. Use cases include replacing a password tag for SFTP/FTP server password.
`output-size <integer>`	Number of megabytes to limit script output to (10 - 1024, default = 10).
`timeout <integer>`	Maximum running time for this script, in seconds (0 - 300, 0 = no timeout, default = 0).

Manual backups with SCP

You can use the secure copy protocol (SCP) to perform manual backups of the FortiProxy configuration.

1. To enable SCP, run the following commands:

```
config system global
    set admin-scp enable
end
```

2. Enable the SSH administrative access on the interface handling the SCP services.
3. Use any Linux client to download the FortiProxy configuration file using the following command:

```
$ scp admin@<FortiProxy_IP>:sys_config <location>
```

The following example is run using Lubuntu 19.04. This backup runs one time from the Linux client.

```
$ scp admin@10.1.5.252:sys_config ~/config/"FPX.autobackup.$(date +%Y%m%d_%H%M%S).conf"
```

The example downloads the configuration file and saves it to the `~/config` folder with a file name of `FPX.autobackup.$(date +%Y%m%d_%H%M%S).conf`.

Using `$(date +%Y%m%d_%H%M%S)` ensures that each configuration file has a unique file name, for example, `FPX.autobackup.20190729_110001.conf`.

Scheduled automatic backups with SCP

To perform an hourly automatic backup, you need to run the SCP command as a cron job.

For example, you can use a bash script to run hourly backups with all the configuration files saved in the `~/config` folder.

NOTE: Remember to change the IP address to your own FortiProxy IP address before adding the following command to a cron job. If the `~/config` folder does not already exist, you need to create it before running the cron job.

```
#!bin/bash

# This command will pull a copy of the FortiProxy (10.1.5.252) using SCP on port 10104
# and save the config to the ~/config folder with the file-naming convention of
# FPX.autobackup.$(date +%Y%m%d_%H%M%S).conf

scp -P 10104 admin@10.1.5.252:sys_config ~/config/"FPX.autobackup.$(date +%Y%m%d_%H%M%S).conf"
```

Save the bash script file to `~/auto_backup/hourly_backup.sh`.

Add execution permission to the bash script file:

```
$ sudo chmod +x ~/auto_backup/hourly_backup.sh
```

Run the `ls -l` command on the Linux client:

```
lubuntu@lubuntu-pc:~/auto_backup$ ls -l
total 4
-rwxr-xr-x 1 lubuntu lubuntu 106 Jul 29 14:41 hourly_backup.sh
lubuntu@lubuntu-pc:~/auto_backup$
```

To add the bash script to the cron table file, use the following command:

```
$ sudo crontab -e

# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task.
#
# To define the time, you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and time zones.
#
# Output of the cron table jobs (including errors) is sent through
# email to the user the cron tab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m. every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information, see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
@hourly ~/auto_backup/hourly_backup.sh <==== Add this to the file and save it.
```

You can change the `@hourly` to `@monthly` or `@weekly` or `@daily`.

To verify that the backups were run correctly, look at the contents of the `~/config` folder:

```
lubuntu@lubuntu-pc:~/config$ ls -l
total 784
-rw------- 1 lubuntu lubuntu 197872 Jul 29 11:00 FPX.autobackup.20190729_110001.conf
-rw------- 1 lubuntu lubuntu 197872 Jul 29 12:00 FPX.autobackup.20190729_120001.conf
-rw------- 1 lubuntu lubuntu 197872 Jul 29 13:00 FPX.autobackup.20190729_130001.conf
-rw------- 1 lubuntu lubuntu 197872 Jul 29 14:00 FPX.autobackup.20190729_140001.conf
lubuntu@lubuntu-pc:~/config$
```

Custom signature keywords

- information
- session
- content
- IP header
- TCP header
- UDP header
- ICMP
- other

Information keywords

attack_id

Syntax: `--attack_id <id_int>;`

Description:

Use this optional value to identify the signature. It cannot be the same value as any other custom rules. If an attack ID is not specified, the FortiProxy automatically assigns an attack ID to the signature.

An attack ID you assign must be between 1000 and 9999.

Example: `--attack_id 1234;`

name

Syntax: `--name <name_str>;`

Description:

Enter the name of the rule. A rule name must be unique. The name you assign must be a string greater than 0 and less than 64 characters in length.

Example: `--name "Buffer_Overflow";`

Session keywords

flow

Syntax: `--flow {from_client[,reversed] | from_server[,reversed] | bi_direction };`

Description:

Specify the traffic direction and state to be inspected. They can be used for all IP traffic.

Example: `--src_port 41523; --flow bi_direction;`

The signature checks traffic to and from port 41523.

If you enable “quarantine attacker”, the optional reversed keyword allows you to change the side of the connection to be quarantined when the signature is detected.

For example, a custom signature written to detect a brute-force log in attack is triggered when “Login Failed” is detected from_server more than 10 times in 5 seconds. If the attacker is quarantined, it is the server that is quarantined in this instance. Adding reversed corrects this problem and quarantines the actual attacker.

service

Syntax: `--service {HTTP | TELNET | FTP | DNS | SMTP | POP3 | IMAP | SNMP | RADIUS | LDAP | MSSQL | RPC | SIP | H323 | NBSS | DCERPC | SSH | SSL};`

Description:

Specify the protocol type to be inspected. This keyword allows you to specify the traffic type by protocol rather than by port. If the decoder has the capability to identify the protocol on any port, the signature can be used to detect the attack no matter what port the service is running on. Currently, HTTP, SIP, SSL, and SSH protocols can be identified on any port based on the content.

app_cat

Syntax: `--app_cat <category_int>;`

Description:

Specify the category of the application signature. Signatures with this keyword are considered as application rules. These signatures will appear under Application Control instead of IPS configuration. To display a complete list of application signature categories, enter the following CLI commands:

```
config application list
   edit default
      config entries
         edit 1
            set category ?
```

weight

Syntax: `--weight <weight_int>;`

Description:

Specify the weight to be assigned to the signature. This keyword allows a signature with the higher weight to have priority over a signature with a lower weight. This is useful to prioritize between custom and stock signatures and also between different custom signatures.

The weight must be between 0 an 255. Most of the signatures in the Application Control signature database have weights of 10; botnet signatures are set to 250. A range of 20 to 50 is recommended for custom signatures.

Content keywords

byte_extract

Syntax: `byte_extract:<bytes_to_extract>, <offset>, <name> \ [, relative][, multiplier <multiplier value>][, <endian>]\ [, string][, hex][, dec][, oct][, align <align value>][, dce];`

Description:

Use the `byte_extract` option to write rules against length-encoded protocols. This reads some of the bytes from the packet payload and saves it to a variable.

byte_jump

Syntax: `--byte_jump <bytes_to_convert>, <offset>[, multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct] [, align];`

Description:

Use the `byte_jump` option to extract a number of bytes from a packet, convert them to their numeric representation, and jump the match reference up that many bytes (for further pattern matching or byte testing). This keyword allows relative pattern matches to take into account numerical values found in network data. The available keyword options include:

- `<bytes_to_convert>`: The number of bytes to examine from the packet.
- `<offset>`: The number of bytes into the payload to start processing.
- `[multiplier]`: multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the result to be skipped.
- `relative`: Use an offset relative to last pattern match.
- `big`: Process the data as big endian (default).
- `little`: Process the data as little endian.
- `string`: The data is a string in the packet.
- `hex`: The converted string data is represented in hexadecimal notation.
- `dec`: The converted string data is represented in decimal notation.
- `oct`: The converted string data is represented in octal notation.
- `align`: Round up the number of converted bytes to the next 32-bit boundary.

byte_test

Syntax: `--byte_test <bytes_to_convert>, <operator>, <value>, <offset>[multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct];`

Description:

Use the `byte_test` keyword to compare a byte field against a specific value (with operator). This keyword is capable of testing binary values or converting representative byte strings to their binary equivalent and testing them. The available keyword options include:

- `<bytes_to_convert>`: The number of bytes to compare.
- `<operator>`: The operation to perform when comparing the value (<,>,=,!,&).
- `<value>`: The value to compare the converted value against.
- `<offset>`: The number of bytes into the payload to start processing.
- `[multiplier]`: multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the result to be skipped.
- `relative`: Use an offset relative to last pattern match.
- `big`: Process the data as big endian (default).
- `little`: Process the data as little endian.
- `string`: The data is a string in the packet.
- `hex`: The converted string data is represented in hexadecimal notation.
- `dec`: The converted string data is represented in decimal notation.
- `oct`: The converted string data is represented in octal notation.

depth

Syntax: `--depth <depth_int>;`

Description:

Use the depth keyword to search for the contents within the specified number of bytes after the starting point defined by the offset keyword. If no offset is specified, the offset is assumed to be equal to 0.

If the value of the depth keyword is smaller than the length of the value of the content keyword, this signature will never be matched.

The depth must be between 0 and 65535.

distance

Syntax: `--distance <dist_int>;`

Description:

Use the distance keyword to search for the contents within the specified number of bytes relative to the end of the previously matched contents. If the within keyword is not specified, continue looking for a match until the end of the payload.

The distance must be between 0 and 65535.

content

Syntax: `--content [!]"<content_str>";`

Description:

Deprecated. See pattern on page 1189 and context on page 1182 keywords. Use the content keyword to search for the content string in the packet payload. The content string must be enclosed in double quotes.

To have the FortiProxy unit search for a packet that does not contain the specified context string, add an exclamation mark (!) before the content string.

Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character.

The double quote ("), pipe sign(|) and colon(:) characters must be escaped using a back slash if specified in a content string.

If the value of the content keyword is greater than the length of the value of the depth keyword, this signature will never be matched.

context

Syntax: `--context {uri | header | body | host};`

Description:

Specify the protocol field to look for the pattern. If context is not specified for a pattern, the FortiProxy unit searches for the pattern anywhere in the packet buffer. The available context variables

are:

- `uri`: Search for the pattern in the HTTP URI line.
- `header`: Search for the pattern in HTTP header lines or SMTP/POP3/SMTP control messages.
- `body`: Search for the pattern in HTTP body or SMTP/POP3/SMTP email body.
- `host`: Search for the pattern in HTTP HOST line.

no_case

Syntax: `--no_case;`

Description:

Use the no-case keyword to force the FortiProxy unit to perform a case-insensitive pattern match.

offset

Syntax: `--offset <offset_int>;`

Description:

Use the offset keyword to look for the contents after the specified number of bytes into the payload. The specified number of bytes is an absolute value in the payload. Follow the offset keyword with the depth keyword to stop looking for a match after a specified number of bytes. If no depth is specified, the FortiProxy unit continues looking for a match until the end of the payload.

The offset must be between 0 and 65535.

pattern

Syntax: `--pattern [!]"<pattern_str>";`

Description:

The FortiProxy unit will search for the specified pattern. A pattern keyword normally is followed by a context keyword to define where to look for the pattern in the packet. If a context keyword is not present, the FortiProxy unit looks for the pattern anywhere in the packet buffer. To have the FortiProxy search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI.

Example: `--pattern "/level/" --pattern "|E8 D9FF FFFF|/bin/sh" --pattern !"|20|RTSP/"`

pcre

Syntax: `--pcre [!]"/<regex>/[ismxAEGRUB]";`

Description:

Similarly to the pattern keyword, use the pcre keyword to specify a pattern using Perl-compatible regular expressions (PCRE). A pcre keyword can be followed by a context keyword to define where to look for the pattern in the packet. If no context keyword is present, the FortiProxy unit looks for the pattern anywhere in the packet buffer.

For more information about PCRE syntax, go to http://www.pcre.org.

The switches include:

- `i`: Case insensitive.
- `s`: Include newlines in the dot metacharacter.
- `m`: By default, the string is treated as one big line of characters. ^ and $ match at the beginning and ending of the string. When m is set, ^ and $ match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer.
- `x`: White space data characters in the pattern are ignored except when escaped or inside a character class.
- `A`: The pattern must match only at the start of the buffer (same as ^).
- `E`: Set $ to match only at the end of the subject string. Without E, $ also matches immediately before the final character if it is a newline (but not before any other newlines).
- `G`: Invert the “greediness” of the quantifiers so that they are not greedy by default, but become greedy if followed by ?.
- `R`: Match relative to the end of the last pattern match. (Similar to distance:0;).
- `U`: Deprecated, see the context on page 1182 keyword. Match the decoded URI buffers.

uri

Syntax: `--uri [!]"<uri_str>";`

Description:

Deprecated. See pattern and context keywords. Use the uri keyword to search for the URI in the packet payload. The URI must be enclosed in double quotes ("). To have the FortiProxy unit search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI. Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character. The double quote ("), pipe sign (|) and colon (:) characters must be escaped using a back slash (\) if specified in a URI string.

within

Syntax: `--within <within_int>;`

Description:

Use this together with the distance keyword to search for the contents within the specified number of bytes of the payload.

The within value must be between 0 and 65535.

IP header keywords

dst_addr

Syntax: `--dst_addr [!]<ipv4>;`

Description:

Use the dst addr keyword to search for the destination IP address. To have the FortiProxy unit search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.

Example: `dst_addr [172.20.0.0/16, 10.1.0.0/16,192.168.0.0/16]`

ip_dscp

Syntax: `--ip_dscp`

Description:

Use the ip_dscp keyword to check the IP DSCP field for the specified value.

ip_id

Syntax: `--ip_id <field_int>;`

Description:

Check the IP ID field for the specified value.

ip_option

Syntax: `--ip_option {rr | eol | nop | ts | sec | lsrr | ssrr | satid | any};`

Description:

Use the ip_option keyword to check various IP option settings.

The available options include:

- `rr`: Check if IP RR (record route) option is present.
- `eol`: Check if IP EOL (end of list) option is present.
- `nop`: Check if IP NOP (no op) option is present.
- `ts`: Check if IP TS (time stamp) option is present.
- `sec`: Check if IP SEC (IP security) option is present.
- `lsrr`: Check if IP LSRR (loose source routing) option is present.
- `ssrr`: Check if IP SSRR (strict source routing) option is present.
- `satid`: Check if IP SATID (stream identifier) option is present.
- `any`: Check if IP any option is present.

ip_tos

Syntax: `--ip_tos <field_int>;`

Description:

Check the IP TOS field for the specified value.

ip_ttl

Syntax: `--ip_ttl [< | >] <ttl_int>;`

Description:

Check the IP time-to-live value against the specified value. Optionally, you can check for an IP time-to-live greater-than (>) or less-than (<) the specified value with the appropriate symbol.

protocol

Syntax: `--protocol {<protocol_int> | tcp | udp | icmp};`

Description:

Check the IP protocol header.

Example: `--protocol tcp;`

src_addr

Syntax: `--src_addr [!]<ipv4>;`

Description:

Use the src_addr keyword to search for the source IP address. To have the FortiProxy unit search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.

Example: `src_addr 192.168.13.0/24`

TCP header keywords

ack

Syntax: `--ack <ack_int>;`

Description:

Check for the specified TCP acknowledge number.

dst_port

Syntax: `--dst_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Use the `dst_port` keyword to specify the destination port number.

You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

seq

Syntax: `--seq [operator,]<number>[,relative];`

Description:

Check for the specified TCP sequence number.

- `operator` includes =,<,>,!.
- `relative` indicates it is relative to the initial sequence number of the TCP session.

src_port

Syntax: `--src_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Use the src_port keyword to specify the source port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

tcp_flags

Syntax: `--tcp_flags <SAFRUP120>[!|*|+] [,<SAFRUP120>];`

Description:

Specify the TCP flags to match in a packet.

- `S`: Match the SYN flag.
- `A`: Match the ACK flag.
- `F`: Match the FIN flag.
- `R`: Match the RST flag.
- `U`: Match the URG flag.
- `P`: Match the PSH flag.
- `1`: Match Reserved bit 1.
- `2`: Match Reserved bit 2.
- `0`: Match No TCP flags set.
- `!`: Match if the specified bits are not set.
- `*`: Match if any of the specified bits are set.
- `+`: Match on the specified bits, plus any others.

The first part if the value (`<SAFRUP120>`) defines the bits that must be present for a successful match.

Example:

`--tcp_flags AP` only matches the case where both `A` and `P` bits are set.

The second part (`[,<SAFRUP120>]`) is optional, and defines the additional bits that can be present for a match.

For example `tcp_flags S,12` matches the following combinations of flags: S, S and 1, S and 2, S and 1 and 2. The modifiers !, * and + cannot be used in the second part.

window_size

Syntax: `--window_size [!]<window_int>;`

Description:

Check for the specified TCP window size. You can specify the window size as a hexadecimal or decimal integer. A hexadecimal value must be preceded by `0x`. To have the FortiProxy search for the absence of the specified window size, add an exclamation mark (`!`) before the window size.

UDP header keywords

dst_port

Syntax: `--dst_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Specify the destination port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

src_port

Syntax: `--src_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Specify the destination port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

ICMP keywords

icmp_code

Syntax: `--icmp_code <code_int>;`

Description:

Specify the ICMP code to match.

icmp_id

Syntax: `--icmp_id <id_int>;`

Description:

Check for the specified ICMP ID value.

icmp_seq

Syntax: `--icmp_seq <seq_int>;`

Description:

Check for the specified ICMP sequence value.

icmp_type

Syntax: `--icmp_type <type_int>;`

Description:

Specify the ICMP type to match.

Other keywords

data_size

Syntax: `--data_size {<size_int> | <<size_int> | ><size_int>;`

Description:

Test the packet payload size. With data_size specified, packet reassembly is turned off automatically. So a signature with data_size and only_stream values set is wrong.

- `<size_int>` is a particular packet size.
- `<<size_int>` is a packet smaller than the specified size.
- `><size_int>` is a packet larger than the specified size.

Examples:

- `--data_size 300;`
- `--data_size <300;`
- `--data_size >300;`

data_at

Syntax: `--data_at <offset_int>[, relative];`

Description:

Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.

dump-all-html

Syntax: `--dump-all-html`

Description:

Dump all HTML files for benchmarking via iSniff. When there is no file type specified, all HTML files are dumped.

rate

Syntax: `--rate <matches_int>,<time_int>;`

Description:

Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.

- `<matches_int>` is the number of times a signature must be detected.
- `<time_int>` is the length of time in which the signature must be detected, in seconds.

For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If `--rate 100,10`; is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. Use this command with `--track` to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.

rpc_num

Syntax: `--rpc_num <app_int>[, <ver_int> | *][, <proc_int> | *>];`

Description:

Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wild card can be used for version and procedure numbers.

same_ip

Syntax: `--same_ip;`

Description:

Check that the source and the destination have the same IP addresses.

track

Syntax: `--track {SRC_IP |DST_IP |DHCP_CLIENT |DNS_DOMAIN}[,block_int];`

Description:

When used with `--rate`, this keyword narrows the custom signature rate totals to individual addresses.

- `SRC_IP`: tracks the packet's source IP.
- `DST_IP`: tracks the packet's destination IP.
- `DHCP_CLIENT`: tracks the DHCP client's MAC address.
- `DNS_DOMAIN`: counts the number of any specific domain name.
- `block_int` has the FortiProxy unit block connections for the specified number of seconds, from the client or to the server, depending on which is specified.

For example, if `--rate 100,10` is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. The FortiProxy unit maintains a single total, regardless of source and destination address.

If the same custom signature also includes `--track` client; matches are totaled separately for each source address. A log entry is added when the signature is detected 100 times in 10 seconds within traffic from the same source address.

The `--track` keyword can also be used without `--rate`. If an integer is specified, the client or server will be blocked for the specified number of seconds every time the signature is detected.

FortiProxy bypass mode

The FPX-2000E, 2000G, 4000E, and 4000G include a PCIe x2 Gigabit Copper One Group Bypass Ethernet Adapter. By default, the ports are independent interfaces. You can configure the two Ethernet ports to run in bypass mode where the connections of the two ports are disconnected from the system and switched over to the other port to create a crossed connection loop-back between the two ports, which means all packets received from one port are transmitted to the adjacent port and vice versa. Bypass mode provides fail open support for maximum up time for the network.

To enable and configure bypass mode:

1. Enable bypass mode:
```
config system bypass
   set bypass-mode [powerup|powerdown|both]
end
```

powerup	Enable bypass mode only when the FortiProxy unit is running.
powerdown	Enable bypass mode only when the FortiProxy unit is down.
both	Always enable bypass mode on the FortiProxy unit regardless of its running status.

2. Configure whether to enable watchdog for bypass interfaces using the following command:
```
config system bypass
   set bypass-watchdog {disable | enable}
end
```

To disable bypass mode:

1. Run the following command:
```
config system bypass
   set bypass-mode off
end
```

Formatting and loading FortiProxy firmware image using TFTP

You can download and install FortiProxy firmware from a local TFTP server via the BIOS, under CLI control. This is useful in cases such as when the `OPEN DEVICE BOOT FAILED` message appears on console.

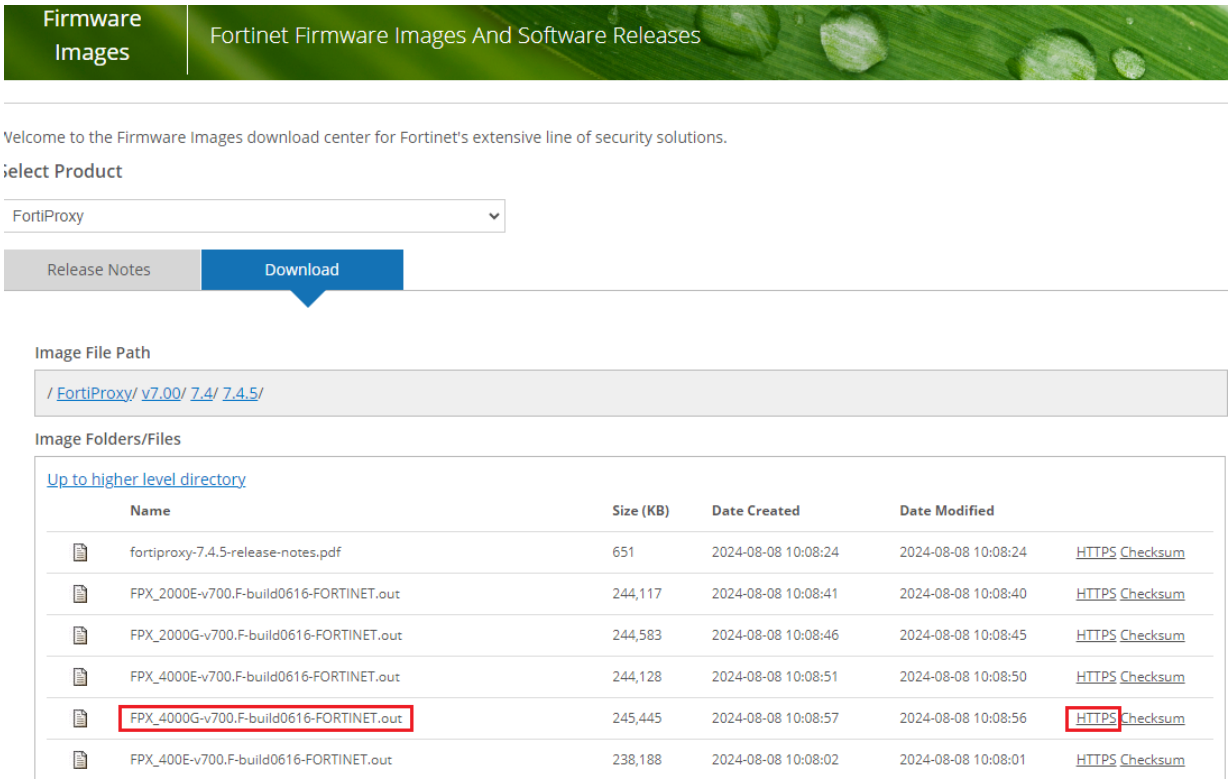
Installing firmware from a local TFTP server under console control will reset the FortiProxy unit to factory default settings. Consider backing up the configuration before starting the formattingprocess. See Configuration backups and reset on page 1006.

Prerequisites

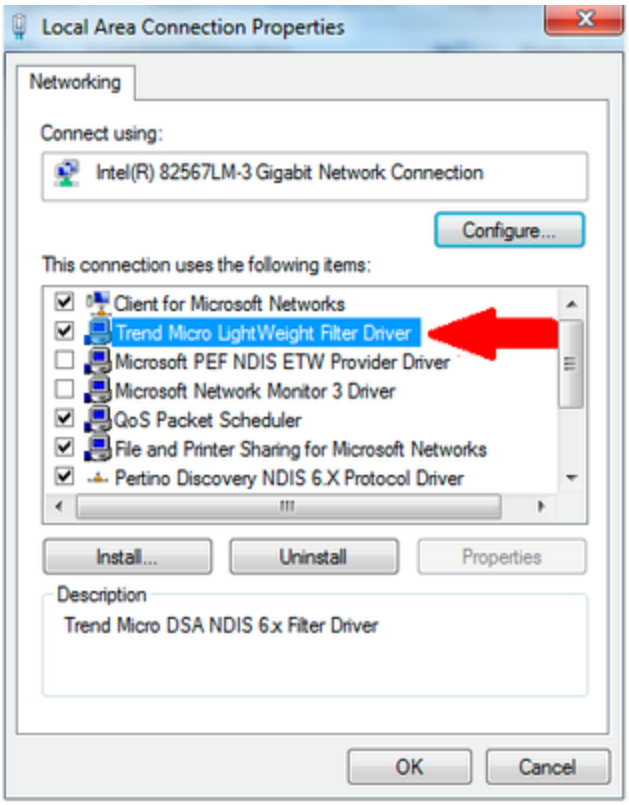
- A null modem, or RJ-45 to DB9 console cable, supplied with the FortiProxy unit
- An Ethernet RJ45 cable
- A terminal client, such as a PC running HyperTerminal (Windows)
- A TFTP server

To format and load FortiProxy firmware image using TFTP:

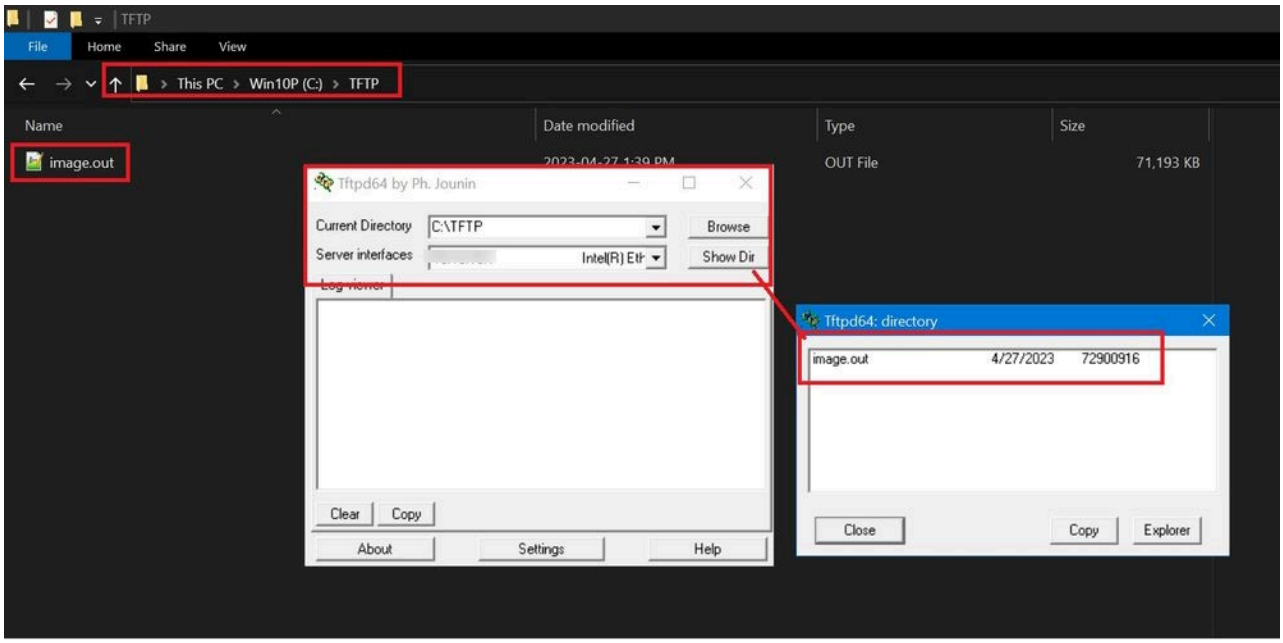
1. Download the FortiProxy firmware and verify the MD5 checksum:
   a. Go to https://support.fortinet.com.
   b. Click *Login* to log in to the Fortinet Support website.
   c. From the *Support* > *Downloads* menu, select *Firmware Download*.
   d. In the *Select Product* dropdown menu, select *FortiProxy*.
   e. On the *Download* tab, navigate to the FortiProxy firmware file for your FortiProxy model or VM platform in the *Image Folders/Files* section.
   f. Click *HTTPS* to download the desired firmware.



2. Download the TFTP server from here and install it on the computer. Make sure the bitness of the TFTP installer matches that of the computer, such as tftp64 for a 64-bit computer.
3. Disable Windows firewall or any other 3rd party packet filtering application (e.g. Trend Micro LightWeight Filter Driver).



4. Create a directory and name it as something like TFTP.
5. Move the FortiProxy image to that directory.
6. Rename the image file to `image.out`.
7. Set the system's ethernet interface IP (can be from any subnet), subnet mask, and default gateway (local IP address that is set on FortiProxy). This example uses the following:
   - **IP address**: 172.18.20.86
   - **Subnet mask**: 255.255.255.0
   - **Default gateway**: 172.18.20.86



8. Connect the computer to the FortiProxy unit using the null modem cable. See the FortiProxy Quick Start Guide for detailed instructions.
9. Restart the FortiProxy.
10. When the console displays `Press any key to display configuration menu...`, press any other key.

```
FortiBootLoader
FortiProxy-4000G (15:52-03.14.2022)
Ver:00020010
Serial number:FPX4KGT622900002
Total RAM: 262144MB
Boot up, boot device capacity: 1920MB.
Press any key to display configuration menu...
```

11. When a list of choices with individual letters of the alphabet appears, press `F` to format the device. The device will reboot after the formatting is complete.

```
[C]:  Configure TFTP parameters.
[R]:  Review TFTP parameters.
[T]:  Initiate TFTP firmware transfer.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot.
[H]:  Display this list of options.
```

12. When a list of choices with letters appear, press `R` to review TFTP parameters.

```
[P]:  Set image download port.
[D]:  Set DHCP mode.
[I]:  Set local IP address.
[S]:  Set local subnet mask.
[G]:  Set local gateway.
[V]:  Set local VLAN ID.
[T]:  Set remote TFTP server IP address.
[F]:  Set firmware image file name.
[E]:  Reset TFTP parameters to factory defaults.
[R]:  Review TFTP parameters.
[N]:  Diagnose networking (ping).
[Q]:  Quit this menu.
[H]:  Display this list of options.
```

```
Enter P,D,I,S,G,V,T,F,E,R,N,Q or H:

Image download port:    1
DHCP status:            disabled
Local VLAN ID:          none
Local IP address:       172.18.20.86
Local subnet mask:      255.255.255.0
Local gateway:          172.17.219.1
TFTP server IP address: 172.18.20.83
Firmware file name:     FPX_4000G-v700-build0132-FORTINET.out
```

13. Once again, when a list of choices with letters appears, press `C` to configure TFTP parameters.

```
[C]:  Configure TFTP parameters.
[R]:  Review TFTP parameters.
[T]:  Initiate TFTP firmware transfer.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot.
[H]:  Display this list of options.

Enter C,R,T,F,B,Q,or H:
```

14. Change the parameters to match the TFTP server configuration using the following provided options:

```
[P]: Set firmware download port.
[D]: Set DHCP mode.
[I]: Set local IP address.
[S]: Set local subnet mask.
[G]: Set local gateway.
[V]: Set local VLAN ID.
[T]: Set remote TFTP server IP address.
[F]: Set firmware file name.
```

```
[E]: Reset TFTP parameters to factory defaults.
[R]: Review TFTP parameters.
[N]: Diagnose networking(ping).
[Q]: Quit this menu.
[H]: Display this list of options.
```

The following are examples of configuring the local IP address, TFTP server IP address, and firmware file name:

```
Enter P,D,I,S,G,V,T,F,E,R,N,Q or H:

Enter local IP address [172.18.20.90]:172.18.20.86
```

```
Enter P,D,I,S,G,V,T,F,E,R,N,Q or H:

Enter remote TFTP server IP address [172.18.20.83]:
```

```
Enter P,D,I,S,G,V,T,F,E,R,N,Q or H:

Enter firmware file name [FPX_4000G-v700-build0132-FORTINET.out]:
```

15. When the configuration is complete, press `T` to initiate the TFTP firmware transfer.

```
Enter C,R,T,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".
MAC:         00:90:0B:A8:C0:FD

Image download port:    1
DHCP status:            disabled
Local VLAN ID:          none
Local IP address:       172.18.20.86
Local subnet mask:      255.255.255.0
Local gateway:          172.17.219.1
TFTP server IP address: 172.18.20.83
Firmware file name:     FPX_4000G-v700-build0132-FORTINET.out
########
```

16. After the transfer is complete, follow the prompts to finish the formatting process and login using the default credentials.

```
Total 146492785 bytes data downloaded.
Verifying the integrity of the firmware image..

Total 397312kB unzipped.

Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?
```



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.