Administration Guide

FortiSASE 26.1.99 Feature





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



May 08, 2026
FortiSASE 26.1.99 Feature Administration Guide
72-26199F-1252593-20260508

TABLE OF CONTENTS

Change log **12**
Introduction **13**
FortiClient agent-based mode using FortiClient 14
Proxy agentless mode 15
Accessing the FortiSASE portal with IPv4 IPv6 connectivity 15
Changing the FortiCloud primary account email 17
Dedicated public IP addresses 17
Prerequisites and considerations 18
Embedded onboarding guide 19
Prerequisites and considerations 22
FortiFlex licensing 22
Prerequisites and considerations 22
Subscription renewal notification 23
Network restrictions 23
Remote agent and edge device user identification 24
Required services and ports 25
Signing in as an IAM user 25
Supporting external IdP users 26
System status notifications 26
New features **27**
Select availability features **39**
Authenticated onboarding 43
BGP MED Setting 44
Central management 45
Considerations 45
Central management for MSSP tenants 46
Custom invitation codes 46
Factory reset 46
Prerequisites 47
IPsec dead peer detection customization 47
Network restrictions removed 47
Private proxy 48
RBI 48
Prerequisites 49
Considerations 49
Licensing 49
SCIM server support 50
Prerequisites 50
Secure Browser 50
Prerequisites 50
Considerations 51

Beta features 52
Digital experience: TCP latency 53
IPsec remote agent support 54
Considerations 55
Tunnel settings 55
FortiSASE security PoPs 55
FortiClient 56
Monitoring 59
Adding a custom dashboard 59
Resetting all dashboards 59
Drilling down on vulnerabilities 60
FortiView monitors 62
Adding a custom monitor 62
Resetting all monitors 63
Monitoring edge device bandwidth usage 63
API-based CASB monitoring 64
Overview 65
Applications 65
Files 66
Alerts 67
Edge Devices 67
Endpoints 69
Operations 71
Digital Experience Monitoring 71
Running a trace job on an endpoint 72
Analyzing trace job result 73
Prerequisites 73
DEM trial 74
SaaS monitoring 75
SPA hub monitoring 78
SPA application monitoring 81
Endpoints 82
Management Connection button 83
Considerations 84
Examples 84
FortiGuard Forensics Analysis 87
Application inventory for managed endpoints 89
Requesting FortiClient diagnostic logs from endpoints 91
Requesting FortiClient debug logs from endpoints 92
Infrastructure 93
Instances not supporting dynamic infrastructure changes 94
Asset Map 95
Connected users 97
Packet capture 98
Connected wireless clients 100
SPA 101

Prerequisites ... 103
Configuring the FortiSASE security PoPs as the FortiGate hub's spokes ... 106
BGP routing design ... 106
Verifying IPsec tunnels on the FortiGate hub ... 140
Testing private access connectivity to FortiGate hub network from remote agents and edge devices ... 142
Testing private access connectivity to FortiGate hub network from remote proxy users ... 143
Testing private access connectivity from FortiGate hub network to remote agents and edge device users ... 143
Verifying BGP routing on the FortiGate hub ... 144
Verifying private access traffic in FortiSASE portal ... 144
Verifying private access traffic from hubs ... 145
Verifying private access hub status and location using the asset map ... 146
Restricting access using a FortiGate SPA hub/spoke policy ... 146
Edge devices ... 149
FortiExtender ... 149
FortiGate ... 164
FortiAP ... 168
Considerations ... 174
Prerequisites and considerations ... 176
Prerequisites ... 176
Considerations ... 176
Captive portal ... 188
On-ramp tunnel ... 196
Configuration workflow ... 197
Prerequisites and considerations ... 197
Prerequisites and considerations ... 197
Configuring IPsec device as Branch On-ramp ... 200
Configuring profile groups and policies to control traffic flow from branch devices ... 207
Configuring a FortiGate IPsec connection to FortiSASE ... 208
Configuring a third-party IPsec connection to FortiSASE ... 226
Viewing IPsec connections ... 234
Reports ... 234
Scheduling a report ... 234
Manually running a report ... 235
Report types ... 235
Logs ... 237
Forwarding logs to an external server ... 238
Administrator Events ... 245
Endpoint management ... 245
Forwarding logs to SOCaaS ... 246
Forwarding logs to FortiAnalyzer Cloud ... 247
Log anonymization ... 249
Log retention policy ... 251
Administration ... 252
Software audit & version ... 252

Automation 259
Network 263
DNS 263
Considerations 265
DNS redirection rules 265
Geofencing 269
Regional compliance 270
Prerequisites and considerations 274
IP management 274
Public IP 275
IPAM 278
Advanced 280
BGP 281
Advertise Hub Priorities 281
BGP MED Setting 284
Proxy configuration 285
Prerequisites and considerations 286
Private proxy 287
Secure proxy migration 293
Security 296
Policies 296
Default policies 297
Adding policies to perform granular firewall actions and inspection 297
Configuring a policy to allow traffic from an Edge device to FortiSASE 299
Configuring a geography-based policy 301
Proxy policies 302
Default proxy policies 303
Configuring a proxy policy 303
Bandwidth control 306
Prerequisites 306
Considerations 307
Shared profiles 307
Per IP profiles 308
Bandwidth control policies 309
Example: Limiting YouTube speeds using bandwidth control 311
Security profiles 312
Security profile groups 313
SSL Inspection 315
AntiVirus 324
Intrusion prevention 325
File Filter 328
DLP 329
Web Filter 355
DNS Filter 370
Application Control With Inline-CASB 376
Video Filter 382
Profile resources 383

ZTNA 388
Agent-based ZTNA 388
Agentless ZTNA 391
Hosts 405
Schedules 407
External feeds 408
Considerations 409
Configuring an external feed 410
Applying an external feed 411
Applications 413
Connect 413
Disconnect 413
Configure 414
Monitor 414
Data Protection 414
Secure Browser 415
Prerequisites 416
Considerations 416
Enable FortiSASE Secure Browser 416
Configure Secure Browser SSO settings 416
Secure Browser profiles 418
User assignment rules and users 422
Onboard users 423
Supported event logs 428
Example: Configuring a custom Secure Browser profile and custom user assignment rule 429
Best practices for common use cases 432
Endpoint management 436
Endpoint profiles 436
Considerations 437
Global connection settings 438
Connection 443
Protection 459
Sandbox 462
ZTNA 464
FSSO 468
Groups & AD Users 469
FortiClient GUI Settings 470
IPsec dead peer detection customization 471
Pre-logon tunnel 472
Endpoint groups 477
Invitation codes 478
Example: Configuring a custom endpoint profile applied to an AD group 479
Example: Configuring FSSOMA support with FortiAuthenticator behind SPA hub for Windows domain endpoint 482
Security posture tags and tagging rules 486
Configuring security posture tags and tagging rules 486
Rule logic example 488

Considerations 489
Tagging rule types 489
Endpoint management settings 496
Prerequisites 497
Endpoint upgrade 497
FortiClient deployment status 499
Considerations 500
Access & authentication 501
Users and groups 502
PKI 503
LDAP 504
Configuring FortiSASE with an LDAP server for remote user authentication in FortiClient agent-based mode 504
Configuring FortiSASE with an LDAP server for remote user authentication in proxy agentless mode 508
Configuring FortiSASE with a RADIUS server for remote user authentication 512
Prerequisites 514
Considerations 514
SSO 515
Configuring FortiSASE with Microsoft Entra ID SSO: SAML configuration fields 515
Configuring FortiSASE with Microsoft Entra ID SSO in FortiClient agent-based mode 517
Configuring FortiSASE with Entra ID SSO in proxy agentless mode 526
Configuring FortiSASE with AD FS SSO 528
Configuring FortiSASE with Okta SSO 535
Configuring FortiSASE with FortiAuthenticator Cloud as SAML IdP proxy for Entra ID SSO 538
Configuring FortiSASE with FortiAuthenticator as SAML IdP for SSO 545
Searching user groups from SAML IdP 552
Testing SSO configuration from FortiSASE 556
Authenticated onboarding 562
SCIM server support 564
Fortinet Single Sign On (FSSO) 578
Prerequisites 579
Considerations 580
Domains 580
Considerations 581
Entra ID domains 581
System 587
Administration 587
Example 587
HTML templates 589
API-based CASB 591
Prerequisites and considerations 592
Certificates 592
Central Management 593
Prerequisites and considerations 594

Prerequisites and considerations 594
Mapping FortiManager objects to FortiSASE configuration settings 596
Enabling central management 598
Configuring FortiManager for central management 600
Verifying configuration updates performed using central management 602
Displaying error messages for failed synchronization attempts 603
Configuring settings using Device Manager in FortiManager 605
Configuring settings using policy packages in FortiManager 612
Configuring security profiles in FortiManager 653
Central management for MSSP tenants 712
Snapshot 717
Factory reset 717
Subscription overview 720
RBI 721
Prerequisites 721
Considerations 722
Licensing 722
Configuration options 722
Example: Configuring RBI with proxy 723
Client onboarding 730
Managed endpoint client onboarding 731
Prerequisites and considerations 731
Allowlisting FortiClient (Windows) processes 732
Allowlisting FortiClient (MacOS) processes 735
Proxy client onboarding 737
PAC file customization 737
Certificate installation 743
Proxy configuration 744
Proxy Chrome extension and Chromebook support 749
Enterprise mobility management 752
Configuring Microsoft Intune integration with FortiClient (iOS) 752
Deploying FortiClient (macOS) using Intune 753
Deploying FortiClient (macOS) using Jamf Pro 759
MSSP portal 770
Considerations 770
Considerations 770
Configuration workflow 771
Resource-based permissions 772
Using the MSSP portal 780
Accessing the MSSP portal 781
Monitoring a tenant's instance 782
Managing a tenant's instance 783
SPA for an MSSP hub 784
Central management for MSSP tenant 784

Troubleshooting 785
FAQs 786
Dedicated public IP addresses 786
Subscriptions 786
I am an existing customer with a registered legacy FortiSASE device-based subscription (EMS05-434) or a registered FortiSASE user-based subscription (EMS05-553). I want to purchase the FortiSASE standard user subscription (EMS05-547), Advanced user subscription (EMS05-676) or the Comprehensive user subscription (EMS05-759). What should I do? 786
I am an existing customer with the FortiSASE standard user subscription (EMS05-547) and want to upgrade to an Advanced user subscription (EMS05-676) or the Comprehensive user subscription (EMS-759). What should I do? 787
I am an existing customer with the FortiSASE standard user subscription (EMS05-547), Advanced user subscription (EMS05-676), or Comprehensive user subscription (EMS-759). I want to shift to using FortiSASE user subscriptions in FortiFlex. What should I do? 788
I am an existing customer with the FortiSASE standard user subscription in FortiFlex and want to upgrade to the Advanced user subscription in FortiFlex or the Comprehensive user subscription in FortiFlex. What should I do? 789
I am an existing partner with the FortiSASE Standard Not-for-Resale (NFR) subscription (EMS05-684) and want to change to the Advanced NFR subscription (EMSAN-676). What should I do? 790
Security PoPs 791
For my new FortiSASE instance, during initial provisioning I receive the message “Error 21400.4: Failed to configure Security PoP”. How can I resolve this issue? 791
For my new FortiSASE instance, I observed the notification “Background provisioning: Provisioning for <security PoP> is still in progress, please check back later.” Should I be concerned with this message? 791
What is the expected impact of applying any security point of presence (PoP) changes to an existing FortiSASE instance once all proper licensing is in place? 792
When connecting to FortiSASE, my endpoint seems to be directed to a security PoP which is not the closest one provisioned to my geographical location. What causes this behavior and how can I troubleshoot it? 792
Shifting from FortiClient EMS to FortiSASE 794
I am an existing customer with an EMS on-premise deployment. How can I move my endpoints to FortiSASE? 794
I am an existing customer with a FortiClient Cloud deployment. What is the path to move to a FortiSASE deployment? 796
How can I configure FortiSASE for endpoint management? 797
Shifting from standalone VPN-only FortiClient (free) to FortiSASE 797
I am an existing customer with a FortiClient VPN-only standalone endpoints connecting to FortiGate using SSL or IPsec connections. What is the path to move my endpoints to FortiSASE? 797
Appendix A - FortiSASE data centers 800
Status page 800
Global data centers list 800
Access locations list 800

Egress IP addresses feed ... 800
Considerations ... 801
Number of security data centers accessible per subscription ... 801
Considerations ... 802
Appendix A1 - Access locations ... 803
Appendix B - REST API ... 811
Appendix C - Tunnel performance ... 812
Latency ... 812
Evaluating and selecting security PoPs for lowest latency ... 812
Jitter and packet loss ... 812
Resolving increased latency with SSL support for DTLS ... 813
Appendix D - Maximum values ... 814
Appendix E - Monthly maintenance ... 815
Monthly maintenance impact ... 815
Monthly maintenance schedule ... 815
Maintenance window group 1: 12 PM to 8 PM EST/EDT ... 816
Maintenance window group 2: 6 AM to 2 PM EST/EDT ... 817
Maintenance window group 2 (Japan): 9 AM to 5 PM EST/EDT ... 817
Maintenance window group 3: 4 PM to 12 AM EST/EDT ... 817
Appendix F - Security and compliance ... 819

Change log

Date	Change description
2026-05-04	Initial release of 26.1.2.1.
2026-05-07	Added: • Changing the FortiCloud primary account email on page 17
2026-05-08	Initial release of 26.1.2.1.1.

Introduction

FortiSASE is a software-as-a-cloud-delivered service that allows clients to securely access the internet with the protection from FortiOS. With FortiSASE, you can ensure to protect remote off-net endpoints and users with the same security policies as when they are on-net, no matter their location. The service is available through a subscription based on the number of users.

FortiSASE works with various FortiCloud services in the background to deliver a seamless service for securing your internet access.

In terms of security, FortiSASE offers the following features to protect clients:

- Antivirus
- Web Filter
- Intrusion prevention
- File filter
- Data loss prevention
- Application control
- SSL inspection

Security features are customizable and offer many familiar settings as you would see on a FortiGate.

Several flexible steering methods are used to steer or redirect network traffic from the user edge to FortiSASE. These steering methods can be used to securely access Internet, private, and SaaS destinations or applications, respectively, and therefore used to implement FortiSASE Secure Internet Access (SIA), Secure Private Access (SPA), and Secure SaaS Access (SSA) use cases.

<table>
<tr><th>Steering Method</th><th colspan="3">Destinations</th></tr>
<tr><td>Agent (FortiClient)</td><td rowspan="3">Internet and web-based applications</td><td rowspan="3">Private applications via SPA hub</td><td rowspan="3">SaaS applications via CASB</td></tr>
<tr><td>IPsec with routing (Thin Edge, Branch On-Ramp)</td></tr>
<tr><td>IPsec with explicit proxy (Private Proxy)</td></tr>
<tr><td>Agentless (Proxy)</td></tr>
<tr><td>FortiSASE use case</td><td>Secure Internet Access (SIA)</td><td>Secure Private Access (SPA)</td><td>Secure SaaS Access (SSA)</td></tr>
</table>

For details on these FortiSASE use cases, see the 4-D FortiSASE Architecture Guide.

For details on the deployment process, see FortiSASE Cloud Deployment.

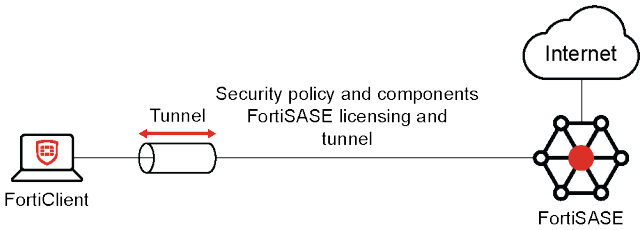
User provisioning is made simple, whether you are creating local users in bulk, integrating users from your Active Directory or LDAP server, or integrating with SAML authentication. You can also easily group your users to apply similar policies.

See Service Organization Controls (SOC2) compliance standard.

FortiClient agent-based mode using FortiClient

In FortiClient agent-based mode, endpoints connect to a FortiSASE tunnel to secure their traffic. Once provisioned, clients are connected through an always-up tunnel connection to ensure FortiSASE scans traffic to the internet.

This mode requires FortiSASE user-based licensing. See the FortiSASE Ordering Guide.



The provisioning process for this mode is as follows:

1. The administrator provisions the FortiSASE environment.
2. The administrator configures policies and security components in FortiSASE as desired, including configuring the desired policies. See Adding policies to perform granular firewall actions and inspection on page 297.
3. The administrator provisions end users on FortiSASE and emails invitations to them. FortiSASE supports remote authentication methods such as LDAP. See Access & authentication on page 501 for descriptions of the provisioning process for different authentication methods.
4. Download FortiClient to endpoints and connect to FortiClient Cloud using the code included in the invitation email. This can be completed by the administrator when preprovisioning endpoints before distributing to end users, or by the end users themselves.
5. FortiClient connects to FortiClient Cloud to activate its FortiSASE subscription and provision the FortiSASE tunnel.
6. End users connect to the FortiSASE tunnel to secure their traffic.

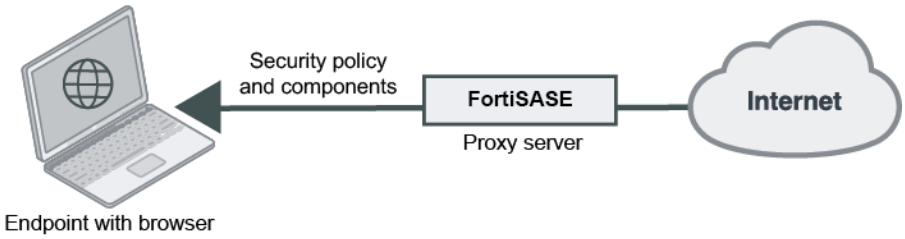
7. FortiSASE applies the appropriate policies to endpoints.
8. The administrator can view logs in FortiSASE and modify the configuration as desired. See Logs on page 237.

This mode also supports configuring Zero Trust Network Access (ZTNA). In this deployment configuration, FortiSASE joins the Fortinet Security Fabric to share endpoint information with the FortiGate, allowing a corporate FortiGate to implement ZTNA for remote users who are already registered to FortiSASE. See the *FortiSASE SPA Using ZTNA Deployment Guide* for details.

Proxy agentless mode

In proxy agentless mode, users configure FortiSASE as a proxy server on their device at the OS level or in a browser. Once configured, the proxy policies configured in FortiSASE protect sessions initiated in browsers.

This mode requires FortiSASE user-based licensing. See the FortiSASE Ordering Guide.



The provisioning process for this mode is as follows:

1. The administrator initializes the FortiSASE environment.
2. The administrator configures policies and security components in FortiSASE as desired, including enabling proxy and configuring the desired proxy policies. See Configuring a proxy policy on page 303.
3. The administrator configures end users on FortiSASE and distributes the proxy server information to them.
4. End users configure their OS or browser to use the FortiSASE proxy server. When the browser displays an authentication prompt, the end user enters their FortiSASE user credentials.
5. FortiSASE applies the appropriate policies to sessions initiated in the browser.
6. The administrator can view logs in FortiSASE and modify the configuration as desired. See Logs on page 237.

Accessing the FortiSASE portal with IPv4 IPv6 connectivity

The FortiSASE portal supports dual stack capability enabling seamless access from workstations using IPv4 or IPv6 addresses. This ensures you can manage FortiSASE configurations effectively regardless of the underlying IPv4 protocol.

To verify FortiSASE management portal access using both IPv4 and IPv6 addresses:

1. Use a Linux shell to resolve the FortiSASE portal domain name and verify it returns both IPv4 and IPv6 addresses:

```
$ host portal.prod.fortisase.com

portal.prod.fortisase.com is an alias for portal.prod.fortisase.66241.fortiwebcloud.net.

portal.prod.fortisase.66241.fortiwebcloud.net is an alias for ipv6.lb-2.ca-central-1.aws.waas-online.net.

ipv6.lb-2.ca-central-1.aws.waas-online.net has address 35.182.106.253

ipv6.lb-2.ca-central-1.aws.waas-online.net has IPv6 address 2600:1f11:8c:9101:b646:e3:30a2:39ae
```

   The DNS response includes both A (IPv4) and AAAA (IPv6) records, ensuring that the domain resolves over both IP protocols. This enables client devices or browsers to select the most appropriate protocol based on their local settings and network availability.

2. Validate connectivity over IPv4 and IPv6 protocols by using the `globalping` utility to send HTTP requests from different geographical locations.

   a. Validate connectivity over IPv4:

```
$ globalping http https://portal.prod.fortisase.com -4
> Falkenstein, DE

HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
X-Controller-Region: us-east-2
...
```

   b. Validate connectivity over IPv6:

```
$ globalping http https://portal.prod.fortisase.com -6
> Helsinki, FI

HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
X-Controller-Region: us-east-2
...
```

   As shown, the portal is reachable over both IPv4 and IPv6 from global locations and receives a `200 OK` for the request sent, enabling improved accessibility in both IPv4- and IPv6-enabled environments.

Changing the FortiCloud primary account email

FortiSASE only supports changing the FortiCloud primary account ID (email) to a new account ID (email) not already associated with an existing FortiCloud account.

When the primary account is logged in, FortiSASE supports the FortiCloud option for updating the primary account ID (email).

To change the FortiCloud primary account email:

1. When logged into FortiSASE with the primary account email address, click on the account email name at the top-right corner of the portal and take note of the numerical account ID.
2. Click *My Account*.
3. In the FortiCloud portal, go to *Account* > *Change Account ID (Email)*.
4. Enter the *New Account ID (Email)* and confirm it in the fields provided.
5. Click *Save*.
6. Go to the FortiCare Support site.
7. Create a new account using the same email address entered in the *New Account ID (Email)* using either:
   - *Quick Links* > *Create Account* at the center of the page.
   - *Create Account* from the top-right corner of the page.
8. Return to the FortiSASE portal and confirm that you can log in with the new account ID (email) and password.
9. Once logged in, click on the account name at the top-right corner of the portal and confirm the numerical account ID has not changed.

Dedicated public IP addresses

The Public IP Deployment Guide provides use cases, subscriptions required, and deployment details.

The shared public IP address design for security PoPs presents some challenges for customers and their remote secure internet access users:

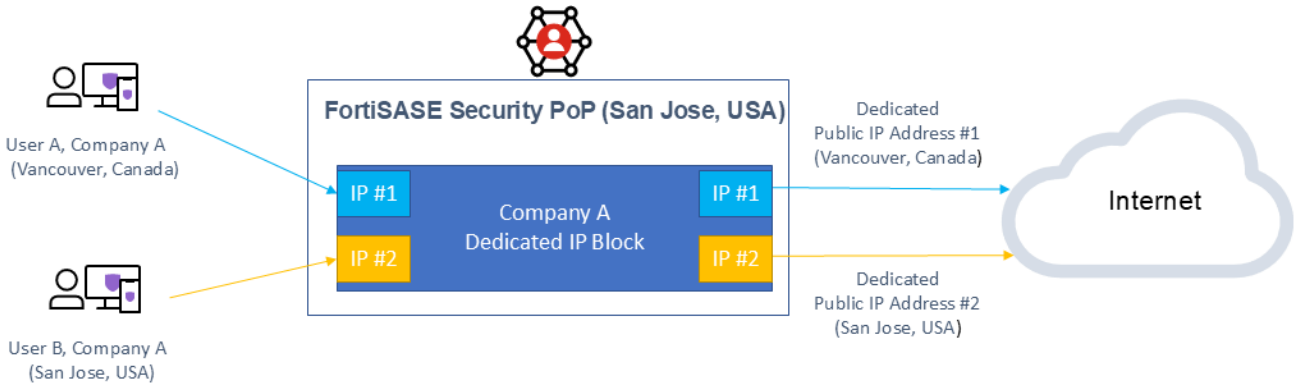
- When using the same public IP address for all outgoing traffic, identification and isolation of each specific customer's remote user traffic is not possible.
- If the public IP address used for outgoing traffic belongs to an IP address block in the same geographical location as the security PoP that users are connected to, their content is limited to that specific security PoP when accessing services relying on geolocation.

Using dedicated public IP addresses for each customer's remote user traffic and public IP addresses that are mapped to a specified country can solve these problems. Thus to address these issues, FortiSASE assigns a dedicated public IP address per security PoP enabling use cases that require a consistent source IP address,

such as IP address-based application access control, geo-restriction compliance, or third-party firewall allowlisting.

The network diagram illustrates some benefits of using FortiSASE dedicated public IP addresses as this section further describes:

- Traffic identification and isolation for IP address reputation control
- Geolocation rules
- Source IP address anchoring. Typically, combined with geolocation rules.



Prerequisites and considerations

Prerequisites

A FortiSASE instance with a Standard, Advanced or Comprehensive remote user subscription includes dedicated public IP addresses per Security PoP by default.

The following summarizes subscription support for geolocation changes and source IP address anchoring:

Subscription tier	Geolocation changes	Source IP address anchoring
Standard	Supported	Supported
Advanced		
Comprehensive		

After licensing has been applied, you must manually configure the dedicated public IP address use cases for FortiSASE on the backend, submitting a request by opening a new FortiCare Support ticket. See Public IP Deployment Guide.

Considerations

- For details about the impact of implementing dedicated IP changes on existing instances, see the FAQ on Dedicated public IP addresses on page 786.

- The number of security PoPs that remote users can access depends on the FortiSASE subscription tier and number of users. See Number of security data centers accessible per subscription on page 801.
- Upon enabling a dedicated IP address for an instance, the proxy port number changes to 9443.
- When using Microsoft Entra ID conditional access policies to restrict access to Entra ID cloud resources for remote users connected to a FortiSASE instance with dedicated IP addresses, defining the IPv4 address ranges of these dedicated IP addresses for these policies is recommended.
- FortiSASE supports requests submitted by opening a new FortiCare Support ticket to configure geolocation rules using the initial set of public IP addresses included with a Standard, Advanced, or Comprehensive subscription.
- For source IP anchoring, you must purchase another Dedicated Public IP add-on subscription with four additional dedicated IP addresses beyond the initial number of dedicated IP addresses per PoP. The additional four dedicated IP addresses can be allocated as desired for source IP anchoring rules such as all in a single security PoP, one per security PoP, or any combination in between.
- As the number of users and bandwidth increases, dynamic scaling of FortiSASE customer environments is required by adding additional dedicated IP addresses to the instance's security PoPs to support a higher session count. When this occurs, the following administrator updates are required, if applicable to customer environments:
  - Depending on the size of the customer, the mode configuration private IP address space used by IPsec between the FortiGate SPA hub and security PoPs should be configured as a /24 subnet. In some cases, it may need to be even larger than a /24 subnet. See IPsec VPN configuration.
  - If the FortiGate SPA hub has policies that restrict access, ensure these policies are configured to accomodate the IPsec mode configuration private IP address space. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.
  - When FortiSASE remote users are on a customer premise where outbound filtering is used, ensure that the security PoP public IP addresses specified in those filters are updated to include the new addresses.
  - It is common for SaaS applications to implement conditional access based on source IP addresses. Since user traffic steered to FortiSASE is sourced with the security POP public IP, ensure conditional access rules in SaaS applications are updated to include the new addresses.
  - The currently configured IPAM pool size needs to large enough to account for additional subnets associated with the added public IP addresses. Each public IP address requires at least 1 /20 subnet from the IPAM pool. See IPAM on page 278.

Embedded onboarding guide

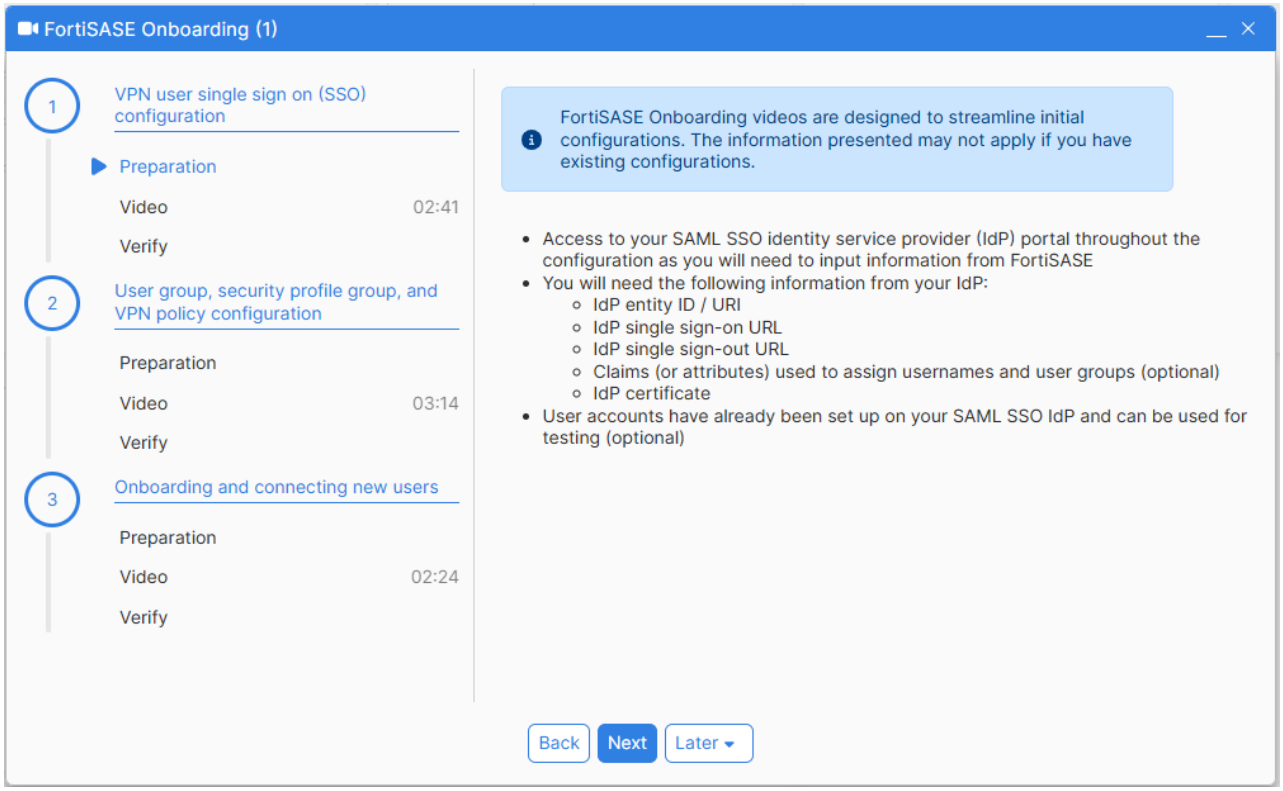
An embedded onboarding guide for FortiSASE displays upon first login. You can also display it later if you skip it. This guide contains instructions and videos embedded into the FortiSASE portal that streamline initial configurations for the secure internet access (SIA) endpoint use case. This use case provides remote users with secure access to the internet using the FortiClient agent. See SIA for agent-based remote users.

The onboarding guide focuses on these configuration topics:

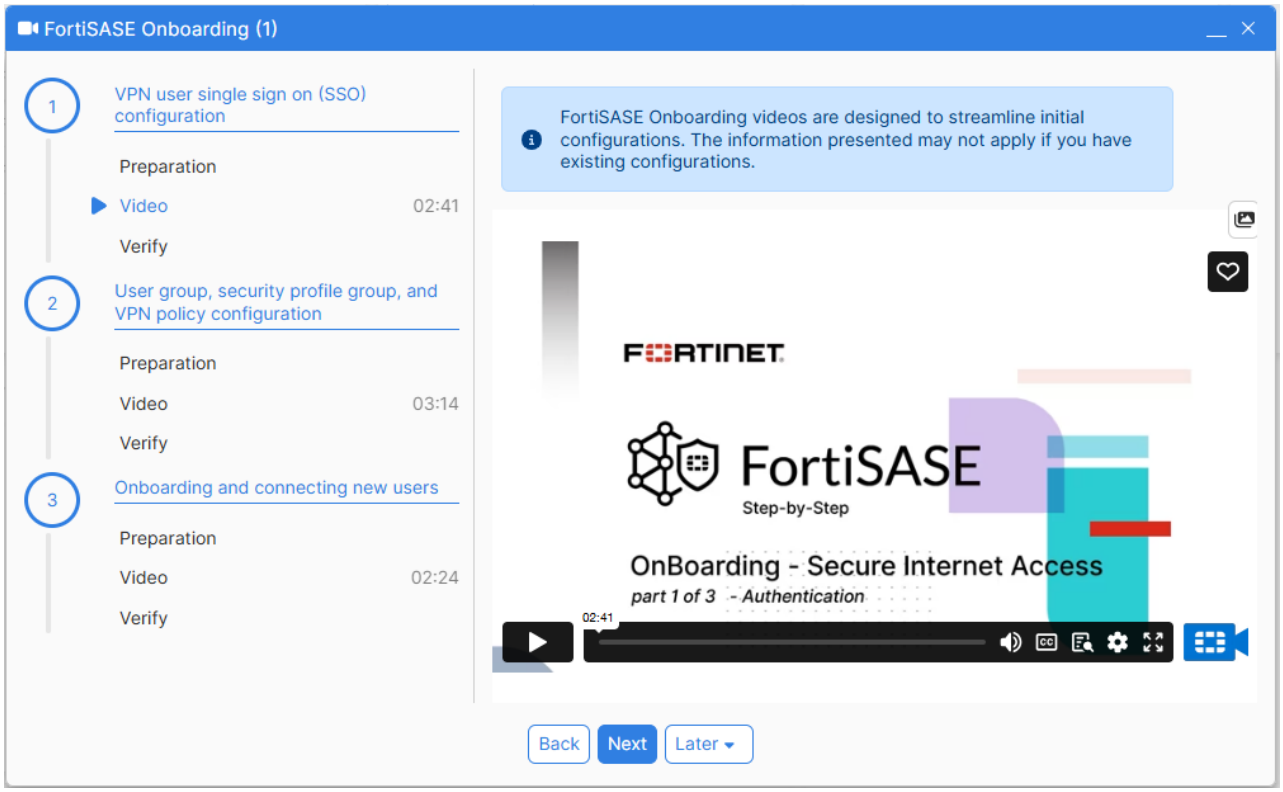
- Agent user single sign-on configuration
- User group, security profile group, and agent policy configuration
- Onboarding and connecting new users

The guide breaks down each topic into the following sections:

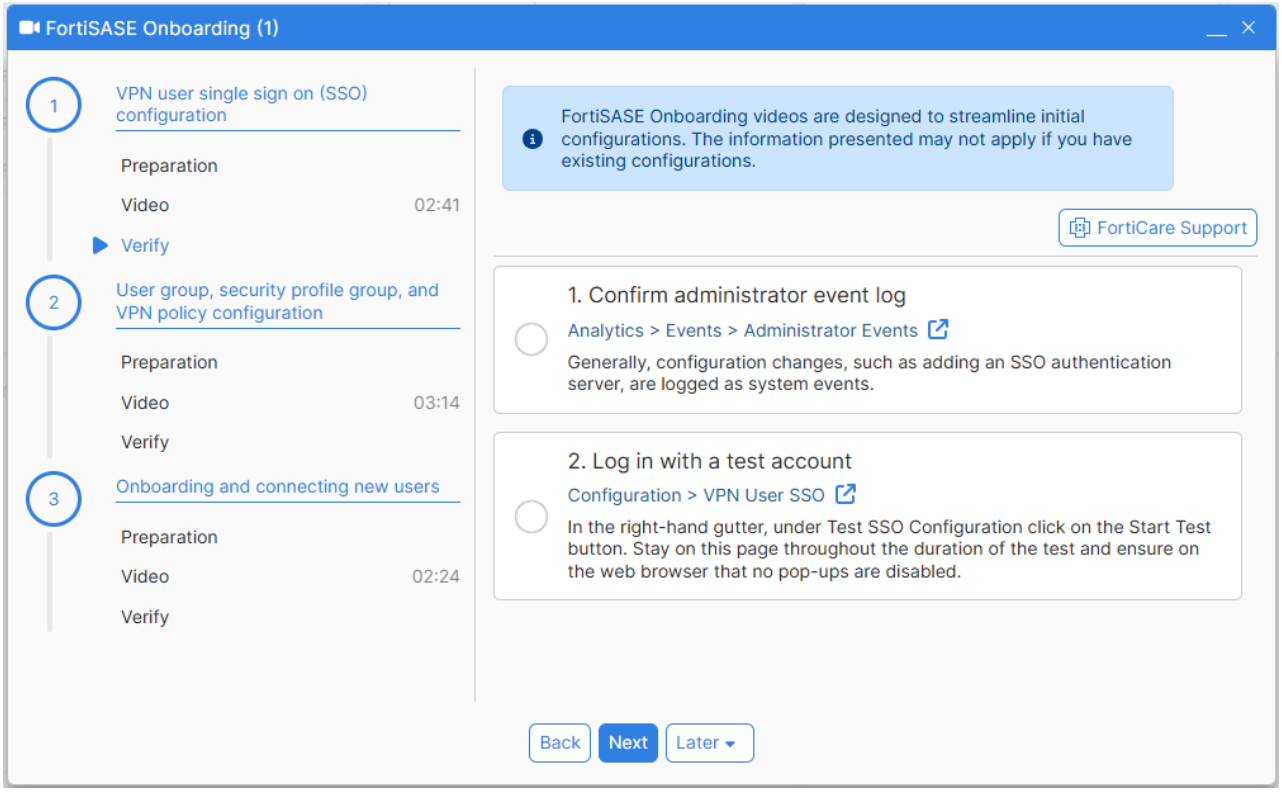
- **Preparation**: steps that you must perform before starting the configuration topic.



- **Video**: brief video that demonstrates the steps that you must perform to complete the configuration or task.



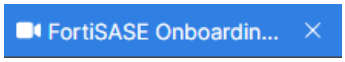
- **Verify**: checklist of steps to perform to ensure that you have configured the FortiSASE settings correctly.



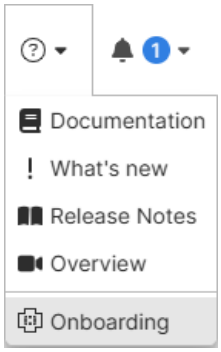
  - To go to the corresponding FortiSASE portal page to perform the verification step, click the link provided.
  - Click the checkbox input next to the verification step to mark it as completed.
  - If you require technical assistance, click *FortiCare Support* to open the Fortinet Support site.

You can go back and forth between sections and topics by clicking the sections in the left pane or by using the *Back* and *Next* buttons, as desired.

Typically, after the *Video* section, you can minimize the guide and perform the configuration settings in the FortiSASE portal as the video demonstrates. You can resume or maximize the guide by clicking the onboarding title at the bottom of the screen.



If you click *Later* or *Skip onboarding* to skip the onboarding for now, you can access the guide later from the Help dropdown in the app header by clicking *Onboarding*.



Prerequisites and considerations

Prerequisites

Access to the embedded onboarding guide in your FortiSASE instance requires an Advanced or Comprehensive remote users FortiSASE subscription. See the FortiSASE Ordering Guide.

Considerations

The information presented may not apply to instances with existing configurations.

FortiFlex licensing

Typically, you apply traditional term-based entitlements to a FortiSASE instance. For these entitlements, see the FortiSASE Ordering Guide.

If you require flexible and usage-based licensing, you can apply a FortiFlex entitlement to your FortiSASE instance.

FortiSASE supports applying FortiFlex entitlements generated from within the FortiFlex portal to your instances. You must apply the appropriate FortiFlex Program and Point Pack SKUs for access to the FortiFlex portal from within your FortiCloud account. See the FortiFlex Program Ordering Guide.

FortiSASE supports the following user-based subscriptions generated from FortiFlex:

- Standard
- Advanced
- Comprehensive

Advanced and Comprehensive user-based subscriptions generated from FortiFlex also support the Branch On-ramp Location subscription. Initial configuration requires a minimum of two security PoPs. You can incrementally increase the number of security PoPs after initial configuration.

For details on supported FortiFlex FortiSASE service offerings and FortiFlex deployment steps, see Service offerings and Deploying FortiFlex.

Prerequisites and considerations

Prerequisites

Before adding a Flex entitlement for FortiSASE from within the FortiFlex portal, ensure that your FortiCloud account does not have any existing FortiClient Cloud or FortiSASE entitlements. Otherwise, you cannot add a

new Flex entitlement for FortiSASE.

Considerations

FortiSASE entitlements created in the FortiFlex portal must be active for at least 90 days.

Subscription renewal notification

The FortiSASE subscription renewal notification keeps administrators informed about upcoming subscription expiries, enabling them to renew their subscriptions promptly to ensure uninterrupted security services. The FortiSASE portal alerts users of impending subscription renewals through an on-login prompt and a bell icon notification in the toolbar.

Administrators can disable subscription renewal notification by selecting *Do not remind me again* in the on-login prompt or clicking the cross icon on the renewal notice under the bell icon, which stops further notifications.

For Standard, Advanced and Comprehensive subscriptions, notifications appear 30 days prior to subscription expiration.

Based on the customer's existing subscriptions, FortiSASE displays upgrade and add-on recommendations such as Secure Access to Private Applications, Seamless Thin-edge Protection, Enhanced Endpoint Diagnostics, and Dedicated Public IP to enhance and expand customer's security coverage.

Network restrictions

For instances created after FortiSASE 23.4.b, the following networks are available for your network configuration:

- 10.0.0.0/8
- 100.64.0.0/10 (except 100.65.0.0/16)
- 172.16.0.0/12
- 192.168.0.0/16

For existing instances created prior to FortiSASE 23.4.b, the networks listed are still unavailable for your network configuration. In these instances, FortiSASE includes support for removing these network restrictions as a select availability feature. See Network restrictions removed on page 47.

Network restrictions are in place since FortiSASE uses some networks and ports for its internal usage and this especially impacts the experience when working with secure private access. See Network restrictions on page 104.

With Remote agent and edge device user identification on page 24 enabled, IPAM private IP address pool(s) configured for agents and edge devices per IP management on page 274 are unavailable for you to use in your network configuration.

Subnets that you can configure as IPAM private IP address pool(s) are:

- 100.65.0.0/16 (default)
- 10.0.0.0/8
- 100.64.0.0/10
- 172.16.0.0/12
- 192.168.0.0/16

The table below summarizes FortiSASE network restrictions:

Network type	Network restrictions removed (default after 23.4.b)	Network restrictions in place (default before 23.4.b)
Available for customer use if not configured as an IPAM private IP address pool	• 10.0.0.0/8 • 100.64.0.0/10 (except 100.65.0.0/16) • 172.16.0.0/12 • 192.168.0.0/16	• 10.0.0.0/8 (except for 10.8.0.0/16 and 10.16.0.0/16) • 172.16.0.0/12 • 192.168.0.0/16
Unavailable for customer use	• 10.252.0.0/16 • 10.253.0.0/16 • Any configured IPAM private IP address pool(s) - 100.65.0.0/16 by default • Any configured FortiExtender and LAN Extension control plane subnet - 10.252.0.0/16 by default	• 10.8.0.0/16 • 10.16.0.0/16 • 100.64.0.0/10 • 10.252.0.0/16 • 10.253.0.0/16

Remote agent and edge device user identification

FortiSASE allows you to identify remote agent and edge device users uniquely in internet and private access traffic logs by enabling these capabilities on newly deployed FortiSASE instances:

- Support for unique remote agent IP address ranges per FortiSASE security PoP using IP address management within one of the selected ranges:
  - 100.65.0.0/16 (default)
  - 10.0.0.0/8
  - 100.64.0.0/10
  - 172.16.0.0/12
  - 192.168.0.0/16
- Removing source NAT for remote agent and edge device traffic destined for secure private access hubs.

Required services and ports

The following summarizes ports that FortiSASE uses for its Security PoPs. In addition to those in the table, FortiSASE also uses ICMP.

Usage	Protocol	Port
SSL portal	TCP	443
DTLS	UDP	
IPsec IKE		500
IPsec NAT-T		4500
CAPWAP		5246
SAML authentication	TCP	7831
Web Filter		8008 8010 8015 8020
Customer-specific proxy port assignment		10445-50445

The following summarizes ports that FortiSASE uses for FortiClient endpoint management.

Usage	Protocol	Port
FortiClient endpoint management connection	TCP	443

Signing in as an IAM user

You can log in to FortiSASE as an Identity & Access Management (IAM) user. You must first create an IAM user by following the steps in Creating a new IAM user. When configuring the IAM user, ensure that you add FortiSASE to the services that the user can access.

> ⚠ Starting in FortiSASE 24.3.b, support for FortiCloud subuser accounts or subaccounts has been discontinued. Therefore, you must use IAM users in cases where multiple users access the FortiSASE customer portal.
>
> To migrate existing subuser accounts from FortiCloud and convert them to IAM users, see Migrating sub users.

To sign in as an IAM user:

1. Go to the FortiSASE portal.
2. Click *Log in with FortiCloud SSO*.
3. Click *IAM user*.
4. Log in with the user credentials from the CSV that you downloaded when creating the IAM user in Creating a new IAM user.

Supporting external IdP users

External identity provider (IdP) users can log into FortiSASE with their company-provided user credentials using a third-party SAML IdP.

For information on managing external IdP roles and users for cloud products, see External IdP roles.

System status notifications

By default, the FortiSASE primary account holder is automatically subscribed to FortiSASE system status email notifications from https://status.fortisase.com.

To manually subscribe to FortiSASE system status notifications via email and other notification types including SMS, Slack, webhooks, Atom feeds, and RSS feeds for yourself and secondary administrators, go to https://status.fortisase.com and click *Subscribe to updates*.

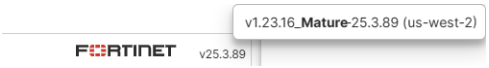
When subscribed to FortiSASE system status notifications, you receive email notifications whenever Fortinet creates, updates, or resolves an incident.

New features

FortiSASE has added powerful new capabilities that are enabled by default on new instances created after the 25.2.c release.

These new capabilities also become available after implementing the *New major features available* best practice upgrade in FortiSASE Mature to migrate to FortiSASE Feature. For details on implementing this best practice upgrade, see New major features available.

- Before the upgrade in a FortiSASE Mature instance, the version tooltip at the bottom-left of the portal displays *Mature* within the version number.



- After the upgrade or on new instances created after 25.2.c in a FortiSASE Feature instance, the version tooltip at the bottom-left of the portal displays *Feature* within the version number.



The versions displayed in the images are based on the 25.3.b release. The exact version numbers displayed in your environment will differ per release.

Below is the list of features available only in the Feature version.

New feature	Description	Requirements
Agent-based zero trust network access (ZTNA) FortiClient endpoint sharing	Added support for sharing the resolved IP and MAC addresses (host tags) of a FortiClient endpoint with ZTNA application gateways (i.e. FortiGate devices) when the endpoint has a security posture tag applied.	None
Agent-based ZTNA destination hosts as IP range or subnet	Added support for specifying ZTNA destination hosts as an IP range or subnet and optionally with a port list or port range when the FortiSASE instance is configured with a default FortiClient version of FortiClient 7.2.8 or later.	Instance configured with a default FortiClient 7.2.8 version or later
Agentless ZTNA support for custom domain and certificate	Added support for using a custom domain and a certificate for the custom domain that can be used to access a ZTNA private application.	Administrator must previously own a custom domain and have already generated a server certificate for the custom domain.

New feature	Description	Requirements
		The administrator must configure the custom domain DNS CNAME record with the FortiSASE private application domain for the private application.
Application control additional configuration settings	Added support for configuring application control filter overrides based on multiple filters including application category, behavior, popularity, protocol, risk, technology, and vendor. Also, added support for configuring actions for custom application signatures.	None
Authenticated onboarding with Entra ID for SAML SSO using an existing Entra ID domain	Added support for configuring authenticated onboarding with Entra ID for SAML SSO using an existing Entra ID domain, which allows an endpoint profile configured with a matching AD group from the domain to be assigned to matching Entra ID-joined endpoints.	Authenticated onboarding is a select availability feature that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
Automation to trigger alert emails for unstable Secure Private Access (SPA) connection.	Added an *Automation* page in *Operation* > *Administration* to allow configuring of actions, such as sending alert emails, based on predefined triggers to proactively notify administrators of events. Currently, alert emails can be triggered for an unstable Secure Private Access (SPA) connection only when SLA failures, routing changes, and BGP neighbor status changes all occur.	Requires licensing and configuration for SPA.
Bandwidth control on page 306	Support for bandwidth policies and profiles used for providing bandwidth control of internet access and private access traffic.	For bandwidth control of private access traffic, requires licensing and configuration for SPA.
Branch On-ramp licensing simplified	Support for simplified branch on-ramp licensing where each on-ramp Security PoP provides up to 1 Gbps for up to 2000 simultaneous dialup IPsec connections, changed from the previous limit of 10 connections.	The Branch On-ramp Connection add-on subscription is discontinued.

New feature	Description	Requirements
Branch On-ramp support for third-party branch devices	Support IPsec connections to Branch On-ramp Security PoPs from third-party IPsec devices.	Requires licensing and configuration for Branch On-ramp feature
Branch On-ramp support with the Standard license	Support for branch on-ramp with the Standard subscription for new and upgraded instances.	An Advanced branch on-ramp subscription must also be applied to a Standard instance to enable the branch on-ramp feature.
Central management for MSSP tenants on page 712	For MSSPs, added central management support for synchronizing multiple tenants' FortiSASE instances from a single FortiManager instance or from multiple FortiManager instances. Currently, each ADOM in FortiManager supports synchronizing configuration with a single FortiSASE instance.	See central management for MSSP tenants Prerequisites and considerations on page 712. Central management is a select availability feature. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
Central management support for policy packages in FortiManager	Added support for synchronizing firewall policies, firewall proxy policies, firewall schedules and security posture tags in policy packages from FortiManager to FortiSASE using the central management select availability feature.	Requires a FortiManager or FortiManager cloud running a supported version. See Central management using FortiManager. Central management is a select availability feature. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
Change summary for configuration audit log	Added support in the *System > Administration* page, for the *Require comments for configuration audit* feature. When enabled, this feature ensures any configuration changes made by an administrator require a change summary to be entered. This includes all configuration changes on FortiSASE, such as those to objects, endpoint profiles, and analytics and reporting configurations.	None

New feature	Description	Requirements
Content disarm and reconstruction (CDR)	Support in the AntiVirus security profile for content disarm and reconstruction (CDR) of Microsoft Office documents and PDF files by removing potentially malicious and untrusted content from them.	CDR does not support SMTP, FTP, and CIFS protocols.
DEM enhancements	Enhancements for Digital Experience Monitoring (DEM), including a path diagram for endpoint traceroute results, support for displaying additional SaaS monitoring metrics, and customizing the list of SaaS applications to monitor.	Requires an Advanced or Comprehensive subscription.
DLP support for EDM	Added support for DLP Exact Data Matching (EDM) that identifies specific data values within an indexed data source. EDM relies on an administrator-defined EDM template, which is used to specify the dataset in a CSV or TXT file that is either uploaded directly to FortiSASE or accessed as an external feed.	None
DLP support for FortiGuard DLP service	Support for configuring and viewing predefined DLP sensors and DLP dictionaries managed by the FortiGuard DLP service in the DLP security profile and in *Security > Traffic > Security profiles > Profile resources*, respectively.	None
DLP support for IDM with fingerprinting	Added support for Indexed Document Matching (IDM) with DLP fingerprinting. IDM creates unique fingerprints for each of the files detected in network and compares all the checksums stored in its database. 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.	None
Edge device support for FortiAP K-series models	FortiSASE adds support for FortiAP devices in the FortiAP 441K series. FortiAP configuration options are also enhanced to streamline the FortiAP configuration process in FortiSASE.	Requires separate FortiSASE subscription subscription for FortiAP edge device support.

New feature	Description	Requirements
Editing security PoP public IP addresses	Added support for editing a public IP of a Security PoP with a geolocation tag (country/region) different than the default for the PoP and for configuring source IP anchoring rule, known as an IP anchor, which associates remote users from a source country/region (and starting in 25.3.a, remote users from a specified user group) with a specific public IP with a configurable geolocation tag.	Requires prior Fortinet request for configuring security PoP public IP addresses features.
Endpoint-to-endpoint communication	Support to enable and manage communication between remote endpoints connected via the FortiSASE Cloud Security tunnel through a Secure Private Access (SPA) Hub. Administrators can enforce granular control by defining endpoint-to-endpoint policies that selectively allow specific traffic between designated endpoints.	Requires licensing and configuration for SPA
Factory reset	Support for performing a factory reset on a FortiSASE instance that returns it to its initial provision point, disconnect all users, and deregister all endpoints.	Enabled by default on instances with NFR and Advanced NFR licenses. It is a select availability feature for all other licenses that requires a FortiCare Support ticket. **All data will be permanently deleted.**
FIDO authentication support	Support for FIDO2 authentication for FortiClient agent tunnels, which is configurable in 'Endpoint profiles' for the 'FortiSASE Cloud Security' tunnel and custom tunnels.	Supported for FortiClient endpoints on Windows and MacOS. Requires FIDO authentication method configured on Entra ID.
File filter support for blocking password protected files	Added support in File Filter for blocking password-protected files of 7z, MSOFFICE, MSOFFICEX, PDF, RAR, and ZIP file types.	None

New feature	Description	Requirements
FortiClient debug log level support	Support for customizing FortiClient *Log Level* per endpoint profile in your FortiSASE instance to simplify debug log collection. In *Endpoint management > Endpoint profiles > FortiClient GUI settings*, enabling *Allow debug log generation* will set the associated endpoints' FortiClient *Log Level* to *Debug*. This feature is disabled by default. When disabled, the *Log Level* is set to *Info*.	None
FortiPAM integration	Added support for FortiPAM integration, allowing FortiSASE managed endpoints to leverage the FortiClient PAM module for secure and controlled privileged access. The feature also enables custom port configuring for FortiPAM integration.	Requires licensed and configured FortiPAM server. Only Windows endpoints support FortiPAM integration. Ensure to use a supported FortiClient version.
Forwarding logs to FortiAnalyzer Cloud on page 247	Support for forwarding logs to a FortiAnalyzer Cloud instance.	Requires the FortiAnalyzer Cloud Storage Add-On License subscription and FortiAnalyzer 7.6.3 or later.
FSSO collector agent integration	Added support to enable integration of FortiSASE with Fortinet single sign on (FSSO) collector agent that enables collection of FSSO records for domain authenticated users. You can use the FSSO records available on FortiSASE as FSSO user groups to authorize user traffic access to resources that FortiSASE protects without having to reauthenticate.	Requires FSSO agent deployed via FortiAuthenticator or via independent collector agent installed on Windows domain controller.
HTTP/3 (QUIC) inspection	Support for SSL inspection of HTTP/3 traffic, which allows security features requiring such inspection to work without the need to block QUIC.	Supported for agent and edge device traffic only.

New feature	Description	Requirements
Hybrid IPsec/SSL mode	For greater performance and security, FortiSASE Cloud Security tunnel will be migrating from SSL to IPsec starting early 2027. FortiSASE Cloud Security tunnel will support a hybrid IPsec/SSL mode during the transition period that is available as an opt-in feature for SSL VPN instances through the *Operations > Administration > Software audit & version* page's best practices. This allows customers time to verify client-side changes for IPsec mode before migrating with confidence.	Available for instances with SSL VPN remote agent support.
Integrated CASB management	Integrated FortiCASB API-based cloud access security broker (CASB) management and protection into FortiSASE for secure SaaS access .	None
IPAM usage chart	Support for displaying IPAM usage information in a chart in *Network > IP management > IPAM*.	None
IPS custom filters	Added support for creating IPS custom filters and for creating custom IPS and Application Control signatures. Also, added central management support for synchronizing IPS custom filters.	None
IPsec autoconnect using session resumption timeout	For instances supporting IPsec and FortiClient 7.4, added support for FortiSASE Cloud Security tunnel autoconnect using the session resumption timeout.	Available for instances with IPsec remote agent and FortiClient 7.4 support.
IPsec dead peer detection customization on page 471	For instances supporting IPsec, added support for customizing dead peer detection settings applicable to IPsec agent tunnels. Dead peer detection reestablishes IPsec agent tunnels on idle connections and cleans up dead IKE peers if required.	Available for FortiSASE instances with IPsec remote agent support.

New feature	Description	Requirements
		It is strongly recommended to schedule a maintenance window before changing dead peer detection settings. Currently connected endpoints will be disconnected from FortiSASE for a few minutes while the change is applied. This is a select availability feature. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
IPsec pre-shared key update support	For IPsec instances, added support for updating the pre-shared key for the FortiSASE Cloud Security tunnel. This enables IPsec instances to support regional compliance rules to on-premise devices and failover sequence features.	Available for instances with IPsec remote agent support. It is strongly recommended to schedule a maintenance window before changing the pre-shared key for IPsec instances. Currently connected endpoints will be disconnected from FortiSASE for a few minutes while the change is applied.
Language support for French and Japanese	Support has been added to view the FortiSASE portal in French and Japanese.	None

New feature	Description	Requirements
License overview page	Added *System > License overview* page to provide granular usage and expiry information for all FortiSASE subscriptions.	None
Navigation reorganization	Navigation menu items have been reorganized for improved usability and to group items with related functionality and usage. Terminology has been standardized for clarity and consistency.	None
New report types	Added support for new report types: • Endpoint vulnerability report • Secure Private Access (SPA) report • Cloud Security Usage Report	None
PAC file editor	Added a built-in custom PAC file editor for creating and editing PAC files hosted on FortiSASE. • These hosted PAC files can be downloaded or referenced via its hosted URL by Proxy (formerly SWG) users. • Each FortiSASE instance supports a maximum of 32 hosted PAC files.	None
PoPs displayed on map	Support for displaying PoPs on a map during provisioning and after provisioning in *Operations > Connectivity > Infrastructure*.	None
Pre-connection posture checks	Support for enforcing pre-connection posture checks using security posture tags to allow or deny endpoints from establishing a connection to the FortiSASE Cloud Security tunnel based on their associated tags.	Only available for FortiSASE instances enabled with IPsec remote agent support
Schedule upgrades from predefined maintenance window slots	Support for administrators to schedule FortiSASE upgrades by selecting from a list of predefined maintenance window slots, directly through the FortiSASE portal	None

New feature	Description	Requirements
SCIM server support on page 50	Support for System for Cross-domain Identity Management (SCIM) for automated user provisioning from Entra ID, FortiAuthenticator, and Okta SAML IdPs. The SCIM client (IdP) sends user and group information to the SCIM server (FortiSASE as SP).	Only available for FortiSASE instances enabled with IPsec remote agent support. Not supported in instances with hybrid IPsec/SSL enabled. SCIM server support is a select availability feature. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
Secondary external log forwarding	Support for configuring and forwarding logs to a secondary external server.	None
Secure Browser on page 415	Support for integrated management of the *FortiSASE Secure Browser* extension used with unmanaged and contractor devices. With the deployment of the *FortiSASE Secure Browser* extension, administrators can gain full visibility into browser activity without deep packet inspection (DPI), can monitor and block Web-based threats, and can prevent data exfiltration.	Requires a FortiSASE instance with an Advanced or Comprehensive remote users FortiSASE subscription. Browser extension is supported in Windows and MacOS on Google Chrome and Microsoft Edge web browsers. SAML SSO users must be integrated with *FortiSASE Secure Browser*. Secure Browser is a select availability feature. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
Secure Proxy	Support for Secure Proxy that provides secure connectivity between the proxy user web client and FortiSASE using HTTPS connections.	Existing instances with Proxy enabled must run best practice for Secure Proxy migration. When using a self-hosted PAC file, must update the PAC file and redeploy it in the self-hosted environment.
Security posture tagging rule updates	Support for configuring new security posture tagging rules, including tagging based on CVEs, using negation to identify non-vulnerable devices, and combining multiple tagging rules using logical AND/OR operators	None

New feature	Description	Requirements
Security profile group performance optimization options	Support for configuring protocol options within security profile group settings, specifically, handling of unknown content types and performance optimization with handling oversized files. Also, added central management synchronization support of protocol options for handling unknown content types and handling oversized files.	None
Simplified pre-logon tunnels	Simplified pre-logon tunnels such that endpoints establish tunnels with the nearest FortiSASE Security PoP using certificate-based authentication. The previous approach was to establish tunnels using certificate-based authentication with a customer-managed FortiGate configured as an SSL or IPsec gateway.	For instances with existing pre-logon tunnels configured, the previous approach is still supported. Only the simplified approach is supported going forward after disabling existing pre-logon tunnels in all endpoint profiles.
SPA advertise hub priorities	Support for enabling Security PoPs to advertise the configured Hub Priority and SLA status using BGP community when announcing remote user's client pool prefixes to Hubs in multiple SPA Hub scenarios.	Requires licensing and configuration for SPA
SPA application monitoring	Support for Secure Private Access (SPA) application monitoring, allowing up to 20 custom applications hosted behind SPA Hubs to be defined and monitored using ICMP health check probes initiated by Security PoPs to verify application availability.	Requires licensing and configuration for SPA
SPA eBGP support to allow multiple AS on SPA hubs	Support for Secure Private Access (SPA) connectivity to SD-WAN networks deployed across different BGP autonomous systems (AS), enabling the configuration of both iBGP & eBGP peering between FortiSASE security PoPs and FortiGate SD-WAN hub/SPA Hubs.	Requires SD-WAN networks deployed across different BGP autonomous systems (AS). Requires licensing and configuration for SPA.
SPA hub monitoring	SPA Monitoring allows administrators to track the health and performance of SPA (Secure Private Access) service connections configured within FortiSASE.	Requires licensing and configuration for SPA

New feature	Description	Requirements
PA preferred hub selection based on BGP MED values	Support for enabling the BGP MED options always-compare-med and deterministic-med on FortiSASE to enable selecting a preferred SPA Hub based on MED values, particularly when receiving prefixes from SPA Hubs belonging to different ASes	Requires SD-WAN networks deployed across different BGP autonomous systems (AS). Requires licensing and configuration for SPA.
Transparent DNS redirection	Rules for DNS redirection, also known as split DNS, transparently apply to all passthrough traffic for FortiClient agent tunnels (including mobile), Edge device clients, and Proxy clients.	None
Web filter additional configuration settings	Added support for additional Web Filter configuration settings: • The ability to prioritize URL filter entries. • Logging search keywords. • Displaying the FortiGuard web filter category and subcategory in a tooltip when hovering over a domain. • Configuring a custom value for the Web Filter warning acknowledgment expiry interval.	None

Select availability features

FortiSASE includes several features with select availability, which are features that are released but not available by default for all customers. Following is a table that describes some of these features and the associated conditions when they are enabled on existing FortiSASE instances.

Select availability feature	Description	Enabled for new instances	Can be enabled for existing instances*	Associated conditions when enabled
Authenticated onboarding on page 43	Authenticating agent based remote users via SAML SSO during their client onboarding using Invitation code	No	Yes	None
BGP MED Setting on page 44	Enables configuring BGP MED options such as always-compare-med and deterministic-med on FortiSASE to improve selecting a preferred SPA Hub based on MED values, particularly when receiving prefixes from SPA Hubs belonging to different ASes.	No	Yes	None
Central management on page 45/Central management for MSSP tenants on page 46	Integration with FortiManager to provide central management for a selected set of configuration settings.	No	Yes	Requires FortiManager 7.4.4 or later for synchronizing configuration settings other than policy packages. Requires FortiManager 7.6.4 or later for synchronizing policy packages.

Select availability feature	Description	Enabled for new instances	Can be enabled for existing instances*	Associated conditions when enabled
Custom invitation codes on page 46	Create custom invitation codes, which are used to onboard non-AD-joined endpoints to a designated endpoint group and associated endpoint profile.	No	Yes	Requires the FortiSASE instance has been provisioned with Feature version support
Factory reset on page 46	Support for performing a factory reset on a FortiSASE instance that returns it to its initial provision point, disconnect all users, and deregister all endpoints.	Yes, for NFR and Advanced NFR subscriptions only	Yes	This feature is available only when logged into the FortiSASE portal with the principal FortiCloud account, where an OTP code is sent via email. This feature is not available from IAM accounts.
IPsec dead peer detection customization on page 47	For instances supporting IPsec, added support for customizing dead peer detection settings applicable to IPsec agent tunnels. Dead peer detection reestablishes IPsec agent tunnels on idle connections and cleans up dead IKE peers if required.	No	Yes	Available for FortiSASE instances with IPsec remote agent support. It is strongly recommended to schedule a maintenance window before changing dead peer detection settings. Currently connected endpoints will be disconnected from FortiSASE for a few minutes while the change is applied.

Select availability feature	Description	Enabled for new instances	Can be enabled for existing instances*	Associated conditions when enabled
Network restrictions removed on page 47	Support for removing network restrictions for customer networks.	Yes	Yes	When enabling this feature, FortiSASE service may be unavailable for brief periods of time. Completing the process requires up to a two-hour scheduled maintenance window.
Private proxy on page 48	Support for securing proxy traffic over Branch On-ramp	No	Yes	The following features must be licensed and configured: • Branch On-ramp • Secure private access A dedicated IP address must be implemented for an instance and licensed accordingly.
RBI on page 48	Isolate browser sessions of certain websites or categories in an isolated environment, which renders content safely in a remote container.	No	Yes	The secure browser extension is recommended over RBI functionality. For more information, see Secure Browser on page 50. RBI includes the following prerequisites: • RBI requires a FortiSASE instance with an Advanced or Comprehensive remote users FortiSASE subscription. See Licensing on page 722.

Select availability feature	Description	Enabled for new instances	Can be enabled for existing instances*	Associated conditions when enabled
				• The FortiSASE deployment is deployed in a Fortinet security PoP only. See Global data centers. • Proxy is enabled under *Network* > *Proxy configuration*. See Proxy configuration on page 285.
SCIM server support on page 50	Support for System for Cross-domain Identity Management (SCIM) for automated user provisioning from Entra ID, FortiAuthenticator, and Okta SAML IdPs. The SCIM client (IdP) sends user and group information to the SCIM server (FortiSASE as SP).	No	Yes	Only available for FortiSASE instances enabled with IPsec remote agent support. Not supported in instances with hybrid IPsec/SSL enabled.

Select availability feature	Description	Enabled for new instances	Can be enabled for existing instances*	Associated conditions when enabled
Secure Browser on page 50	Support for integrated management of the *FortiSASE Secure Browser* extension used with unmanaged and contractor devices. With the deployment of the *FortiSASE Secure Browser* extension, administrators can gain full visibility into browser activity without deep packet inspection (DPI), can monitor and block Web-based threats, and can prevent data exfiltration.	No	Yes	If the Secure Browser extension has already been deployed on endpoints as part of *FortiMail Workspace Security*, specifically, *FortiMail Browser Security* support, then the administrator should not enable Secure Browser in FortiSASE. Requires a FortiSASE instance with an Advanced or Comprehensive remote users FortiSASE subscription. Browser extension is supported in Windows and MacOS on Google Chrome and Microsoft Edge web browsers. SAML SSO users must be integrated with *FortiSASE Secure Browser*.

* A customer can request enabling a select availability feature for an existing FortiSASE instance by creating a new ticket with FortiCare Support.

Authenticated onboarding

This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

FortiSASE enhances security during managed endpoint client onboarding by enforcing user authentication via SAML single sign on, ensuring only authenticated users and endpoints can register. This prevents unauthorized endpoints, even those with a valid invitation code to connect to FortiSASE Management service. For details on client onboarding using Invitation code, see Client onboarding on page 730 and Managed endpoint client onboarding on page 731.

In this process, the FortiSASE Management service functions as the SAML Service Provider (SP) and integrates seamlessly with other SAML Identity providers (IdPs), including FortiAuthenticator, Okta, and Entra ID.

Once the feature is configured, following updates take effect:

- **New invitation code generation**: FortiSASE generates a new invitation code for endpoints to connecting to FortiSASE Management service, replacing previously issued invitation codes. This ensures that only endpoints that are authenticated via configured SAML IdP can connect.
- **Automatic migration to use new invitation code**: All currently managed endpoints are automatically migrated to use the new invitation code, reducing administrative overhead and ensuring a smooth transition.
- **Updated Pre-configured Installers**: Pre-configured FortiClient installers available for download from the FortiSASE Management portal are automatically updated with the latest invitation code. Organizations using these installers for bulk deployment must ensure they distribute the latest versions.
- **Enterprise Mobility management considerations**: If your organization deploys endpoints using an Enterprise Mobility Management (EMM) solution, such as Microsoft Intune, you must update the configurations to reflect the new FortiClient installer. For details, see Enterprise mobility management on page 752.
- **Re-authentication required for existing endpoint**: All previously registered endpoints are prompted and required to re-authenticate with FortiSASE. This ensures that only authorized users and devices remain connected to FortiSASE Management service.

For more information to configure Authenticated onboarding with Entra ID as IdP, see Authenticated onboarding on page 562.

BGP MED Setting

FortiSASE now supports enabling the BGP Multi-Exit Discriminator (MED) options always-compare-med and deterministic-med to improve route selection when multiple Secure Private Access (SPA) Hubs advertise the same prefix.

In multi-hub SPA deployments, particularly when receiving prefixes from SPA Hubs in different autonomous systems (ASes), the default BGP behavior ignores MED values during prefix comparison to select a SPA Hub. This can lead to suboptimal path selection, where the preferred SPA Hub is not chosen based on MED priorities. The following BGP MED options can be enabled or disabled.

- *Always Compare MED*: It forces BGP to evaluate MED values for routes received from different ASes, ensuring that MED is a consistent decision factor regardless of AS origin.
- *Deterministic MED*: It standardizes MED comparisons by grouping routes by their neighboring AS before selecting the best path, ensuring consistent and predictable results when multiple routes have the same prefix but different MED values.

The *BGP MED Settings* options is not visible in the FortiSASE portal by default. To enable this feature for a new or existing FortiSASE instance, submit a request to FortiCare Support by creating a new support ticket.

Central management

Some customers require a centralized way to manage configuration for their on-premise FortiGate devices and remote users connecting using FortiSASE. FortiSASE integrates with FortiManager to provide central management for a selected set of configuration settings. In FortiManager, configuration settings such as addresses, address groups, and security profile groups are also known as objects.

The following configuration settings synchronize from FortiManager to FortiSASE:

- Policy packages with the following configuration:
  - Firewall policies
  - Firewall proxy policies
  - Firewall schedules
  - Security posture tags
- Security profile group:
  - SSL/SSH Inspection (SSL Inspection only)
  - AntiVirus Profile
  - Web Filter Profile: support for empty custom categories that requires editing and adding web sites to them in FortiSASE after synchronization
  - IPS Profile
  - File Filter Profile support for blocking password-protected files
  - DLP Profile
  - DNS Filter
  - Application Control
  - Video Filter profile
- External feeds (associated with Web Filter and DNS Filter profiles only):
  - Web filter FQDNs
  - DNS filter domains
  - External hosts (associated with DNS Filter profiles)
- Firewall address and address group
- Services and service groups
- Security profile group
- Local, PKI, and LDAP users and user groups
- Authentication sources (SSO via SAML, LDAP, RADIUS, FSSO)

See Central Management on page 593.

This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

Considerations

- Central management supports only one-way configuration synchronization from FortiManager to FortiSASE. Therefore, avoid deleting objects from FortiManager to prevent any conflicts.

- Central management supports synchronizing a maximum of 3000 objects at once from FortiManager.
- If you attempt to synchronize any security profiles or other configuration settings from FortiManager that FortiSASE does not support, they are ignored and not synchronized to FortiSASE.

  FortiSASE treats all flow-based features synchronized from FortiManager as proxy-based features (best match).
- After enabling central management, objects synchronized from FortiManager to FortiSASE are considered read-only and you cannot modify them directly in FortiSASE.

Central management for MSSP tenants

For MSSPs, FortiSASE supports central management for synchronizing multiple tenants' FortiSASE instances (MSSP tenants) from a single FortiManager instance or from multiple FortiManager instances.

- A FortiManager key, if configured, allows a FortiManager appliance registered under a FortiCare account belonging to a parent Organization Unit (OU) to manage the FortiSASE tenant.
- The FortiManager key can be revoked to only allow connections from FortiManager appliances registered to the current FortiCare account and disable connections from parent OU FortiManagers.
- The FortiManager key will be strictly matched and must match in both FortiManager and FortiSASE connector settings. If a key is revoked on the FortiSASE tenant, then the key must also be removed on the FortiManager intending to manage the tenant.

Central management is still a select availability feature that requires a Fortinet Support ticket to enable it on new and existing instances.

See Central management for MSSP tenants on page 712.

Custom invitation codes

FortiSASE supports creating custom invitation codes, which you can use to onboard non-Active Directory-joined endpoints to a designated endpoint group and associated endpoint profile. Once onboarded, you can manually reassign endpoints.

Support for custom invitation codes is a select availability feature in FortiSASE that is not enabled by default on new instances and requires that the instance has been provisioned with Feature version support. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

See Invitation codes on page 478.

Factory reset

When the Prerequisites on page 47 below are met, FortiSASE supports performing a factory reset on a FortiSASE instance that returns it to its initial provision point, disconnect all users, and deregister all endpoints.

> ⚠ After running a factory reset on a FortiSASE instance, **all data will be permanently deleted**, including:
>
> - Profiles, policies, and objects
> - Edge and On-ramp device configurations
> - Log data
> - Invitation codes and endpoint profiles

See Factory reset on page 717.

Prerequisites

- This feature is enabled by default on FortiSASE instances with the Not-for-Resale (NFR) and Advanced NFR subscriptions applied.
- For FortiSASE instances with other licenses, this is a select availability feature that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE Feature instance, create a new ticket with FortiCare Support.
- This feature is available only when logged into the FortiSASE portal with the principal FortiCloud account, where an OTP code is sent via email. This feature is not available from IAM accounts.

IPsec dead peer detection customization

For instances supporting IPsec, FortiSASE supports customizing dead peer detection settings applicable to IPsec agent tunnels. Dead peer detection reestablishes IPsec agent tunnels on idle connections and cleans up dead IKE peers if required.

This is a select availability feature. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

See IPsec dead peer detection customization on page 471.

Network restrictions removed

FortiSASE includes support for removing network restrictions.

The following networks are available for your network configuration:

- 10.0.0.0/8
- 100.64.0.0/10 (except 100.65.0.0/16)
- 172.16.0.0/12
- 192.168.0.0/16

This feature is a select availability feature in FortiSASE that is not enabled by default on existing instances created prior to FortiSASE 23.4.b. If you require this feature for your existing FortiSASE instance, create a new ticket with FortiCare Support.

With the requested network restrictions removed, note the following:

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for tunnel traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

Private proxy

FortiSASE supports private proxy. With private proxy, clients route their traffic to an on-premises Branch On-ramp device, which further routes traffic to an encapsulated and encrypted tunnel to FortiSASE. This configuration ensures traffic in transit between the proxy client and FortiSASE is secure.

Similar to proxy, private proxy allows users to access the Internet securely over HTTP and HTTPS protocols and to access private resources securely behind a FortiSASE SPA hub.

This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

See Private proxy on page 287.

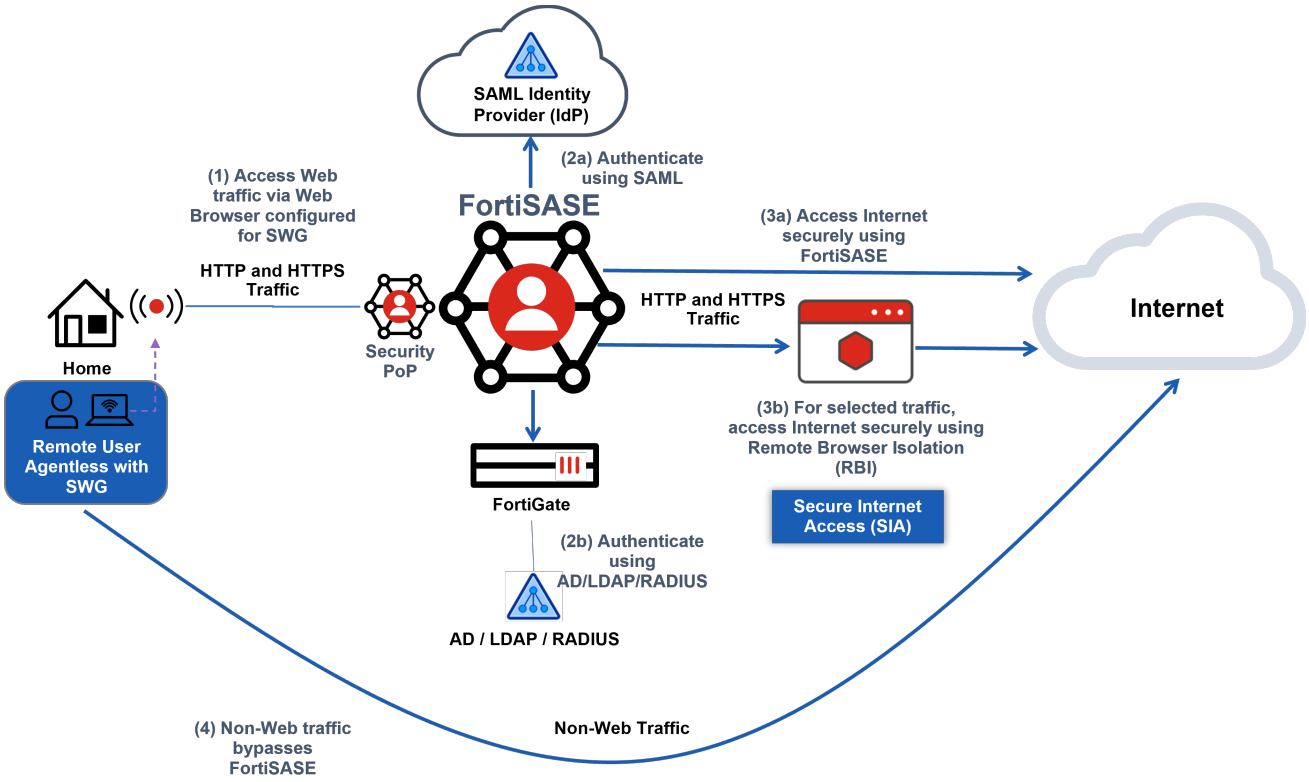
RBI

Remote browser isolation (RBI) is a select availability feature that is disabled by default for all instances where it is not already enabled. The recommended alternative to RBI functionality is the Secure Browser extension. See Secure Browser on page 415.

To mitigate web-based threats for end users proxying traffic through FortiSASE, you can enable remote browser isolation (RBI) to isolate browser sessions of certain websites or categories in an isolated environment, which renders content safely in a remote container.

FortiSASE supports RBI for proxy users.

See RBI on page 721.



Prerequisites

The following requirements must be met for the feature to be available in the GUI:

- RBI requires a FortiSASE instance with an Advanced or Comprehensive remote users FortiSASE subscription. See Licensing on page 722.
- The FortiSASE deployment is deployed in a Fortinet security PoP only. See Global data centers.
- Proxy is enabled under *Network* > *Proxy configuration*. See Proxy configuration on page 285.

Considerations

- Each instance is entitled to a maximum isolation data per month as listed in RBI. When the limit is exceeded, traffic configured to be isolated will be blocked for all users.
- When configuring RBI with SWG SSO, ensure the security profile group used for the "CSP_REPORT" proxy policy is using certificate inspection instead of deep inspection.

Licensing

The FortiSASE instance must have an Advanced or Comprehensive remote users subscription applied to it. For limitations, see RBI.

SCIM server support

FortiSASE supports acting as a System for Cross-domain Identity Management (SCIM) server for automated user provisioning from Entra ID, FortiAuthenticator, and Okta SAML IdPs. The SCIM client (IdP) sends user and group information to the SCIM server (FortiSASE as SP).

See SCIM server support on page 564.

Prerequisites

- SCIM server support is a select availability feature. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
- Only available for FortiSASE instances enabled with IPsec remote agent support.
- Not supported in instances with hybrid IPsec/SSL enabled.

Secure Browser

FortiSASE supports integrated management of the FortiSASE Secure Browser extension used with unmanaged and contractor devices or deployed on top of existing agent (FortiClient) and agentless (Proxy) deployments. With the deployment of the FortiSASE Secure Browser extension, administrators can gain full visibility into browser activity without deep inspection, can monitor and block web-based threats, and can prevent data exfiltration.

The web browser is the most common application used on endpoints for accessing internet and local applications. This makes it the most common vector for highly evasive attacks such as phishing, malware and other malicious content and files. In addition, the browser is also a source of data loss of sensitive information through copy-and-paste of content to file formats, physical printing, or by unintentionally screen sharing during remote meetings.

FortiSASE Secure Browser through a browser extension for supported web browsers including Google Chrome and Microsoft Edge can mitigate client-side threats on endpoints themselves and complement the protection already provided by steering web traffic to FortiSASE using agent and agentless solutions.

This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

Prerequisites

See Secure Browser.

Considerations

- Currently, the *Display watermark* website display option is not applied when saving a local copy of a website.
- Currently, the *Pasting text copied from specified websites* option for URL domain group overrides is not applied for websites including AI applications containing code blocks with an inline copy button.
- In private browsing mode, browser extensions are disabled by default and must be enabled by the end user. For most deployments, it is highly recommended to disable private browsing mode (Incognito mode in Google Chrome and InPrivate mode in Microsoft Edge) in web browsers on all devices.
- IdP attribute mapping is important for user assignment rules, used to match the contents of attributes to assign secure browser profiles to specific users or groups of users. *Email* is a required attribute for Secure Browser user assignment rules.

See Secure Browser on page 415.

Beta features

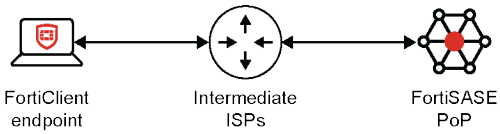
Features marked as "Beta" are available to use but may have constraints. These features are subject to continual improvements. Feedback is encouraged. Following is a table that describes some of these features and the associated conditions when you enable them on existing FortiSASE instances.

Beta feature	Description	Enabled for new instances	Can be enabled for existing instances*	Associated conditions when enabled
Digital experience: TCP latency on page 53	In *View Endpoint Details > Digital Experience > Network metrics*, display a chart of TCP latency from the endpoint to the security PoP. Digital experience monitoring (DEM) requires an Advanced or Comprehensive remote users FortiSASE subscription. Instances with a Standard or Not-for-Resale subscription can opt in for a free 90-day DEM trial.	No	Yes	The endpoint must have an active management connection via invitation code. The DEM agent is installed on an endpoint with a *DEM agent status* of *Online*. For tunnel-connected Windows endpoints, to ensure TCP latency is being measured for the underlay network, you must configure an FQDN steering bypass destination using the Turbo URL. It may take up to one day after enabling this feature for the TCP latency chart to populate for endpoints.

* A customer can request enabling a beta feature for an existing FortiSASE instance by creating a new ticket with FortiCare Support.

Digital experience: TCP latency

Digital experience monitoring (DEM) allows you to view TCP latency metrics for managed endpoints, offering deeper visibility into the WAN (underlay) network performance from the endpoint to the FortiSASE security PoP.



To support the viewing of TCP latency metrics, the following must be in place:

- The endpoint must have an active management connection via invitation code.
- The DEM agent is installed on the endpoint with a *DEM agent status* of *Online*.

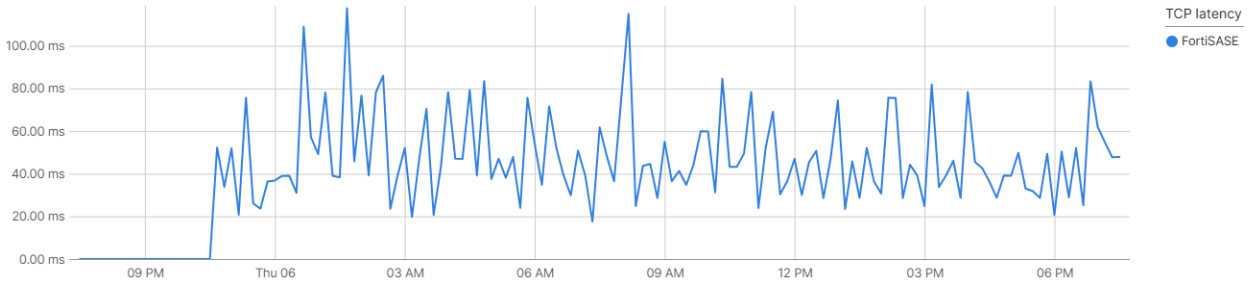
For tunnel-connected Windows endpoints, to ensure TCP latency is being measured for the underlay network, perform these steps:

1. In *Endpoint management* > *Endpoint profiles*, edit the applicable profile for the endpoint.
2. In the endpoint profile *Connection* tab, create an FQDN steering bypass destination using the Turbo URL of the FortiSASE instance. You can be obtain this from the *Base URL* in *Access & authentication* > *SSO*. See Steering bypass destinations on page 453.

It may take up to one day after enabling this feature for the TCP latency chart to populate for endpoints.

To view TCP latency for an endpoint:

1. Go to *Operations* > *Connectivity* > *Managed Endpoints*.
2. Select the desired endpoint and click *View Endpoint Details*. A slide in appears.
3. Click the *Digital Experience* tab.
4. Click the *Network metrics* subtab and observe the data in the TCP latency chart.



This is a beta feature that is not enabled by default on new instances. It has several constraints and is subject to continual improvements. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

IPsec remote agent support

> ⚠ Starting in FortiSASE Feature 25.4.b, IPsec remote agent support for an instance previously configured with SSL remote agent support no longer involves data loss and client redeployment since resetting your FortiSASE instance to default is no longer required. Nevertheless, a scheduled maintenance window is required because temporary network disruption, including user sessions, still occurs. See SSL to IPsec transition mode on page 254.

FortiSASE supports remote user connectivity using IPsec instead of SSL.

- The recommended version for instances requiring IPsec remote agent support is dependent on when the instance was created:
  - For new instances, the recommended version is FortiClient 7.4.6.
  - For existing instances created before 25.4.c, the recommended version is FortiClient 7.2.14.
- IPsec remote agent support is enabled by default on new instances starting in 24.4.b.1.

To support IPsec for remote agents:

- Remote users must install FortiClient 7.2 or 7.4 on their endpoints, as needed.
- Administrators must configure and use single sign on, RADIUS, or local authentication for agent authentication.

FortiSASE supports these features for IPsec remote agents:

- Split tunneling
- Split DNS
- Agent policies

Global connection settings are common settings that apply to all endpoint profiles, including the Default endpoint profile. Therefore, any changes made to these settings apply to all endpoints across different endpoint profiles.

To access the global connection settings, go to *Endpoint management* > *Endpoint profiles* and from the toolbar, select *Settings*.

Settings	Description	Default	Minimum value (seconds)	Maximum value (seconds)
Authentication settings (only for agent-based endpoints)				

Settings		Description	Default	Minimum value (seconds)	Maximum value (seconds)
	Authentication timeout	Duration, in seconds, after which remote users must reauthenticate to connect to FortiSASE secure internet access, regardless of whether the user session is active or idle.	If enabled, 86400 seconds (24 hours)	120 (2 minutes)	172800 (48 hours)

For a new FortiSASE instance, this feature is enabled by default. To add support for this feature to your existing FortiSASE Feature instance, run the *FortiSASE Cloud Security tunnel – hybrid IPsec/SSL mode* best practice in *Operations > Administration > Software audit & version*. See SSL to IPsec transition mode on page 254.

Considerations

- LDAP authentication is unavailable for remote agents using IPsec.
- FortiClient (Windows) endpoints support application-based split tunnel or full tunnel with FortiSASE. FortiClient endpoints on other platforms support full tunnel. See Supported FortiClient features.

Tunnel settings

FortiSASE instances with IPsec support use different tunnel settings, including varying Diffie-Hellman (DH) groups, depending on the connection type and whether you apply the settings to FortiSASE security PoPs or FortiClient.

FortiSASE security PoPs

The default tunnel settings that FortiSASE security PoPs use for secure internet access (SIA) are as follows:

Setting	Value
Tunnel settings	

Setting	Value
IKE version	*Version 2*
Mode Config	Enabled
Phase 1	
IKE proposal	Encryption: AES128, Authentication: SHA256 Encryption: AES256, Authentication: SHA256 Encryption: AES128-GCM, Authentication: PRFSHA256 Encryption: AES256-GCM, Authentication: PRFSHA384 Encryption: Chacha20-Poly1305, Authentication: PRFSHA2
DH Group	5, 15
Key Life	86400 seconds
Dead Peer Detection	Enabled
NAT Traversal	
Phase 2	
IKE proposal	Encryption: AES128, Authentication: SHA1 Encryption: AES256, Authentication: SHA1 Encryption: AES128, Authentication: SHA256 Encryption: AES256, Authentication: SHA256 Encryption: AES128-GCM, Authentication: None Encryption: AES256-GCM, Authentication: None Encryption: Chacha20-Poly1305, Authentication: None
Key Life	43200 seconds
Replay Detection	Enabled
Perfect Forward Secrecy (PFS)	
DH Group	5, 15

FortiClient

The following are the tunnel settings that the FortiSASE endpoint management service configures on FortiClient. These settings are used when FortiClient establishes a connection to FortiSASE security PoPs for SIA.

Setting	Value
Tunnel settings	
IKE version	*Version 2*

Setting	Value
Mode Config	Enabled
Phase 1	
IKE proposal	Encryption: AES128, Authentication: SHA256 Encryption: AES256, Authentication: SHA256
DH Group	5, 15
Key Life	86400 seconds
Dead Peer Detection	Enabled
NAT Traversal	
Phase 2	
IKE proposal	Encryption: AES128, Authentication: SHA1 Encryption: AES256, Authentication: SHA1
Key Life	43200 seconds
Replay Detection	Enabled
Perfect Forward Secrecy (PFS)	
DH Group	15

FortiSASE uses these settings when FortiClient establishes a connection to custom or alternative IPsec tunnels defined in endpoint profiles in *Endpoint management > Endpoint profiles* under *Custom tunnels*. You must apply these settings to custom or alternative IPsec gateways. See Custom tunnels on page 455.

Setting	Value
Tunnel settings	
IKE version	*Version 2*
Mode Config	Enabled
Phase 1	
IKE proposal	Encryption: AES128, Authentication: SHA256 Encryption: AES256, Authentication: SHA256
DH Group	15
Key Life	86400 seconds
Dead Peer Detection	Enabled
NAT Traversal	Enabled
Phase 2	
IKE proposal	Encryption: AES128, Authentication: SHA1 Encryption: AES256, Authentication: SHA1

Setting	Value
Key Life	43200 seconds
Replay Detection	Enabled
Perfect Forward Secrecy (PFS)	Enabled
DH Group	15

Monitoring

FortiSASE includes dashboards and monitors so you can easily monitor device inventory, security threats, traffic, and network health. FortiSASE includes the following default dashboards:

Dashboard	Description
Status	Provides an overview of your current FortiSASE environment and endpoint status.
Security	Displays the status of security features for Internet Access and Private Access traffic for the selected Profile Group and a summary of vulnerabilities detected on endpoints managed by FortiSASE.
FortiView	Comprehensive monitoring system for your network that integrates real-time and historical data into a single view. You can use it to log and monitor threats to networks, filter data on multiple levels, and keep track of administrative activity.

Adding a custom dashboard

You can create and modify a dashboard of a customizable widget array.

To add a custom dashboard:

1. Under *Monitoring* > *Dashboards*, click *+*.
2. In *Add Dashboard*, enter the desired name. Click *OK*.
3. The blank dashboard displays. Click *Add Widget*.
4. In the *Add Dashboard Widget* pane, select the desired widget to add to the dashboard. Repeat to add all desired widgets.
5. You can further customize the dashboard by moving and resizing widgets. To move a widget, hover over the widget title, then click and drag the widget to the desired location. To resize the widget, from the menu in the upper right corner of the widget, select *Resize*, and select the desired number of spaces for the widget to occupy. The following shows a custom dashboard that differs from the default status and security dashboards:

Resetting all dashboards

You can reset all dashboards. This deletes all custom dashboards from FortiSASE and resets the Status and Security dashboards to their default configurations. If you deleted a default dashboard, the reset restores it.

To reset all dashboards:

1. Click the *Actions* icon beside the + button under *Monitoring* > *Dashboards*.
2. Select *Reset all Dashboards*.
3. In the confirmation message, click *OK*.

Drilling down on vulnerabilities

On the *Security* dashboard, you can drill down on vulnerabilities and schedule automatic patching of selected vulnerabilities if configured in an endpoint profile.

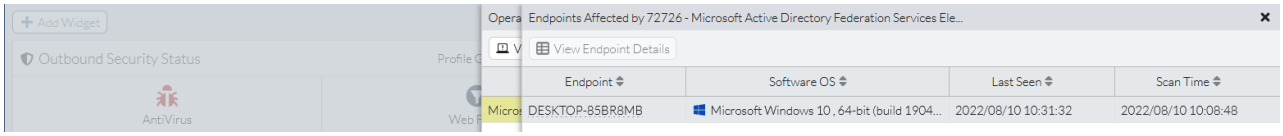
To drill down on vulnerabilities that belong to the same category:

1. Go to *Monitoring* > *Security*.
2. In the *Vulnerability summary* widget, click the desired category, such as *Operating System*. FortiSASE displays a pane that shows all endpoints that have operating system vulnerabilities.

To drill down to view all endpoints that certain vulnerabilities affect:

1. Go to *Monitoring* > *Security*.
2. In the *Vulnerability summary* widget, click the desired category, such as *Operating System*, or risk level, such as *Medium*.
3. FortiSASE displays a pane that shows all endpoints that have the applicable vulnerabilities. To view endpoints that a specific vulnerability affects, do one of the following:
   - Click the desired vulnerability, then click *View affected endpoints*.
   - Right-click the endpoint, then click *View Affected Endpoints*.

   FortiSASE displays information for all endpoints that vulnerability affects.

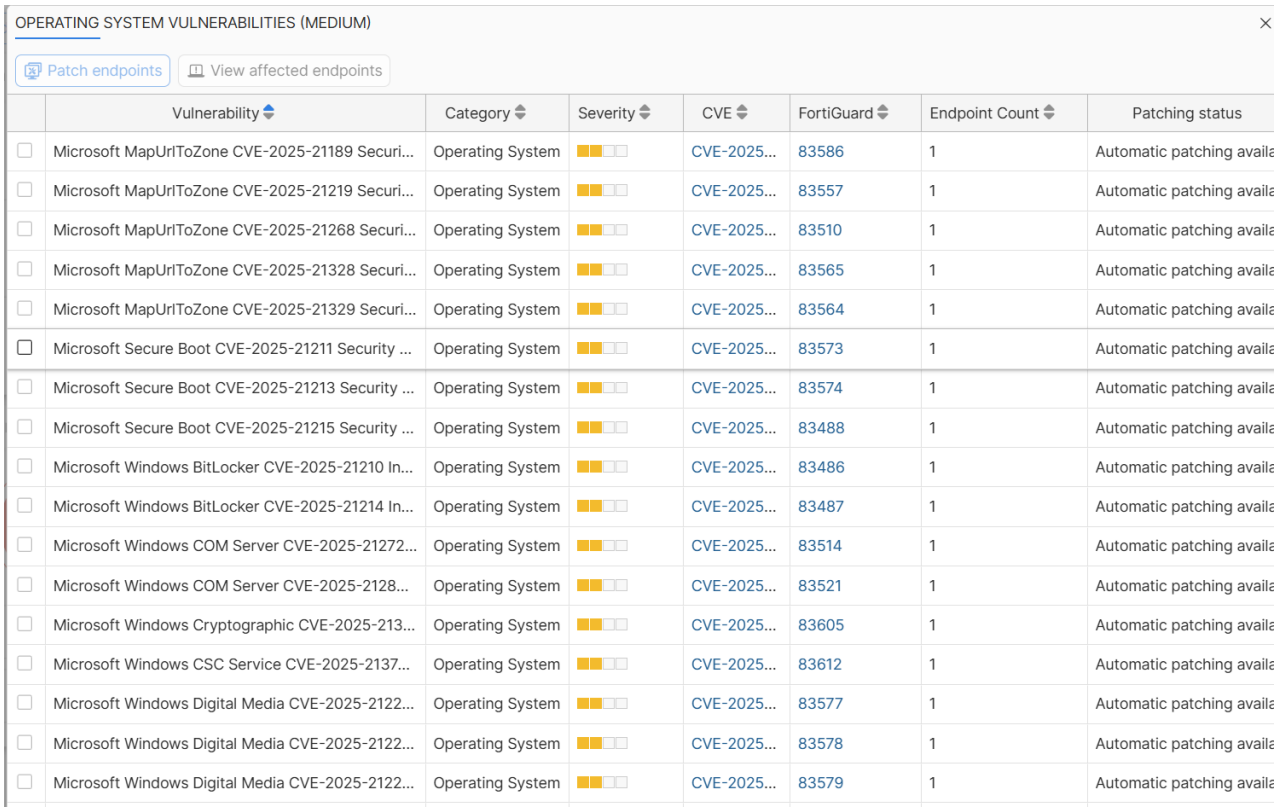


As described below, you can also schedule automatically patching selected individual vulnerabilities on-demand from the *Vulnerability summary* widget in *Monitoring* > *Security*.

Automatically patch vulnerabilities when configured with the *Minimum severity level* in an endpoint profile should be sufficient to automatically patch vulnerabilities after performing vulnerability scans. See Protection on page 459.

To schedule automatic patching of selected vulnerabilities when configured in an endpoint profile:

1. Go to *Monitoring* > *Security*.
2. In the *Vulnerability summary* widget, click the desired category, such as *Operating System*, or risk level, such as *Medium*. FortiSASE displays a pane that shows all endpoints that have the applicable vulnerabilities. Note the following *Patching status* values:



Patching Status value	Description
Manual patching required	Vulnerability requires endpoint users to download and install software to patch it. This vulnerability cannot be patched using the automatic patching feature.
Automatic patching available	Vulnerability can be patched using the automatic patching feature and patch software can be scheduled to be downloaded and installed automatically on all affected endpoints.
Scheduled	Patch software has been scheduled to be automatically downloaded and installed on affected endpoints after they receive the next configuration update from FortiSASE Endpoint Management Service
Failed	Automatic patching has failed on affected endpoints. Ensure they have network connectivity and perform troubleshooting prior to rescheduling the next automatic patch request.

3. To schedule automatic patching of selected vulnerabilities:
   a. Select one or more vulnerabilities with *Patching status* of *Automatic patching available* by clicking the checkbox next to the vulnerability.
   b. Click *Patch endpoints*. You should observe the message *Successfully scheduled endpoints to be patched*.
4. The *Patching status* of the selected vulnerabilities should be changed to *Scheduled* indicating that FortiSASE has sent the request to endpoints to perform automatic patching. Upon receiving the next configuration update from the Endpoint Management Service (EMS), affected endpoints initiate automatic vulnerability patching.

FortiView monitors

The following FortiView monitors are available in FortiSASE:

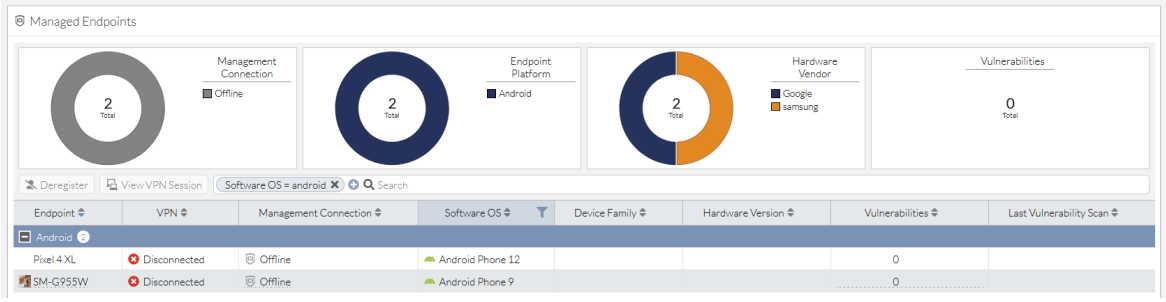
Dashboard	Displays...
Sources	Sources by traffic volume and drilldown by source.
Edge Devices	Edge devices by traffic volume and drilldown by Edge device.
Destinations	Destinations by traffic volume and drilldown by destination.
Applications	Applications by traffic volume and drilldown by application.
Inline-CASB	Cloud applications detected by Application Control with Inline-CASB and drilldown by application.
Websites	Websites by session count and drilldown by domain.
Policies	Policies by traffic volume and drilldown by policy number.
Sessions	Sessions by traffic source.
VPN	Tunnel connections by user.
Threats	Threats and drilldown by threat.
WiFi clients	WiFi clients by traffic volume.

Adding a custom monitor

You can create and modify a custom monitor. For example, consider that you want to create a monitor to monitor all managed Android endpoints. You can create a custom monitor based on the Managed Endpoints monitor, and apply a filter to display only Android endpoints. You can simply view this custom monitor whenever you want to monitor your Android endpoints.

To add a custom monitor:

1. Under *Monitoring* > *Monitors*, click +.
2. In *Add Monitor*, select the desired FortiView or status monitor. The example selects *Managed Endpoints*.
3. In the *Name* field, enter the desired name. Click *OK*. You can further customize the monitor by applying filters or configuring the sort order on columns as desired. The example has a filter applied to display only Android endpoints.



Resetting all monitors

You can reset all monitors. This deletes all custom monitors from FortiSASE and resets the default monitors to their default configurations. If you deleted a default monitor, the reset restores it.

To reset all dashboards:

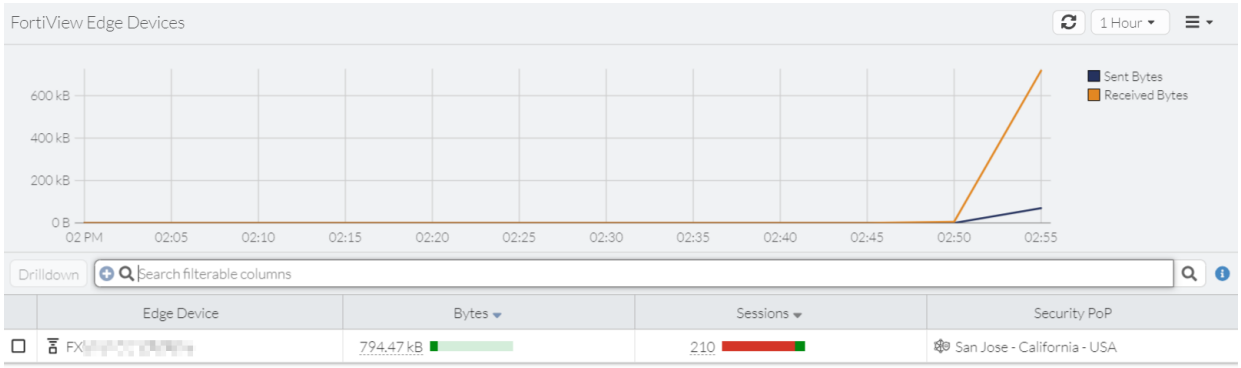
1. Click the *Actions* icon beside the + button under *Monitoring* > *Monitors*.
2. Select *Reset all Monitors*.
3. In the confirmation, click *OK*.

Monitoring edge device bandwidth usage

You can view FortiExtender devices' bandwidth usage from the FortiView Edge Device monitor.

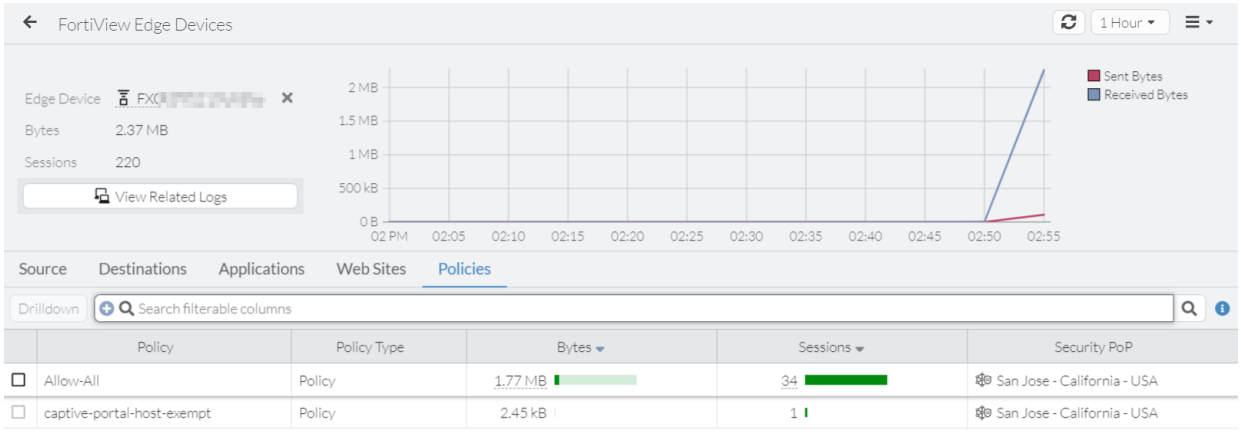
To drill down on edge device bandwidth usage data:

1. Go to *Monitoring* > *Monitors* > *FortiView Edge Devices*.

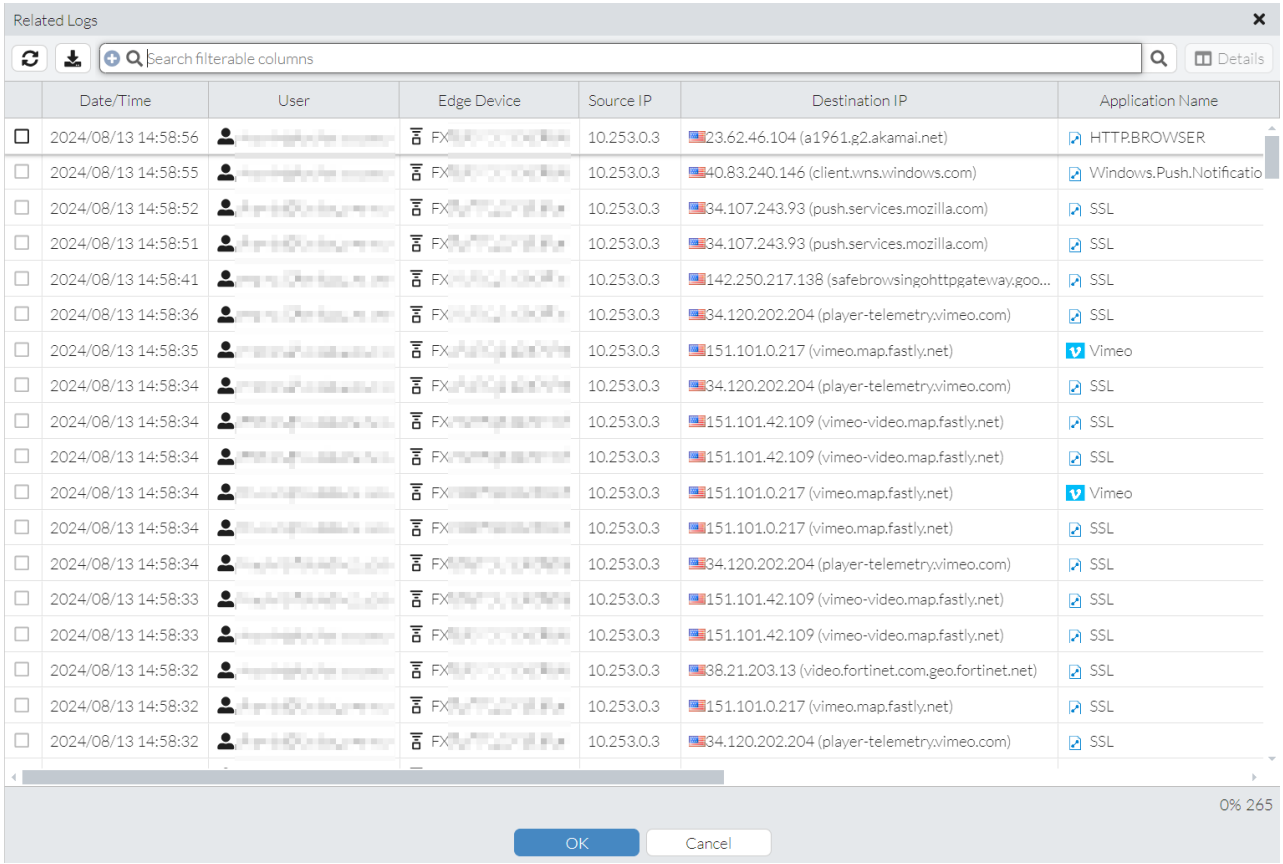


2. Select the desired edge device.
3. Click *Drilldown*.

4. Go to the *Source*, *Destinations*, *Applications*, *Web Sites*, and *Policies* tabs to view the respective traffic.



5. Click *View Related Logs* to view sessions associated with the selected tab.



API-based CASB monitoring

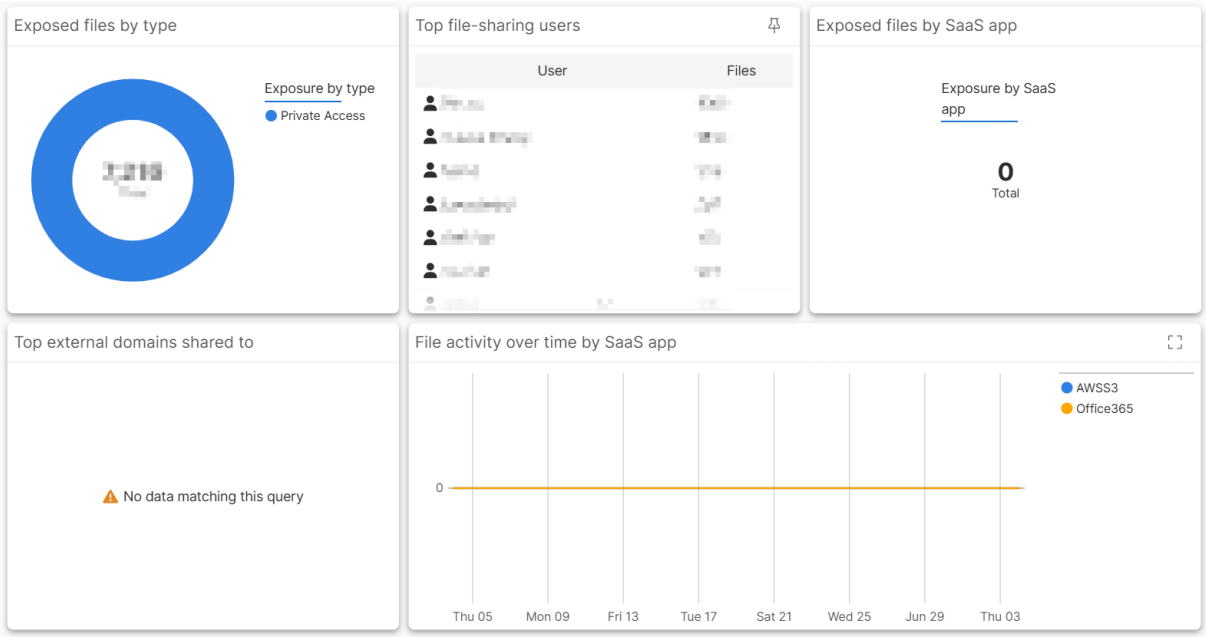
You can view API-based CASB status and information through the corresponding pages.

Dashboard	Displays...
Overview	Overview and key usage statistics of onboarded cloud application
Applications	Connection status of onboarded cloud applications
Files	Files that the API-based CASB monitors
Alerts	Log of alerts of API-based CASB policies that user activity triggered

These pages require supported cloud applications to first be onboarded with the API-based CASB. See API-based CASB on page 591.

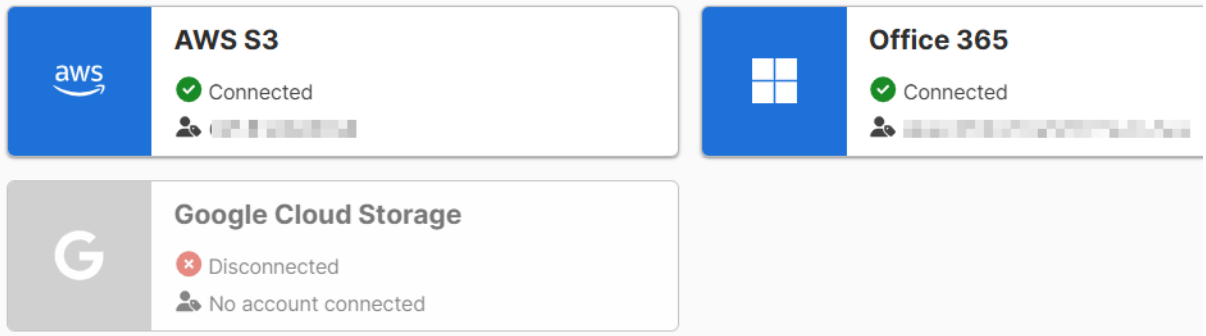
Overview

In *Monitoring* > *Dashboards* > *API-based CASB* > *Overview*, API-based CASB presents an overview of the cloud application and visually summarizes key usage statistics depending on category, and trends over different time periods. The page presents this overview and acts as the starting point for visibility into the cloud application.



Applications

In *Monitoring* > *Dashboards* > *API-based CASB* > *Applications*, the API-based CASB provides status of the onboarded cloud applications.



You can click on the card for any previously onboarded cloud application to drill down further with *Alerts* and *Files* tabs on analytics focused on the specific cloud application. You can drill down further by clicking within elements on each tab.

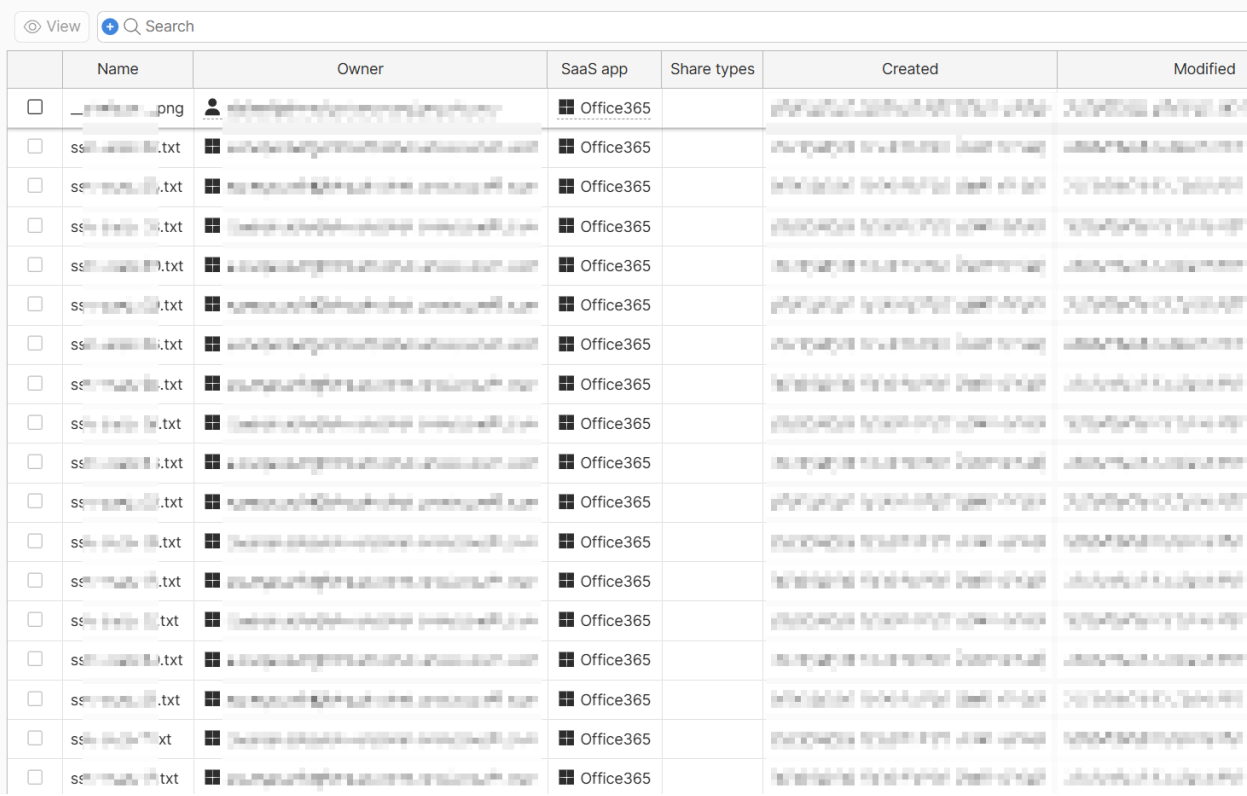
By clicking on the card for a supported cloud application that has not yet been onboarded, you will be taken to the *Security > API-based CASB > Applications* page where you can click on the card and select *Connect* to start the onboarding process.

The API-based CASB feature supports onboarding these cloud applications:

- AWS S3
- Google Cloud Storage
- Office 365

Files

In the *Monitoring > Dashboards > API-based CASB > Files* page, the API-based CASB feature shows all the files it currently monitors. When the cloud application is first added to the API-based CASB feature, files are pulled from the cloud application account to the *Files* page. Thereafter, API-based CASB feature automatically updates the *Files* page when users attempt to access files on the cloud application account.



Alerts

In the *Monitoring* > *Dashboards* > *API-based CASB* > *Alerts* page, the API-based CASB feature provides a log of alerts when any of the enabled policies is triggered by user activity.

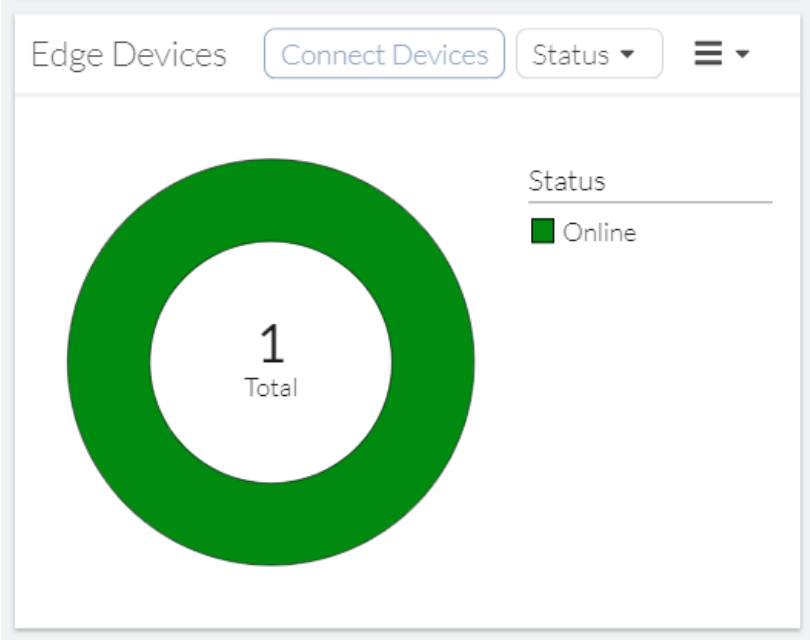
Edge Devices

You can view edge devices through the corresponding status widget, which displays online status, security PoPs, and subscriptions through corresponding dropdown menus.

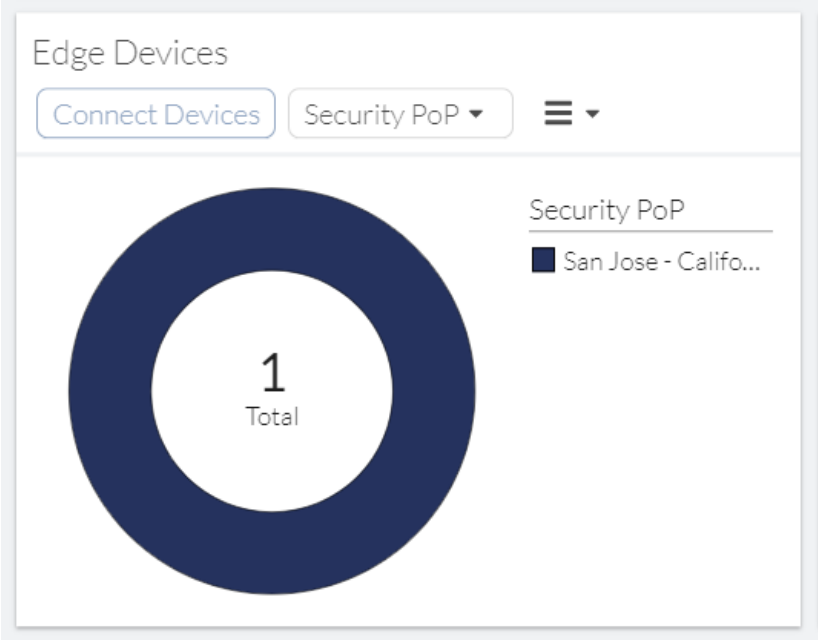
In the following example, FortiSASE manages an edge device, the FortiExtender 200F. It is properly registered in the same FortiCloud account as FortiSASE and licensed with a FortiSASE subscription.

To view edge device details:

1. Go to *Monitoring* > *Dashboards* > *Status* and in the *Edge devices* widget, observe *Status* is selected in the dropdown menu, by default, and shows the current status of edge devices.



2. Click *Security PoP* in the dropdown menu and observe the Security PoP that the edge device is connected to.



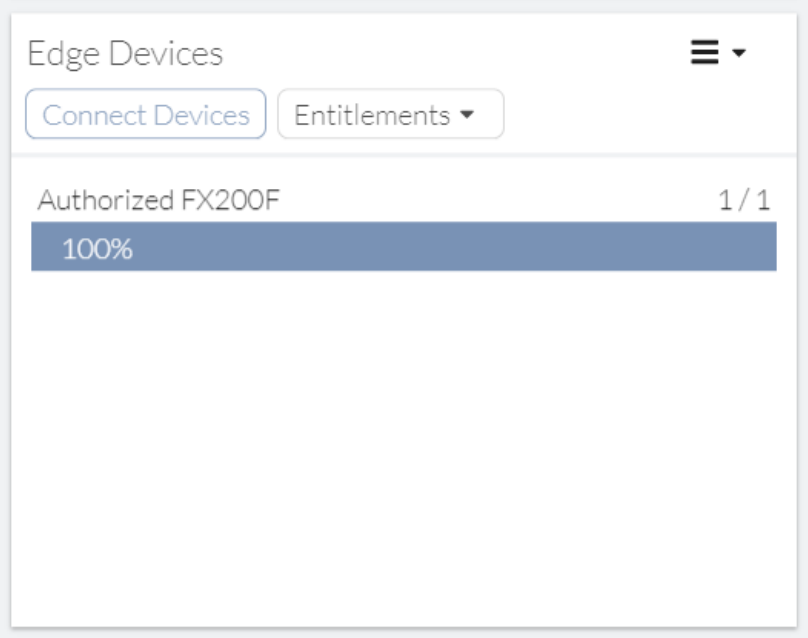
3. Click on the *Entitlements* dropdown menu.

> The *Entitlements* dropdown menu is only available if you have applied at least one FortiSASE subscription to a FortiExtender device.

4. Within the *Entitlements* view, view the following statuses:

- Number of authorized FortiExtender devices
- Total number of subscriptions

In the following screenshot, the *Edge Devices* widget's *Entitlements* view displays one authorized edge device management subscription. In this case, FortiSASE can manage only one edge device and this edge device is already authorized.

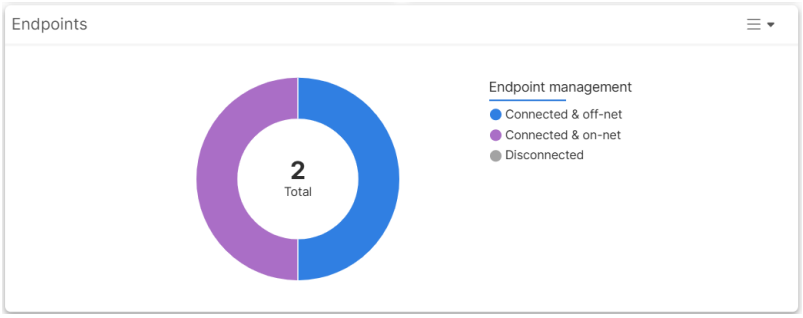


Endpoints

You can monitor FortiClient managed endpoints through the *Endpoints* status widget, which displays endpoint management with the following states:

Endpoint management state	Description
Connected	Indicates endpoints with endpoint management status of *Online* and with on-net rules not configured on the matching endpoint profile.
Connected & off-net	Indicates endpoints with endpoint management status of *Online*, with on-net rules configured on the matching endpoint profile, and with on-net rules not being satisfied indicating the endpoints are off-net.
Connected & on-net	Indicates endpoints with endpoint management status of *Online*, with on-net rules configured on the matching endpoint profile, and with on-net rules being satisfied indicating the endpoints are on-net.
Disconnected	Indicates endpoints with endpoint management status of *Offline*.

In the following example, with the *Endpoints* widget visible and resized to display the endpoint management state clearly, FortiSASE is managing two endpoints, one in the *Connected & off-net* state and another in the *Connected & on-net* state.



Operations

In *Operations*, you can configure the following:

- Digital Experience Monitoring on page 71
- Endpoints on page 82
- Connected users on page 97
- Connected wireless clients on page 100
- SPA on page 101
- Edge devices on page 149
- On-ramp tunnel on page 196
- Reports on page 234
- Logs on page 237
- Administration on page 252

Digital Experience Monitoring

Digital experience monitoring (DEM) serves as a valuable tool for network administrators in diagnosing connectivity and network issues for remote users along with monitoring their real-time network bandwidth, CPU, memory, and hard disk usage. It also enables tracing end-to-end network performance, from an endpoint to a FortiSASE point of presence (PoP) and to a SaaS application using a DEM agent installed on the endpoint. DEM provides insights into potential network issues between a FortiClient endpoint, security PoP, SaaS applications, and the internet service providers (ISP) connecting them.

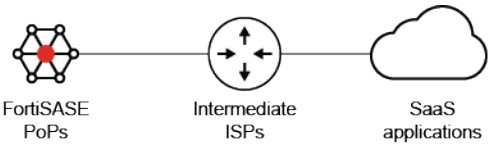
To navigate DEM:

1. Go to *Operations* > *Connectivity* > *Endpoints* to see the list of managed and unmanaged endpoints.
2. Select an endpoint and click *View Endpoint Details*. A slide-in appears and the following endpoint details are visible:

GUI option	Description
Details	Shows general endpoint information such as the hostname, management connection to FortiSASE, and tunnel status. See Endpoints on page 82. DEM displays information on all detected network interfaces and their IP addresses, and a real-time network bandwidth graph that shows total bandwidth used by endpoint.
FortiClient	Shows FortiClient information, such as the version and features installed.
Installed Applications	Shows a list of software installed on the endpoint. See Application inventory for managed endpoints on page 89.

GUI option	Description
FortiGuard Forensics Analysis	Shows information related to the FortiGuard forensics analysis. See FortiGuard Forensics Analysis on page 87.
Hardware	Shows information regarding endpoint hardware such as vendor, model, and CPU. It displays a real-time graph that shows total hard disk, CPU, and memory usage on the endpoint.
Digital Experience	Shows DEM agent status: offline, online, or agent is not installed. To get end-to-end network performance visibility from the endpoint to a particular SaaS application, run a trace job for the selected endpoint. SeeTo run a trace job on an endpoint: on page 72.
Packet Capture	Perform real-time packet capture on FortiSASE security points of presence (PoP) to monitor the traffic of agent-based FortiClient endpoints and agentless proxy users that are successfully authenticated and connected to FortiSASE secure internet access. See Packet capture on page 98.

DEM displays a list of SaaS applications and health check metrics for first-mile connectivity between the geographical security PoPs provisioned for your FortiSASE instance and SaaS applications, as the following diagram shows.



Running a trace job on an endpoint

FortiSASE can run a trace job on the endpoint using DEM agent. This assists in troubleshooting various performance bottlenecks in the network by providing link metrics such as average RTT and packet loss on various hops of the network.

To run the trace job, the following must be true:

- DEM agent is installed on endpoint.
- *DEM agent status* must be *Online* under *Digital Experience* tab under *Operations > Connectivity > Managed Endpoints> View Endpoint Details* for selected endpoint.
- Application Control security profile and internet access firewall policy must not block ping or ICMP traffic.

To run a trace job on an endpoint:

1. Go to *Operations > Connectivity > Endpoints*.
2. Select the desired endpoint and click *View Endpoint Details*. A slide in appears.
3. Click the *Digital Experience* tab.
4. Click the *Generate traceroute* subtab. The *DEM agent status* must be *Online*. From the *SaaS application* dropdown list, select an application to test the connection to from the selected endpoint.
5. Under *Monitor for*, configure a suitable time to run the trace job for the specified duration.

6. Click *Start* to schedule the job.

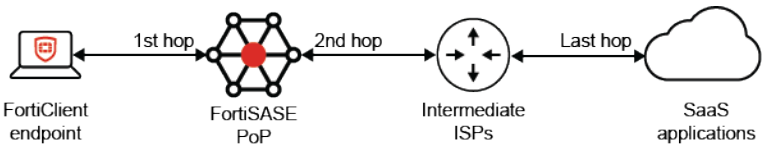
   If you interrupt the current running job by clicking *Stop*, FortiSASE deletes the historical traceroute data collected so far and you must restart the job.

7. The first trace job output displays within five minutes after clicking *Start*, after which FortiSASE presents output every three minutes until the selected *Monitor for* duration expires. The results display in two tabs: *Tabular results* and *Path diagram*. The *Path diagram* tab displays a path diagram for each traceroute that was completed. You can use the searchbar to search for specific hops, and highlight specific latency or packet loss thresholds of interest. For example, you can highlight hops with an average packet loss greater than 60%. FortiSASE stores the results displayed for three days only for the latest trace job. To analyze the trace job, see Analyzing trace job result on page 73.

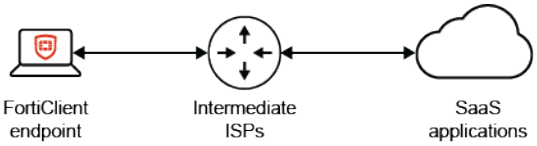
Analyzing trace job result

The trace job output gives information on average RTT (ms) and packet loss (%) on various hops of the network. To identify the hop accurately, understanding whether the selected endpoint is connected to the FortiSASE tunnel for secure internet access (SIA) or not is important.

When an endpoint is connected to the FortiSASE tunnel, it accesses SaaS applications using SIA. Thus, the first and second hops of the trace are the entry and exit interface IP address of the security PoP that the endpoint is connected to. The remaining hops are the ISPs in between until the last hop, which is the selected SaaS application.



When an endpoint is not connected to the FortiSASE tunnel, it accesses SaaS applications directly using its local internet breakout bypassing the security PoP. Thus, the performance metrics (average RTT and packet loss) displayed do not include the security PoP.



Some ISPs do not respond to the trace packets that the DEM agent sends and requests time out. For such hops, their entry is marked as *** in the trace result output.

Each FortiSASE administrator can only run one trace job on unique endpoints simultaneously.

Prerequisites

DEM requires an Advanced or Comprehensive remote users FortiSASE subscription. However, a Standard or Not-for-Resale (NFR) remote users FortiSASE subscription can opt in for a free 90-day trial and activate DEM on a maximum of 10 endpoints. See the FortiSASE Ordering Guide and DEM trial on page 74.

For new FortiSASE instances with a Standard, Advanced or Comprehensive subscription, the DEM agent is packaged along with the FortiClient installer and available to download as a single executable file from FortiSASE when users download FortiClient. See Managed endpoint client onboarding on page 731.

For existing FortiSASE instances with an Advanced or Comprehensive subscription, endpoint users are prompted to begin upgrading to a FortiClient version that supports the DEM agent and the DEM agent is installed automatically during this upgrade. Whereas existing FortiSASE instances with Standard or Not-for-Resale (NFR) subscriptions are notified about a new FortiClient version packaged with DEM agent, and endpoint upgrade rule(s) are disabled. The endpoint upgrade rule must then be manually re-enabled to install DEM agent on required endpoints, see Endpoint upgrade on page 497.

When the DEM agent is first installed and run on a Windows endpoint, a FortiClient agent tunnel connection to FortiSASE is required to initialize DEM for the endpoint.

To uninstall the DEM agent, do the following:

- On macOS, use the uninstaller tool to uninstall FortiClient and the DEM agent together.
- On Windows, use the installer package to uninstall FortiClient and the DEM agent together. You cannot uninstall DEM agent using *Add* or *Remove Program* in Control Panel.

DEM trial

DEM requires an Advanced or Comprehensive remote users FortiSASE subscription. However, a Standard or Not-for-Resale (NFR) remote users FortiSASE subscription can opt in for a free 90-day trial and activate DEM on a maximum of 10 endpoints. See the FortiSASE Ordering Guide.

Endpoints that are activated for a DEM trial are assigned to the DEM Trial endpoint profile, visible under *Endpoint management > Endpoint profiles*.

To activate a DEM trial on an endpoint, do the following:

1. Go to *Operations > Connectivity > Endpoints*, select the desired endpoint, and click *View Endpoint Details*.
2. In the slide-in, go to *Digital Experience* and click *Activate trial for this endpoint*.
3. Click *Activate trial*.

To pause DEM on an endpoint, do the following:

1. Go to *Endpoint management > Endpoint profiles*, select the *DEM trial* endpoint profile and click *Edit*.
2. Under *Profile Configuration*, select *DEM trial*.
3. Select the desired endpoint and click *Pause*.

When to pause and then resume the DEM trial:

- When upgrading to an Advanced or Comprehensive remote users subscription, you must reassign any endpoints that are enrolled in a DEM trial to their original endpoint profile or the Default profile. To reassign the endpoint, pausing the trial for the endpoint is required.
- When deleting a domain, domain-joined endpoints will match the Default profile. To ensure domain-joined endpoints continue to match the DEM trial profile, you must pause the trial for the selected endpoints, delete the domain, and resume the DEM trial for the same endpoints.

For a Standard or Not-for-Resale (NFR) remote users FortiSASE subscription, you must activate DEM on at least one endpoint to view the SaaS application list under *Operations > Connectivity > Digital experience monitoring*.

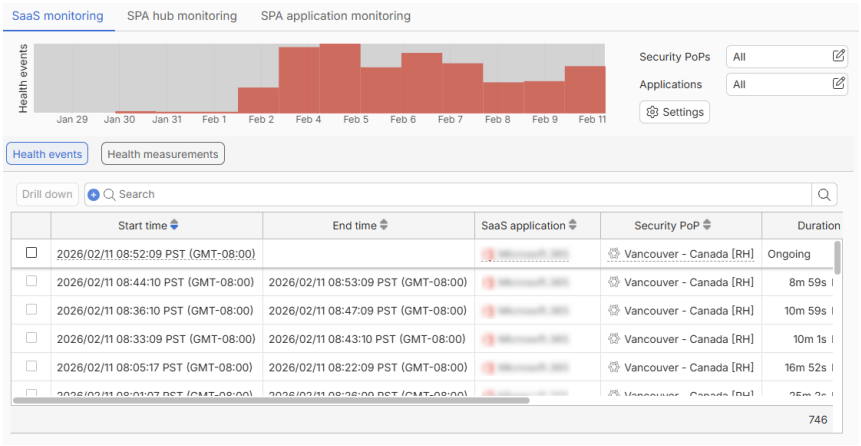
SaaS monitoring

To assist network administrators with troubleshooting remote user connectivity issues to common SaaS applications, FortiSASE includes a digital experience monitoring (DEM) feature accessible from *Operations* > *Connectivity* > *Digital experience monitoring*, under the *SaaS monitoring* tab.

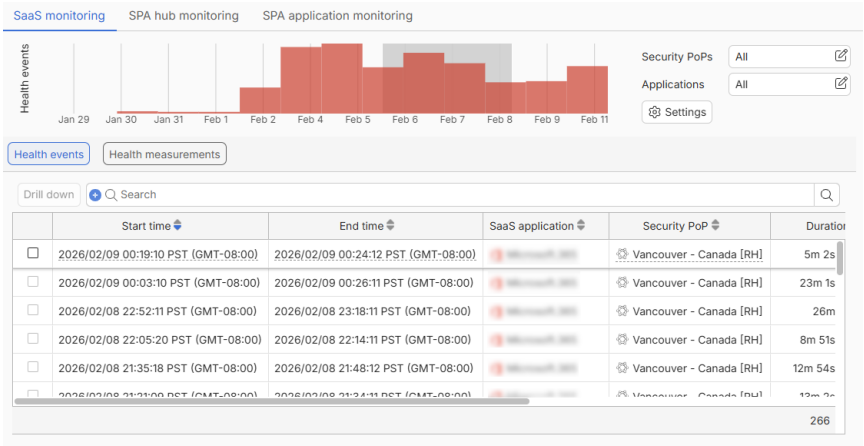
You can also add a *Digital Experience Monitoring* widget to *Monitoring* > *Dashboards* > *Status*.

To monitor end-to-end network performance from an endpoint to a security PoP and to a SaaS application, see Digital Experience Monitoring on page 71.

The accumulation of health events over a period of time are displayed in the *SaaS monitoring* tab as a time brush graph. Recent health events are displayed as red in the graph, with detailed information included in the *Health events* and *Health measurements* tables and charts.



Dragging the edges of the gray time brush allows you to focus in on a desired time period. *Health events* and *Health measurements* displayed will reflect the chosen time period.

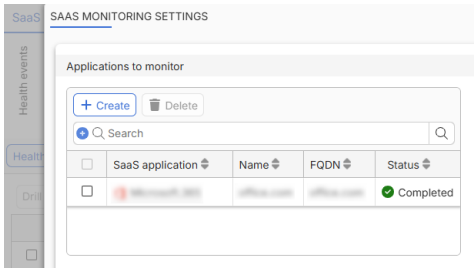


The *Security PoPs* and *Applications* dropdown menus allow you to filter results further by desired Security PoP location and SaaS application. Results displayed in the *Health events* and *Health measurements* tables and charts will only display events that occurred within the set filters and time period.

You can customize the list of monitored applications by adding and deleting applications in the *Settings*. You can configure a maximum of 20 applications for monitoring.

To customize the list of SaaS applications to monitor:

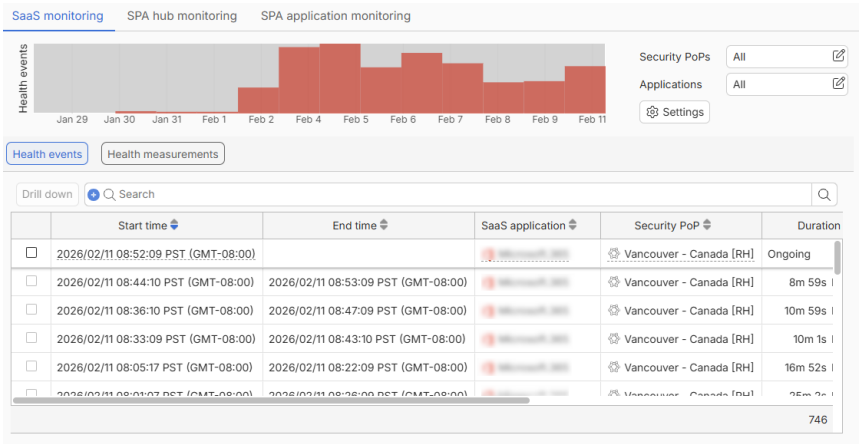
1. Go to *Operations* > *Connectivity* > *Digital experience monitoring*.
2. Click *Settings* near the *Security PoPs* and *Applications* fields.



3. To add an application to the list, in *Applications to monitor*, click *Create*.
   a. Do one of the following:
      - Some SaaS applications are preconfigured on the FortiSASE portal. To add a preconfigured application to the list, select *Pre-configured apps*, then select the desired application from the dropdown list. FortiSASE automatically populates the *Name* and *FQDN* fields accordingly. Click *OK*.
      - To define your own application, select *Custom apps*. Configure the *Name* and *FQDN* fields for your desired SaaS application.
   b. Click *OK*. Once the status is *Completed*, the new SaaS application will be monitored in the *Health events* table.
4. To remove an application from the list, select the application, then click *Delete*. Click *OK* in the confirmation dialog.

Health events

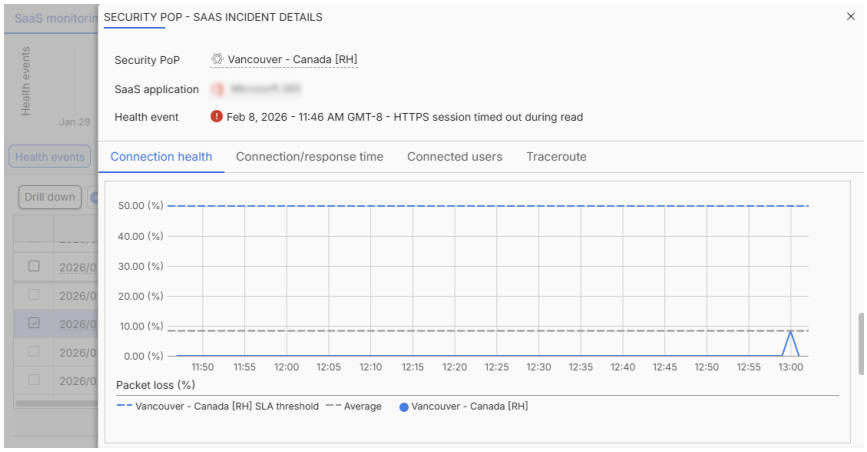
Go to *Operations* > *Connectivity* > *Digital experience monitoring* > *SaaS monitoring*. The *Health events* tab displays health event information for SaaS applications, including the severity, duration, and status. The incidents displayed will reflect the security PoPs and applications selected in the filters.



You can view detailed information on a specific incident by selecting the desired event and clicking *Drill down*. You can view charts regarding the network and application performance around that event:

- *Connection health*: Displays health graphs to review information on jitter, latency, packet loss, and MOS.
- *Connection/response time*: Displays time graphs to review information about TCP connection, DNS and HTTP(S) response, and so on.
- *Connected users*: Displays a list of users that accessed the SaaS application from the specified security PoP around when the incident occurred.
- *Traceroute*: Displays a trace route against the SaaS application at the time of the incident. The trace route can be displayed as *Tabular results* or as a *Path diagram*. If you are viewing the *Path diagram*, you can configure the available fields to highlight hops in the diagram based on average RTT and packet loss.

If there is no *End time* associated with the health event selected, the incident details will display information leading from the *Start time* to the present moment.

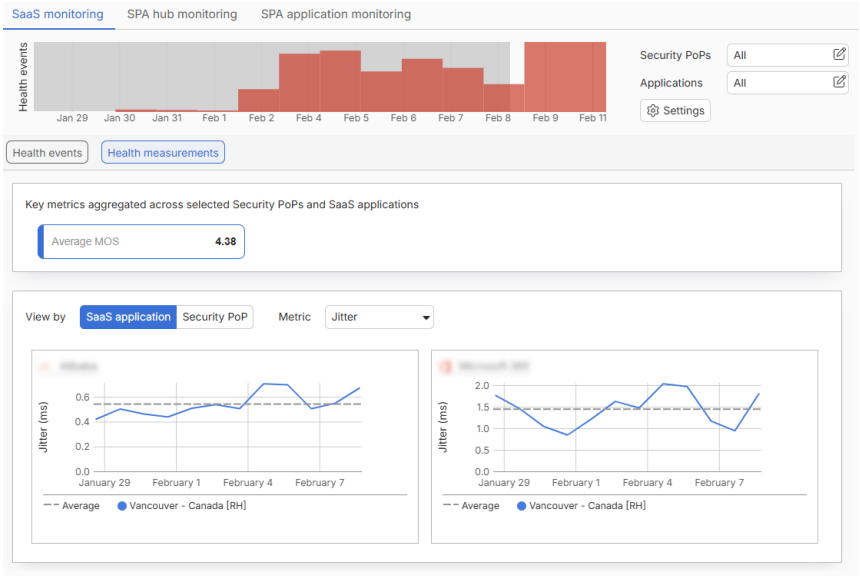


Health measurements

The *Health measurements* tab displays a list of SaaS applications and health check metrics for first-mile connectivity between the geographical security PoPs provisioned for your FortiSASE instance and these SaaS applications. An administrator can use this information to determine if remote user traffic is passing through a security PoP with ideal connectivity or with some ongoing connectivity issues.

HTTP measurements are taken once every five minutes. ICMP measurements are taken every minute. Probe traffic is permitted or dropped at the discretion of individual SaaS applications. Newly monitored apps may require up to six hours to gather data and may not be immediately available.

The *Health measurements* charts can be filtered to display information by *SaaS application* or *Security PoP*, and by the selected *Metric*. Available metrics include MOS, packet loss, latency, HTTPS response, and so on. The charts displayed will reflect the security PoPs and applications selected in the filters.



SPA hub monitoring

The SPA hub monitoring feature is available under *Operations > Connectivity > Digital experience monitoring* within *SPA hub monitoring* tab. It is included with all FortiSASE remote user subscription types and does not require a separate subscription.

SPA hub monitoring allows administrators to track the health and performance of SPA (Secure Private Access) service connections configured within FortiSASE. Each FortiSASE Security PoP sends periodic ICMP probes to a designated IP address referred to as the *Health Check IP* to measure SLA metrics (i.e. jitter, latency, packet loss) from each Security PoPs to the configured service connections (i.e. SPA Hub(s)). The *Health Check IP* is specified under *Network > BGP* during SPA Hub configuration.

These SLA metrics are displayed in real time and are useful for evaluating the quality of SPA service connection between Security PoPs and SPA Hubs, useful for SPA hub selection.

The SLA metrics are presented in two intuitive views within the SPA Monitoring feature:

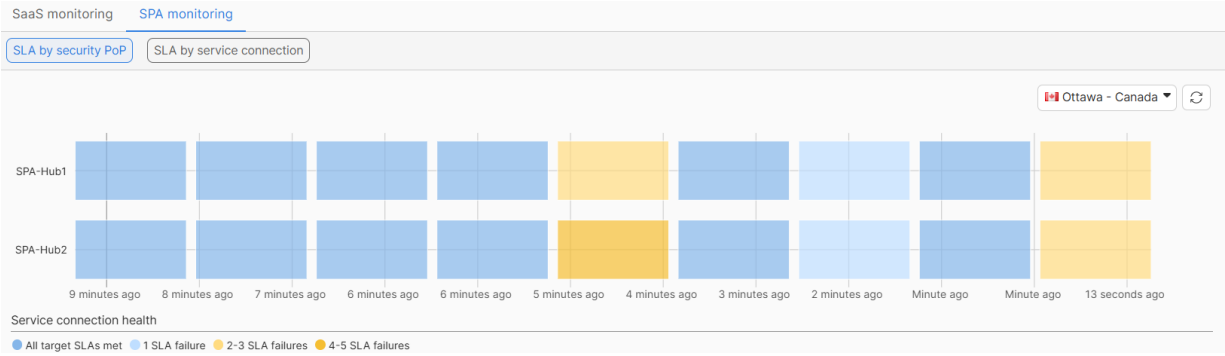
- *SLA by Security PoP*: This view displays the historical SLA data for all SPA service connections associated with a selected Security PoP. It provides a Security PoP centric perspective, allowing administrators to analyze the performance of multiple service connections from a specific security PoP.
- *SLA by Service Connection*: This view offers a service connection centric perspective, showing SLA history across all Security PoPs for a specific SPA service connection. This is useful for tracking performance inconsistencies or degradations across different Security PoPs for the same SPA service connection.

Note that SLA metrics are only displayed for the most recent 10 minutes. If SLA metric data is missing or not displayed for a particular SPA service connection, consider checking the following:

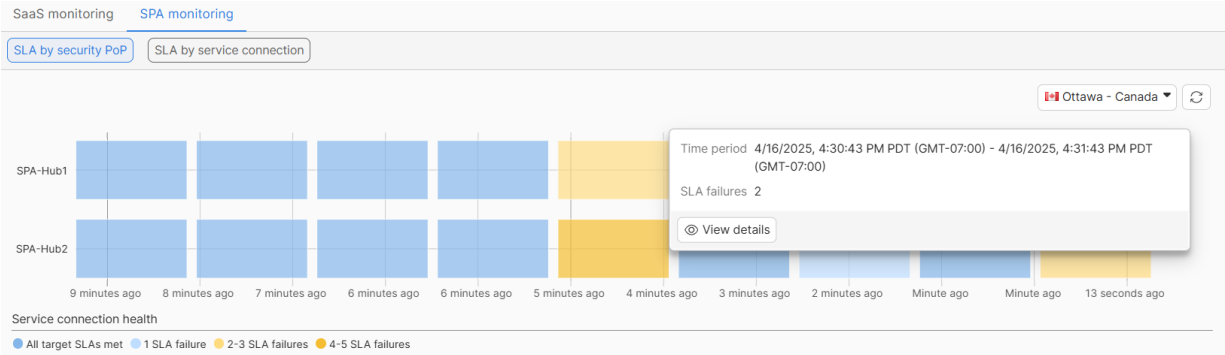
- Health Check IP reachability: The Health Check IP configured for each SPA Hub must be reachable from the FortiSASE Security PoPs. This is crucial for successful ICMP probing. If the IP is unreachable, ICMP probes will fail, and SLA metrics will not be generated.
- Enable ICMP replies: The device associated with the Health Check IP must be configured to respond to ICMP echo requests (ping). Without ICMP replies, SLA metrics cannot be gathered.

To monitor SLA performance and diagnose potential performance issues:

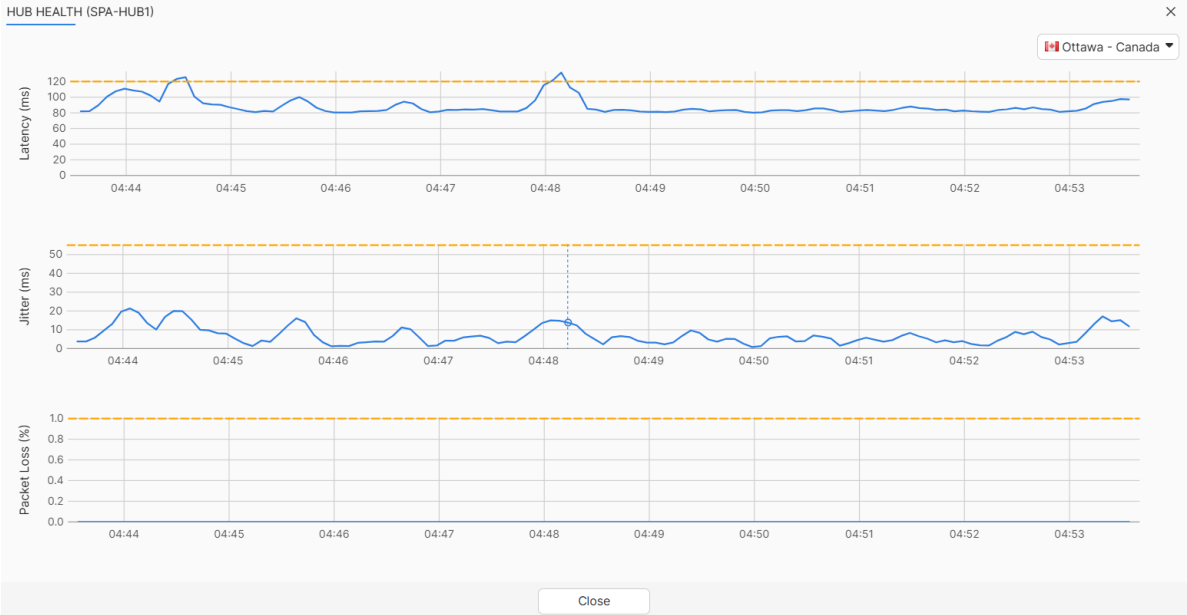
1. Go to *Network* > *BGP*, and make sure *Health Check IP* field is populated with a valid and reachable IP address. This IP is used for connectivity checks and is critical for accurate SLA monitoring.
2. Go to *Operations* > *Connectivity* > *Digital experience monitoring* and select the *SPA hub monitoring* tab.
3. To view SLA by Security PoP, do the following:
   a. Select the option *SLA by security PoP*.
   b. Use the dropdown on the right to select desired Security PoP.
   c. The SLA heatmap displays rectangular grids, each representing a one minute time slice. The color of each grid indicates the severity or number of SLA violations during that time window, based on a predefined color legend.
   d. This visual overview helps quickly identify when and where performance issues occurred.



   e. Hover over any affected rectangular grid and click *View Details*.



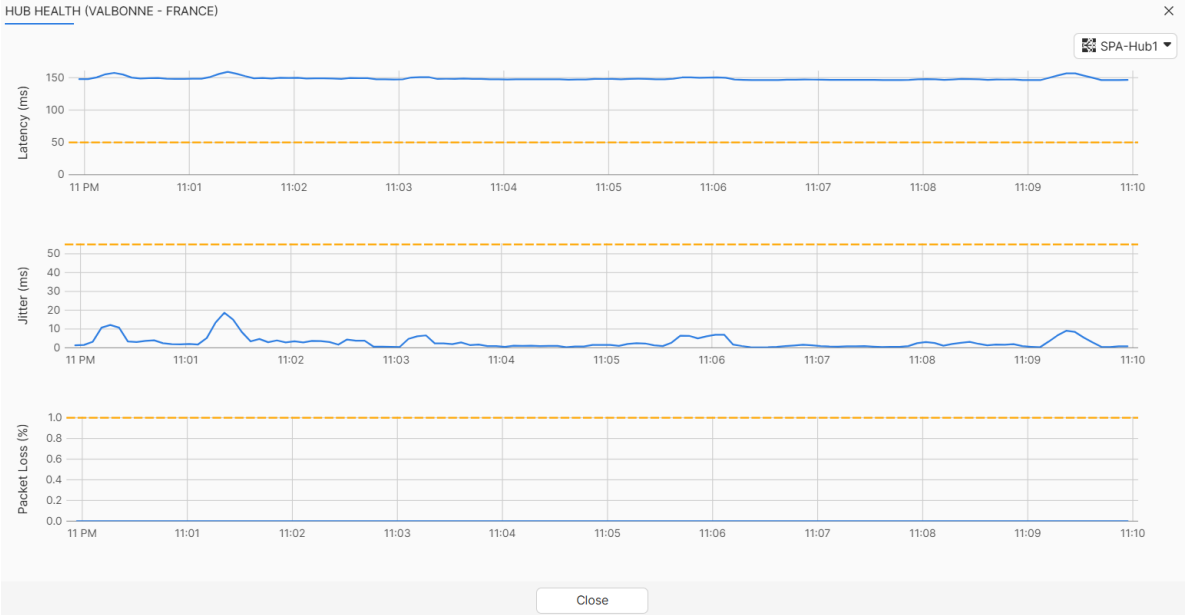
   f. A detailed graph will appear, showing SLA metrics such as Latency, Jitter, and Packet Loss for the selected time period. For example, the graph below display SLA performance data from a Security PoP in *Ottawa, Canada* to a *SPA-Hub1* service connection. A dotted yellow line represents the configured threshold for each metric. SLA violations occur when the measured values cross this threshold. To modify these thresholds, see Editing SLA thresholds on page 121.



4. To view SLA by Service connections:
   a. Under the *SPA hub monitoring* tab, switch to the *SLA by service connection* tab and use dropdown to select a suitable SPA service connection.
   b. This view shows SLA performance from all available Security PoPs to the selected service connection, allowing you to compare how different security PoPs are performing relatively against same SPA service connection.



   c. Select the affected rectangular grid from the heatmap to bring up detailed SLA metric graphs to analyze the trend and pinpoint potential root causes based on latency spikes, packet drops, or jitter anomalies.



SPA application monitoring

FortiSASE introduces support for Secure Private Access (SPA) application monitoring, enabling administrators to proactively monitor the availability of up to 20 custom applications hosted behind SPA Hubs. This enhancement improves visibility, ensures high availability, and provides a foundational layer of observability for mission-critical internal applications accessed via SPA.

By leveraging ICMP health check probes initiated by Fortinet Security PoPs to the defined custom application every second, administrators can verify the availability of internal applications exposed through SPA.

To configure custom applications for SPA application monitoring:

1. Navigate to *Operations* > *Connectivity* > *Digital experience monitoring*, and select the *SPA application monitoring* tab.
2. Go to the *Settings* tab.
3. Click *Create* and enter the details of the custom application:

Field	Value
Name	Enter a suitable name.
Server	Enter a valid, private IPv4 address of the application server.
SLA target	Enable the required toggles and define the Latency, Jitter, and Packet Loss threshold for the server.

4. Click *OK*.

To view and monitor the metrics of defined SPA applications:

1. Navigate to *Operations* > *Connectivity* > *Digital experience monitoring*, and select the *SPA application monitoring* tab.
2. Select the *SLA failure* tab to view the actual measured metrics (Latency, Jitter and Packet loss) and their configured thresholds arranged by Security PoP against the configured SPA Hub service connections. If the actual measured metrics cross the configured thresholds, it is highlighted.
3. Open the *SLA Failure* tab to view the measured Latency, Jitter, and Packet Loss values alongside their configured thresholds, arranged in a sequence by per Security PoP against their configured SPA Hub service connections. Any threshold breaches are highlighted.
4. To view the historical values for the measured metrics, select the desired Security PoP and click *Drilldown*.

Endpoints

You can view managed endpoints via *Operations* > *Connectivity* > *Endpoints*.

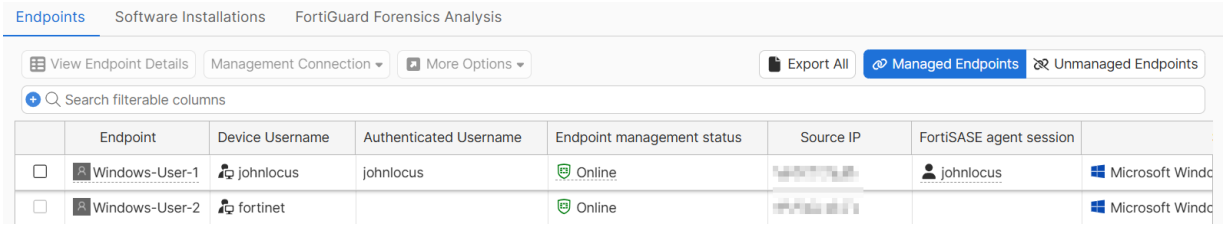
Alternatively, you can display the Endpoints status widget or status monitor under Dashboards as follows:

- Go to *Monitoring* > *Dashboards* > *Status* and under the *Endpoints* widget, click *Click to Expand*.
  - If this widget does not exist, add a new Managed Endpoints widget as Adding a custom dashboard on page 59 describes.
  - For details on the endpoint management states displayed in the *Endpoints* widget, see Endpoints on page 69.
- Go to an existing Managed Endpoints monitor. If this monitor does not exist, add a new Managed Endpoints monitor as Adding a custom monitor on page 62 describes.

The page, status widget, and status monitor all display a list of endpoints that show endpoint information, including but not limited to the following:

- Device username
- Authenticated username
- Endpoint management status
- Security PoP connection status
- Source IP
- FortiSASE tunnel IP address
- FortiSASE agent session
- Platform
- Vulnerabilities detected
- FortiClient version and ID
- Zero trust network access tags
- Profile
- Last seen

To add them to the display, hover over the first column and click the gear icon to select desired columns.



The *Endpoints* view contains the following buttons at the top of the page:

- When an endpoint is selected, you can use the *View Endpoint Details* button to display detailed endpoint information that FortiClient gathers on the endpoint device.
- The *Management Connection* button allows enabling/disabling the management connection for endpoints.
- When the endpoint has *Endpoint management status* as *Online*, you can click *More Options* to access the following actions:
  - *Export Diagnostic Logs*. You can only export diagnostic logs for online Windows endpoints.
  - *View tunnel session*
  - *Show in FortiView*
  - *Show Matching Traffic Logs*
- The *Export All* button exports the list of endpoints in a CSV file format that includes endpoint details such as device username name, IP and MAC addresses, FortiClient version, and so on.

  You can toggle between *Managed Endpoints* and *Unmanaged Endpoints* views.

Management Connection button

By default, the management connection for all endpoints is enabled. Therefore, you do not need to enable the management connection for an endpoint when you have not yet disabled it.

To determine whether an endpoint is still active, check its *Last Seen* column value. This helps you make an informed decision about whether to continue managing the endpoint on FortiSASE.

If you decide to remove the endpoint from management, you can do so by disabling its management connection. This action results in the following:

- The endpoint is permanently excluded from management and cannot register with FortiSASE using an invitation code unless its management connection is reenabled.
- FortiSASE removes the endpoint profile and zero trust network access (ZTNA) tagging settings from the selected endpoint.
- A subscription seat is freed up for use by other endpoints.

After an endpoint has previously been removed from management, you can add it to management by enabling its management connection with the following results:

- FortiSASE is now managing the endpoint and the endpoint is allowed to register with FortiSASE using an invitation code.
- FortiSASE applies the endpoint profile and security posture tagging settings configured in *Endpoint management > Endpoint profiles* and *Endpoint management > Security posture tags* respectively to the selected endpoint.
- The endpoint uses up a subscription seat.

To remove an endpoint from management:

1. Go to the *Endpoints* page, status widget, or status monitor.
2. Click *Managed Endpoint* to enter that view.
3. Select the desired endpoint.
4. Click *Management Connection > Disable*. After disabling the endpoint's management connection, the endpoint should disappear from the *Managed Endpoints* view and appear in the *Unmanaged Endpoints* view.

To add an endpoint to management when it has been previously removed from management:

1. Go to the *Endpoints* page, status widget, or status monitor.
2. Click *Unmanaged Endpoints* to enter that view.
3. Select the desired endpoint.
4. Click *Management Connection > Enable*. After enabling the endpoint's management connection, the endpoint disappears from the *Unmanaged Endpoints* view and does not appear in the *Managed Endpoints* view until it reconnects to FortiSASE.

Considerations

- When you remove an endpoint from management by disabling its management connection, in FortiClient the endpoint's zero trust telemetry connection will be disconnected.
- The *Disable* option within *Management Connection* is not equivalent to the *Deregister* button in previous FortiSASE versions.
  - In previous versions, *Deregister* just disconnected the endpoint from FortiSASE and allowed the possibility for the endpoint to remain managed and reregister with FortiSASE.
  - Currently, once you configure *Management Connection > Disable* for an endpoint, it is permanently excluded from management. Namely, it is considered an unmanaged endpoint, and cannot register with FortiSASE.

  To allow an unmanaged endpoint to be managed by and register with FortiSASE, you must select the endpoint and configure *Management Connection > Enable*.
- For FortiClient (macOS) endpoint management connections to be successfully established with FortiSASE Endpoint Management Service, in FortiSASE you must create a policy with deep inspection disabled for Fortinet infrastructure destinations (Fortinet-FortiSASE, Fortinet-FortiCloud, Fortinet-FortiClient.EMS, and Fortinet-FortiSandbox.Cloud) to exempt this traffic.

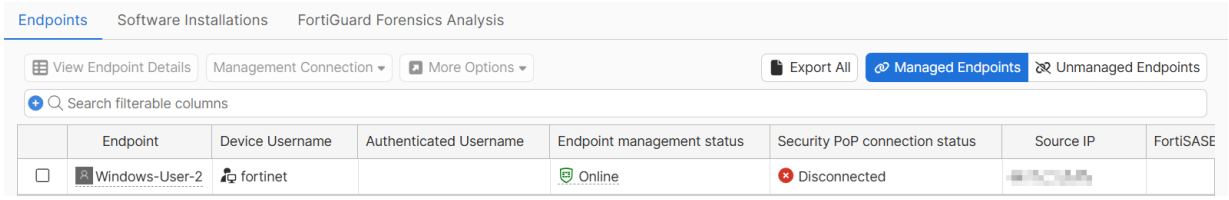
Examples

The following topics provide examples of actions you can perform from *Endpoints*.

Example: Confirming an endpoint is added to management by default

To confirm an endpoint is added to management by default:

1. Initially, the desired endpoint has not yet attempted to connect to FortiSASE. Go to *Operations* > *Connectivity* > *Endpoints*, click the *Unmanaged Endpoints* view and confirm the endpoint is not yet visible there.
2. Go to *Access & authentication* > *Access* > *Users and groups* and click *Onboard Users*.
3. Set *FortiClient Installer* to *Download*.
4. Under *Manual Installer* to the right of the *Invitation Code* field, click the copy icon to copy the invitation code.
5. On the endpoint, open FortiClient. On the *Zero Trust Telemetry* tab, paste the copied FortiSASE invitation code and click *Connect*. The endpoint successfully establishes a zero trust telemetry connection with FortiSASE. Upon connection, FortiClient receives an endpoint policy from FortiSASE. A system tray bubble message displays once the download completes.
6. Go to *Operations* > *Connectivity* > *Endpoints* and click *Managed Endpoints*. Confirm the endpoint is visible in that view and that the *Endpoint management status* is *Online*. If the endpoint reboots, it continues to establish its zero trust telemetry connection with FortiSASE and receives an endpoint policy each time.



Example: Removing an endpoint from management

The *Disable* option within *Management Connection* is not equivalent to the *Deregister* button in previous FortiSASE versions.

In previous versions, *Deregister* just disconnected the endpoint from FortiSASE and allowed the possibility for the endpoint to remain managed and reregister with FortiSASE.

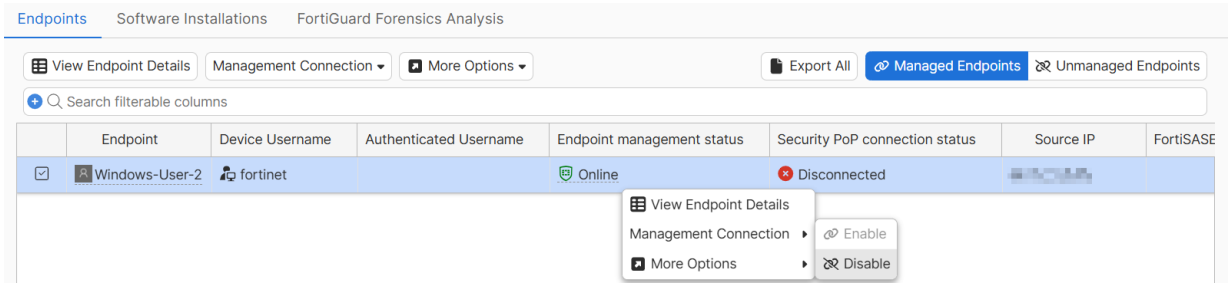
Currently, once you configure *Management Connection* > *Disable* for an endpoint, it is permanently excluded from management. Namely, it is considered an unmanaged endpoint, and cannot register with FortiSASE.

To allow an unmanaged endpoint to be managed by and register with FortiSASE, you must select the endpoint and configure *Management Connection* > *Enable*.

To remove an endpoint from management:

1. Consider that the device has been managed and is registered to and connected to FortiSASE. Go to *Operations* > *Connectivity* > *Endpoints*, click the *Managed Endpoints* view, and confirm the endpoint is visible there.

2. Select the endpoint, select *Management Connection* > *Disable*, and click *OK* to confirm. In FortiClient after the telemetry sync timer elapses, the endpoint's zero trust telemetry connection and the FortiSASE tunnel connection both disconnect after previously having been connected.

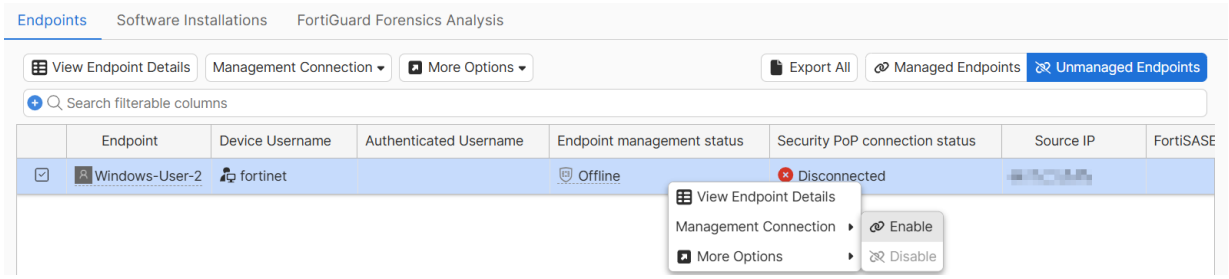


3. Confirm that the endpoint has disappeared from the *Managed Endpoints* view.
4. Go to *Operations* > *Connectivity* > *Endpoints* and click *Unmanaged Endpoints*. Confirm the endpoint is visible in that view.
5. Go to *Access & authentication* > *Access* > *Users and groups* and click *Onboard Users*.
6. Set *FortiClient Installer* to *Download*.
7. Under *Manual Installer* to the right of the *Invitation Code* field, click the copy icon to copy the invitation code.
8. On the endpoint, open FortiClient. On the *Zero Trust Telemetry* tab, paste the copied FortiSASE invitation code and click *Connect*. The endpoint no longer successfully establishes its zero trust telemetry connection with FortiSASE since you have excluded it from management.
9. If the endpoint reboots, repeat step 8. FortiClient attempts to connect to FortiSASE and never succeeds with registering and receiving an endpoint policy each time. This confirms that the unmanaged endpoint has been excluded from management as desired.

Example: Adding an endpoint to management after it was previously removed

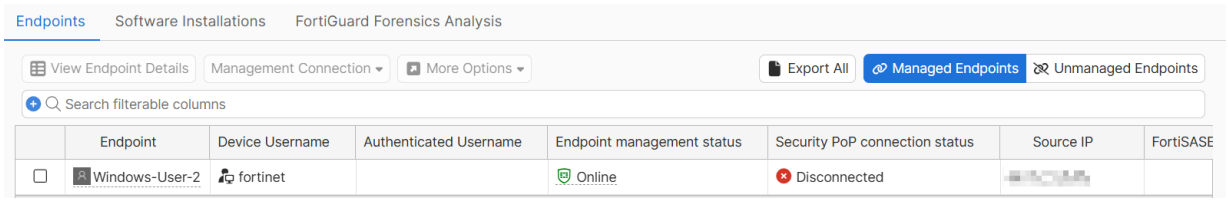
To add an endpoint to management after it was previously removed:

1. Consider that the device has been unmanaged and previously removed from management. Go to *Operations* > *Connectivity* > *Endpoints*, click the *Unmanaged Endpoints* view and confirm the endpoint is visible there.
2. Select the endpoint, select *Management Connection* > *Enable*, and click *OK* to confirm.



3. Go to *Access & authentication* > *Access* > *Users and groups* and click *Onboard Users*.
4. Set *FortiClient Installer* to *Download*.

5. Under *Manual Installer* to the right of the *Invitation Code* field, click the copy icon to copy the invitation code.
6. On the endpoint, open FortiClient. On the *Zero Trust Telemetry* tab, paste the copied FortiSASE invitation code and click *Connect*. The endpoint successfully establishes a zero trust telemetry connection with FortiSASE. Upon connection, FortiClient receives an endpoint policy from FortiSASE. A system tray bubble message displays once the download completes.
7. Go to *Operations* > *Connectivity* > *Endpoints* and click *Managed Endpoints*. Confirm the endpoint is visible in that view and that the *Endpoint management status* is *Online*. If the endpoint reboots, it continues to establish its zero trust telemetry connection with FortiSASE and receives an endpoint policy each time.



FortiGuard Forensics Analysis

FortiSASE supports the FortiGuard Endpoint Forensics Analysis service, which provides remote endpoint analysis to help you respond to and recover from cyber incidents. You can request detailed analysis of the endpoint from the Forensics team if you observe high-risk applications or traffic, malware, intrusion attempts, malicious emails, lateral movement, and so on, on that endpoint. For each engagement, forensics analysts from Fortinet's FortiGuard Labs remotely assist in collecting, examining, and presenting digital evidence, including a final detailed report. See the FortiClient Forensic Service datasheet.

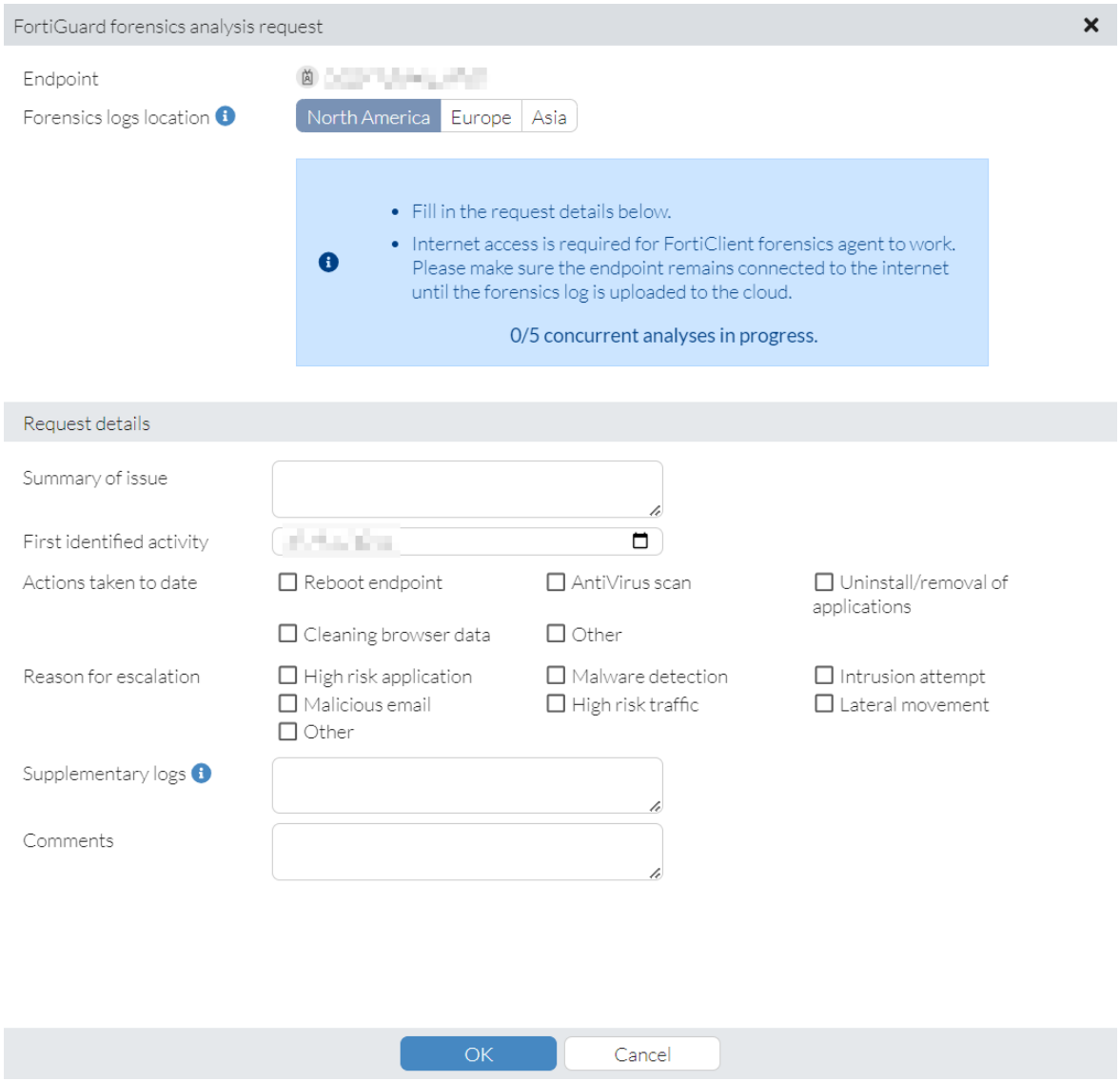
FortiSASE supports requesting a new FortiGuard Forensics Analysis for a suspicious endpoint and viewing a summary of analysis requests from *Operations* > *Connectivity* > *Managed Endpoints*. The FortiSASE administrator must complete a request form and ensure the suspicious endpoint remains connected to the internet to allow the forensics agent to work on the endpoint.

The verdict along with a downloadable report are updated in FortiSASE within five business days. You can have a maximum of five forensic analysis requests in progress at a given time.

To request a FortiGuard Forensics Analysis on a Windows endpoint:

1. Go to *Operations* > *Connectivity* > *Endpoints*.
2. In the *Endpoints* tab, select the desired endpoint and click *View Endpoint Details*.
3. In the *FortiGuard Forensics Analysis* tab, click *Request analysis*.

4. FortiSASE displays a request form. Do the following:
   a. Select a *Forensics logs location*. A FortiClient forensics agent will upload logs to this location.
   b. Fill in the request details:



5. Click *OK* to submit the request. At this point, a forensics analysis service request is initiated for the endpoint and is forwarded to a FortiClient forensics agent. The request form slide-in closes and returns to the *FortiGuard Forensics Analysis* tab.
6. In the FortiSASE app header, you will see a FortiGuard Forensic Analysis notification indicating a service request has been initiated for the endpoint. Click on *View* to open the Forensic Service portal, which allows further communication between the FortiSASE administrator and the Forensics team.
7. Once the Forensics team has completed the analysis, in the FortiSASE app header, you will see a FortiGuard Forensic Analysis notification indicating that the report is ready. Click on *Download* to download the report.

To view a list of FortiGuard Forensics Analysis service requests:

1. Go to *Operations* > *Connectivity* > *Endpoints*.
2. In the *FortiGuard Forensics Analysis* tab, you can view a list of analysis requests initiated from FortiSASE.

3. Under *Report*, click on *Download* to download a completed report.
4. Under *Service Request*, click on *View* to open the request in the *Forensic Service* portal.

Prerequisites and considerations

Prerequisites

FortiGuard Forensics Analysis supports Windows endpoints running FortiClient 7.2 that are connected to the FortiSASE Endpoint Management Service and are online.

The FortiClient forensics agent requires internet access to work. Ensure the endpoint remains connected to the internet until the forensics log is uploaded to the cloud.

Considerations

FortiGuard Forensics Analysis only works with the root account in an instance using organizational units and the managed security services provider portal.

Application inventory for managed endpoints

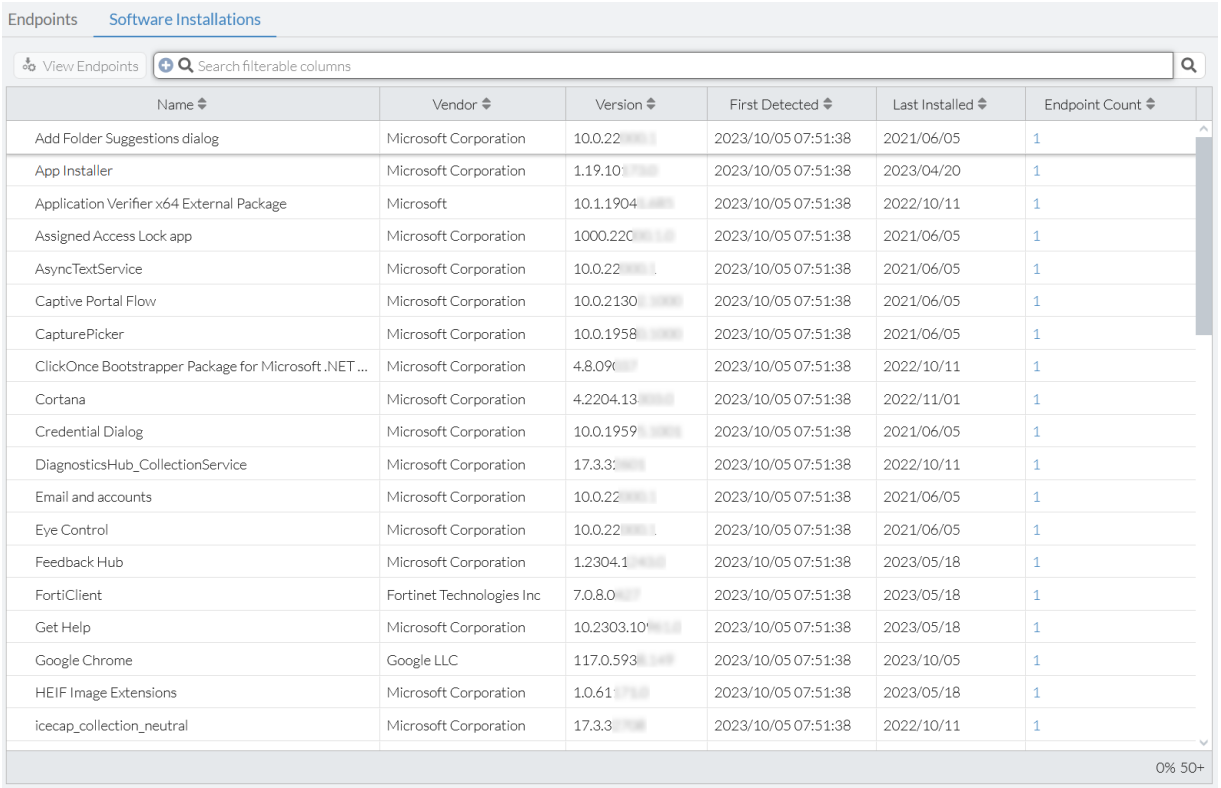
You may want to view which applications have been installed on FortiSASE managed endpoints.

For managed endpoints, FortiClient sends the software inventory information to FortiSASE when it first registers to FortiSASE. If software changes occur on the endpoint, such as installing new software, updating existing software, or removing existing software, FortiClient sends an updated inventory to FortiSASE.

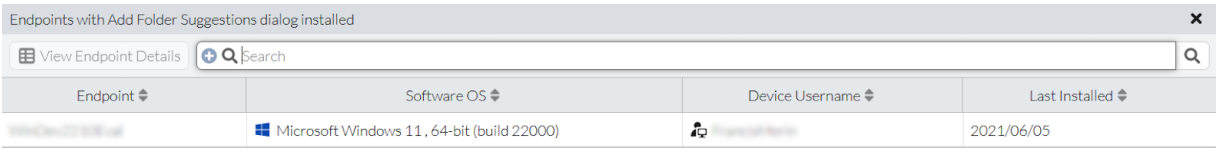
Based on this information sent by FortiClient, you can view the application inventory for FortiSASE managed endpoints as follows:

- Go to *Operations* > *Connectivity* > *Endpoints* and select the *Software Installations* tab to view a global list of applications installed on all endpoints.

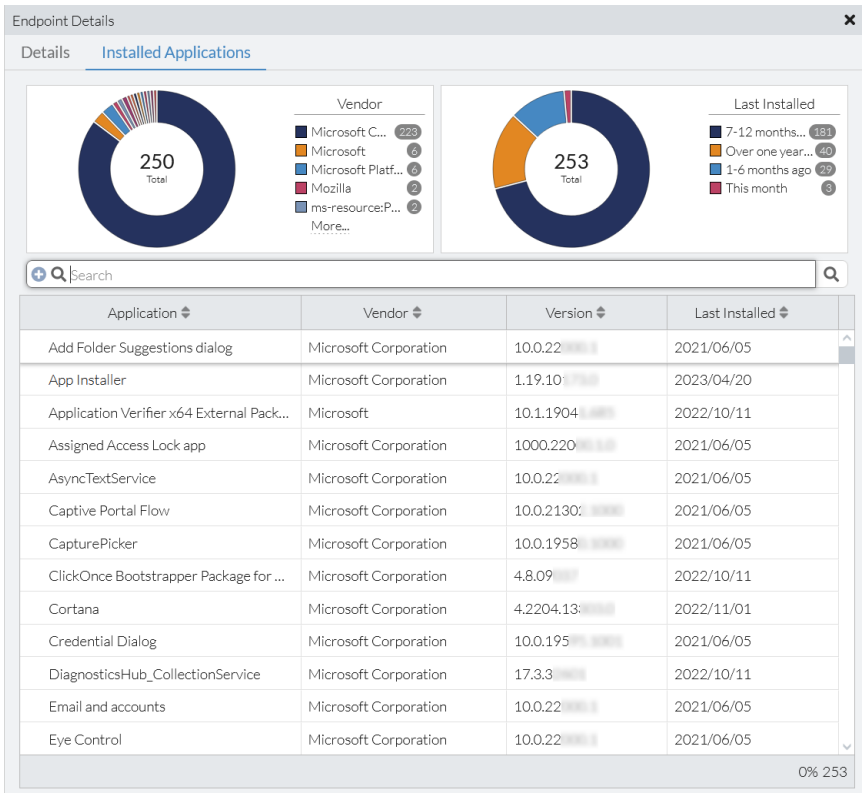
- The *Endpoint Count* field displays the number of endpoints with the specific application installed.



- You can select an application and either click *View Endpoints* or right-click and select *View Endpoints* to view which endpoints have the application installed.



- Go to *Operations* > *Connectivity* > *Endpoints*, select the *Endpoints* tab, select an endpoint, and either click *View Endpoints Details* or right-click and select *View Endpoint Details*. From the *Endpoint Details* pane, click *Installed Applications* to view a list of installed applications for the selected endpoint.



Each list includes details for each application such as vendor and version information.

Requesting FortiClient diagnostic logs from endpoints

This feature only works with Windows endpoints that fulfill the following criteria:

- Running FortiClient
- Online
- Managed by FortiSASE Endpoint Management Service

FortiSASE supports requesting the export of FortiClient diagnostic logs on-demand from a single online Windows endpoint from one of the following:

- *Details* tab in *View Endpoint Details*
- *More options* in the *Endpoints* tab in *Endpoints*

Once the endpoint receives the log request, log collection will take place in the background. This process takes approximately 20 minutes. When new logs are generated, then the old ones will be overwritten.

To request FortiClient diagnostic logs from an endpoint:

1. Go to *Operations* > *Connectivity* > *Endpoints*.
2. Select a Windows endpoint that is online and perform one of these steps:
   - Click *View Endpoint Details* and in the *Details* tab, next to the *Diagnostic Logs* field, click *Request new logs*.

- Click *More Options* > *Export Diagnostic Logs* and in the *Export diagnostic logs* prompt, click *Request new logs*.

3. In the top right, observe the notification *Successfully requested diagnostic logs from the endpoint* displays, indicating that FortiSASE sent the request successfully.

To download previously requested FortiClient diagnostic logs from an endpoint:

1. Go to *Operations* > *Connectivity* > *Endpoints*.
2. Select a Windows endpoint that you previously sent a log request to and perform one of these steps:
   - Click *View Endpoint Details* and in the *Details* tab, next to the *Diagnostic Logs* field, click *Download* to download the available diagnostic logs for the endpoint.
   - Click *More Options* > *Export Diagnostic Logs* and in the *Export diagnostic logs* prompt, click *Download* to download the available diagnostic logs for the endpoint.

Requesting FortiClient debug logs from endpoints

This feature only works with Windows and macOS endpoints that fulfill the following criteria:
- Running FortiClient
- Online
- Managed by FortiSASE Endpoint Management Service

FortiSASE supports requesting the export of FortiClient debug logs on-demand from a single online Windows or macOS endpoint from one of the following:

- *Details* tab in *View Endpoint Details*
- *More Options* in the *Endpoints* tab in *Endpoints*

Once the endpoint receives the log request, log collection will take place in the background. This process takes approximately 20 minutes. When new logs are generated, then the old ones will be overwritten.

To request FortiClient debug logs from an endpoint:

1. Go to *Operations* > *Connectivity* > *Endpoints*.
2. Select a Windows or macOS endpoint that is online and perform one of these steps:
   - Click *View Endpoint Details* and in the *Details* tab, next to the *Debug Logs* field, click *Export Debug Logs*.
   - Click *More Options* > *Export Debug Logs* and in the *Request debug logs* prompt, click *Request new logs*.
3. In the top right, observe the notification *Successfully requested logs from the endpoint* displays, indicating that FortiSASE sent the request successfully.

To download previously requested FortiClient debug logs from an endpoint:

1. Go to *Operations* > *Logs* > *Endpoint management* > *Endpoint diagnostic & debug logs*.
2. Select the entry for the desired entry. The *Status* column displays whether the logs are ready for download.
3. Click *Download* to download the available debug logs for the endpoint.

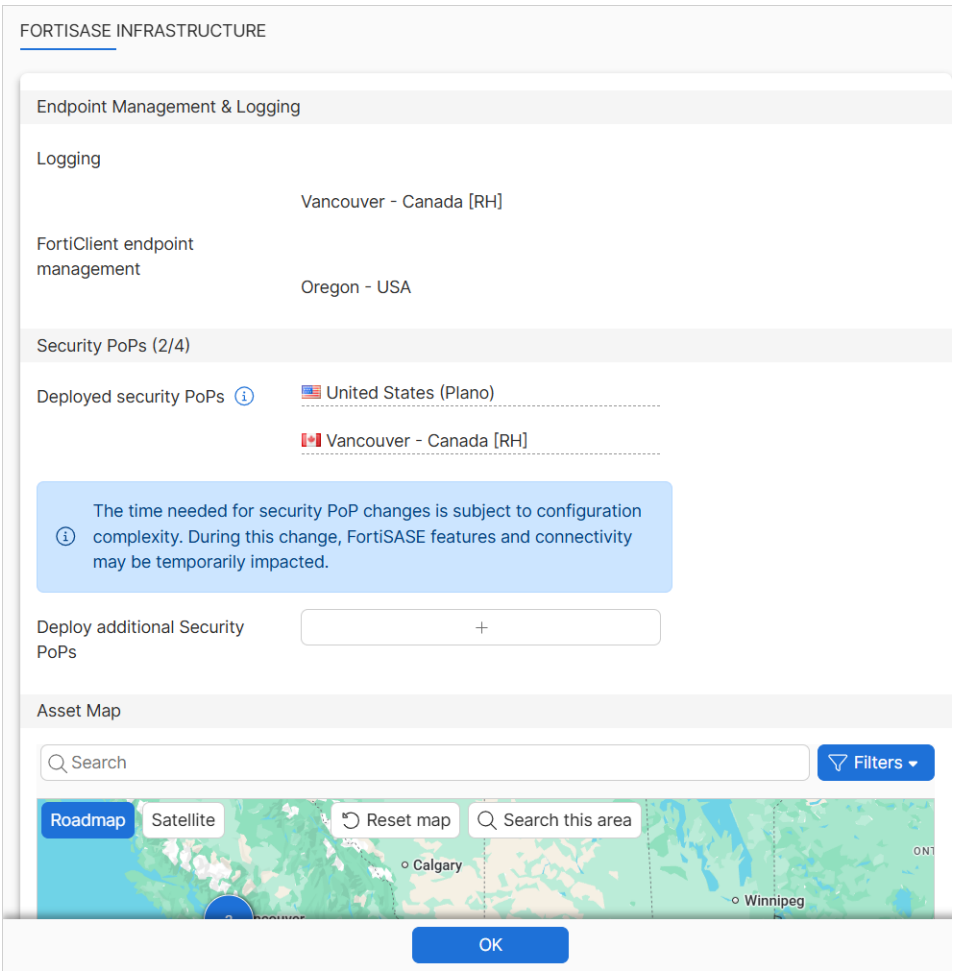
Infrastructure

> You can only use this feature to add or change security PoPs.
>
> Contact FortiCare Support to change the logging or FortiClient endpoint management security PoP or to delete a security PoP.

For some FortiSASE instances, administrators can add and change security PoPs dynamically from *Operations > Connectivity > Infrastructure*.

This feature is available only when a FortiSASE instance meets these specific conditions:

- The following features are not configured:
  - Proxy
  - Source IP address anchoring
- Default remote agents' IP address range has not been exceeded.
- The following have not been deployed:
  - Edge devices
  - Branch On-ramp security PoPs
- You have not made other custom changes to the instance.



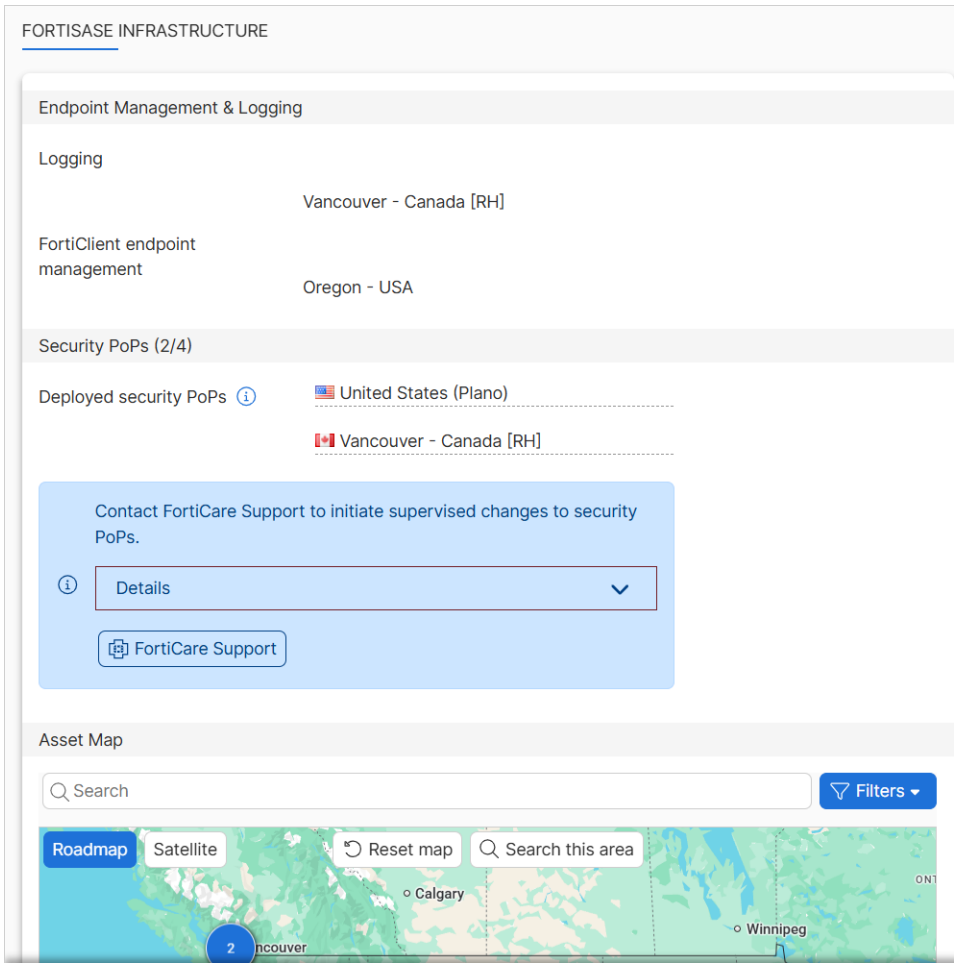
You can configure a change in the *Deploy additional Security PoPs* field by clicking + to add one or more security PoPs up to the maximum number per subscription and number of users. Once you have configured a change, select *OK* to apply the change.

> The time needed for security site changes is subject to configuration complexity. During this change, FortiSASE features and connectivity may be temporarily impacted. See Security PoPs on page 791 for the expected impact of applying infrastructure changes.

Selecting more PoPs improves redundancy and lowers latency for remote users who will connect to the geographically closest available PoP. See Appendix C - Tunnel performance on page 812.

Instances not supporting dynamic infrastructure changes

If your FortiSASE instance does not meet the aforementioned conditions for this feature and does not support this feature, you observe a different *Operations* > *Connectivity* > *Infrastructure* page.



Contact FortiCare Support to initiate supervised changes to security sites. When opening a new ticket, include the following information:

- A list of sites to remove, if any
- A list of sites to add, if any
- Preferred timing for the change

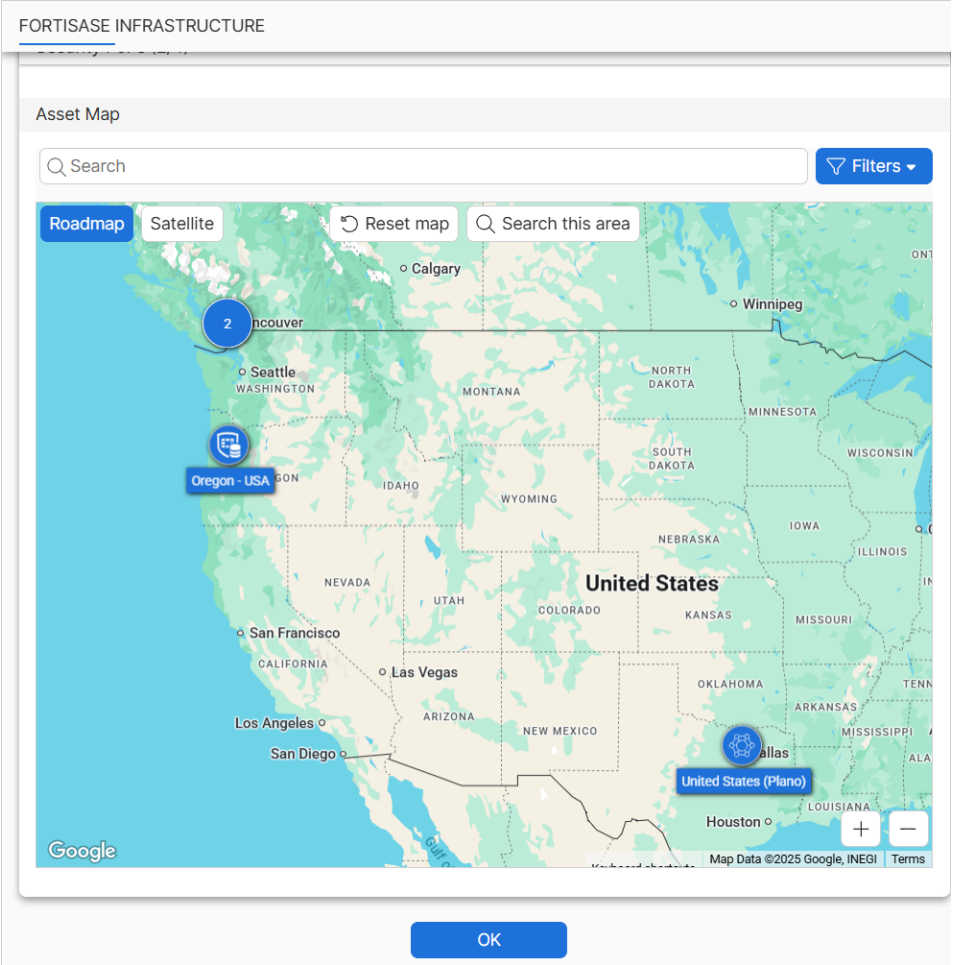
Asset Map

On the Infrastructure page, an asset map is available which displays the geographical locations of these FortiSASE PoPs:

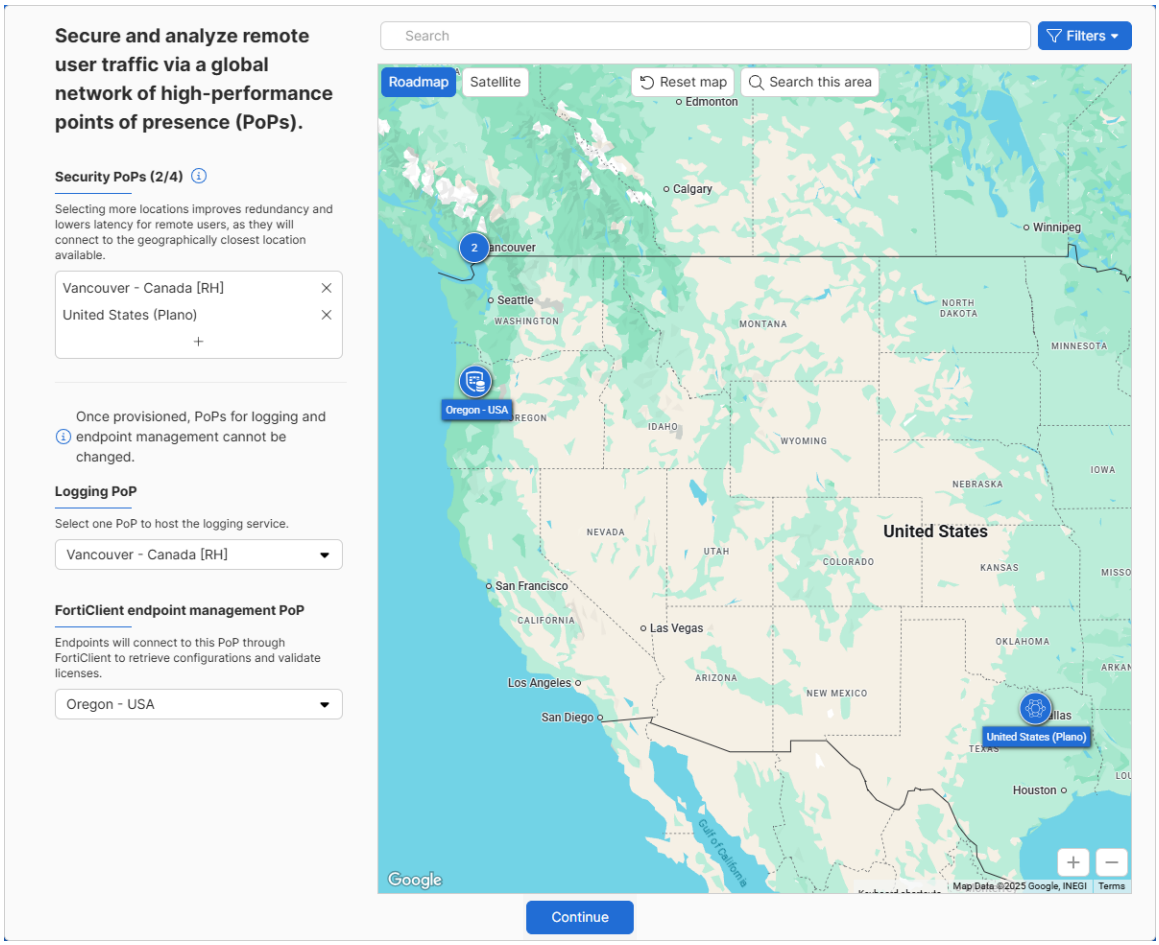
- Security PoPs
- FortiClient endpoint management PoPs
- Logging PoPs

You can filter the map using these PoP types.

This map helps visualize relative distances between PoPs. Also, the map can be helpful with selecting PoPs closest to the location of your agents and edge endpoints.



FortiSASE also presents a map during the provisioning process, specifically, in the PoP selection dialog.



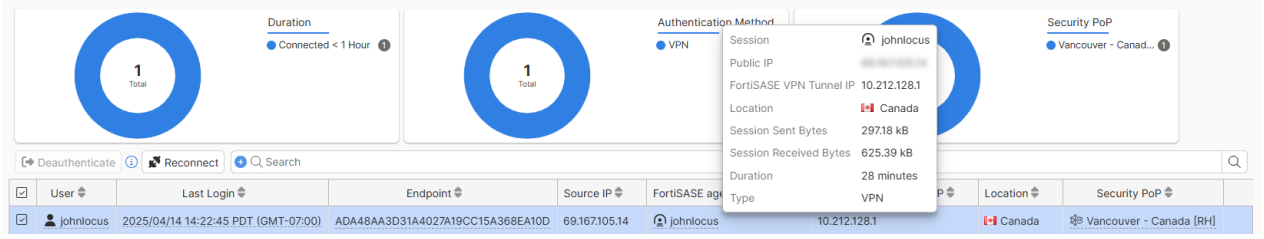
Connected users

Administrators can view remote user's session information and group details that have successfully authenticated and connected to FortiSASE secure internet access. When multiple user groups are configured on FortiSASE, the user's group information is particularly useful to determine whether the remote user belongs to the desired user group. See Users and groups on page 502.

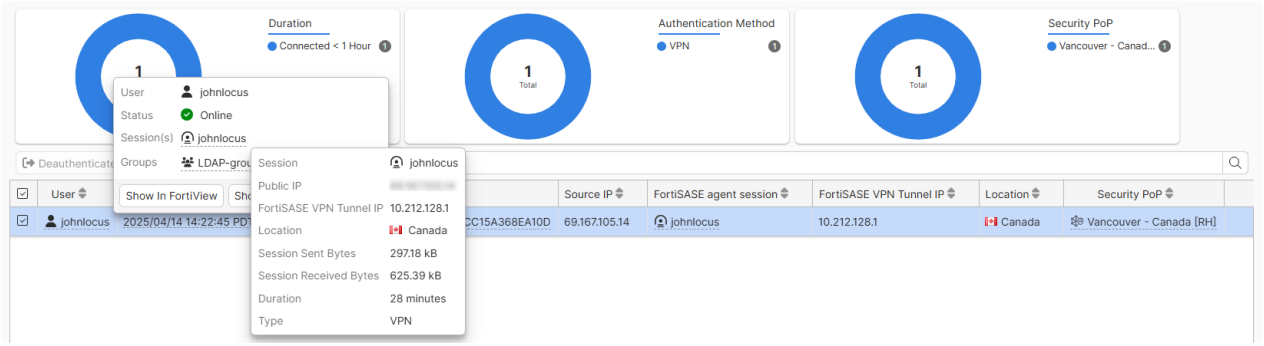
To view the user's session and group information:

1. Go to *Operations* > *Connectivity* > *Connected users*.
2. Add the *FortiSASE agent session* column to the display, by hovering over the first column and clicking the gear icon to select *FortiSASE agent session*. Then hover over a connected user under the *FortiSASE agent session* column to see a tooltip that displays the user's information including its *Source IP* (the public IP), *FortiSASE VPN Tunnel IP*, and relevant user session information.

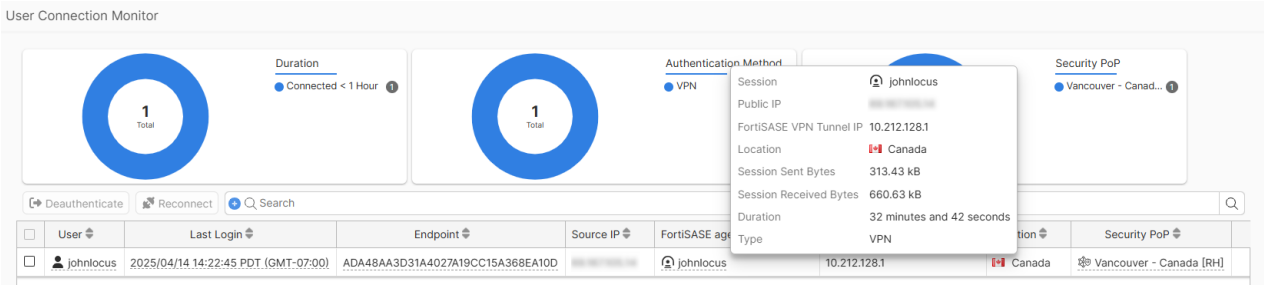
   Knowing a user's FortiSASE tunnel IP address is commonly useful in scenarios where administrators need to troubleshoot traffic flow from server to client in a Secure Private Access (SPA) deployment for types of applications such as VoIP or remote access.



Alternatively, hover over on the connected user under *User* column and notice the user's group information under the *Groups* row in the tooltip. Within the same tooltip hover over the user's *Session(s)* row to view the tooltip information presented in the *FortiSASE agent session* column, as shown below.



3. Additionally, you can add the *User connection* monitor under *Dashboards* to view the same information. See Adding a custom dashboard on page 59.



After a remote user's authentication, *Connected Users* shows all matching groups for agent-based users (FortiClient users). For agentless proxy users, it only displays the first group that the user matched.

Packet capture

FortiSASE administrators can perform real-time packet capture on FortiSASE security points of presence (PoP) to monitor the traffic of agent-based FortiClient endpoints and agentless proxy users that are successfully authenticated and connected to FortiSASE secure internet access. You can view these endpoints from *Operations* > *Connectivity* > *Connected users*. The packet capture tool offers traffic filtering options based on protocol, source and destination IP addresses, and port numbers along with support for TCP dump syntax. You can download the packet captures as .pcap files for in-depth analysis on third-party tools like Wireshark.

To run packet capture on a FortiSASE security PoP:

1. Go to *Operations* > *Connectivity* > *Connected users* and select the desired endpoint from the list.
2. Right-click the selected endpoint and select *Open packet capture*.
3. In the *PACKET CAPTURE* pane, enter the following:

Field	Description
Region	This field is prefilled based on the security PoP the selected endpoint is connected to. To select another *Region*, use the dropdown menu.
Watch	This field is prefilled based on the type of remote user connected, such as *Agent* or *Proxy*.
Maximum captured packets	Specify the maximum packet count to capture. The maximum value is 20000 packets.
Filtering Syntax	Choose *Basic* to use standard GUI-based filters or *Advanced* to enter custom TCP dump syntax.
Included protocols	Select *Any* to capture all traffic types or *Specify* to select specific protocols like ESP, ICMP, TCP, and UDP. Click + to add multiple protocols.
Source IP addresses	This field is prefilled based on the tunnel IP address assigned to the selected endpoint. Choose *Any* to capture traffic from all endpoints in the selected region or *Specify* to enter specific source IP addresses.
Destination IP addresses	Select *Any* for all destination IP addresses or *Specify* to target particular destination IP addresses.
Source ports	Select *Any* to capture traffic from all source ports or *Specify* for particular source ports. Click + to add multiple source ports.
Destination Ports	Select *Any* for all destination ports or *Specify* to enter unique destination ports. Click + to add multiple source ports.

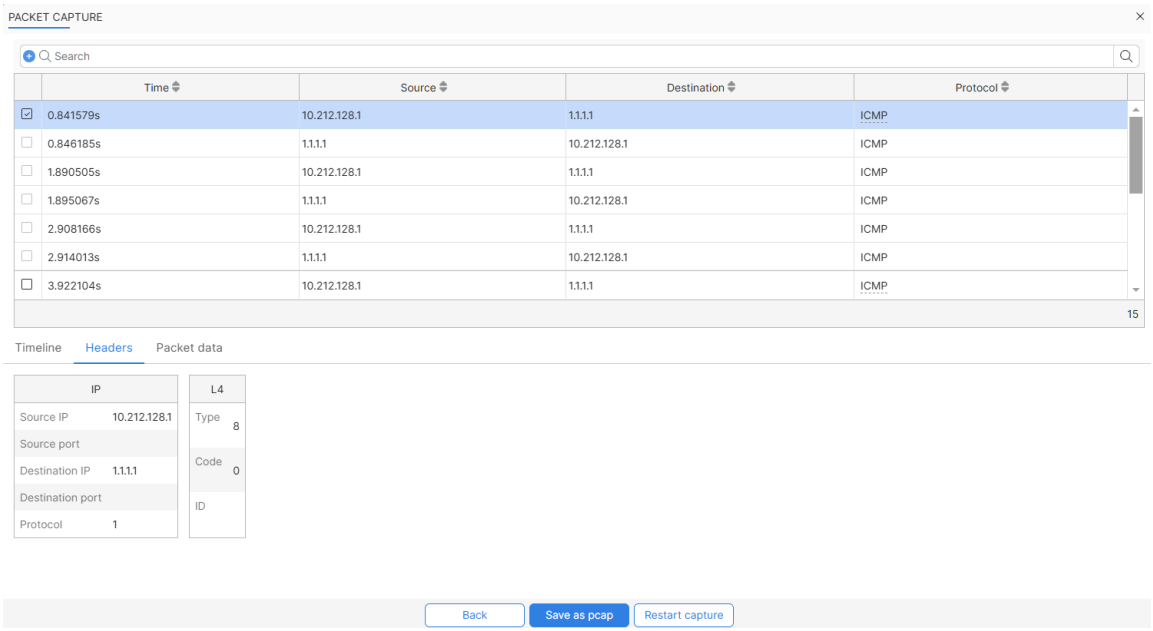


To capture bidirectional traffic flow effectively, specify the source and destination IP addresses for traffic in both directions. This means setting up the capture to include:

- Forward direction: source IP address (A) to destination IP address (B)
- Reverse direction: source IP address (B) to destination IP address (A)

By capturing IP addresses for both directions, you ensure that the capture includes all packets involved in the communication, including responses or acknowledgments.

4. Click *Start capture* to initiate packet capture.
5. Wait for the packet limit to be reached or click *Stop capture* to end packet capture. Captured packets appear in sequence in the table. To add more columns to this table, use the gear icon.
6. To view detailed Layer 3 (L3) and Layer 4 (L4) information, select a packet and view its *Timeline*, *Headers*, and *Packet data* columns.



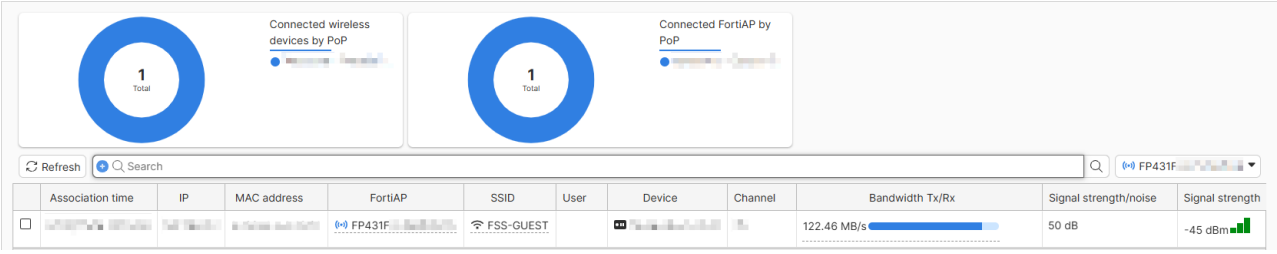
7. (Optional) Click *Restart capture* to reinitiate packet captures using same filters.
8. (Optional) Click *Save as pcap* to download and view the captured packets using third party tools such as Wireshark.

To run the packet capture tool using the Endpoints tab:

1. Go to *Operations* > *Connectivity* > *Endpoints*.
2. From the endpoint list, select an endpoint where the *Endpoint management status* column displays as *Online*.
3. Click *View Endpoint Details*.
4. In the slide-in, go to *Packet Capture* to initiate a packet capture.

Connected wireless clients

Administrators can view details of wireless devices connected to FortAP edge devices managed by FortiSASE.



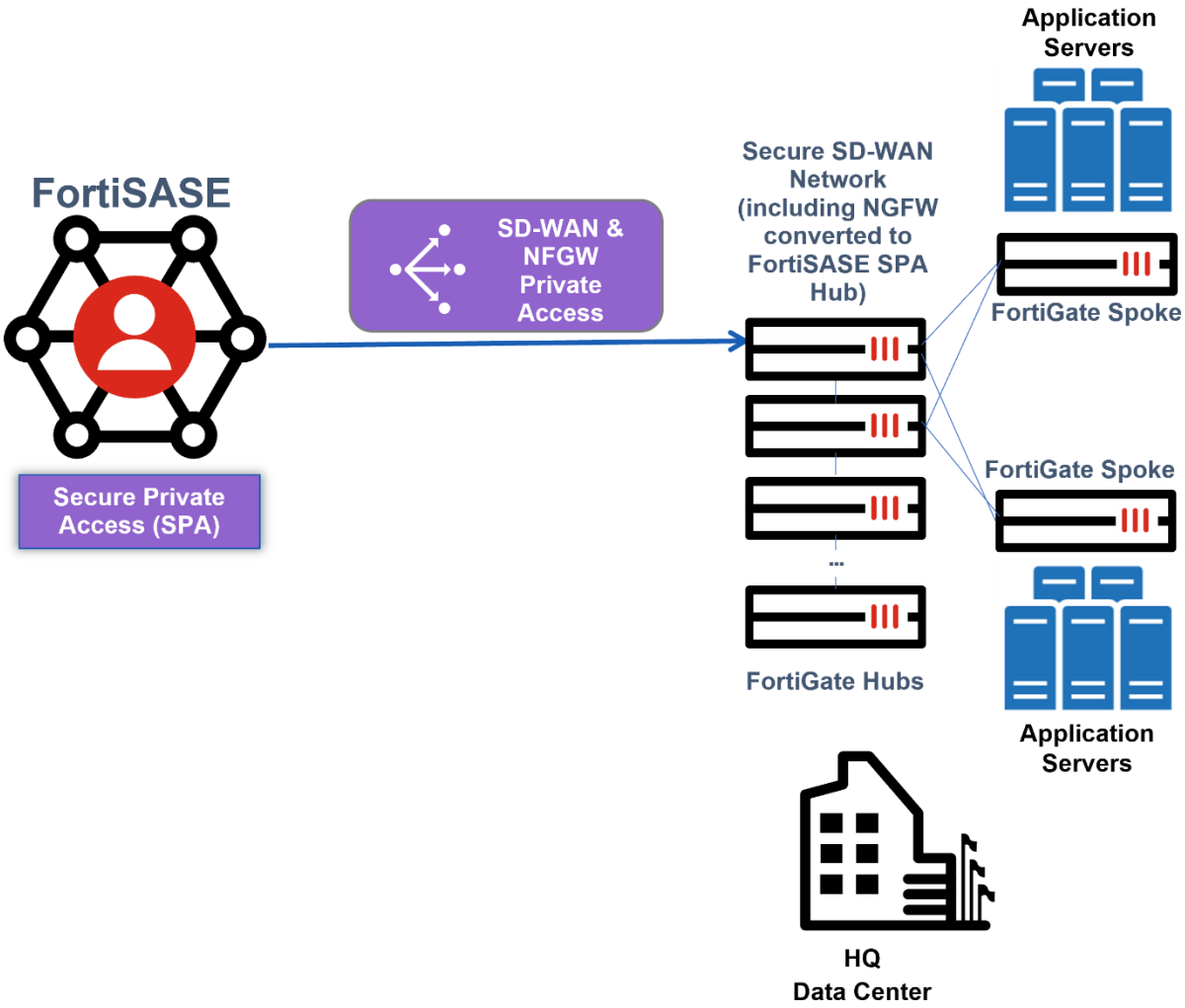
By right-clicking on a wireless client, you can choose *Show in FortiView* and either view *Sessions* or *WiFi Clients* to go to the respective FortiView pages.

For wireless client views, the *User* column is only available if the SSID is configured with the following WiFi Security Modes and the user has been authenticated by these modes:

- *WPA2 Enterprise*
- *WPA3 Enterprise Only*
- *Captive Portal Only*

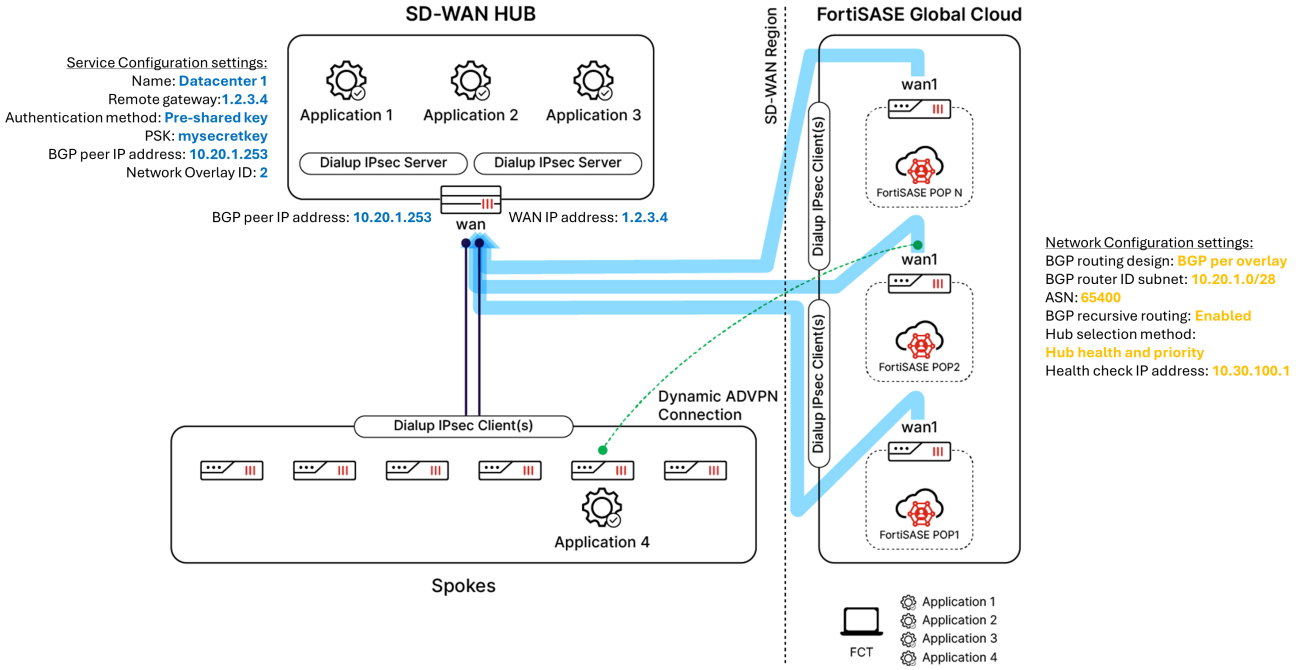
SPA

For securing FortiSASE remote user access to private TCP-based and UDP-based applications, FortiSASE supports secure private access (SPA) using SD-WAN or SPA using a next generation firewall converted to a standalone FortiSASE SPA hub. FortiSASE SPA supports up to 12 FortiGate hubs.



For SPA use cases, the security points of presence (PoPs) act as spokes to the FortiGate hub (FortiGate SD-WAN hub or FortiSASE SPA hub), relying on IPsec overlays and BGP to secure and route traffic between security PoPs and the networks behind the organization's FortiGate hub.

FortiSASE security PoP and the organization's FortiGate hubs form a traditional hub-and-spoke topology that supports the Fortinet autodiscovery VPN (ADVPN) configuration. ADVPN is an IPsec technology that allows a traditional hub-and-spoke VPN's spokes to establish dynamic, on-demand, direct tunnels, known as shortcut tunnels, between each other to avoid routing through the topology's hub device.



FortiSASE remote users may access private resources behind FortiGate hub(s) directly through FortiSASE to hub(s) IPsec tunnels. If a private resource is behind an organization's spoke device, they may connect directly to that resource through an on-demand, direct, and dynamic ADVPN tunnel.

The SPA use cases with FortiGate hubs allow traffic flow in the following directions:

From...	To...
Remote agents	FortiGate hubs (or spokes connected to hubs)
FortiGate hubs (or spokes connected to hubs)	Remote agents

FortiSASE supports these main routing design methods:

- BGP per overlay (default)
- BGP on loopback

See Supported features for each SPA BGP routing design on page 105.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

The example network topology uses the following settings configured in FortiSASE:

Configuration setting	Value used in example network topology
Network > BGP	
BGP Routing Design	*BGP per overlay*
BGP Router ID Subnet	10.20.1.0/28
SPA hubs belong to	*FortiSASE autonomous system*
FortiSASE ASN	65400
Hub Selection Method	*Hub health and priority*
Health Check IP	10.30.100.1
Endpoint-to-endpoint Traffic	Disabled
BGP Recursive Routing	Enabled
Operations > Connectivity > Secure private access	
Name	Datacenter 1
Remote Gateway	1.2.3.4
Authentication Method	*Pre-shared key*
Pre-shared Key	mysecretkey
BGP Peer IP	10.20.1.253
Network Overlay ID	2

Prerequisites

FortiSASE supports these main routing design methods:

- BGP per overlay (default)
- BGP on loopback

See Supported features for each SPA BGP routing design on page 105.

The following deployments are documented using the BGP per overlay (default) routing design:

- For the FortiGate SD-WAN secure private access (SPA) use case, SD-WAN network deployments are expected to conform to Fortinet's best practices for SD-WAN architecture and deployment for the following topologies:
  - SD-WAN with a single datacenter/hub
  - SD-WAN with dual datacenters/hubs
  - SD-WAN with up to 12 datacenters/hubs

  For deployment details, see the SPA with a FortiGate SD-WAN deployment in the Feature SPA Deployment Guide using BGP per Overlay.
- For the FortiGate next generation firewall (NGFW) SPA use case, you must first convert the NGFW to a standalone IPsec hub. For deployment details, see the FortiGate NGFW to FortiSASE SPA hub conversion deployment in the Feature SPA Deployment Guide using BGP per Overlay.

- For the FortiGate NGFW SPA use case running FortiOS 7.2.4 and above, you can use Fabric Overlay Orchestrator to convert the NGFW to a standalone IPsec hub. For deployment details, see the FortiGate NGFW to SPA hub conversion using Fabric Overlay Orchestrator in the Feature SPA Deployment Guide using BGP per Overlay.
  - When using Fabric Overlay Orchestrator with FortiOS 7.4.5 or later, you can copy easy configuration keys from the hub FortiGate to simplify SPA setup on FortiSASE. See SPA easy configuration key for FortiSASE.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

SPA subscription and account prerequisites

SPA requires a subscription per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See SPA Service Connection subscription and SPA FortiCloud account prerequisites.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

Network restrictions

Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following remaining network restrictions when network restrictions have been removed per Network restrictions removed on page 47, and ensure your network configuration does not overlap with them.

The FortiExtender and LAN Extension control plane subnet are configurable (default subnet: 10.252.0.0/16). See IP management on page 274.



With Remote agent and edge device user identification on page 24 enabled, IPAM private IP address pool(s) configured for agents and edge devices per IP management on page 274 are unavailable for you to use in your network configuration.

Subnets that you can configure as IPAM private IP address pool(s) are:

- 100.65.0.0/16 (default)
- 10.0.0.0/8
- 100.64.0.0/10
- 172.16.0.0/12
- 192.168.0.0/16

Routing best practice for SPA hub

When advertising prefixes from SPA hubs, ensure that only the prefixes intended to be routed through SPA are advertised to FortiSASE security points of presence (PoPs). Avoid advertising the following prefixes, as they may unintentionally redirect traffic through SPA and disrupt FortiSASE routing behavior:

- 0.0.0.0/0 (default route)
- 0.0.0.0/1
- 128.0.0.0/1

FortiSASE security PoPs rely on their internal routing tables to handle internet-bound traffic from internal components. Advertising undesired prefixes to PoPs can result in traffic being misrouted through the SPA hub, resulting in connectivity issues.

The following TCP ports are reserved for FortiSASE internal usage and you cannot use them for secure private access (SPA) connections. See Required services and ports on page 25:

- 8008
- 8010
- 8015
- 8020

If you must use these non-standard and reserved ports for SPA connections, open a FortiCare support ticket to request allowing these ports for SPA usage for your instance.

Supported features for each SPA BGP routing design

FortiSASE supports these main routing design methods:

- BGP per overlay (default)
- BGP on loopback

The following is a summary of the features supported based on the BGP routing design:

Feature	BGP per overlay	BGP on loopback
Additional IPsec overlay	No	Yes
ADVPN Route Tag	No	Yes
Agentless ZTNA	Yes	
DNS redirection rules	Yes	
External feeds	Yes	No
Forwarding logs to on-premise private FortiAnalyzer	Yes	
FSSO with private FortiAuthenticator	Yes	No
Hub selection method as BGP med	Yes	

Feature	BGP per overlay	BGP on loopback
Hub selection method as Hub health and priority		
Peering via eBGP		
Peering via iBGP		

Configuring the FortiSASE security PoPs as the FortiGate hub's spokes

Ensure that you are aware of secure private access (SPA) Prerequisites on page 103.

To allow FortiSASE remote users with SPA to resources behind your FortiGate hub (FortiSASE SPA hub/FortiGate SD-WAN hub) network, you can configure FortiSASE security points of presence (PoP) as spokes in your hub-and-spoke network in *Operations* > *Connectivity* > *Secure private access*.

Configuration workflow

To configure SPA service connections (hubs), you must follow this configuration workflow:

1. Under *Network* > *BGP*, configure the common network configuration settings. See Configuring network configuration on page 107.
2. Under *Operations* > *Connectivity* > *Secure private access*, click *Create*, and configure a new service connection (hub). See Configuring a new service connection on page 113.

You cannot configure a service connection or hub without first configuring *Network Configuration* settings.

BGP routing design

FortiSASE supports FortiGate hubs for SPA using BGP per overlay (default) or BGP on loopback. It allows configuring FortiGate hubs that reside in the same ASN as FortiSASE (iBGP peering) or in a different ASN (iBGP and eBGP peering). See the following table for an overview of each routing design and example FortiGate hub and spoke reference configurations that you can use for a typical SD-WAN dual hub deployment:

BGP routing design overview	Example hub configuration for dual hub architecture	Example spoke configuration for dual hub architecture
BGP per overlay (default)	SD-WAN dual hub with VPN overlay and BGP routing - HUBs	SD-WAN dual hub with VPN overlay and BGP routing - Branches
BGP on loopback	BGP on loopback (Dual-Hub region) - Hub	BGP on loopback (Dual-Hub region) - Spoke

Configuring network configuration

Before proceeding with configuring hubs or service connections, you must configure common secure private access (SPA) network configuration that all service connections use.

BGP routing design

FortiSASE supports FortiGate hubs for SPA using BGP per overlay (default) or BGP on loopback. It allows configuring FortiGate hubs that reside in the same ASN as FortiSASE (iBGP peering) or in a different ASN (iBGP and eBGP peering). See the following table for an overview of each routing design and example FortiGate hub and spoke reference configurations that you can use for a typical SD-WAN dual hub deployment:

BGP routing design overview	Example hub configuration for dual hub architecture	Example spoke configuration for dual hub architecture
BGP per overlay (default)	SD-WAN dual hub with VPN overlay and BGP routing - HUBs	SD-WAN dual hub with VPN overlay and BGP routing - Branches
BGP on loopback	BGP on loopback (Dual-Hub region) - Hub	BGP on loopback (Dual-Hub region) - Spoke

To configure SPA network configuration:

Example values for SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

1. Go to *Network* > *BGP*.
2. (Optional) You can use an easy configuration key to simplify SPA setup on FortiSASE by automatically populating key fields in *Network* > *BGP* and *Create Secure Private Access Service Connection* based on the FortiGate hub configuration. The easy configuration key is available on FortiOS 7.4.5 and later versions when the FortiGate is configured as a hub using Fabric overlay orchestrator. The FortiGate must have a valid SPA Service Connection subscription and be registered under the same FortiCloud account as FortiSASE. See SPA using a FortiSASE SPA hub with Fabric overlay orchestrator. You must set the following network attributes to use the key:

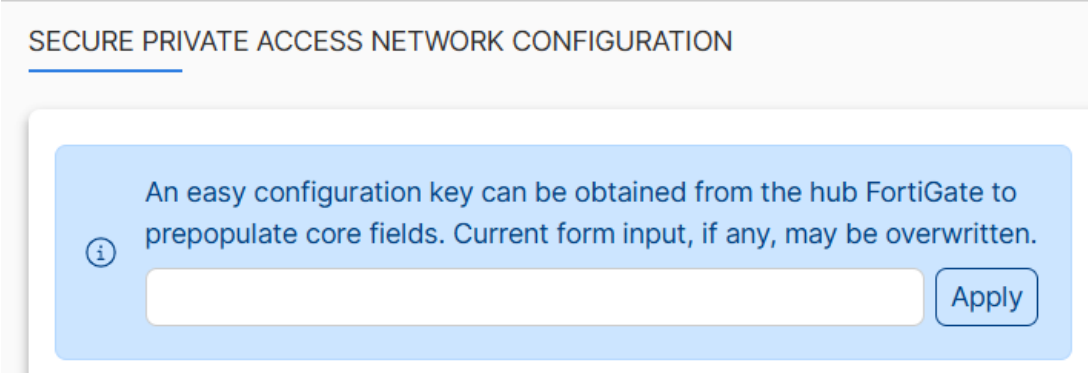
a. Under *Network* > *BGP*, set the following attributes. Otherwise, you cannot use the key:

Network attributes	Must be configured as...
BGP Routing Design	*BGP per overlay*
Hub Selection Method	*Hub Health and Priority*

b. After configuring the attributes under *Network* > *BGP*, you must configure the following authentication method under *Operations* > *Connectivity* > *Secure private access* to use the easy configuration key:

Network attributes	Must be configured as...
Authentication Method	*Pre-shared Key*

c. After completing the configuration on the hub FortiGate using Fabric overlay orchestrator, copy the key and paste it in *Network* > *BGP* under the field in *Secure Private Access Network Configuration* on FortiSASE. See SPA easy configuration key for FortiSASE and SPA using a FortiSASE SPA hub with Fabric overlay orchestrator.



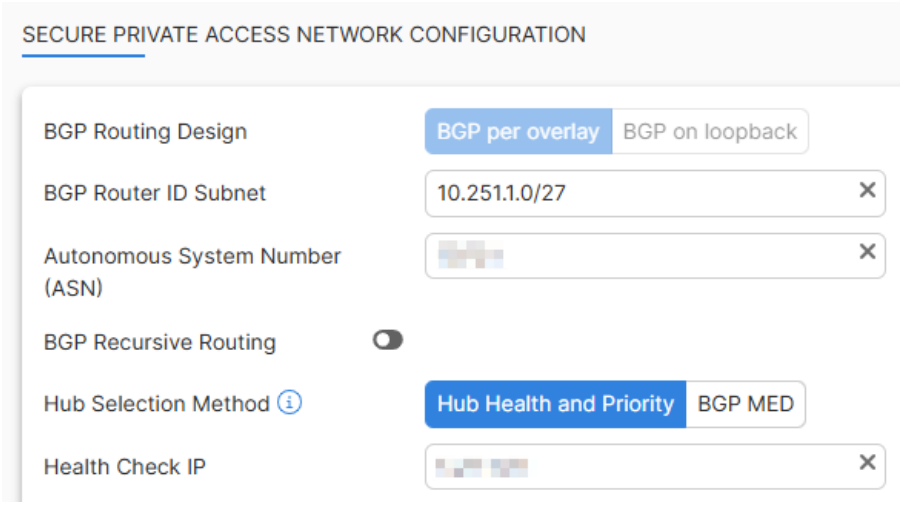
d. Click *Apply*. FortiSASE autopopulates fields such as *BGP Router ID Subnet*, *Autonomous System Number (ASN)*, and *Health Check IP* based off the FortiGate hub configuration. Click *Save* to finish SPA network configuration. You can proceed to Configuring a new service connection on page 113 without completing the remaining steps in this section.

3. Under *Network* > *BGP*, under *Secure Private Access Network Configuration* page, for *BGP Routing Design*, select one of the following:
   - BGP per overlay (default selection)
   - BGP on loopback. FortiSASE automatically selects and grays out *BGP Recursive Routing* after you selecting this option.
4. Fill in the rest of the fields with values of the attributes of the FortiGate hub network connection. FortiSASE validates the input and notifies you of any invalid values. See the following table:

Network attributes	Description	Example
BGP Routing Design	FortiSASE supports these main routing design methods: • BGP per overlay (default) • BGP on loopback	BGP per overlay

Network attributes	Description	Example
	You can use only a single BGP routing design method for all hubs and spokes. You cannot mix them.	
BGP router ID subnet	Define the subnet from which loopback interface IP addresses will be assigned to the entitled FortiSASE security PoPs. The loopback interface IP address assigned from this subnet will be used as the BGP router ID on the FortiSASE security PoPs. Each security PoP will receive one IP address in this subnet. /28 is the minimum subnet size. Note that a subnet larger than /28 may be required if the number of entitled security PoPs exceeds 16 and/or if any entitled PoPs have been provisioned to exceed the default maximum number of remote agents per region of 4096 (/20).	10.20.1.0/28
SPA hubs belong to	If all SPA hub(s) are in the same BGP autonomous system number (ASN) as FortiSASE, select *FortiSASE autonomous system*. This option enables iBGP peering between FortiSASE and the SPA hub(s). If the SPA hub(s) are distributed across both the same and different BGP autonomous system numbers (ASNs) relative to FortiSASE, select *Different autonomous systems*. This configuration enables eBGP peering with SPA hubs in different ASNs and iBGP peering with those in the same ASN as FortiSASE.	
FortiSASE ASN	BGP autonomous system (AS) number of your hubs. Typically, this should be the same on both hubs.	65400
BGP recursive routing	Enabling the BGP recursive routing setting allows for interhub connectivity and redundancy to networks behind the active hub if each hub has a physical connection to the others for cases when connectivity between a FortiSASE security PoP and the active hub fails. For example, consider that this BGP configuration setting enabled and a FortiSASE security PoP's connectivity with hub 1 goes down. To ensure the security PoP can reach a network behind hub 1, it would route traffic to hub 2 first, then route it to hub 1 via its interhub connection, followed by routing the traffic to the desired destination network behind hub 1.	Enabled

Network attributes	Description	Example
Hub selection method	Method by which FortiSASE selects hub. By default, FortiSASE uses hub health and priority: • **Hub health and priority**: periodically obtain jitter, latency, and packet loss measurements for each hub via the health check IP address. FortiSASE selects the highest priority hub within each security PoP that meets SLA requirements. A hub can be assigned a different priority level in different security PoPs. This method is not available when support for configuring multi-ASN is enabled using *SPA hubs belongs to* setting. • **BGP MED**: BGP multi-exit discriminator (MED) is an attribute that an autonomous system advertising routes to another peer sets. FortiSASE learns MED from the configured hubs. See BGP multi-exit discriminator.	Hub health and priority
Health check IP address	IP address of a server behind the hub that should be used to set up the SD-WAN performance SLA rule. The health check IP address is used to periodically obtain jitter, latency, and packet loss measurements per hub.	10.30.100.1
Endpoint-to-endpoint Traffic	Enables endpoints connected through Secure Internet Access (SIA) to communicate directly with each other. It is useful for applications that require client-to-client file transfers or remote access for IT troubleshooting. This setting becomes visible only after at least one Secure Private Access (SPA) Hub is configured. After enabling and saving the setting, you must re-announce the prefixes learned from FortiSASE spokes on the SPA Hub. Administrators can then regulate endpoint-to-endpoint traffic flows by configuring Private Access policies. See Enabling endpoint to endpoint communication on page 112.	Disabled

5. 

6. Click *Save*.

Considerations

- You can use only a single BGP routing design method for all hubs and spokes. You cannot mix design methods. You cannot change the BGP routing design method once you save it. You must delete the service connection(s) and network configuration and reconfigure them with a different BGP routing design method. You can change *SPA hub belongs to* from using a single ASN to using multi-ASN, but cannot change the setting from using multi-ASN to use a single ASN.
- Any configuration changes on the hub FortiGate via Fortinet Security Fabric overlay orchestrator generates a new easy configuration key and does not automatically update on FortiSASE. To avoid issues, copy the latest key from the hub after completing its configuration.
- Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following remaining network restrictions when network restrictions have been removed per Network restrictions removed on page 47, and ensure your network configuration does not overlap with them.

  The FortiExtender and LAN Extension control plane subnet are configurable (default subnet: 10.252.0.0/16). See IP management on page 274.
- For BGP per overlay, the FortiSASE security PoPs use their IPsec tunnel overlay interface(s) with IP address (es) assigned by the FortiGate hub(s) via IKE mode config for BGP peering with the FortiGate hub(s). The BGP peer IP address defined in the service connection(s) should be an IPsec interface on the FortiGate hub (s). For BGP on loopback, the FortiSASE security PoPs use their loopback interface with IP address assigned from the BGP router ID subnet for BGP peering with the FortiGate hub(s). The BGP peer IP address defined in the service connection(s) should be a loopback interface on the FortiGate hub(s). In both routing designs, the BGP peer IP address defined in each service connection should not fall within the BGP router ID subnet. A common strategy to avoid this is to pick a subnet, such as a /24, and allocate a portion of that subnet for the FortiSASE security PoPs, such as a /25, and the remaining portion of it for the FortiGate hub (s).
- When using the BGP MED option, user-defined hub priorities are not used because the SD-WAN SLA rule is disabled in this case.
- While configuring the health check IP address is optional for the BGP MED selection method, the health check IP address provides insight into the service connection health.
- **Routing best practice for SPA hub**

When advertising prefixes from SPA hubs, ensure that only the prefixes intended to be routed through SPA are advertised to FortiSASE security points of presence (PoPs). Avoid advertising the following prefixes, as they may unintentionally redirect traffic through SPA and disrupt FortiSASE routing behavior:

- 0.0.0.0/0 (default route)
- 0.0.0.0/1
- 128.0.0.0/1

FortiSASE security PoPs rely on their internal routing tables to handle internet-bound traffic from internal components. Advertising undesired prefixes to PoPs can result in traffic being misrouted through the SPA hub, resulting in connectivity issues.

Enabling endpoint to endpoint communication

FortiSASE enables administrators to configure and manage direct, secure communication between remote endpoints connected through the FortiSASE Cloud Security tunnel. This capability becomes available in the FortiSASE portal after configuring at least one Secure Private Access (SPA) Hub.

With this feature, remote endpoints such as laptops, desktops, or mobile devices connected via Secure Internet Access (SIA) can exchange data over an encrypted channel. This is particularly useful for collaboration scenarios where remote users need to share files, access peer-hosted services, or participate in real-time applications without sending traffic through external networks.

Traffic is routed between endpoints through the SPA Hub.

Administrators can enforce granular controls by defining Secure Private Access policies to specify allowed devices and permitted traffic types, thereby preventing unauthorized lateral movement between endpoints. Policy configuration in the FortiSASE portal is available under *Security* > *Policies* > *Secure Private Access* and should be applied as follows:

- You must configure *To hubs* and *From hubs* policies.
- For endpoints connected to the same Security PoP, you must also configure *Endpoint to endpoint* policies.

To enable the endpoint-to-endpoint communication:

1. Navigate to *Network* > *BGP*.
2. Enable the *Endpoint-to-endpoint Traffic* toggle.
3. Click *Save*.
4. On the SPA Hubs, you must re-announce the BGP prefixes learnt from FortiSASE Security PoPs.

To configure endpoint-to-endpoint traffic policies if endpoints are connected to same Security PoP:

1. Navigate to *Security* > *Policies* and select *Secure private access* tab.
2. Under the *Endpoint to endpoint* tab, click *Create*.
3. Enter the following details:

Field	Value
Name	Enter a suitable name.

Field	Value
Security posture tag	(Optional) Select a security posture tag that must be required for the endpoints.
User	Select *All Users* to allow all authenticated endpoints or select *Specify* to select a specific user group used to connect to Secure Internet Access to further restrict access only to specific authenticated users.
Service	Click + to select desired services to be allowed.
Schedule	Always
Action	Set *Accept* to allow the traffic, set *Deny* to block traffic.
Status	Set to *Enable* to enable the policy.

4. (Optional) Enable *Log Violation Traffic* to log denied traffic.
5. Click *OK*.

To configure To Hub and From Hub policies if endpoints are connected to different Security PoP:

- Refer to Configuring a private access policy for client-to-server traffic on page 126 and Configuring a private access policy for server-to-client traffic on page 128.

Configuring a new service connection

You can create a new service connection (hub) using one of the following BGP routing design methods:

- BGP per overlay (default)
- BGP on loopback

You configured the corresponding BGP routing design method under *Network > BGP*.

After you create a service connection, you can update its authentication method using *Update Authentication Method* to switch from using a preshared key (PSK) to a certificate or vice-versa. You can also use this option to update the existing authentication method settings, such as updating the PSK or updating the PKI user or certificate.

To configure service connections or hubs for BGP per overlay:

Example values for SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

1. Go to *Operations > Connectivity > Secure private access*.
2. Click *Create*.
3. (Optional) You can use an easy configuration key to simplify SPA setup on FortiSASE by automatically populating key fields in *Network > BGP* and *Create Secure Private Access Service Connection* based on the FortiGate hub configuration. The easy configuration key is available on FortiOS 7.4.5 and later versions when the FortiGate is configured as a hub using Fabric overlay orchestrator. The FortiGate must have a valid SPA Service Connection subscription and be registered under the same FortiCloud account as

FortiSASE. See SPA using a FortiSASE SPA hub with Fabric overlay orchestrator. Do the following to configure the key:

a. In *Network* > *BGP*, set the following attributes. Otherwise, you cannot use the key:

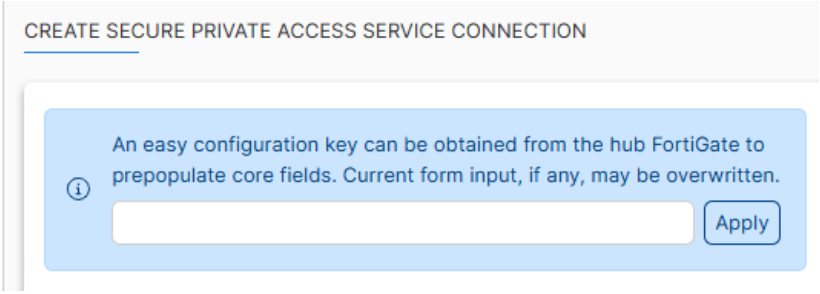
Network attribute	Must be configured as...
BGP Routing Design	*BGP per overlay*
Hub Selection Method	*Hub Health and Priority*

b. In *Operations* > *Connectivity* > *Secure private access*, click *Create*. Configure the following:

Network attributes	Must be configured as...
Authentication Method	*Pre-shared Key*

c. After completing the configuration on the hub FortiGate using Fabric overlay orchestrator, copy the key and paste it in the field in *Create Secure Private Access Network Configuration* on FortiSASE. See SPA easy configuration key for FortiSASE.

d. Click *OK*. FortiSASE autopopulates fields based off the FortiGate hub configuration.



e. Manually configure the remaining fields:

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1
Pre-shared key (PSK)	When *Authentication Method* is configured as *Pre-shared key*, define the hub PSK.	mysecretkey

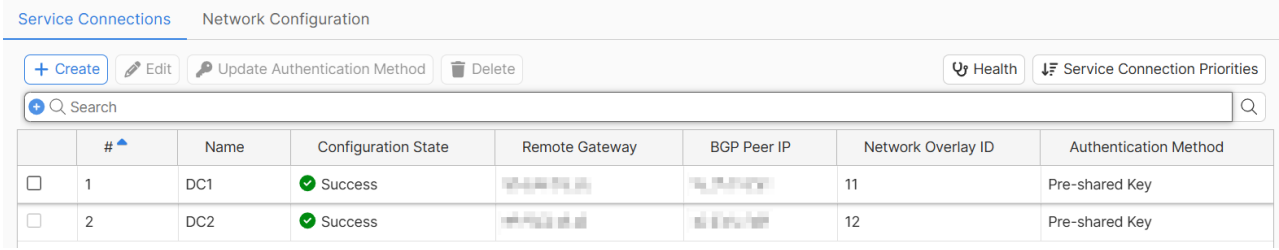
f. Click *OK* to finish configuring the SPA service connection. Once FortiSASE successfully configures the connection, it notifies you. The *Configuration State* column value changes from *Creating* to *Success*. You can proceed to Viewing health and VPN tunnel status on page 119 without completing the remaining steps in this section.

4. Fill in the rest of the fields with the attributes of the FortiGate hub or service connection. FortiSASE validates the input and notifies you of any invalid values.

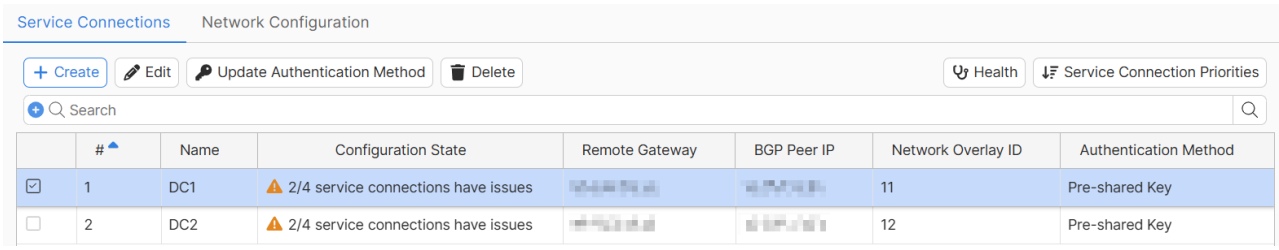
Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1
Autonomous System Number (ASN)	ASN number of the FortiGate hub. Only configurable if the support for multi-ASN configuration is enabled under *Network > BGP*.	65000
Remote Gateway	IPsec remote gateway (public IP address) for the hub.	1.2.3.4
Authentication Method	Method used to authenticate with the FortiGate hub. Supports *Pre-shared Key* (default) and *Certificate*.	*Pre-shared Key*
Pre-shared Key	If you configured *Authentication Method* as *Pre-shared Key*, define the hub PSK.	mysecretkey
PKI User	If you configured *Authentication Method* as *Certificate*, select the PKI user with a valid subject and CA certificate that FortiSASE uses to validate the hub certificate. You can directly create the PKI user from *Create* or via *Configuration > PKI*, then select it here.	mypeer
Certificate	If you configured *Authentication Method* as *Certificate*, select the certificate for the FortiSASE security PoP to present. You must import this certificate into FortiSASE via *System > Certificates* as a *Local Certificate*.	Fortinet_Factory
BGP Peer IP	On the hub, the IP address used as the BGP peer ID	10.20.1.253
Network overlay ID	Define a unique network ID for each hub. If a active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec tunnels towards each hub have different network overlay IDs.	2

5. Click *Save*.
6. Once FortiSASE successfully configures the service connection, it notifies you. The value in the *Configuration State* column changes from *Creating* to *Success*.
7. (Optional) Repeat the steps to configure up to a total of twelve service connections as necessary to support your secure private access service connection network topology. The following shows the GUI after

configuring two service connections:



If there are any issues with the underlying service connections for each hub, the *Configuration State* column displays the number of connections with issues. For example, for a FortiSASE instance with four security PoPs, if two of the four service connections for each hub have issues, FortiSASE displays these as follows:



To configure service connections or hubs for BGP on loopback:

> Example values for SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

1. Go to *Operations* > *Connectivity* > *Secure private access*.
2. Click *Create*.
3. For the *Create a Secure Private Access Service Connection* step, fill in the fields with the attributes of the FortiGate hub or service connection. FortiSASE performs input validation and notifies you of any invalid values.

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1
Autonomous System Number (ASN)	ASN number of the FortiGate hub. Only configurable if the support for multi-ASN configuration is enabled under *Network* > *BGP*.	65000
Remote Gateway	IPsec remote gateway (public IP address) for the hub.	1.2.3.4
Authentication Method	Method used to authenticate with the FortiGate hub. Supports *Pre-shared Key* (default) and *Certificate*.	*Pre-shared Key*

Network attributes	Description	Example
Pre-shared Key	When *Authentication Method* is configured as *Pre-shared Key*, define the hub PSK.	mysecretkey
PKI User	If you configured *Authentication Method* as *Certificate*, select the PKI user with a valid subject and CA certificate that FortiSASE uses to validate the hub certificate. You can directly create the PKI user from *Create* or via *Configuration > PKI*, then select it here.	mypeer
Certificate	When *Authentication Method* is configured as *Certificate*, select the certificate to be presented by the FortiSASE security PoP. You must import this certificate into FortiSASE via *System > Certificates* as a *Local Certificate*.	Fortinet_Factory
ADVPN Route Tag	For *BGP on loopback* only, ADVPN route tag number for spoke to tag incoming routes advertised from a hub. See Enhanced BGP next hop updates and ADVPN shortcut override.	1
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	10.20.1.253
Network overlay ID	Define a unique network ID for each hub. If a active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec tunnels towards each hub have different network overlay IDs.	2

4. (Optional) If on the same hub you have a redundant WAN interface configured as the gateway, you can configure an additional IPsec tunnel from FortiSASE to redundant WAN interface. This additional IPsec overlay can be typically used as a redundant IPsec overlay. This configuration option is only available for *BGP on loopback* routing design. A maximum of one backup or redundant IPsec tunnel can be configured per Service Connection.

   To create additional IPsec overlay, click *Create* and fill in the attributes below.

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1

Network attributes	Description	Example
Remote gateway	IPsec remote gateway (public IP address of redundant WAN interface) for the hub.	1.2.3.5
Authentication method	Method used to authenticate with the FortiGate hub. Supports *Pre-shared key* (default) and *Certificate*.	Pre-shared key
Pre-shared key (PSK)	When *Authentication Method* is configured as *Pre-shared key*, define the hub PSK. This can be same or different than the Main IPsec overlay PSK.	mysecretkey
Network Overlay ID	Define a unique network ID for each hub. If a active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec tunnels towards each hub have different network overlay IDs.	mypeer

5. Click *Save*.
6. Once FortiSASE successfully configures the service connection, it notifies you. The value in the *Configuration State* column changes from *Creating* to *Success*. For *BGP on loopback*, *Configuration State* is based on the first overlay connection to the hub. If you have redundant IPsec overlays configured for your Service Connection, the backup IPsec overlay will always appear below the Main overlay.
7. (Optional) Repeat the steps to configure up to a total of twelve service connections as necessary to support your secure private access service connection network topology.

To update the authentication method settings for a service connection:

1. Go to *Operations* > *Connectivity* > *Secure private access*.
2. Click *Update Authentication Method*.
3. Select the *Authentication Method* and configure the corresponding parameter(s):
   a. *New Pre-shared Key* when *Pre-shared Key* is selected.
   b. *PKI User* and *Certificate* when *Certificate* is selected.
4. Click *OK*. Once FortiSASE successfully updates the authentication method for the service connection, it notifies you with the message *Authentication method updated successfully*.

Considerations

- If a hub FortiGate behind a NAT device is configured using the Fabric overlay orchestrator, the easy configuration key does not include the NAT IP address. You must manually update *Remote Gateway* with the NAT device public IP address on FortiSASE and ensure required port forwarding is set up on the NAT device to allow IPsec traffic to pass through. For required port details, see Required services and ports on page 25.
- Any configuration changes on the hub FortiGate via Fabric overlay orchestrator generates a new easy configuration key and does not automatically update on FortiSASE. To avoid issues, copy the latest key from the hub after completing its configuration.
- For FortiSASE security points of presence (PoP), the SD-WAN performance SLA (health check) setting has the following default parameters:

- **Latency threshold**: 120 ms
- **Jitter threshold**: 55 ms
- **Packet loss threshold**: 1%

You can edit these parameters in FortiSASE. See Editing SLA thresholds on page 121.

Also, for FortiSASE security PoPs, the SD-WAN rule is configured with SLA mode, where the security PoPs choose the highest priority hub that satisfies the SLA to forward traffic.

In the SD-WAN rule used by each FortiSASE security PoP, the interface preference order matters when selecting equal priority hubs. Therefore, to define interface preference order, you must configure service connections in FortiSASE in the desired order of preference from the most preferred hub to the least preferred hub.

- Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following remaining network restrictions when network restrictions have been removed per Network restrictions removed on page 47, and ensure your network configuration does not overlap with them.

  The FortiExtender and LAN Extension control plane subnet are configurable (default subnet: 10.252.0.0/16). See IP management on page 274.
- For BGP per overlay, the FortiSASE security PoPs use their IPsec tunnel overlay interface(s) with IP address (es) assigned by the FortiGate hub(s) via IKE mode config for BGP peering with the FortiGate hub(s). The BGP peer IP address defined in the service connection(s) should be an IPsec interface on the FortiGate hub (s). For BGP on loopback, the FortiSASE security PoPs use their loopback interface with IP address assigned from the BGP router ID subnet for BGP peering with the FortiGate hub(s). The BGP peer IP address defined in the service connection(s) should be a loopback interface on the FortiGate hub(s). In both routing designs, the BGP peer IP address defined in each service connection should not fall within the BGP router ID subnet. A common strategy to avoid this is to pick a subnet, such as a /24, and allocate a portion of that subnet for the FortiSASE security PoPs, such as a /25, and the remaining portion of it for the FortiGate hub (s).
- **Routing best practice for SPA hub**

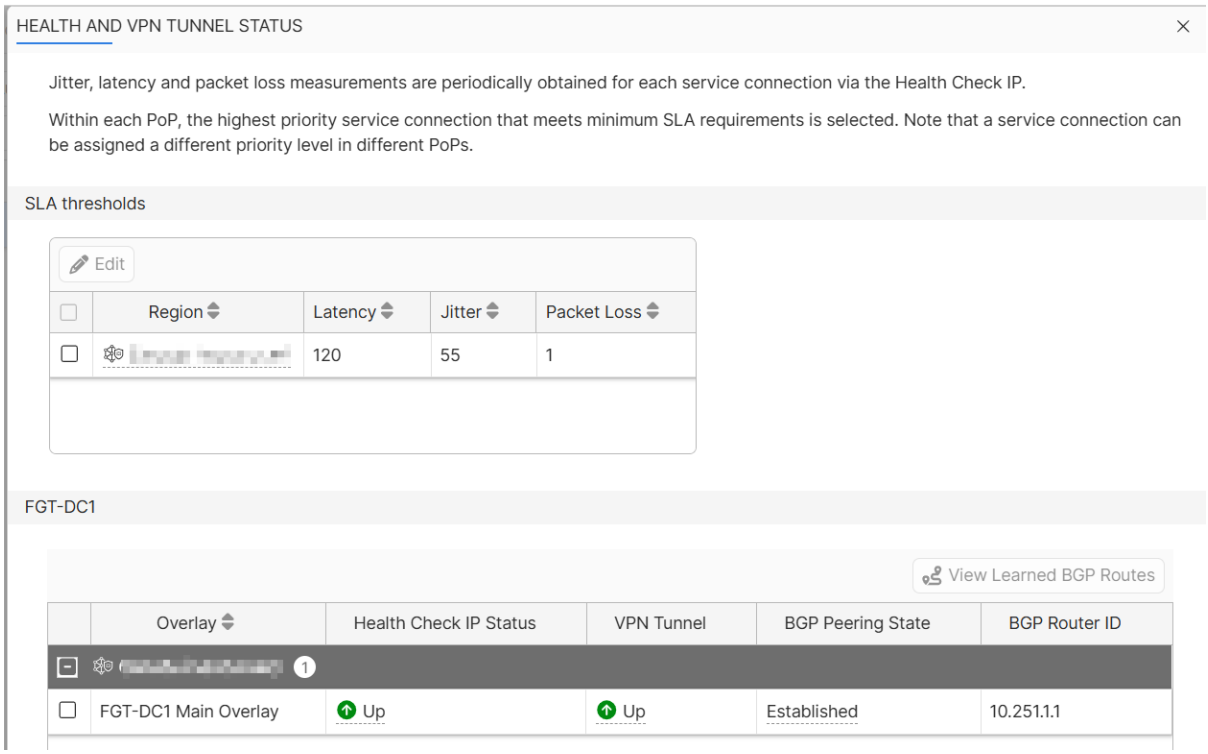
  When advertising prefixes from SPA hubs, ensure that only the prefixes intended to be routed through SPA are advertised to FortiSASE security points of presence (PoPs). Avoid advertising the following prefixes, as they may unintentionally redirect traffic through SPA and disrupt FortiSASE routing behavior:
  - 0.0.0.0/0 (default route)
  - 0.0.0.0/1
  - 128.0.0.0/1

  FortiSASE security PoPs rely on their internal routing tables to handle internet-bound traffic from internal components. Advertising undesired prefixes to PoPs can result in traffic being misrouted through the SPA hub, resulting in connectivity issues.
- Currently, FortiSASE only supports establishing an FSSO connection to a private FortiAuthenticator behind an SPA hub configured for BGP per overlay.

Viewing health and VPN tunnel status

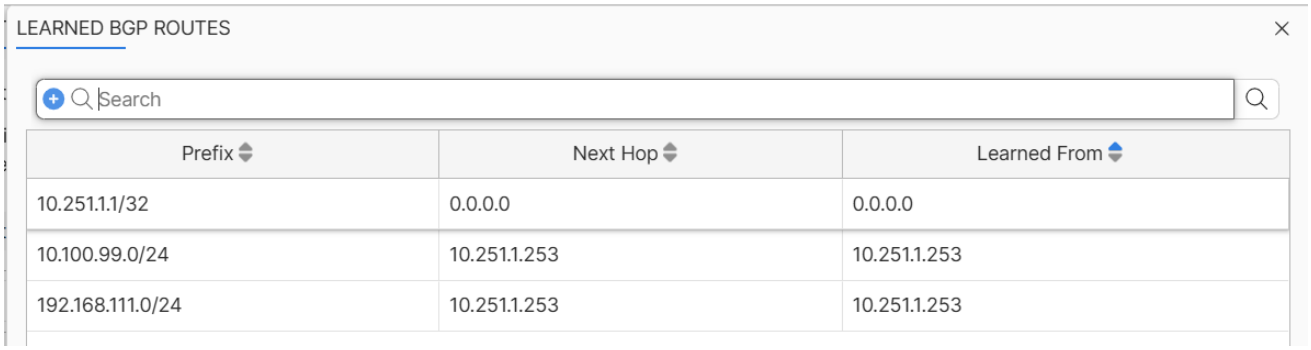
Click *Health* at the top of *Operations > Connectivity > Secure private access* to view *Health and VPN Tunnel Status*, which shows all configured hubs' health and VPN tunnel status. This page provides monitoring of the IPsec VPN tunnel, BGP peering state, and health check IP address status that you can use for troubleshooting scenarios with configured hubs.

For example, you can view hubs' health and VPN tunnel status from this page:



To display real-time SLA metrics useful for evaluating the quality of an SPA service connection between a Security PoP and SPA hub, you can use the SPA hub monitoring feature available under *Operations > Connectivity > Digital experience monitoring within SPA hub monitoring* tab. It is included with all FortiSASE remote user subscription types and does not require a separate subscription. See SPA hub monitoring on page 78.

For any hub, selecting a point of presence and clicking *View Learned BGP Routes* displays the learned BGP routes for that hub. For example, the learned BGP routes for the example DC1 are as follows:

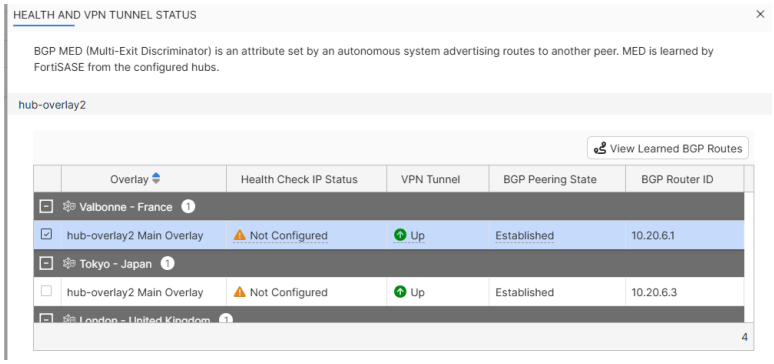


Similarly, to see the MED values that the BGP secure private access advertises, see Viewing MED values of SPA routes on page 121.

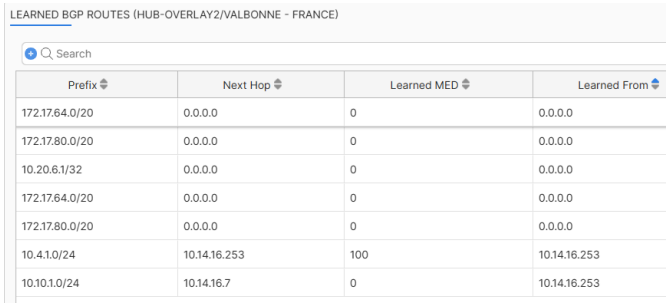
Viewing MED values of SPA routes

If you set *Hub Selection Method* under *Network* > *BGP* to *BGP MED* and configure multiple BGP hubs, FortiSASE can use the multiexit discriminator (MED) BGP path attribute attached with BGP routes that the secure private access (SPA) hub advertises to select a SPA hub for a given prefix. FortiSASE prefers the SPA hub that advertises the lowest MED value for a prefix. For details on configuring MED on a FortiGate device acting as an SPA hub, see BGP multi-exit discriminator.

To view the MED values that the SPA hub advertises, go to *Operations* > *Connectivity* > *Secure private access*, and click *Health* at the top of the page.



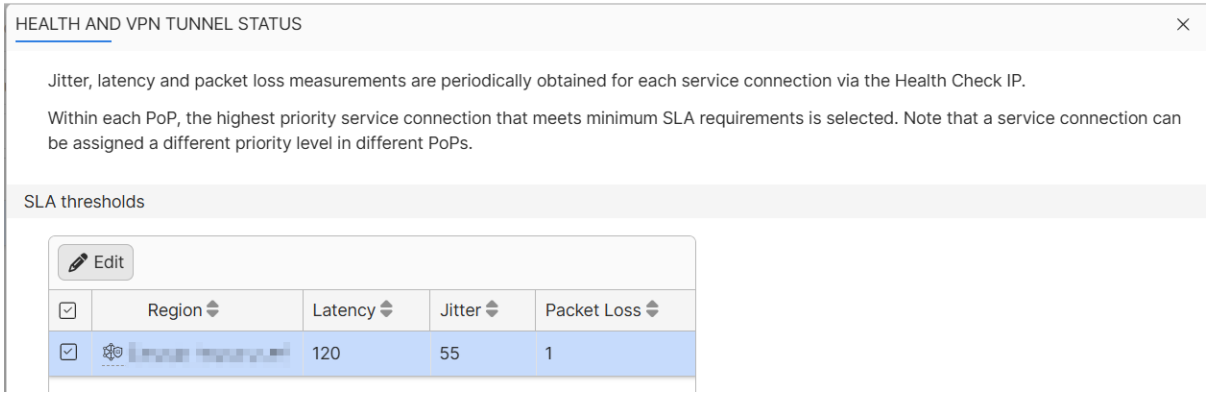
Select the desired service connection for a security PoP and click *View Learned BGP Routes*, and observe the MED values that display under the *Learned MED* column for each prefix.



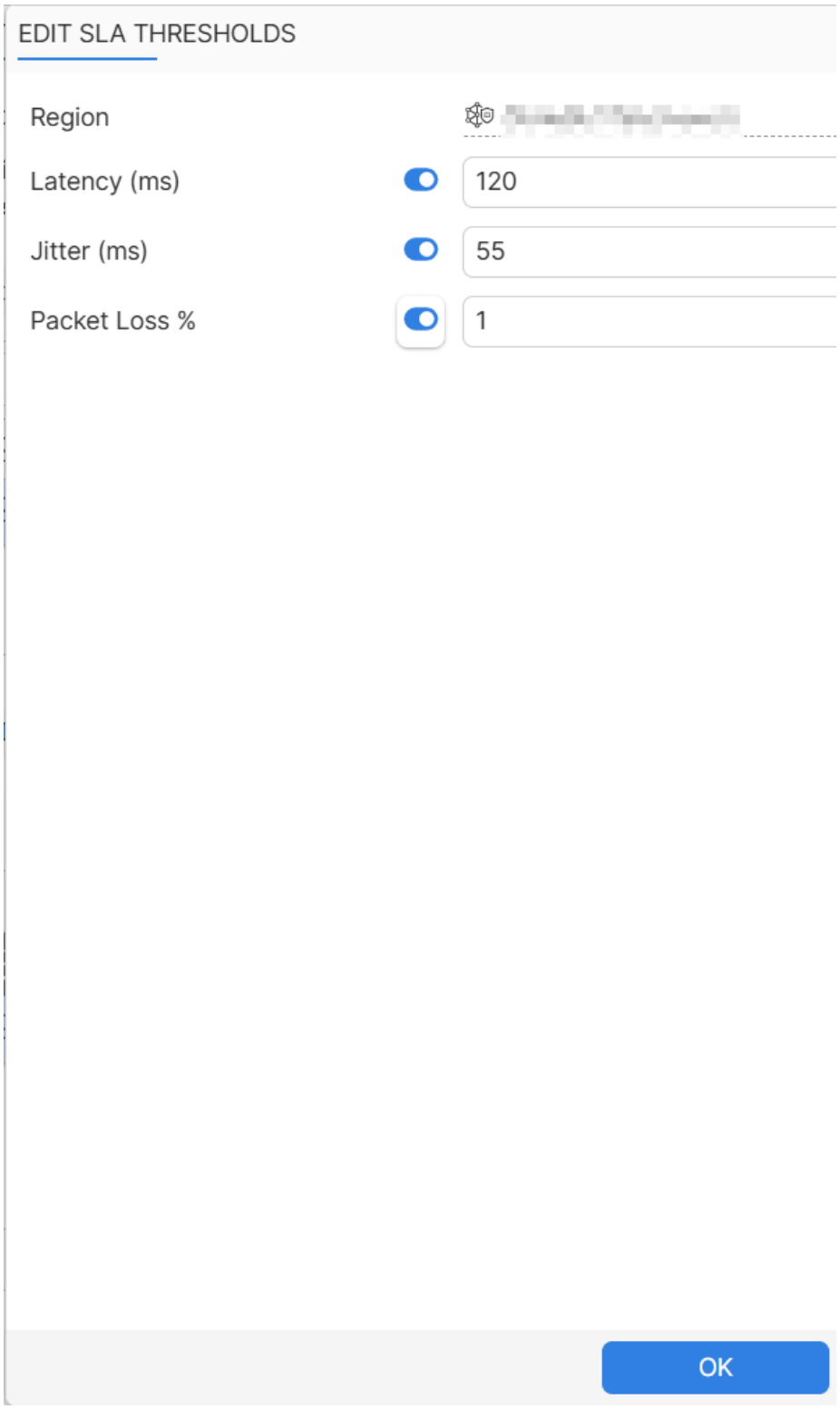
Editing SLA thresholds

You can customize latency, jitter, and packet loss SLA thresholds per security point of presence (PoP) used for secure private access hub SD-WAN health checks when *Hub Selection Method* is *Hub Health and Priority*. See Configuring network configuration on page 107.

SLA thresholds can be edited from *Operations* > *Connectivity* > *Secure private access* by selecting a service connection and clicking *Health*, and then selecting a security PoP and clicking *Edit* to edit the SLA thresholds.



In the *Edit SLA Thresholds* slide-in, the default SLA threshold values are listed. You can edit each threshold by enabling it, entering a suitable value and clicking *OK*.

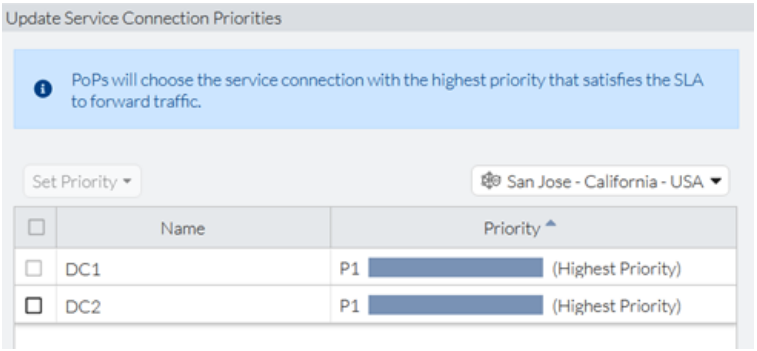

EDIT SLA THRESHOLDS
Region
Latency (ms)
120
Jitter (ms)
55
Packet Loss %
1
OK

Updating service connection priorities

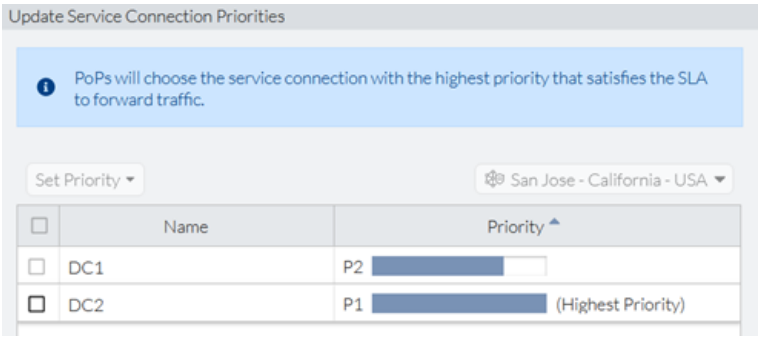
When you configure the hub selection method as hub health and priority within each point of presence (PoP), FortiSASE selects the highest priority hub that meets minimum SLA requirements. You can assign a hub a different priority level in different PoPs using the *Service Connection Priorities* page. A lower numerical value indicates a higher priority for a hub and vice-versa.

To update hub priorities:

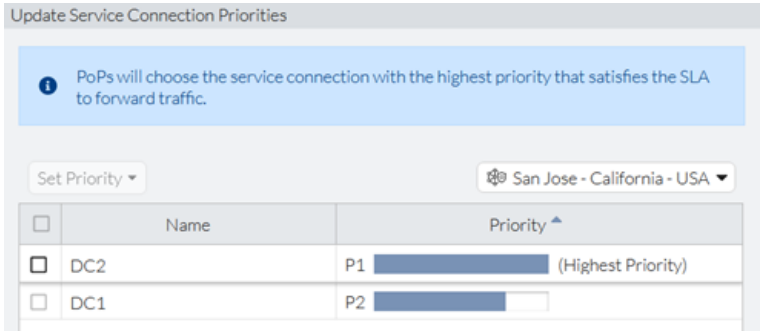
1. Go to *Operations* > *Connectivity* > *Secure private access*. Click *Service Connection Priorities*.
2. From the *Security PoP* dropdown list, select the desired security PoP hub. The example selects the San Jose – California – USA security PoP.



3. Select the desired hub and do one of the following to set the priority:
   - From the *Set Priority* dropdown list, select the desired priority. P1 is the highest priority, and P2 is the lowest priority.
   - Right-click the hub, select *Set Priority*, and select the desired priority. P1 is the highest priority, and P2 is the lowest priority.
4. Set the priority for each hub that influences hub selection. The example modifies hub priorities so that DC1 has a priority of P2 and DC2 has a priority of P1:



5. Click *Apply* to save the updated priority values. The page sorts the hubs from highest to lowest priority:



6. (Optional) Repeat the steps to update hub priorities for other security PoPs.

Deleting a hub configuration

You cannot directly update hub configuration. You must delete any current configuration and reconfigure using new settings to update it.

To delete a hub configuration:

1. Go to *Operations* > *Connectivity* > *Secure private access*.
2. Select the desired hub(s).

   If you have redundant IPsec overlay configured (only configurable in BGP on loopback routing design), deleting the Main IPsec overlay also deletes the redundant IPsec overlay configuration.

3. Click *Delete*.
4. In the confirmation dialog, click *OK*. The *Configuration State* column value for the hub changes from *Up* to *Deleting*. After a moment, FortiSASE removes the hub's table entry and deletes the hub configuration.

Configuring SPA using the REST API

You can perform secure private access (SPA) configuration using the FortiSASE REST API to manage the common SPA network connection and service connections to FortiGate SPA hubs and retrieve the status of these connections. See Appendix B - REST API on page 811.

All SPA configuration operations are possible in the REST API except for viewing health and VPN tunnel status.

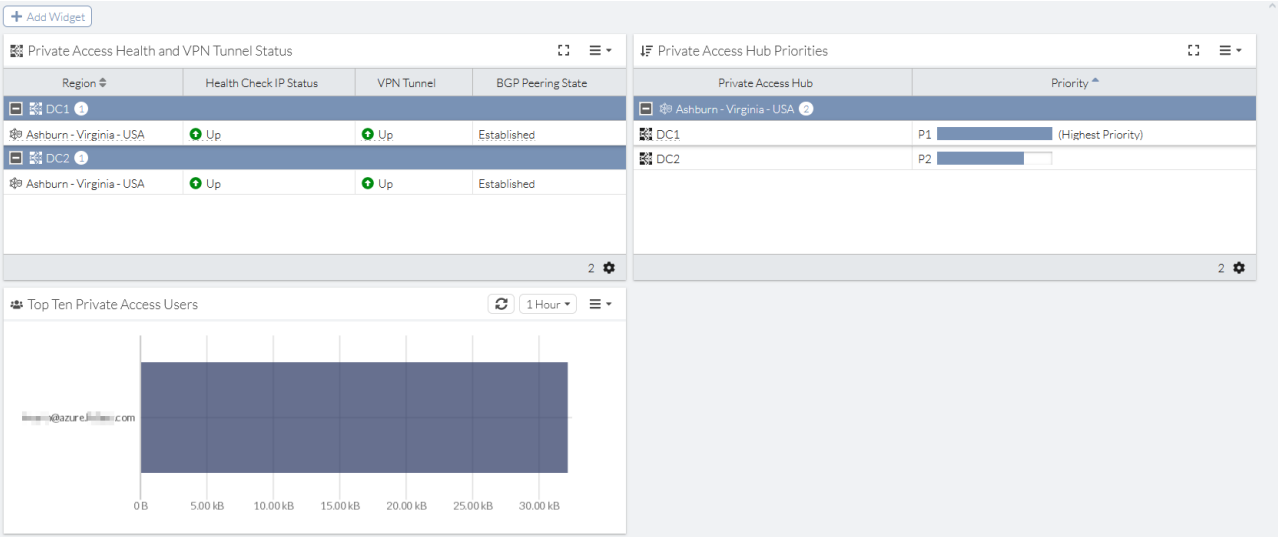
Only BGP on loopback supports multiple IPsec overlays in the REST API.

Monitoring private access hubs

To monitor private access hubs when you have configured them, view the following widgets in the *Monitoring* > *Dashboards* > *Private Access* page:

- Private Access Health and VPN Tunnel Status
- Private Access Hub Priorities
- Top Ten Private Access Users

The following provides private access widgets with data for two private access hubs:



Configuring a private access policy for client-to-server traffic

Secure private access (SPA) client-to-server communication is the typical SPA use case, allowing traffic initiated from remote users (agent users, proxy users, edge devices) to SPA hubs (or local networks behind SPA hubs).

For details on SPA server-to-client communication, see Configuring a private access policy for server-to-client traffic on page 128.

To configure a private access policy from remote agents and edge devices to SPA hubs:

1. Go to *Security* > *Traffic* > *Policies*.
2. Click the *Secure private access* tab and then click the *To hubs* subtab.
3. Click *Create* to create a new policy.
4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• *All*: all FortiSASE agents and edge devices • *Agent users*: remote endpoint users • *Edge Device*: Edge devices such as FortiExtender
Source	• *All Edge Devices*: Applies to all edge devices • *Specify*: specify selected hosts and host groups if you selected *Agent users*, or authorized Edge devices if you selected *Edge*

Field	Value
	Device.
User	• *Specify*: specify selected users and user groups for all source scopes • *Captive Portal Exempt*: If *Source Scope* is set to *Edge Device*, exempt the edge device traffic from encountering a captive portal to determine the identity of a connected endpoint. By default, a captive portal is enforced when edge device traffic matches policies with *Source Scope* set to *All*.
Destination	• *Private Access Traffic*: all private access traffic • *Specify*: specify selected private access hosts or host groups
Service	Click *+* and select services or service groups.
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select a profile group.
Basic Certificate Inspection Override	Enabled or disabled. When this option is enabled, the SSL inspection profile in the selected profile group is replaced by a basic certificate-inspection profile. If you need more granular control over SSL certificate inspection, create and assign a new security profile group with custom settings.
Schedule	Select *always* or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

5. Click *OK*.

To configure a private access policy from proxy users to SPA hubs:

1. Go to *Security* > *Traffic* > *Proxy policies*.
2. Click the *Secure private access* tab and then click the *To hubs* subtab.
3. Click *+Create* to create a new policy.
4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• *All*: all HTTP and HTTPS traffic from proxy users • *Specify*: specify selected hosts and host groups
User	• *All Proxy Users*: All proxy users • *Specify*: specify selected users or users groups

Field	Value
Destination	• *Private Access Traffic*: all private access traffic • *Specify*: specify selected private access hosts or host groups
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select a profile group.
Basic Certificate Inspection Override	Enabled or disabled. When this option is enabled, the SSL inspection profile in the selected profile group is replaced by a basic certificate-inspection profile. If you need more granular control over SSL certificate inspection, create and assign a new security profile group with custom settings.
Schedule	Select *always* or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

5. Click *OK*.

Considerations

- For SSL remote agents, whenever changes are made to an existing Internet Access or Private Access policy, they take effect only after SSL agents reconnect to FortiSASE.
- With the addition of support for identity-based policies for edge devices in FortiSASE 24.3.a, the behaviour of edge device traffic based on policies has changed in existing FortiSASE instances:
  - Any policies you created before FortiSASE 24.3.a, specifically for edge devices, namely, policies with *Source Scope* set to *Edge Devices* will have *User* set to *Captive Portal Exempt*.
  - Any policies you created before FortiSASE 24.3.a with *Source Scope* set to *All* will not be modified. Therefore, any edge devices whose traffic matched an *All* allow policy before will now have authentication enforced using the captive portal. You must explicitly create a new exemption policy and place it above any *All* allow policies to avoid captive portal authentication for any impacted edge devices. See Configuring an exemption policy for an edge device on page 191.
- When SSO authentication is used with the captive portal for edge devices, you must add an exemption policy for the SAML IdP URLs specified using hosts or infrastructure selections for the Destination field to allow SSO authentication traffic destined for the IdP to bypass the captive portal. See Configuring an exemption policy for SSO authentication for Entra ID on page 190.

Configuring a private access policy for server-to-client traffic

Secure private access (SPA) server-to-client communication allows traffic initiated from SPA hubs (or local networks behind SPA hubs) to remote users (currently agents only). This communication requires the Remote agent and edge device user identification on page 24 feature and additional configuration steps on the FortiGate SPA hub itself. See Prerequisites and considerations on page 130.

For details on SPA client-to-server communication, see Configuring a private access policy for client-to-server traffic on page 126.

To configure a private access policy to remote users from SPA hubs:

1. Go to *Security* > *Traffic* > *Policies*.
2. Click the *Secure private access* tab and then click the *From hubs* subtab.
3. Click *+Create* to create a new policy.
4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• *Private Access Traffic*: all private access traffic • *Specify*: specify selected private access hosts or host groups.
Destination	• *All*: all FortiSASE users/devices • *Agent users*: remote endpoint users
Service	Click *+* and select services or service groups.
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select a profile group.
Basic Certificate Inspection Override	Enabled or disabled. When this option is enabled, the SSL inspection profile in the selected profile group is replaced by a basic certificate-inspection profile. If you need more granular control over SSL certificate inspection, create and assign a new security profile group with custom settings.
Schedule	Select *always* or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

5. Click *OK*.

To configure a FortiGate SPA hub firewall policy required for traffic from SPA hubs:

On the FortiGate SPA hub, you must configure a firewall policy allowing traffic from the desired local interface(s) or spokes behind the hub to the remote agents and edge device users via the SPA overlay. This policy ensures that traffic from networks connected to the FortiGate SPA hub are allowed to FortiSASE remote agents and edge device users.

In this example, for the FortiGate SPA hub, the SPA overlay (IPsec tunnel) is defined as *fgt_hub1* and the local connected networks DMZ_HQ and LAN_HQ are on port2 and port4, respectively. Therefore, we create a policy that allows traffic from the local connected networks on the hub to the FortiSASE remote agents.

1. On the FortiGate SPA hub, go to *Policy & Objects* > *Firewall Policy*.
2. Click *+Create New* to create a new policy.
3. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Incoming Interface	*DMZ_HQ (port2)* *LAN_HQ (port4)*
Outgoing Interface	*fgt_hub1*
Source	*all*
Destination	*All*
Schedule	*always*
Service	*ALL*
Action	*ACCEPT*
NAT	You can enable or disable NAT depending on the IP configuration of the organization's FortiGate SPA hub.
IP Pool Configuration	*Use Outgoing Interface Address*

4. Click *OK*.

Prerequisites and considerations

Prerequisites

- The display of the *From hubs* subtab and resulting functionality requires a FortiSASE instance with the remote agent identification feature, which is included with new instances created after the FortiSASE 24.3.b release and may need to be added on instances created before that release. See Remote agent and edge device user identification on page 24. Otherwise, the *From hubs* subtab does not display.
- Currently, FortiSASE supports traffic from SPA hubs to remote agents only.
- On the FortiGate SPA hub, you must configure a firewall policy allowing traffic from the desired local interface(s) or spokes behind the hub to the remote agents via the SPA overlay. This policy ensures that traffic from networks connected to the FortiGate SPA hub are allowed to FortiSASE remote agents.

Considerations

- For SSL remote agents, whenever changes are made to an existing Internet Access or Private Access policy, they take effect only after SSL agents reconnect to FortiSASE.
- With the addition of support for identity-based policies for edge devices in FortiSASE 24.3.a, the behaviour of edge device traffic based on policies has changed in existing FortiSASE instances:
  - Any policies you created before FortiSASE 24.3.a, specifically for edge devices, namely, policies with *Source Scope* set to *Edge Devices* will have *User* set to *Captive Portal Exempt*.
  - Any policies you created before FortiSASE 24.3.a with *Source Scope* set to *All* will not be modified. Therefore, any edge devices whose traffic matched an *All* allow policy before will now have

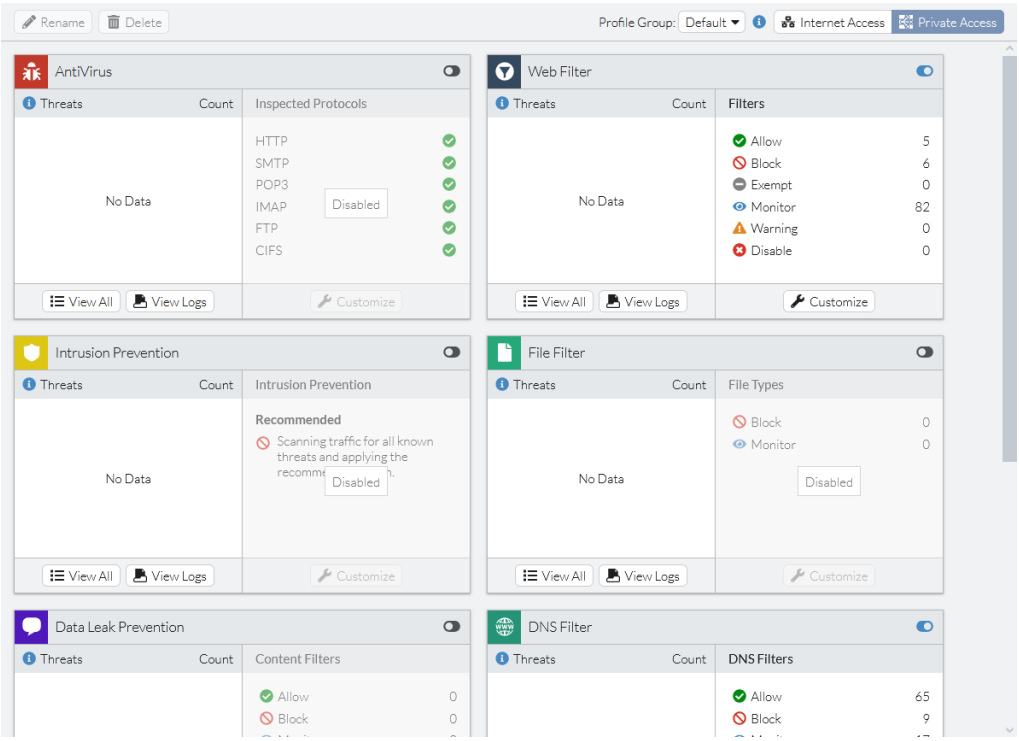
authentication enforced using the captive portal. You must explicitly create a new exemption policy and place it above any *All* allow policies to avoid captive portal authentication for any impacted edge devices. See Configuring an exemption policy for an edge device on page 191.

- When SSO authentication is used with the captive portal for edge devices, you must add an exemption policy for the SAML IdP URLs specified using hosts or infrastructure selections for the Destination field to allow SSO authentication traffic destined for the IdP to bypass the captive portal. See Configuring an exemption policy for SSO authentication for Entra ID on page 190.

Configuring a private access security profile

To configure a private access security profile:

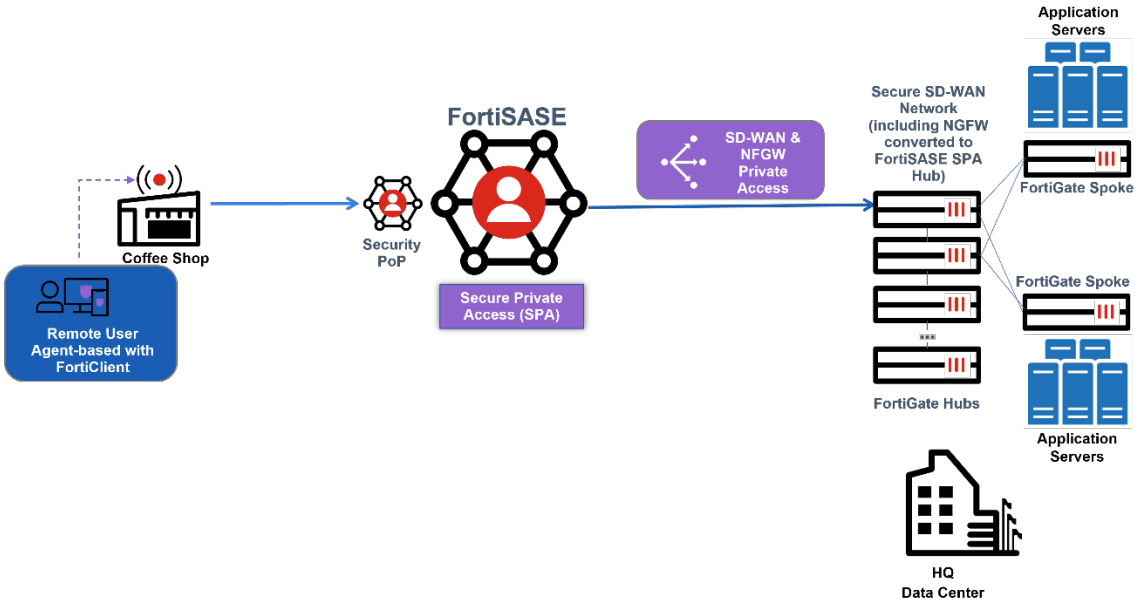
1. Go to *Security* > *Traffic* > *Security profiles*.
2. Enable or disable profiles as desired. For enabled security profiles, customize as desired.



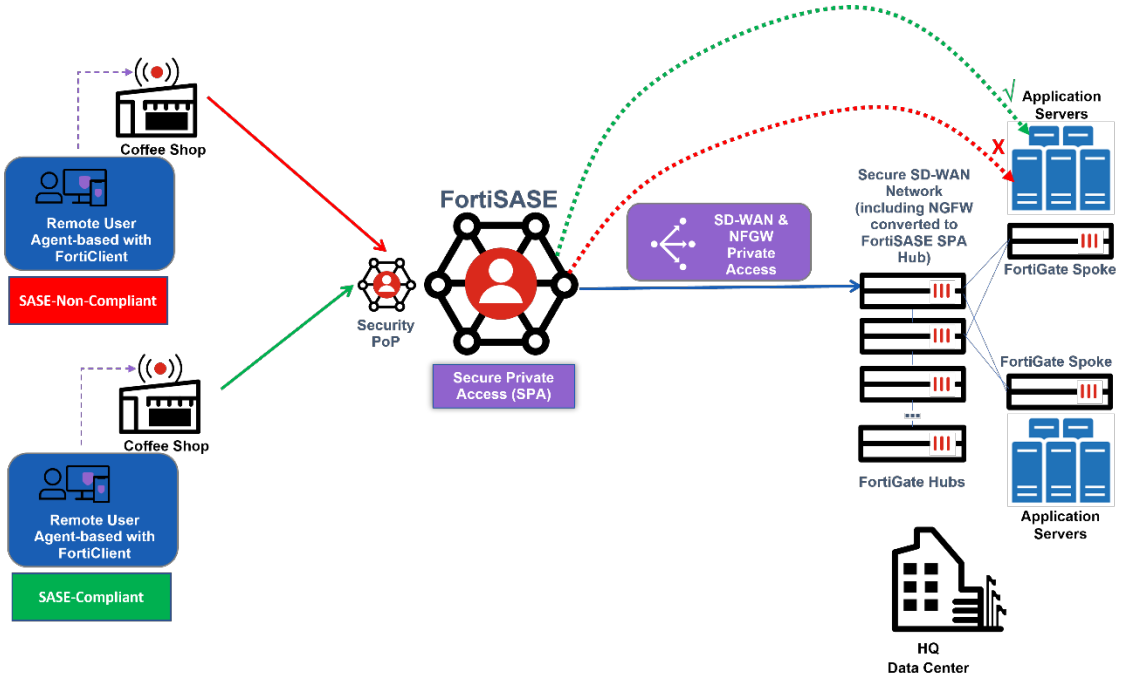
The security settings for internet and private access are identical. For details on configuring security settings, see Security profiles on page 312.

Configuring security posture tags in private access policies

By default, for the secure private access (SPA) use cases using a FortiGate hub configured through the *Secure private access* page, all FortiSASE agent-based remote users have unrestricted access to private applications behind the hub network through an Allow-All Private Traffic private access policy.



To restrict SPA to private applications of any protocol (TCP, UDP, ICMP, and so on) behind a FortiGate hub, in the FortiSASE portal you can configure security posture tagging rules that apply security posture tags to remote users based on specified endpoint posture checks. You can then specify these tags as the source in a dynamic private access policy to deny or allow access as desired.



Using security posture tags to configure dynamic policies

You can use tags to build dynamic policies that you do not need to manually reconfigure whenever an endpoint's status changes. For example, consider that you want to deny Windows endpoints without antivirus (AV)

installed and running as detected by FortiClient from accessing private applications behind the FortiGate hub. You would configure the following:

- Rule that applies a SASE-Compliant tag to Windows endpoints that FortiClient detects as having AV software installed and running
- Rule that applies a SASE-Non-Compliant tag to Windows endpoints that FortiClient detects as not having AV software installed
- Private access policy that allows Windows endpoints with the SASE-Compliant tag to access a specific server behind the FortiGate hub
- Private access policy that denies Windows endpoints with the SASE-Non-Compliant tag from accessing a specific server behind the FortiGate hub

As FortiSASE receives information from endpoints, it dynamically removes and applies the SASE-Non-Compliant tag to endpoints. For example, if an endpoint that previously had the SASE-Non-Compliant tag applied has its AV software installed or enabled as detected by FortiClient, then FortiSASE automatically removes the SASE-Non-Compliant tag from the endpoint and applies the SASE-Compliant tag instead. Consequently, the endpoint would then be able to access private applications behind the FortiGate hub.

Therefore, a dynamic policy is a policy that has one or more security posture tags specified as its source.

For details on configuring dynamic tags and policies, see Security posture tags and tagging rules on page 486.

Configuration workflow

You can follow this configuration workflow, which the document describes in detail using the example configuration of a dynamic private access policy that allows access to private applications, which in this example is a private server behind the FortiGate hub:

1. Configure a security posture tagging rule set for compliant endpoints.
2. Configure a security posture tagging rule set for non-compliant endpoints.
3. Configure a dynamic private access policy to allow access to a specific private server from compliant endpoints.
4. Configure a dynamic private access policy to deny access to a specific private server from non-compliant endpoints.
5. Test the dynamic private access policies using ICMP ping to the specific private server from a compliant endpoint and from a non-compliant endpoint, respectively.



A similar workflow applies to a private access policy that allows or denies access to applications of any other protocols besides ICMP, such as TCP or UDP applications.

Configuring security posture tagging rule sets to dynamically tag agent-based remote users

This example demonstrates how to configure security posture tag names and tagging rule sets with the following posture checks:

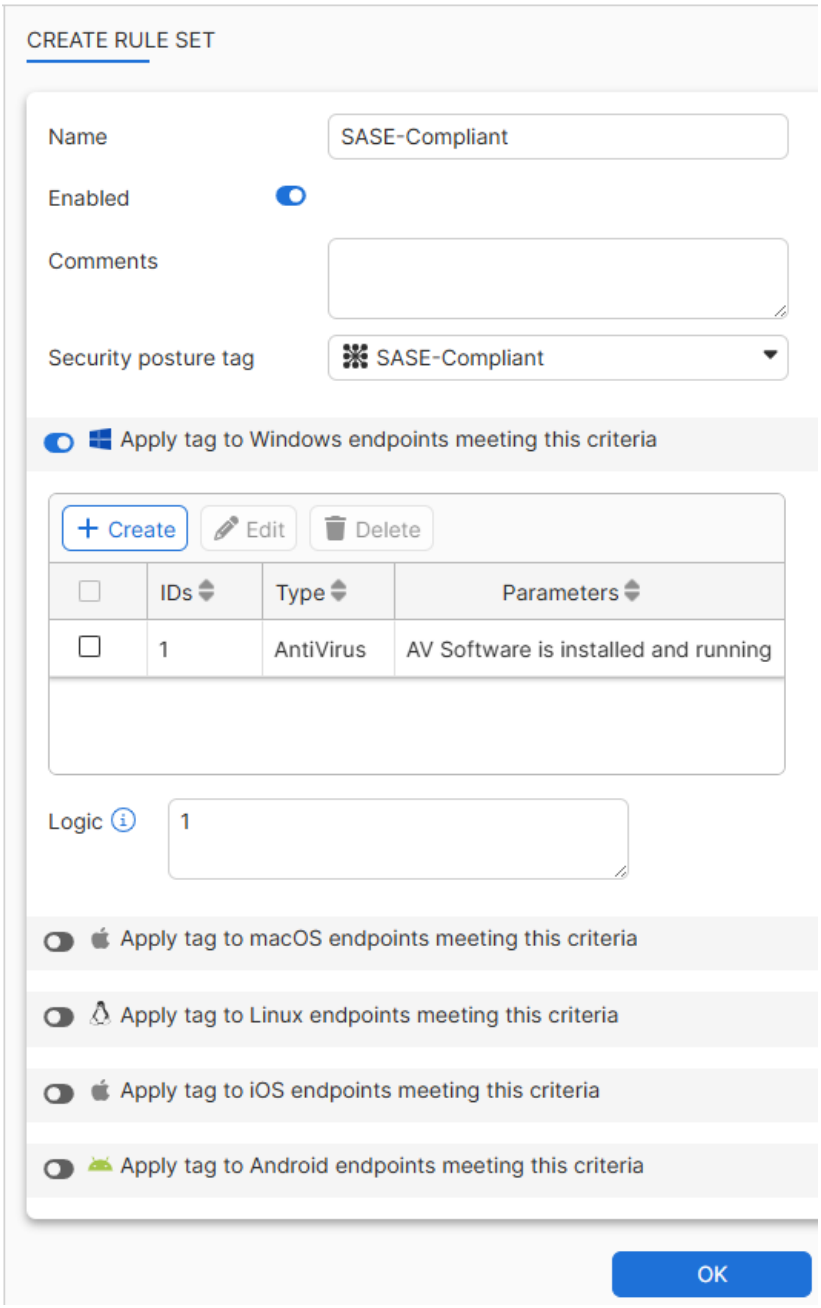
- Endpoint is running Windows and has antivirus (AV) software installed and running
- Endpoint is running Windows and does not have AV software installed or running

See Security posture tags and tagging rules on page 486.

To configure a tagging rule set for compliant endpoints:

1. Go to *Endpoint management* > *Security posture tags* > *Tagging rules*, and click *Create*.
2. In the *Name* field, enter the desired rule set name. For example, SASE-Compliant.
3. Toggle *Enabled* on or off to enable or disable the rule.
4. (Optional) In the *Comments* field, enter any desired comments.
5. In the *Security posture tag* dropdown list, do one of the following:
   - Select an existing tag.
   - Create a tag named SASE-Compliant. Click *+* and in the slide in enter desired tag name, SASE-Compliant. The tag name can be same or different as the rule name. Click *OK*.
6. Enable *Apply tag to Windows endpoints meeting this criteria*.
7. Configure the rule:
   a. Click *Create*.
   b. From the *Rule type* dropdown list, select *Antivirus*.
   c. From the *Antivirus* dropdown list, select *AntiVirus Software is installed and running*.
   d. Click *OK*.

8. Click *OK*.



To configure a security posture tagging rule set for non-compliant endpoints:

1. Go to *Endpoint management* > *Security posture tags* > *Tagging rules*, and click *Create*.
2. In the *Name* field, enter the desired rule set name. For example, SASE-Non-Compliant.
3. Toggle *Enabled* on or off to enable or disable the rule.
4. (Optional) In the *Comments* field, enter any desired comments.

5. In the *Security posture tag* dropdown list, do one of the following:
   - Select an existing tag.
   - Create a tag named SASE-Compliant. Click *+* and in the slide in enter desired tag name, SASE-Compliant. The tag name can be same or different as the rule name. Click *OK*.
6. Enable *Apply tag to Windows endpoints meeting this criteria*.
7. Configure the rule:
   a. Click *Create*.
   b. From the *Rule type* dropdown list, select *Antivirus*.
   c. Enable *Negate*.
   d. From the *Antivirus* dropdown list, select *AntiVirus Software is installed and running*.
   e. Click *OK*.
8. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
9. Click *OK*.

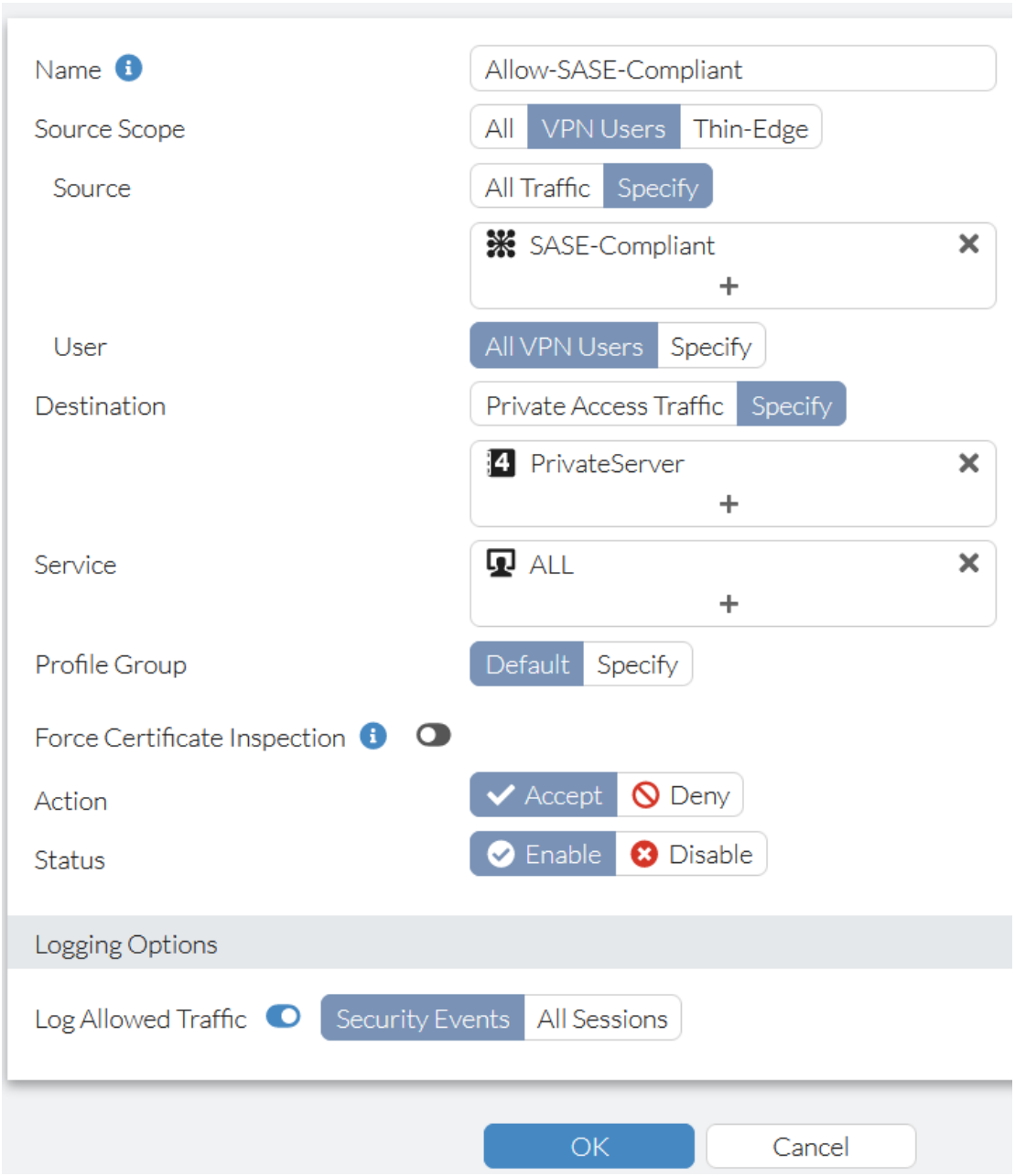
Configuring dynamic private access policies using security posture tags

This example demonstrates how to configure dynamic private access policies using the security posture tags that you created in Configuring security posture tagging rule sets to dynamically tag agent-based remote users on page 133 to allow endpoints tagged as SASE-Compliant with access to selected private resources and to deny access to selected private resources for endpoints tagged as SASE-Non-Compliant.

To configure a dynamic private access policy for compliant endpoints:

1. Go to *Security > Traffic > Policies*.
2. Select *Secure private access* to display the list of private access policies
3. Click *Create*.
4. Configure the policy:
   a. For *Name*, enter Allow-SASE-Compliant.
   b. For *Source Scope*, select *Agent users*.
   c. In the *Source* field, select *Specify* and click *+*. From the *Select Entries* panel, under *ZTNA Tag > Private Access*, select the *SASE-Compliant* tag.
   d. For *Destination*, select *Specify*, click *+*, and in the *Select Entries* panel click *+Create* and click *IPv4 Host* to a create a new host for the specific server as follows:
      i. For *Location*, select *Private Access Hub*.
      ii. For *Category*, *IPv4 Host* is selected.
      iii. In the *Name* field, enter the desired name. In this example, the name is PrivateServer.
      iv. From the *Type* dropdown list, select *Subnet*.
      v. In the *IP/Netmask* field, enter 10.100.99.101/32.
      vi. Click *OK*.
      Select the newly created host to set it as the *Destination*.
   e. For *Service*, click *+* and from the *Select Entries* panel select *ALL*.
   f. For *Action*, select *Accept*.
   g. For *Status*, select *Enable*.

5. Click *OK*.

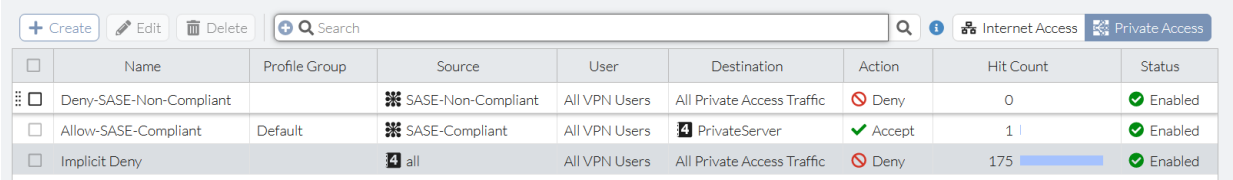


6. In *Security > Traffic > Policies* with *Secure private access* selected, ensure that you order the policies so that the Allow-SASE-Compliant policy is before the Allow-All Private Traffic policy. With this ordering of policies, FortiSASE allows endpoints that match the dynamic policy access to the specific private server.

To configure a dynamic private access policy for non-compliant endpoints:

1. Go to *Security > Traffic > Policies*.
2. Select *Secure private access* to display the list of private access policies
3. Click *Create*.

4. Configure the policy:
   a. For *Name*, enter Deny-SASE-Non-Compliant.
   b. For *Source Scope*, select *Agent users*.
   c. In the *Source* field, select *Specify* and click *+*. From the *Select Entries* panel, under *ZTNA Tag* > *Private Access*, select the *SASE-Non-Compliant* tag.
   d. For *Destination*, select *Private Access Traffic*.
   e. For *Service*, click *+* and from the *Select Entries* panel select *ALL*.
   f. For *Action*, select *Deny*.
   g. For *Status*, select *Enable*.
5. Click *OK*.
6. In *Security* > *Traffic* > *Policies* with *Secure private access* selected, do the following:
   a. Ensure that you order the policies so that the Allow-SASE-Compliant policy is before the Allow-All Private Traffic policy. With this ordering of policies, FortiSASE allows endpoints that match the dynamic policy access to the specific private server.
   b. Delete the Allow-All Private Traffic and Allow-All Private Traffic Thin edge policies.

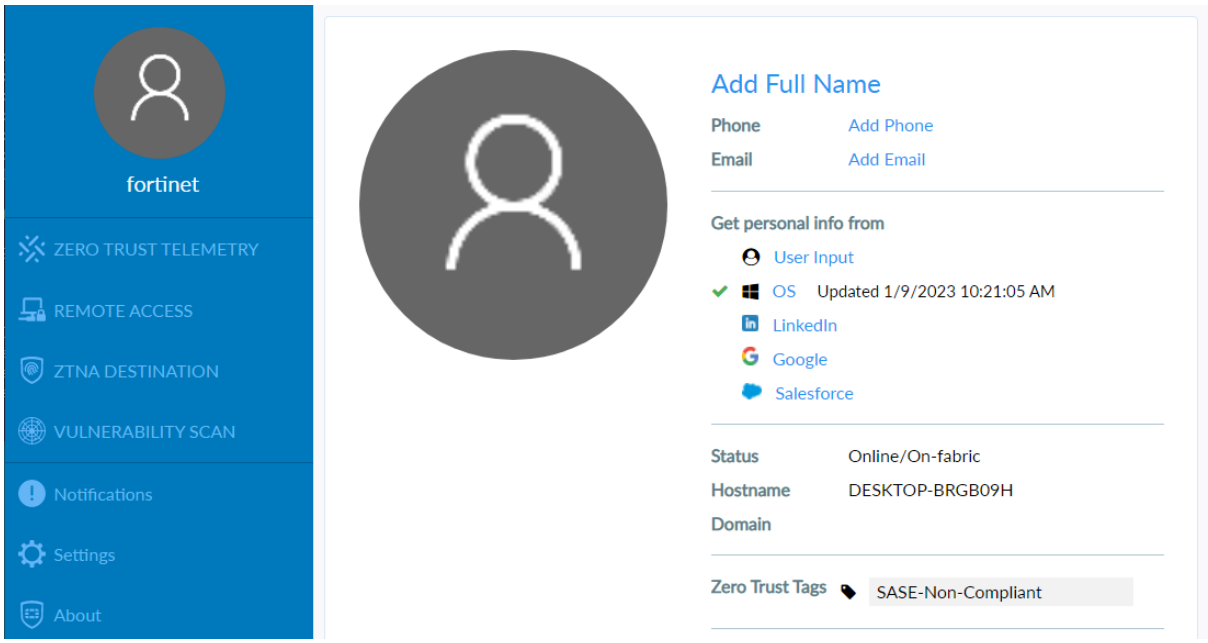


Testing the dynamic private access policy

(Optional) To display tags on the FortiClient endpoint:

1. In FortiSASE, go to *Endpoint management* > *Endpoint profiles*.
2. Create a new profile or edit an existing one.
3. On the *FortiClient GUI settings* tab, enable *Show security posture tags*.

4. Click *OK*. When this option is enabled, detected tags appear on the FortiClient avatar page.



To test that FortiSASE allows a FortiClient endpoint tagged as SASE-Compliant access to a private server:

1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the agent authentication defined on FortiSASE. Click *Connect*.
4. In Windows Defender, set *Real-time protection* to *On* as Stay protected with Windows Security describes. This turns on antivirus (AV) and ensures that FortiSASE dynamically tags the endpoint as compliant.
5. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Compliant Zero Trust tag applied.
6. In Windows Command Prompt, enter `ping 10.100.99.101` to test an ICMP ping to the specified private server with IP address 10.100.99.101 behind the FortiGate hub.
7. Observe the following output indicating the ping succeeded since FortiSASE allows access:

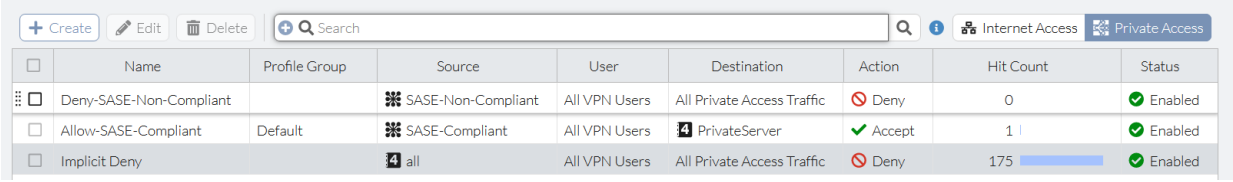
```
C:\> ping 10.100.99.101

Pinging 10.100.99.101 with 32 bytes of data:
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=136ms TTL=62

Ping statistics for 10.100.99.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 136ms, Maximum = 137ms, Average = 136ms
```

8. In FortiSASE, in *Security* > *Traffic* > *Policies*, observe that the Allow-SASE-Compliant dynamic private access policy hit count increased and that the Deny-SASE-Non-Compliant dynamic private access policy

hit count has not changed.



To test that FortiSASE denies a FortiClient endpoint tagged as SASE-Non-Compliant access to a private server:

1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the agent authentication defined on FortiSASE. Click *Connect*.
4. In Windows Defender, set *Real-time protection* to *Off* as Stay protected with Windows Security describes. This turns off AV and ensures that FortiSASE dynamically tags the endpoint as non-compliant.
5. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Non-Compliant Zero Trust tag applied.
6. In Windows Command Prompt, enter `ping 10.100.99.101` to test an ICMP ping to the specified private server with IP address 10.100.99.101 behind the FortiGate hub.
7. Observe the following output indicating the ICMP ping has timed out since access to the specific server is denied:

```
C:\> ping 10.100.99.101

Pinging 10.100.99.101 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.100.99.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

8. In FortiSASE, in *Security* > *Traffic* > *Policies*, observe that the Allow-SASE-Compliant dynamic private access policy hit count has not changed and that the Deny-SASE-Non-Compliant dynamic private access policy hit count increased.

Verifying IPsec tunnels on the FortiGate hub

Verify that the IPsec tunnels immediately appear on the FortiGate hub from all configured FortiSASE security points of presence(PoP).

On the FortiGate hub, verify that the IPsec tunnels from the FortiSASE security PoPs acting as spokes by going to *Dashboard* > *Network* and clicking the *IPsec* widget to expand it.

To verify IPsec tunnels using the CLI:

1. Run at least one of the following commands. For a VDOM-enabled hub FortiGate, enter the proper VDOM before running the command(s):
```
diagnose vpn ike gateway list
diagnose vpn tunnel list
get vpn ipsec tunnel summary
```
   a. For `diagnose vpn ike gateway list`, confirm that the phase 1 IKE security associations (SA) for the FortiSASE security PoPs with corresponding peer IDs are established. Confirm that the IKE SA and IPsec SA show created and established as 1/1. The following shows sample output for this command:

```
vd: root/0
name: ToSpokes_1
version: 2
…
created: 923s ago
peer-id: region8-fos001-tiui7pzu-1
…
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  …
  direction: responder
  status: established 923-923s ago = 10ms
  proposal: aes128-sha256
  child: no
  …
  PPK: no
  message-id sent/recv: 1/2
  lifetime/rekey: 86400/85206
  DPD sent/recv: 00000001/00000001
  peer-id: region8-fos001-tiui7pzu-1
```

2. For `diagnose vpn tunnel list`, confirm that the phase 2 IPsec SAs for the FortiSASE security PoPs are established. Confirm that the SA field exist and are populated. The following shows sample output for this command:

```
name=ToSpokes_1 ver=2 serial=3ba 208.85.68.228:4500->154.52.6.89:52270 tun_id=10.150.160.2
tun_id6=::10.0.3.147 dst_mtu=1500 dpd-link=on
 weight=1
bound_if=25 lgwy=static/1 tun=intf/2 mode=dial_inst/3 encap=none/9096 options[2388]=npu rgwy-
chg rport-chg frag-rfc  run_state=0 accept_
traffic=1 overlay_id=0
parent=ToSpokes index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0 ad=s/1
stat: rxp=2689 txp=1042 rxb=16418 txb=18338
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=52270
proxyid=ToSpokes proto=0 sa=1 ref=4 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1422 expire=42258/0B replaywin=2048
```

```
      seqno=411 esn=0 replaywin_lastseq=00000a80 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43187/43200
  dec: spi=fd64b472 esp=aes key=16 0ab999cd40bc420cc78556f84b37747f
       ah=sha1 key=20 2e9f19e91d696d530adefb3d219ad1c74d08dcd8
  enc: spi=14c9a05c esp=aes key=16 5446e233d666319b8f88fd1768f774b0
       ah=sha1 key=20 15989dc3ef5fd1d0b385df93241e0d6a0b373826
  dec:pkts/bytes=2689/16346, enc:pkts/bytes=1042/21844
  npu_flag=03 npu_rgwy=154.52.6.89 npu_lgwy=208.85.68.228 npu_selid=33d dec_npuid=1 enc_
npuid=1
```

3. For `get vpn ipsec tunnel summary`, confirm that the phase 2 IPsec selectors for the FortiSASE security PoPs are sending and receiving traffic. Confirm that `selectors(total,up): 1/1`, `rx(pkt,err)`, and `tx(pkt,err)` are non-zero. The following shows sample output for this command:

```
'ToSpokes_0' 154.52.29.50:64916  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx(pkt,err):
1043/0
'ToSpokes_1' 154.52.6.89:52270  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx(pkt,err):
1042/0
'ToSpokes_2' 50.208.126.11:0  selectors(total,up): 1/1  rx(pkt,err): 22149/0  tx(pkt,err):
55050/37
…
'ToSpokes_4' 206.47.184.245:64916  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx(pkt,err):
1043/0
…
```

Testing private access connectivity to FortiGate hub network from remote agents and edge devices

By using ping, you can verify access to the FortiGate hub network from FortiSASE remote users, namely, FortiClient users connected to FortiSASE in FortiClient agent-based mode and users behind FortiSASE edge devices.

For example, from a FortiClient user connected to FortiSASE, use ping within a Windows Command Prompt to verify access to a host behind the FortiGate hub internal network. The example pings 10.50.101.50, which is on an internal network. The following shows sample output:

```
C:\>ping 10.50.101.50
Pinging 10.50.101.50 with 32 bytes of data:
Reply from 10.50.101.50: bytes=32 time=80ms TTL=62
Reply from 10.50.101.50: bytes=32 time=80ms TTL=62
Reply from 10.50.101.50: bytes=32 time=80ms TTL=62
Reply from 10.50.101.50: bytes=32 time=84ms TTL=62
```

Testing private access connectivity to FortiGate hub network from remote proxy users

This example requires *Network* > *Proxy configuration* and *Access & authentication* > *Authentication Sources* > *Proxy* to be configured appropriately. See Proxy client onboarding on page 737 and Configuring FortiSASE with Entra ID SSO in proxy agentless mode on page 526.

By default, all proxy users can access all private access resources. You can limit proxy user access to private access resources by creating a private access policy for proxy users.

You can verify access to the FortiGate hub network from FortiSASE proxy users by using a web browser to access a host on the hub local network.

For example, consider the case when a host on the hub local network has an HTTP server running on 10.100.99.101 and only the default private access policy for proxy users is in place in FortiSASE.

To test private access connectivity to FortiGate hub network from remote proxy users:

1. From a web browser configured for proxy enter http://10.100.99.101.
2. If this is the first time going out to the internet, you will be prompted by SAML SSO to enter your credentials.
3. After entering your credentials, you should be able to access the web site at http://10.100.99.101 .

Testing private access connectivity from FortiGate hub network to remote agents and edge device users

This test depends on a private access policy being defined in the *From Hub* direction.

You can verify access from the FortiGate hub network to FortiSASE agents, namely FortiClient users connected to FortiSASE in FortiClient agent-based mode and to edge device users using ping.

From a host behind the FortiGate hub internal network, use ping to verify access to a FortiClient user or an edge device user connected to FortiSASE

The example pings the FortiClient user with 100.65.0.1 from 10.100.99.104, which is a host on an internal network. The following shows sample output:

```
root@internal-server-01:~# ping 100.65.0.1
PING 100.65.0.1 (100.65.0.1) 56(84) bytes of data.
64 bytes from 100.65.0.1: icmp_seq=1 ttl=126 time=73.3 ms
64 bytes from 100.65.0.1: icmp_seq=2 ttl=126 time=72.5 ms
64 bytes from 100.65.0.1: icmp_seq=3 ttl=126 time=74.0 ms
64 bytes from 100.65.0.1: icmp_seq=4 ttl=126 time=72.1 ms
^C
--- 100.65.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 72.127/73.008/74.034/0.735 ms
```

Verifying BGP routing on the FortiGate hub

To verify that all BGP peering is up on the FortiGate hub:

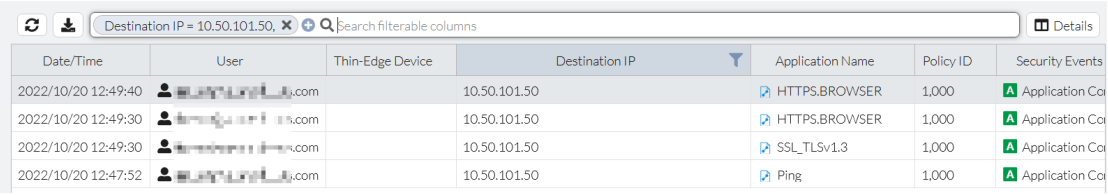
1. Check the BGP peering status and the advertised routes using the following CLI commands. Replace x.x.x.x with the BGP neighbor IP address:
   ```
   get router info bgp summary
   get router info bgp neighbors x.x.x.x advertised-routes
   ```
2. On the GUI, verify routing by going to *Dashboard* > *Networks*. Click the *Static & Dynamic Routing* widget to expand it, then select *BGP Neighbors* from the dropdown list in the top right corner.

Verifying private access traffic in FortiSASE portal

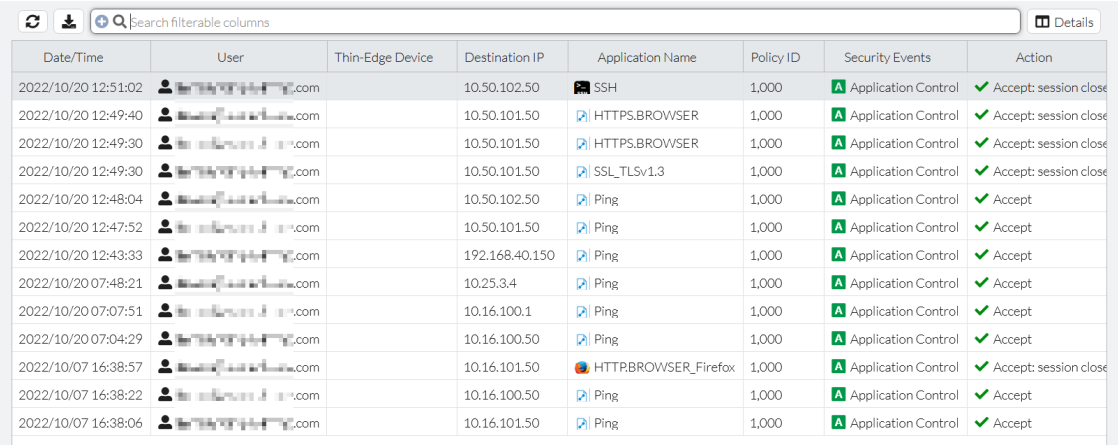
In the FortiSASE portal, you can verify traffic from FortiSASE remote users has reached private access destinations through these methods:

- From *Operations* > *Logs* > *Traffic* by viewing either the *All Internet and Private Access Traffic* page or the *Private Access Traffic* page
- From *Monitoring* > *Monitors* > *FortiView Sources*, *Monitoring* > *Monitors* > *FortiView Destinations*, or *Monitoring* > *Monitors* > *FortiView Policies* and filtering on the private access destination IP address

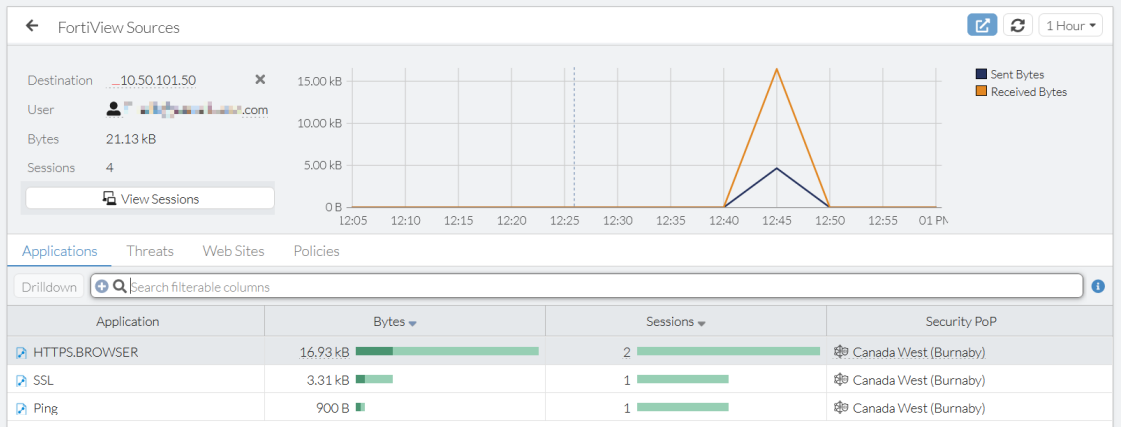
Following is an example of the *Operations* > *Logs* > *Traffic* > *All Internet and Private Access Traffic* page, filtered for the private access destination IP address 10.50.101.50.



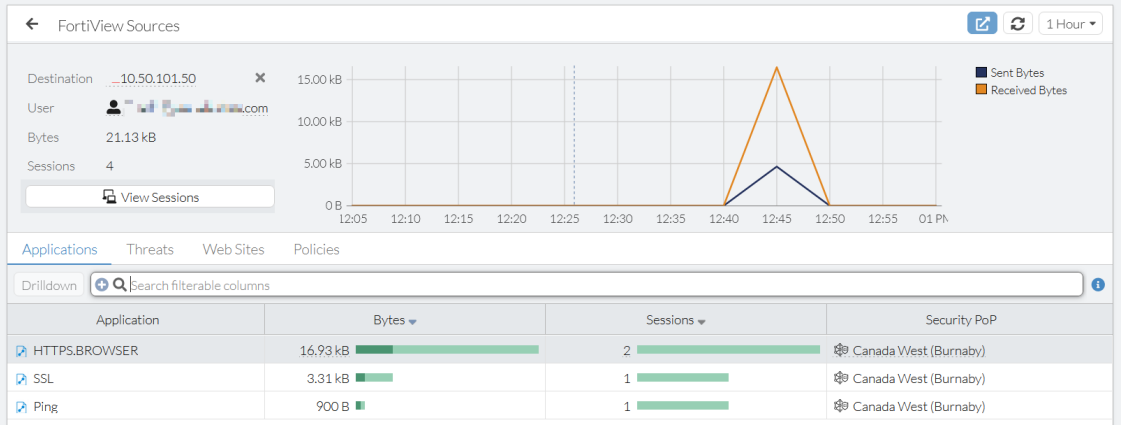
Following is an example of the *Operations* > *Logs* > *Traffic* > *Private Access Traffic (To Hubs)* page.



Following are examples of the *Monitoring* > *Monitors* > *FortiView Sources*, *Monitoring* > *Monitors* > *FortiView Destinations*, or *Monitoring* > *Monitors* > *FortiView Policies* pages, filtered on the private access destination IP address 10.50.101.50.







Verifying private access traffic from hubs

Verifying private access traffic from SPA hubs to FortiSASE remote users depends on a private access policy being defined in the *From Hub* direction.

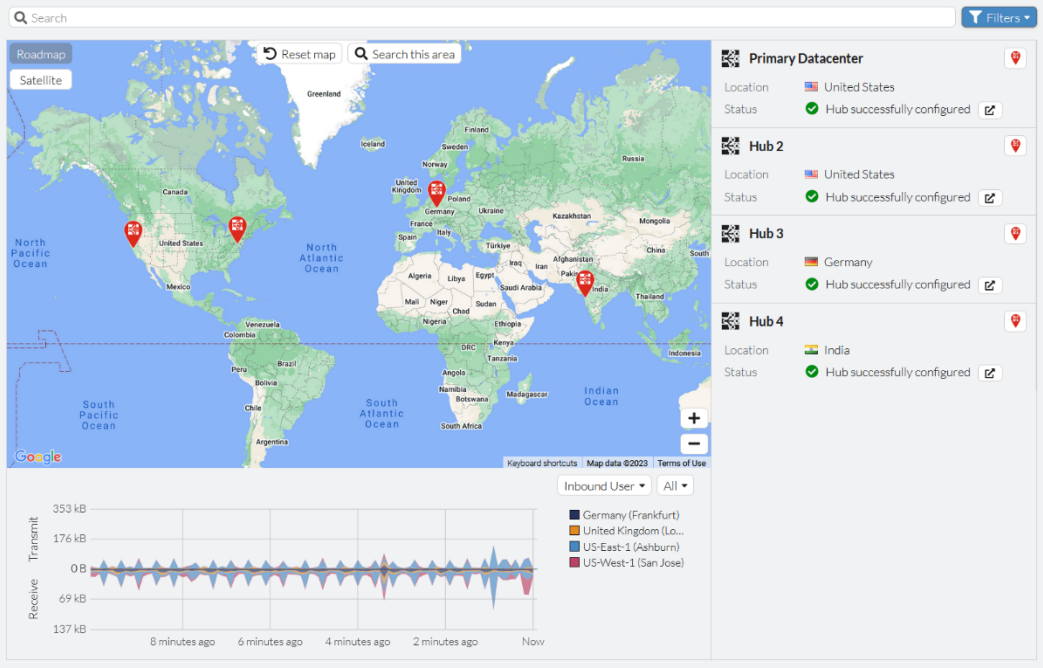
In the FortiSASE portal, you can verify traffic from SPA hub sources (local networks or connected spokes) has reached FortiSASE remote user and edge device user destinations through these methods:

- From *Operations* > *Logs* > *Traffic* by viewing *All Internet and Private Access Traffic* or *Private Access Traffic (From Hubs)*
- From *Monitoring* > *Monitors* > *FortiView Sources*, *Monitoring* > *Monitors* > *FortiView Destinations*, or *Monitoring* > *Monitors* > *FortiView Policies* and filtering on the remote agent and edge device user destination IP address

Verifying private access hub status and location using the asset map

The *Operations* > *Connectivity* > *Asset map* page in the FortiSASE portal supports filtering on *Private Access Hub* assets to display their status and geographical location.

Following is an example of the asset map filtered on *Private Access Hub* assets.



Restricting access using a FortiGate SPA hub/spoke policy

Depending on your network topology, the private server you are providing access to through SPA may either be connected to the FortiGate SPA hub device directly or to a FortiGate spoke device that is connected to the hub device using an IPsec overlay, specifically, ADVPN.

If you have previously configured SPA, then you are already using a firewall policy on either your FortiGate SPA hub device or FortiGate spoke device (if applicable to your network topology) to the LAN interface that your private server is connected to. As a best practice, you may have restricted access to your private server from agents only by specifying the IPAM subnet as a source address. See IPAM on page 278.

You can update this firewall policy to restrict access to your private server from security PoPs for DNS redirection, LDAP and RADIUS servers, and agentless ZTNA users by adding the SPA BGP spoke IP range as a source address. This spoke IP range determines the private IP addresses that the SPA hub assigns after Security PoPs establish IPsec VPN connections with it. This spoke IP range is configured on the FortiGate SPA hub as part of the IPsec VPN Phase 1 configuration in the IKEv2 mode configuration address range settings.

To restrict access using a FortiGate SPA device firewall policy:

1. On the FortiGate SPA hub, confirm the IKEv2 mode configuration address range using these CLI commands:

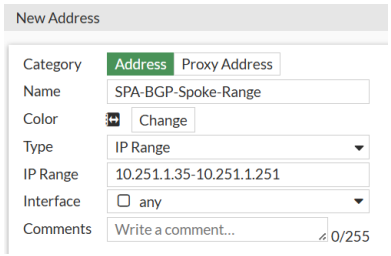
```
show vpn ipsec phase1-interface | grep ipv4-
```

Example output:

```
FGT # show vpn ipsec phase1-interface | grep ipv4-
set ipv4-start-ip 10.251.1.35
set ipv4-end-ip 10.251.1.251
set ipv4-netmask 255.255.255.0
```

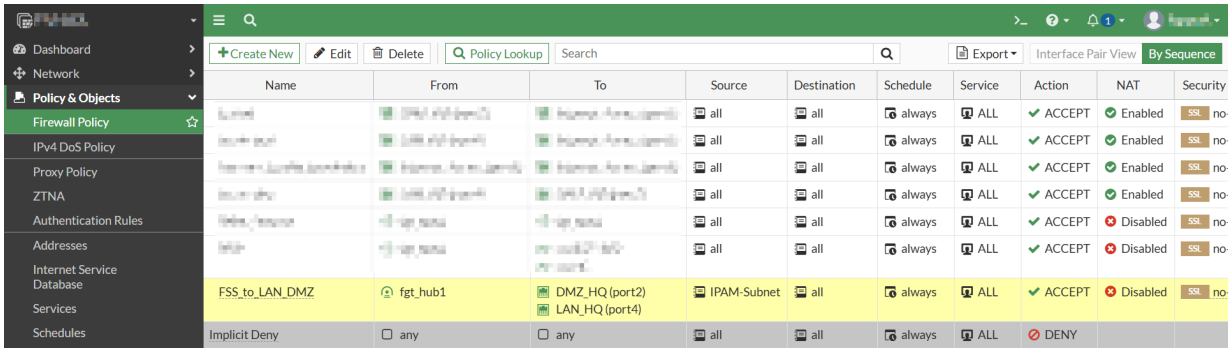
In the above example, the IKEv2 mode configuration address range is from 10.251.1.35-10.251.1.251.

2. On the FortiGate SPA hub or spoke device, configure a firewall address object for the SPA BGP spoke IP range and use it in the firewall policy used to restrict access to the HTTPS private server:
   a. In *Policy & Objects* > *Addresses*, click *Create New* > *Address*. Create a new address object containing the IP range from the SPA hub.



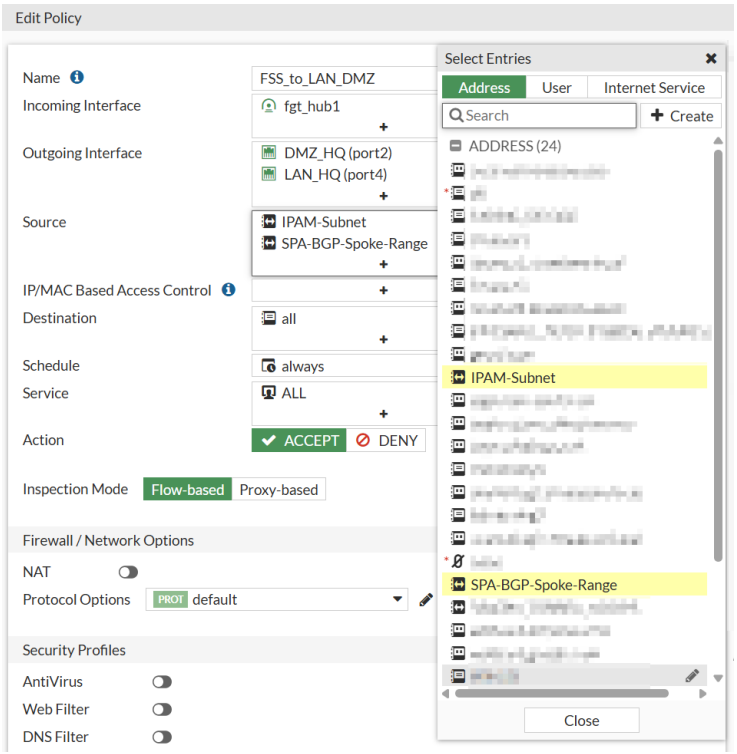
   In this example, an IP range address object named SPA-BGP-Spoke-Range is created for 10.251.1.35-10.251.1.251.

   b. In *Policy & Objects* > *Firewall Policy*, locate the existing firewall policy from the IPsec overlay interface to the LAN interface connected to the private HTTPS application server. Depending on your configuration, the source address for this policy may either be all or with an address object for the IPAM subnet used by agents.

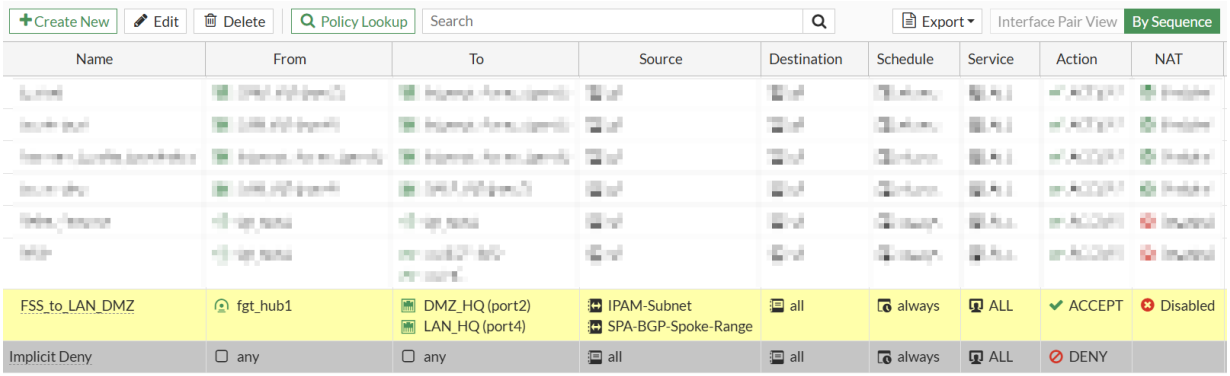


In this example, the firewall policy of interest is the FSS_to_LAN_DMZ policy from IPsec overlay interface fgt_hub1 to DMZ_HQ (port2) and LAN_HQ (port4) LAN interfaces with source set to IPAM-Subnet to allow agents to access private resources.

c. Select and edit the firewall policy, adding the address object with the SPA BGP spoke IP range as a source. Click *OK*.



The firewall policy should display both the IPAM-Subnet and added SPA-BGP-Spoke-Range as the *Source* of the policy.



Access to the private server is now restricted to agents and security PoPs, or and agentless ZTNA users, depending on the SPA-dependent feature that you are using.

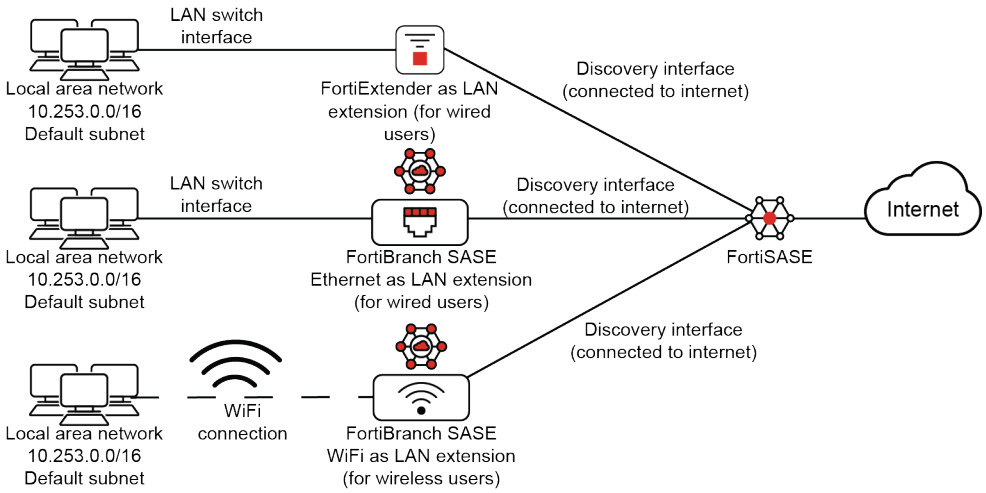
Edge devices

When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless proxy users and site-based edge device users. See Installing a certificate for deep inspection mode on page 317.

FortiExtender

Topics referencing FortiExtender in the FortiSASE Administration guide also apply to FortiBranchSASE.

FortiSASE supports management and integration of a FortiExtender configured as a LAN extension. A FortiExtender with the LAN extension configuration allows a microbranch deployment. A microbranch deployment is a branch office with a LAN behind a FortiExtender with secure internet access over a backhaul connection to FortiSASE. By relying on FortiExtender instead of FortiClient to handle secure connectivity to FortiSASE, this solution essentially extends the single-user single-device FortiClient endpoint case to a multiuser multidevice LAN environment. FortiSASE uses IP address management (IPAM) to automatically configure IP address or netmask settings for clients connected to edge devices with a subnet within the specified *IP pools for tunnel and edge devices* which cannot be manually configured for each edge device and is allocated without VLAN capability. See IP management on page 274.



Prerequisites and considerations

See Prerequisites and considerations on page 150.

Prerequisites and considerations

Topics referencing FortiExtender in the FortiSASE Administration guide also apply to FortiBranchSASE.

Supported models and firmware

For a list of model and firmware version prerequisites, see SIA for FortiExtender site-based remote users.

FortiCloud account prerequisites

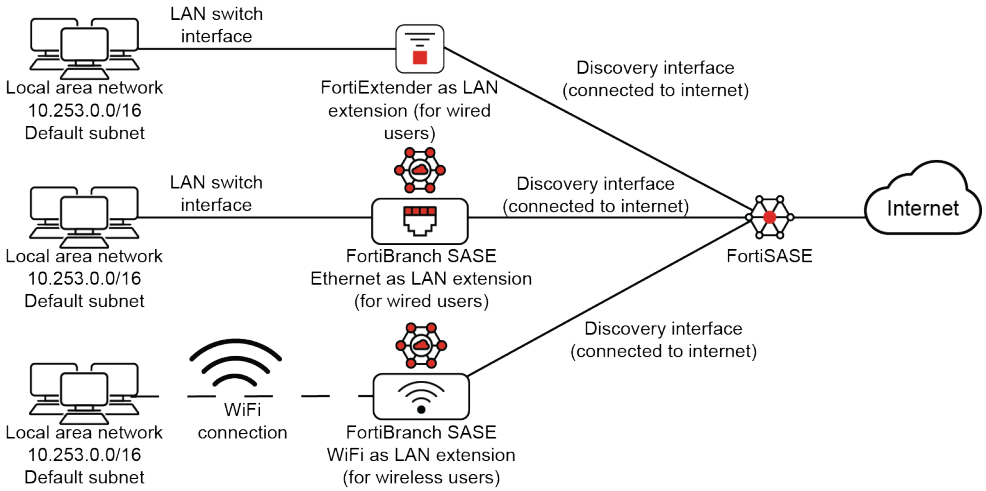
You must register FortiExtender devices used with the LAN extension feature to the same FortiCloud account used to log into FortiSASE before using this feature.

To activate FortiExtender management support on FortiSASE, you must purchase and apply a FortiSASE ThinEdge License to each FortiExtender device registered.

For details on registering products, see Registering assets.

Network topology

The following diagram depicts the network topology that the FortiExtender as a FortiSASE LAN extension configuration uses:



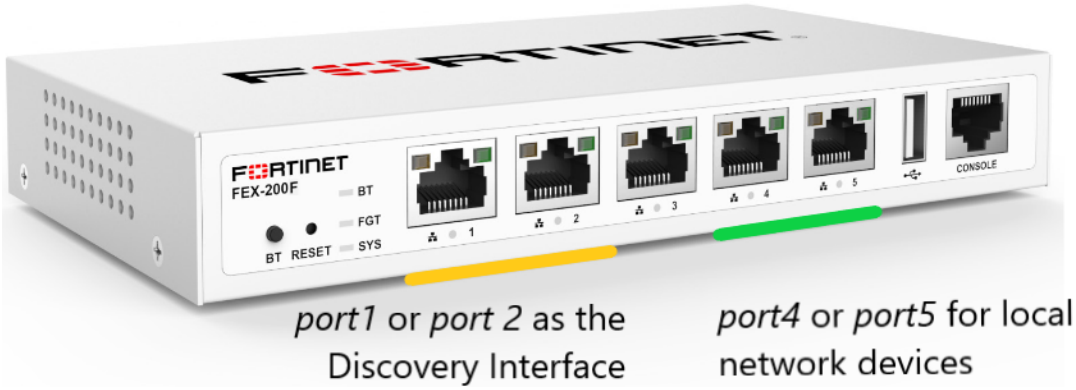
By default, using DHCP, FortiSASE dynamically assigns IP addresses to devices connected to the local network of the FortiExtender, that is, the LAN switch interface. In addition, FortiSASE uses IP address management (IPAM) to automatically configure IP address or netmask settings for clients connected to edge devices with a subnet within the specified *IP pools for tunnel and edge devices* which cannot be manually configured for each edge device and is allocated without VLAN capability. See IP management on page 274.

You should connect the FortiExtender's discovery interface to the internet. FortiExtender uses this interface for communication with FortiSASE. You can configure this interface to use DHCP or static IP addressing from the GUI or CLI.

For the FortiExtender 200F, specifically, note the following:

- Connecting the local network devices to port4 or port5 within the LAN switch interface is recommended.
- port1 or port2 are designated with the WAN role and you can use one or both ports as the discovery interface.

See the following picture for reference:



For details on the FortiExtender 200F and FortiBranchSASE models, see Key features for FortiExtender models on page 151.

Key features for FortiExtender models

Certain FortiExtender models are equipped with wired, wireless, or both capabilities, along with advanced performance metrics to extend your microbranch LAN deployments. These models, also known as FortiBranchSASE, provide superior performance and flexibility. FortiBranchSASE models such as the FBS-20G-WiFi and FBS-10F-WiFi support both wired and wireless connections, effectively expanding your microbranch LAN coverage to accommodate both wired and wireless users.

The table lists the key features for different FortiExtender models that FortiSASE supports for the LAN extension feature:

Feature	FortiExtender-200F	FortiBranchSASE-20G	FortiBranchSASE-20G-WiFi	FortiBranchSASE-10F-WiFi
LAN extension	✓	✓	✓	✓
Zero Touch Provisioning	✓	✓	✓	✓
Wi-Fi support			✓	✓
Ethernet support	✓	✓	✓	✓
Available Ethernet ports	5x 1GE RJ45	4 x 1GE RJ45 + 1 SFP/RJ45	4 x 1GE RJ45 + 1 SFP/RJ45	2 x 1GE RJ45
Dedicated WAN ports	2x 1GE RJ45 WAN (port1, port2)	1x SFP+1GE RJ45 (Combo) 1GE RJ45 WAN	1x SFP+1GE RJ45 (Combo) 1GE RJ45 WAN	1x 1GE RJ45 WAN

Feature	FortiExtender-200F	FortiBranchSASE-20G	FortiBranchSASE-20G-WiFi	FortiBranchSASE-10F-WiFi
Maximum WAN links	2	2	2	1
LAN switch ports	3x 1GE RJ45 LAN	3x 1GE RJ45 LAN	3x 1GE RJ45 LAN	1x 1GE RJ45 LAN

For information on FortiBranchSASE models, see FortiBranchSASE series datasheet.

Connecting and logging into the FortiExtender

To connect to the FortiExtender using a computer and log into the FortiExtender GUI:

1. Use an Ethernet cable to connect a LAN port in the back of the FortiExtender to your computer's Ethernet port.
2. Configure the computer to be on the same subnet as the FortiExtender by changing its IP address to 192.168.200.100 and the netmask to 255.255.255.0.
3. In a web browser, go to the default FortiExtender web GUI address: http://192.168.200.99.
4. In the username and password fields, enter admin, then press *Enter*.

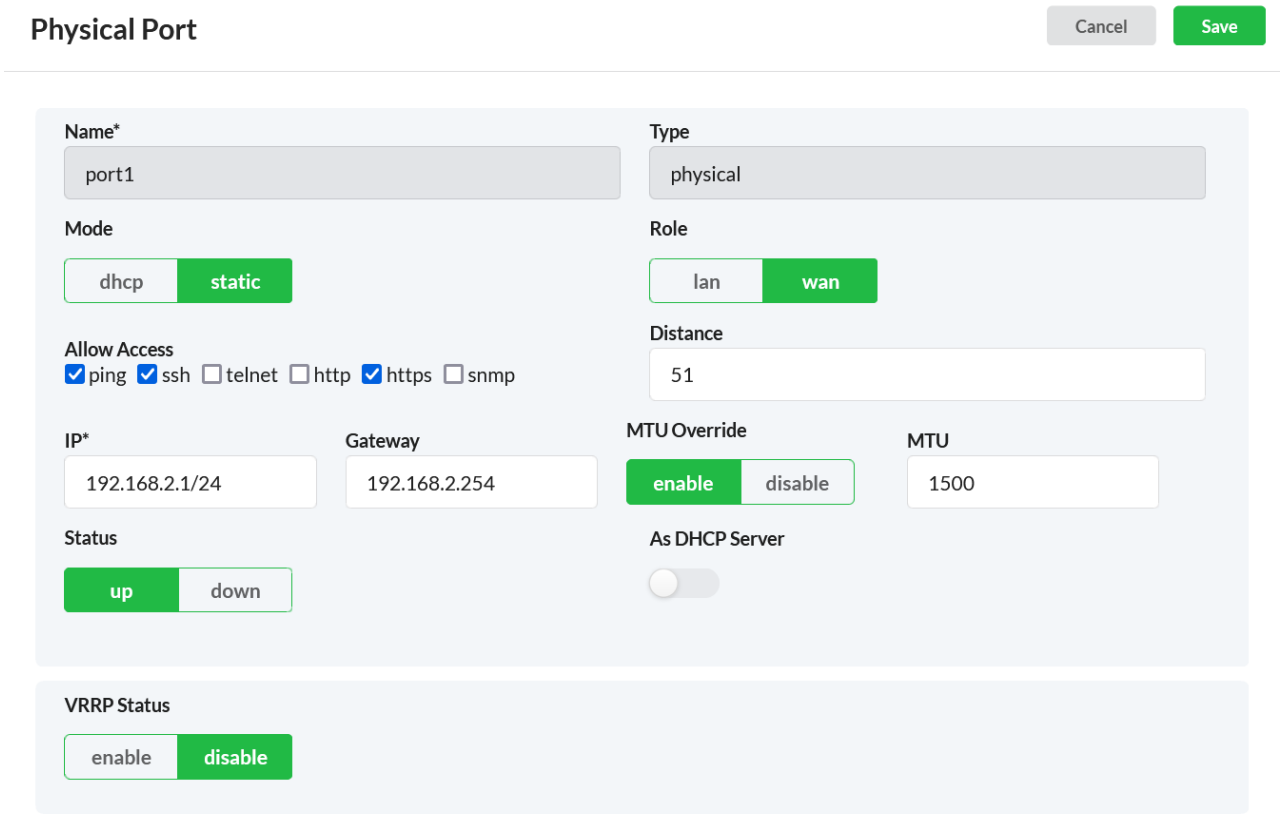
Configuring the discovery interface's IP address

You can configure the discovery interface's IP address via the FortiExtender GUI or CLI.

To configure the discovery interface's IP address via the GUI:

1. Log into the FortiExtender GUI as Connecting and logging into the FortiExtender on page 152 describes.
2. Go to *Networking* > *Interface*.
3. Under *Physical Port*, select the port to configure as the discovery interface.
4. Click the pencil icon beside the desired port.
5. Under *Mode*, select *dhcp* or *static*. If you select *static*, configure the required IP address in the *IP* field, using IP address/subnet format, and the desired gateway settings in the *Gateway* field.

6. Click *Save*.



To configure the discovery interface's IP address via the CLI:

Use the following CLI commands where `<port>` is `port1` or `port2` on the FortiExtender 200F and `<mode>` is `dhcp` or `static`:

```
config system interface
  edit <port>
    set mode { dhcp | static }
    set ip <interface IP address/subnet>
    set gateway <gateway IP address for static IP address configuration>
  next
end
```

For example, to configure the FortiExtender 200F port1 with a static IP address and subnet of 192.168.2.1/24 and default gateway of 192.168.2.254, use the following CLI commands:

```
config system interface
  edit port1
    set mode static
    set ip 192.168.2.1/24
    set gateway 192.168.2.254
  next
end
```

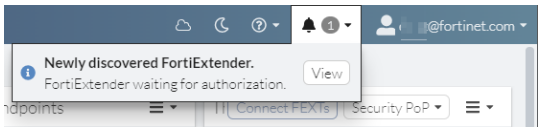
SSL deep inspection for site-based users

When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless proxy users and site-based edge device users. See Installing a certificate for deep inspection mode on page 317.

Viewing notifications for a new FortiExtender

> Topics referencing FortiExtender in the FortiSASE Administration guide also apply to FortiBranchSASE.

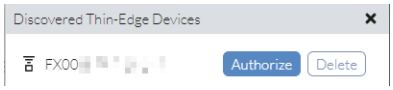
When a new FortiExtender powers on, the bell icon in the header displays a notification about the new device. In this example, the 1 beside *Network* in the left navigation pane also indicates the new device.



A popup notification also displays.



Clicking *View* from the notifications displays a pane with the option to authorize or delete the FortiExtender.



Configuring FortiExtender as FortiSASE LAN Extension

> Topics referencing FortiExtender in the FortiSASE Administration guide also apply to FortiBranchSASE.

In *Operations* > *Connectivity* > *Edge devices* > *FortiExtenders*, you can authorize, deauthorize, and delete FortiExtenders:

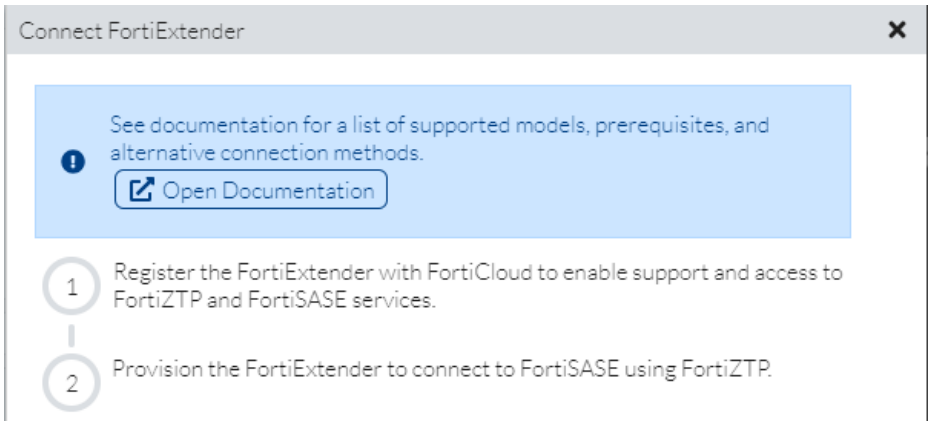
Connecting FortiExtender to FortiSASE using FortiZTP

> Topics referencing FortiExtender in the FortiSASE Administration guide also apply to FortiBranchSASE.

Prior to connecting a FortiExtender to FortiSASE, you can view the instructions in the *Connect FEXTs* dialog in FortiSASE.

To view instructions to connect a FortiExtender to FortiSASE:

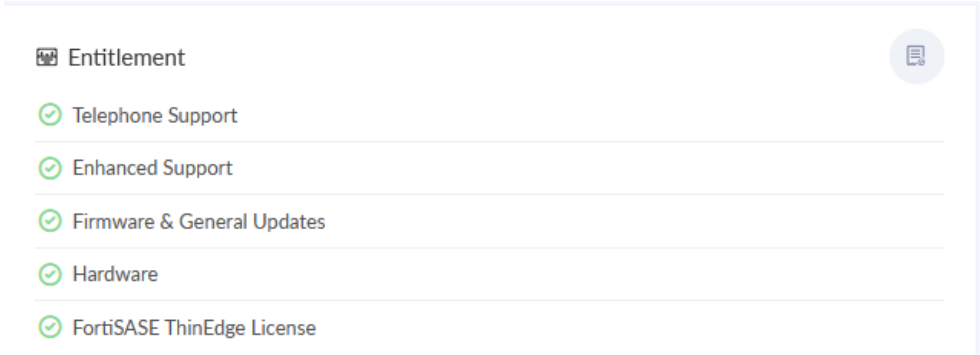
1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiExtenders*.
2. Click *Connect FEXTs*. The instructions display.



In addition to the instructions in Connect FortiExtender, to ensure proper connectivity, you generally must upgrade the FortiExtender to the latest firmware version known to work with FortiSASE. See SIA for site-based remote users and Upgrade instructions.

To register FortiExtender and FortiSASE subscription on FortiCloud:

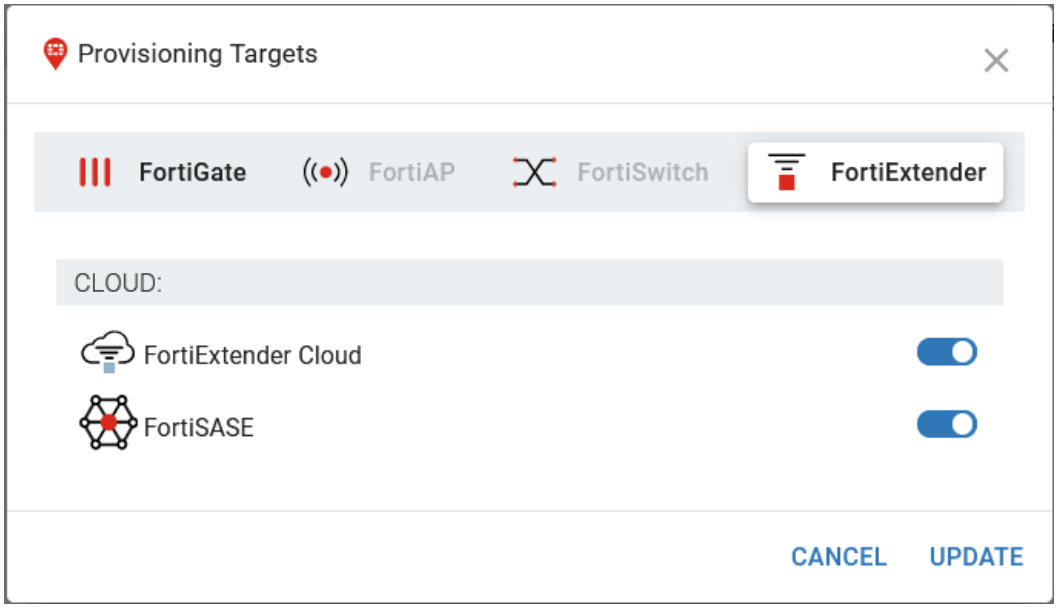
1. Sign in to your FortiCloud account.
2. Go to *Products* and click the *Register More* button.
3. In the *Register Product* dialog, in the *Registration Code* field, enter the FortiExtender serial number and follow the dialogs to complete registering the FortiExtender. For details on registering products, see Registering assets.
4. In the *Register Product* dialog, in the *Registration Code* field enter, the FortiSASE ThinEdge License registration code and follow the dialogs to complete registering the FortiSASE Thin Edge license. For details on registering products, see Registering assets.
5. Go to *Products* and *Product List* to confirm that the FortiExtender device and has been registered. Click the FortiExtender serial number. Ensure that *Entitlement* lists FortiSASE ThinEdge License.



To provision a FortiExtender to FortiSASE using FortiZTP:

1. In FortiSASE, click *Services*. Under *Cloud Services*, click *FortiZTP*. The remaining steps are performed in FortiZTP.

2. Click the *Provisioning Settings* button on the right.
3. On the *FortiExtender* tab, ensure that *FortiSASE* is enabled.



4. Click *UPDATE*.
5. On the *UNPROVISIONED* tab, do one of the following:
   - To provision a single FortiExtender, click the *Provision* icon.
   - To provision multiple FortiExtenders, select the checkboxes for the desired FortiExtenders, then click the *PROVISION* button.
6. Under *TARGET LOCATION* in the *Provision devices* dialog, select FortiSASE. Only options that you have configured in *Provisioning Settings* appear in this dialog.
7. Do one of the following:
   - Click *NEXT*. You can choose to associate the FortiExtender with a profile. Select the desired profile, then click *PROVISION NOW*.
   - Click *PROVISION NOW*.

After completing the aforementioned steps, you can proceed to authorize the FortiExtender in FortiSASE as Authorizing a FortiExtender on page 160 describes.

Connecting a FortiExtender to FortiSASE using alternative connection methods

Topics referencing FortiExtender in the FortiSASE Administration guide also apply to FortiBranchSASE.

You can connect a FortiExtender to FortiSASE using alternative connection methods, namely via the FortiExtender GUI or CLI.

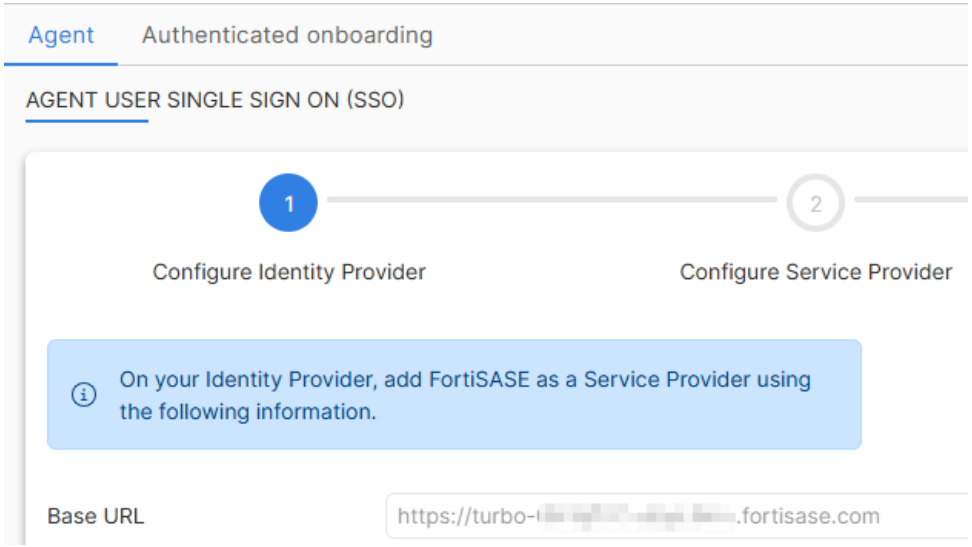
For ease of configuration, following the steps in Connecting FortiExtender to FortiSASE using FortiZTP on page 154 is recommended.

As a reference, this section describes alternative connection methods other than using FortiZTP.

Before using the FortiExtender GUI or CLI steps, you must obtain the FortiSASE domain name from FortiSASE.

To obtain the FortiSASE domain name from FortiSASE:

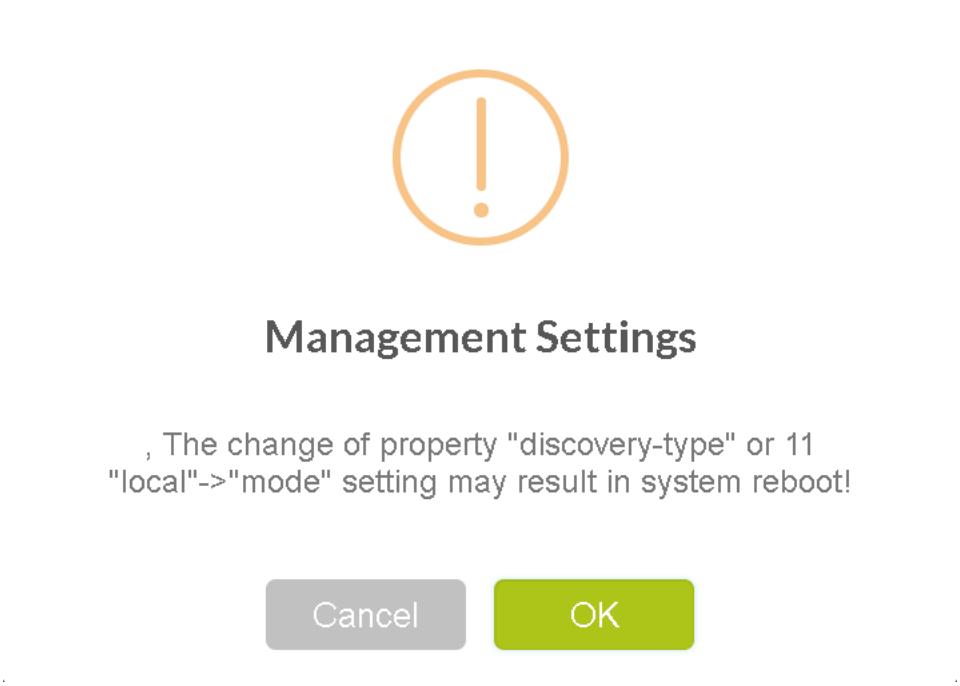
1. Go to *Access & authentication* > *SSO*.
2. View the URL in the *Base URL* field and note the FortiSASE domain name after the https:// string. In the example, the FortiSASE domain name is turbo...fortisase.com.



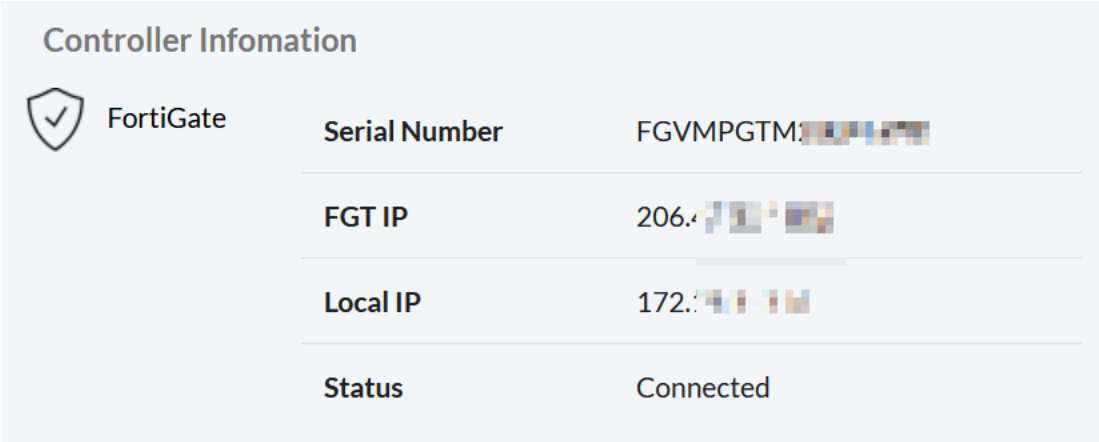
To connect a FortiExtender to FortiSASE via the GUI:

1. Log in to the FortiExtender GUI.
2. Go to *Settings* > *Management*.
3. Beside *Management Setup*, click the pencil icon to edit these settings and configure the following settings:
   a. *Controller*: *fortigate*
   b. *Discovery Type*: *static*
   c. *Discovery Interface*: <interface connected to the internet>
   d. For *Static Access Control Address*, click the pencil icon next to *ID 1* to edit this entry. Enter Server: <FortiSASE domain name here from *Connect FEXTs* dialog>. Click *Save*.
4. Click *Save*.

5. Click *OK* in the dialog to have changes take effect and reboot the FortiExtender.



6. To confirm the FortiExtender's connection to FortiSASE, log in to the FortiExtender GUI and go to *Dashboard*. Under *Controller Information*, confirm that *FGT IP* is non-zero, and *Status* is *Connected*.



To connect a FortiExtender to FortiSASE via the CLI:

The following commands are adapted from FortiExtender LAN extension in public cloud FGT-VM.

1. Connect FortiExtender to FortiSASE:

```
config system management
  set discovery-type fortigate
  config fortigate
    set ac-discovery-type static
    config static-ac-addr
      edit 1
```

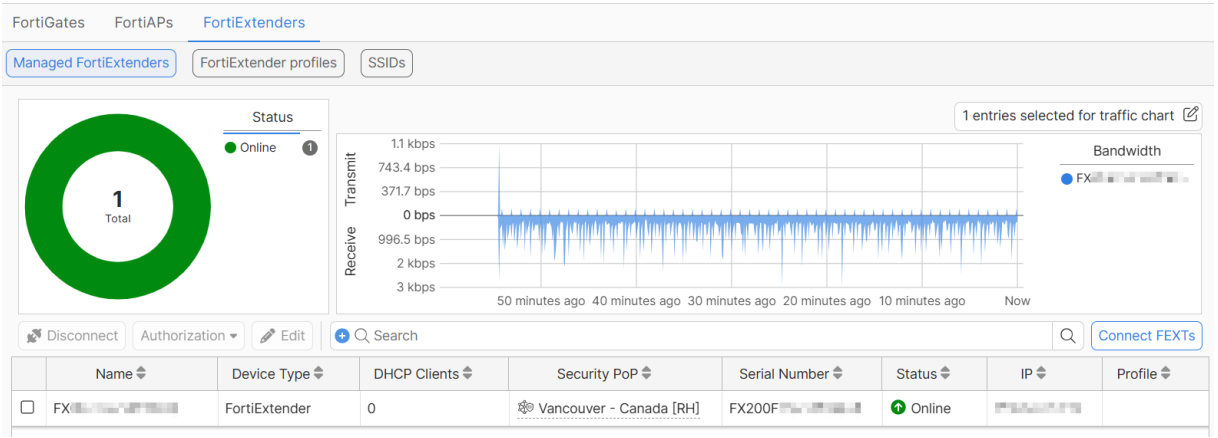
```
        set server <FortiSASE domain name here from Connect FEXTs dialog>
      next
    end
    set discovery-intf port1
  end
end
```

2. To confirm the FortiExtender's connection to FortiSASE, run the `get extender status` command in the FortiExtender CLI. Confirm that `controller-addr` is non-zero and `management-state` is `CWWS_RUN`. The following shows sample output:

```
FX200FXXXXXXXXXX # get extender status
Extender Status
    name                : FX200FXXXXXXXXXX
    mode                : CAPWAP
    fext-addr           : 172.XX.XXX.XXX
    ingress-intf        : port1
    controller-addr     : 206.XX.XXX.XXX:5246
    controller-name     : FGXXXXXXXXXXXXXX
    uptime              : 0 days, 1 hours, 18 minutes, 31 seconds
    management-state    : CWWS_RUN
    base-mac            : AA:BB:CC:11:22:33
    network-mode        : lan-extension
    fgt-backup-mode     : backup
    discovery-type      : static
    discovery-interval  : 5
    echo-interval       : 30
    report-interval     : 30
    statistics-interval : 120
    mdm-fw-server       : fortiextender-firmware.forticloud.com
    os-fw-server        : fortiextender-firmware.forticloud.com
```

Managed FortiExtenders

You can manage a FortiExtender or FortiBranchSASE device from *Operations* > *Connectivity* > *Edge devices* > *FortiExtenders* in the *Managed FortiExtenders* tab.



The *Managed FortiExtenders* tab presents these charts for monitoring:

- Usage chart with a summary of FortiExtender device status
- Bandwidth chart displaying inbound FortiExtender edge device traffic. Using the button at top-right of the chart, up to 10 FortiExtender edge devices can be selected and summarized in this chart.

From this page, you can perform these tasks:

- Authorizing a FortiExtender on page 160
- Deauthorizing a FortiExtender on page 160
- Disconnecting a FortiExtender on page 161
- Configuring SSIDs and FortiExtender profiles for FortiBranchSASE on page 161

Authorizing a FortiExtender

If FortiSASE does not find a *FortiSASE ThinEdge License*, it disables the *Authorization > Authorize* button and hovering over the *Authorize* button displays *No authorization entitlements for FortiExtenders*. Therefore, you can only authorize licensed FortiExtenders.

Ensure that you apply a *FortiSASE ThinEdge License* to each FortiExtender that FortiSASE will manage.

If the number of FortiExtender devices to be authorized exceeds the number of *FortiSASE ThinEdge Licenses* available, FortiSASE disables the *Authorization > Authorize* button and hovering over the *Authorize* button displays *All X licensed FortiExtenders have been authorized. Deauthorize a device or purchase additional entitlements to authorize additional FortiExtenders* where X is the total number of registered subscriptions for edge device management.

Proceed as the tooltip advises to ensure that FortiSASE can manage your FortiExtenders.

To authorize a FortiExtender:

1. Go to *Operations > Connectivity > Edge devices > FortiExtenders*.
2. On the *Managed FortiExtenders* tab, select the desired FortiExtender.
3. Do one of the following:
   - Under *Authorization*, click *Authorize*.
   - Right-click the device and select *Authorization > Authorize*.
4. When authorizing a FortiBranchSASE device, a slide-in appears. Use the *Profile* dropdown list to select a FortiExtender profile and click *OK*.
5. After authorization, FortiSASE displays the FortiExtender status as offline. Refresh the *FortiExtenders* page. The FortiExtender device status changes to online.

Deauthorizing a FortiExtender

To deauthorize a FortiExtender:

1. Go to *Operations > Connectivity > Edge devices > FortiExtenders*.
2. Select the desired FortiExtender.

3. Do one of the following:
   - Under *Authorization*, click the *Deauthorize* button.
   - Right-click the device and select *Authorization* > *Deauthorize*.

   After deauthorization, FortiSASE displays the FortiExtender status as *FortiCare Registered*.

Disconnecting a FortiExtender

If a FortiExtender device is deregistered from the FortiCloud account, disconnecting this device removes the listed device from FortiSASE *Operations* > *Connectivity* > *Edge devices* > *FortiExtenders*.

To disconnect a FortiExtender:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiExtenders*.
2. Select the desired FortiExtender.
3. Do one of the following:
   - Click *Disconnect*.
   - Right-click the device and select *Disconnect*.

Configuring SSIDs and FortiExtender profiles for FortiBranchSASE

Certain FortiExtender models are equipped with wired, wireless, or both capabilities, along with advanced performance metrics to extend your microbranch LAN deployments. These models, also known as FortiBranchSASE, provide superior performance and flexibility. FortiBranchSASE models such as the FBS-20G-WiFi and FBS-10F-WiFi support wired and wireless connections, effectively expanding your microbranch LAN coverage to accommodate wired and wireless users.

FortiSASE enables centralized management and configuration of your wireless network by defining one or more SSIDs, allowing wireless users to connect seamlessly. FortiSASE uses IP address management (IPAM) to automatically configure IP address or netmask settings for an SSID.

When FortiSASE detects a FortiBranchSASE model, a default FortiExtender profile is automatically configured. You can use this default profile or create a custom one to override default settings for individual devices.

To configure SSIDs for FortiBranchSASE:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiExtenders*.
2. Select the *SSIDs* tab and click *Create*.
3. Enter desired name in the *Name* field.
4. Under *WiFi Settings*, complete the following settings:

Field	Description
SSID	Enter the name for the SSID.
Client Limit	Enable the toggle to specify the limit for the number of clients that are allowed to connect to the SSID.
Broadcast SSID	Enable SSID broadcast.

5. Under *WiFi Security*, complete the following settings:

Field	Description
Mode	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. • *WPA2 Personal*: WPA2 is WiFi Protected Access version 2. Users use a pre-shared key (password) to obtain access. • *WPA2 Enterprise*: similar to WPA2 Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password. • *WPA3 Enterprise Only*: WPA3 enterprise with Protected Management Frames (PMF) mandatory. Best used for enterprise networks. Each user is separately authenticated by user name and password. • *Captive Portal Only*: Captive portal will be enforced based on the security groups selected in the individual FortiExtender configuration. To avoid captive portal, ensure you have a policy for the FortiExtender which exempts captive portal authentication, see Configuring an exemption policy for an edge device on page 191.
Pre-shared Key	Available only when *Mode* is *WPA2 Personal*. Preshared key must be 8 to 63 characters long.
Authentication server address	Available only when *Mode* is *WPA2 Enterprise* or *WPA3 Enterprise Only*. Enter the IP address or resolvable FQDN of the RADIUS server.
Authentication server port	Available only when *Mode* is *WPA2 Enterprise* or *WPA3 Enterprise Only*. Enter the authentication port number used by RADIUS server.
Authentication server secret	Available only when *Mode* is *WPA2 Enterprise* or *WPA3 Enterprise Only*. Enter the password used to connect to the RADIUS server.

6. Click *OK*.

To configure FortiExtender Profiles:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiExtenders* and select the *FortiExtender profiles* tab.
2. Select the default FortiExtender profile created by FortiSASE based on the model detected by FortiSASE and click *Edit* or click *Create* for new FortiExtender profile.
3. (Optional) On default FortiExtender profile click *Change* next to *Login password*, to change default FortiBranchSASE's login password.
4. For new profile, use *Model* dropdown to select your model.
5. For new profile, enter a password in *Login password* field. This changes the login password on FortiBranchSASE device.
6. Using *Country/Region* dropdown, select the country where FortiBranchSASE device is deployed.
7. Under *WiFi configuration*, select *2.4GHZ Radio* or/and *5GHz Radio* and set its *Status* to *Enable*.

8. Complete the following settings below:

Field	Description
Status	Activates the selected radio when set to *Enable*
Operating standard	Select the wireless protocols to support. The available choices depend on the radio's capabilities. Where multiple protocols are supported, the letter suffixes are combined: "802.11ax/n/g" means 802.11ax and 802.11n and 802.11g.
Extension channel	Specify whether the additional channel for extended bandwidth is placed above or below the primary channel. Options include *Auto*, *Higher*, and *Lower*.
Bandwidth	Select the range of frequency range used by WiFi channels to transmit data.
Guard interval	Choose an appropriate time buffer to mitigate Intersymbol Interference (ISI) based on your microbranch deployment environment. Available options include *Auto*, *400 ns*, and *800 ns*.
Transmit power	Adjust the transmit power by selecting a percentage of the maximum power allowed based on the configured country/region and FortiBranchSASE device. Use the slider to set a suitable percentage.
Channels	Select the specific channel(s) to use. The available options depend on the IEEE wireless protocol selected under *Operating Standard*.
LAN extension SSID	Select the SSID from the dropdown menu that you want to broadcast on the selected radio.

9. Click *OK*. To apply the FortiExtender profile to a FortiBranchSASE device, see Authorizing a FortiExtender on page 160.

Troubleshooting a FortiExtender that FortiSASE does not see

Topics referencing FortiExtender in the FortiSASE Administration guide also apply to FortiBranchSASE.

If after configuring the FortiExtender, FortiSASE does not see it, take the following troubleshooting steps.

To troubleshoot a FortiExtender that FortiSASE does not see:

1. Ensure that FortiExtender is updated to the latest firmware. See Upgrade instructions.
2. Ensure that the FortiExtender is registered in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 150.
3. Ensure you connect your internet connection to the discovery interface and local LAN to the LAN interfaces:
   a. For FortiExtender 200F, the discovery interface is either port 1 or 2 and the LAN interfaces are ports 4 and 5. See Network topology on page 150.
   b. For FortiBranchSASE, the discovery interface and the LAN interfaces depend on the device model. See Recommended port configurations.

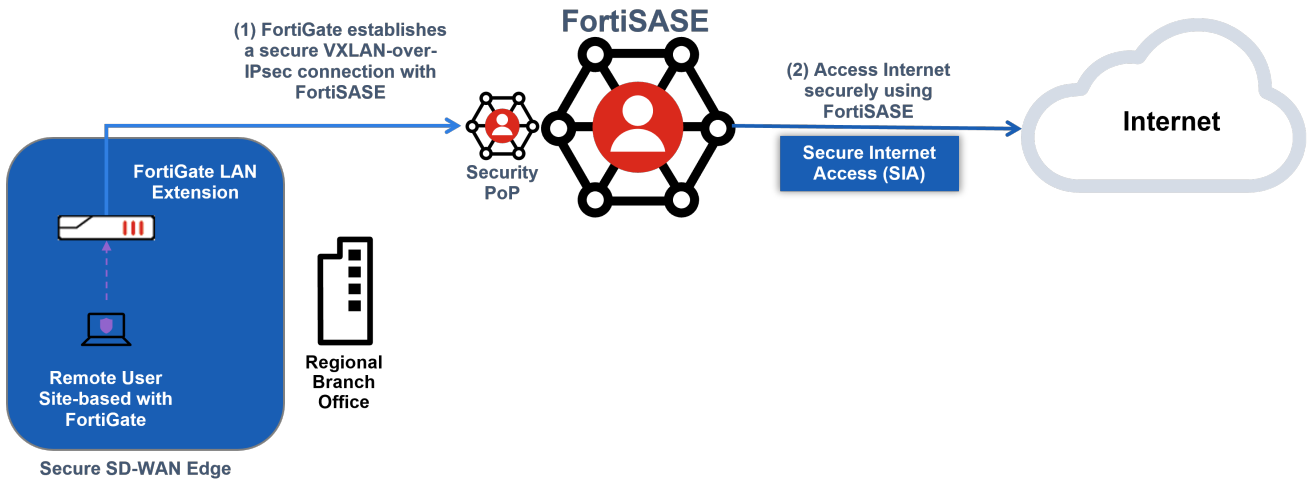
After properly configuring and connecting a FortiExtender, it takes a few minutes to connect FortiExtender to FortiSASE, after which FortiSASE takes over DHCP and serves as your default gateway. Until then, traffic traverses your local internet connection.

FortiGate

Ensure that you are aware of FortiGate Prerequisites on page 164.

You can configure a FortiGate SD-WAN device as a FortiSASE LAN extension, also known as a FortiGate Secure Edge, by setting up a VXLAN-over-IPsec tunnel between the FortiGate and FortiSASE. This creates a layer 2 network between FortiSASE and the network behind the remote FortiGate. In this use case, because the FortiGate is responsible for centralizing its remote users' site connectivity to the FortiSASE firewall-as-a-service (FWaaS), you only need to configure the endpoints in their IP settings to forward traffic to the FortiGate as the default gateway.

Therefore, this use case minimizes individual workstation or device setup because you do not need to install FortiClient on endpoints or configure explicit web proxy settings on web browser-based endpoints.



Prerequisites

Supported models and firmware

For a list of model and firmware version prerequisites, see SIA for FortiGate site-based remote users.

FortiCloud account prerequisites

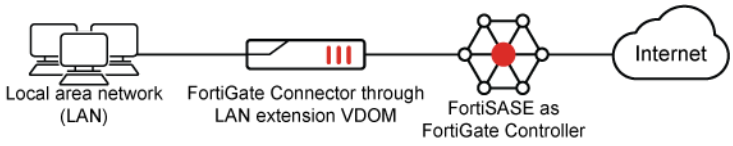
You must register FortiGate devices used with the LAN extension feature to the same FortiCloud account used to log into FortiSASE before using this feature.

To activate FortiGate management support on FortiSASE, you must purchase and apply a FortiSASE subscription subscription per FortiGate device registered. See the FortiSASE Ordering Guide.

For details on registering products, see Registering assets.

Network topology

The following diagram depicts the network topology that the FortiGate as a FortiSASE LAN extension configuration uses:



The FortiGate LAN extension feature is used in this topology where the FortiGate Connector is the on-premise FortiGate Secure Edge device and the FortiGate Controller is FortiSASE.

A new VDOM can be created on the FortiGate Connector and its type can be set to LAN extension. This configuration allows the VDOM to function as a FortiGate in LAN extension mode.

Connecting and logging into the FortiGate

For details on connecting and logging into the FortiGate GUI, see Connecting using a web browser.

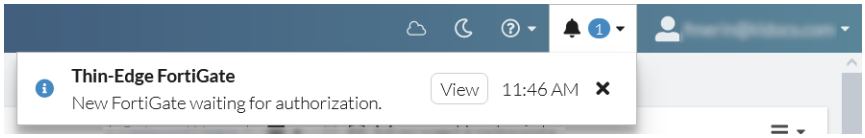
For details on connecting and logging into the FortiGate CLI, see Connecting to the CLI.

SSL deep inspection for site-based users

When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless proxy users and site-based edge device users. See Installing a certificate for deep inspection mode on page 317.

Viewing notifications for a new FortiGate

When a new FortiGate powers on, the bell icon in the header displays a notification about the new device. In this example, the 1 beside *Network* in the left navigation pane also indicates the new device.



Clicking *View* from the notifications, displays the FortiGate in the *Operations* > *Connectivity* > *Edge devices* > *FortiGates* page.

Alternatively, you can see the number of FortiGates waiting for authorization beside *Operations* > *Connectivity* > *Edge devices* > *FortiGates* in the navigation bar on the left.

Configuring FortiGate as FortiSASE LAN Extension

Connecting FortiGate to FortiSASE using the GUI and CLI

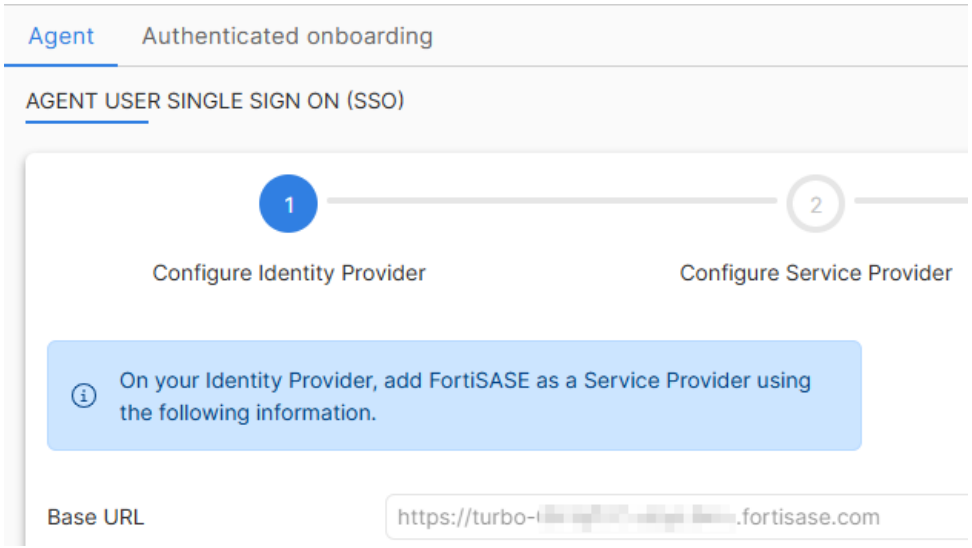
To connect the FortiGate as FortiSASE LAN extension or FortiGate secure edge, follow this configuration workflow:

1. Obtain the FortiSASE domain name from FortiSASE.
2. Configure the FortiGate to connect to FortiSASE using the FortiSASE domain name.

For details on configuring the FortiGate secure edge to connect to FortiSASE using the GUI or CLI, see FortiGate secure edge to FortiSASE. In these configuration steps, the FortiGate secure edge fulfills the FortiGate connector role while FortiSASE fulfills the FortiGate controller role.

To obtain the FortiSASE domain name from FortiSASE:

1. Go to *Access & authentication* > *SSO*.
2. View the URL in the *Base URL* field and note the FortiSASE domain name after the https:// string. In the example, the FortiSASE domain name is turbo...fortisase.com.



Troubleshooting a FortiGate that FortiSASE does not see

If after configuring the FortiGate, FortiSASE does not see it, take the following troubleshooting steps:

To troubleshoot a FortiGate that FortiSASE does not see:

1. Ensure that the FortiGate is registered in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 164.
2. Ensure that the FortiGate is registered with a FortiSASE subscription subscription in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 164.
3. Verify the IPsec tunnels' phase 1 and phase 2 negotiations on the FortiGate Connector:

```
# diagnose vpn ike gateway list
# diagnose vpn tunnel list
```

4. Verify the LAN extension status on the Connector:

```
Connector-FGT (lan-ext) # get extender lanextension-vdom-status
Control-Channel:
        controller ip: 1.1.1.1
        controller port: 5246
        controller name: FGVMPGTM00000ABC
        missed echo: 0
        up time(seconds): 75194
        status: EXTWS_RUN
Data-Channel:
uplink [0]: wan1
        IPsec tunnel ul-wan1
        VxLAN interface vx-wan1
downlink [0]: internal1
downlink [1]: lan-ext-link1
```

In this example, the Connector is in a working state.

Authorizing a FortiGate

If no FortiSASE subscription subscription is found for a FortiGate, then the *Authorization* > *Authorize* button will be disabled and hovering over the *Authorize* button will display the tooltip "No authorization entitlements for this Device". Therefore, only licensed FortiGates can be authorized.

Ensure you apply a FortiSASE subscription to each FortiGate to be managed by FortiSASE.

To authorize a FortiGate:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiGates*.
2. Select the desired FortiGate.
3. Do one of the following:
   a. Under *Authorization*, click the *Authorize* button.
   b. Right-click the device and select *Authorization* > *Authorize*.
4. After authorization, FortiSASE displays the FortiGate status as *Offline*. Refresh the *FortiGates* page. The FortiGate device status changes to *Online*.

Deauthorizing a FortiGate

To deauthorize a FortiGate:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiGates*.
2. Select the desired FortiGate.
3. Do one of the following:

a. Under *Authorization*, click the *Deauthorize* button.
b. Right-click the device and select *Authorization* > *Deauthorize*.

After deauthorization, FortiSASE displays the FortiGate status as *Unauthorized*.

Disconnecting a FortiGate

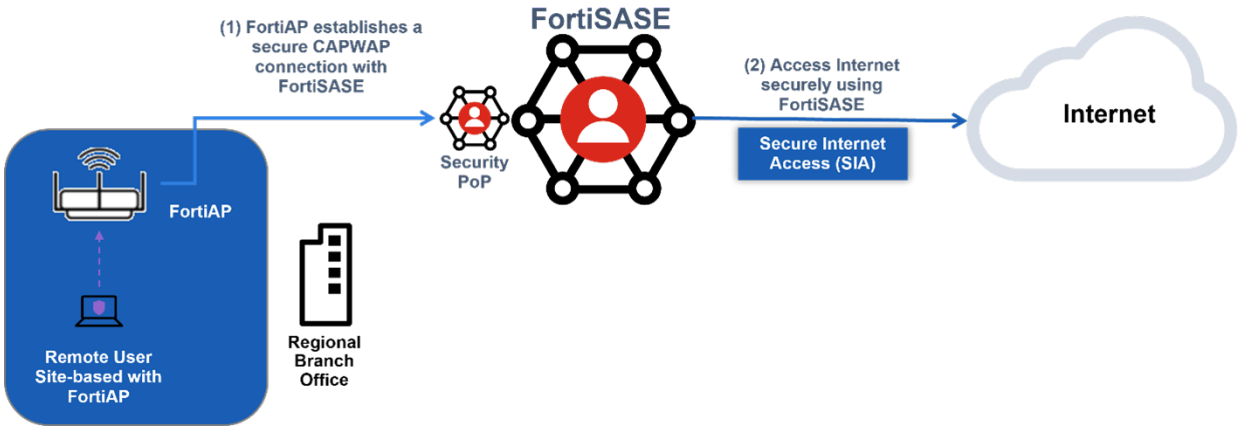
If a FortiGate device has been deregistered from the FortiCloud account, then disconnecting this device will remove the listed device from the FortiSASE *Operations* > *Connectivity* > *Edge devices* > *FortiGates* page.

To disconnect a FortiGate:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiGates*.
2. Select the desired FortiGate.
3. Do one of the following:
   a. Click the *Disconnect* button.
   b. Right-click the device and select *Disconnect*.

FortiAP

FortiSASE supports management and integration of a FortiAP as an edge device allowing for a microbranch deployment. A microbranch deployment is a branch office with a FortiAP managed over a backhaul connection to FortiSASE that provides secure internet access to Wi-Fi clients. By relying on FortiAP instead of FortiClient to handle secure connectivity to FortiSASE, this solution essentially extends the single-user single-device FortiClient endpoint case to a multiuser multidevice Wi-Fi environment. FortiSASE uses IP address management (IPAM) to automatically configure IP address or netmask settings for clients connected to edge devices with a subnet within the specified *IP pools for tunnel and edge devices* which cannot be manually configured for each edge device and is allocated without VLAN capability. See IP management on page 274.



Prerequisites

See Prerequisites on page 169.

Prerequisites

Supported models and firmware

For a list of supported FortiAP devices and firmware versions, see SIA for FortiAP site-based remote users.

FortiCloud account prerequisites

You must register FortiAP devices to the same FortiCloud account used to log into FortiSASE before using this feature.

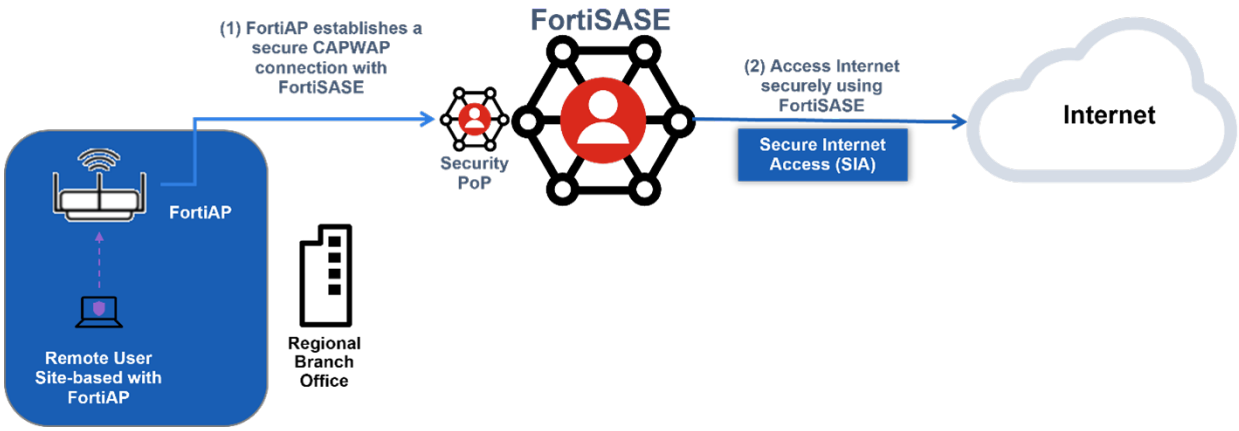
To activate FortiAP management support on FortiSASE, you must purchase and apply a FortiSASE subscription subscription to each FortiAP device registered.

For a list of supported FortiAP devices and firmware versions, see SIA for FortiAP site-based remote users.

For details on registering products, see Registering assets.

Network topology

The following diagram depicts the network topology that the FortiAP as a FortiSASE edge device configuration uses:



A CAPWAP tunnel is established between FortiSASE and the FortiAP device.

There are two channels inside the CAPWAP tunnel:

- Control channel for managing traffic, which is always encrypted by DTLS.
- Data channel for carrying client data packets, which can be configured to be encrypted or not.

For a FortiAP to be managed by FortiSASE, the data channel is encrypted using an IPsec tunnel between FortiSASE and the FortiAP that carries CAPWAP data packets and includes the FortiAP serial number within this tunnel.

By default, using DHCP, FortiSASE dynamically assigns IP addresses to Wi-Fi devices connected to the FortiAP. In addition, FortiSASE uses IP address management (IPAM) to automatically configure IP address or netmask settings for clients connected to edge devices with a subnet within the specified *IP pools for tunnel and edge devices* which cannot be manually configured for each edge device and is allocated without VLAN capability. See IP management on page 274.

Connecting and logging into the FortiAP

You can use one of these methods for connecting and logging into the FortiAP device:

- Connect to the FortiAP using a computer with a direct wired connection to the FortiAP
- Reset the FortiAP to allow access using FortiAP Configuration mode

To connect to the FortiAP using a computer with a direct wired connection for GUI or CLI access:

1. Connect an Ethernet cable from the LAN port in the back of the FortiAP to one of the following:
   a. FortiSwitch with Power-over-Ethernet (PoE) enabled on the port and then use another Ethernet cable to connect a computer's Ethernet port to one of the free ports on the FortiSwitch.
   b. PoE injector and then use another Ethernet cable to connect from the PoE injector to a computer's Ethernet port.
2. Configure the computer to be on the same subnet as the FortiAP by changing its IP address to 192.168.1.1 and the netmask to 255.255.255.0.
3. Access the GUI or CLI using 192.168.1.2:
   a. In a web browser, go to the default FortiAP web GUI address: https://192.168.1.2 .
   b. Using SSH, go to 192.168.1.2.
4. In the *Username* field, enter admin and keep the password blank if this is a new setup. Otherwise, in the *Password* field, enter the password associated with the admin account.
5. Create a new password that adheres to the listed password policy and then click *Change Password*.

To reset the FortiAP to use FortiAP Configuration mode for GUI or CLI access:

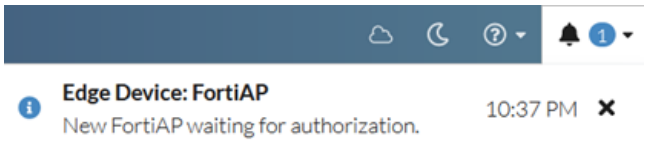
1. Ensure that the FortiAP is booted up.
2. Use a pin to push and hold the reset button for five to ten seconds. FortiAP reboots and then enters Configuration mode. FortiAP starts to broadcast an open security SSID `FAP-config-<serial-number>`, for example `FAP-config-FP421F0000000000`.
3. Access the GUI or CLI of the FortiAP Configuration mode using 192.168.100.1:
   a. In a web browser, go to the default FortiAP web GUI address: https://192.168.100.1 .
   b. Using SSH, go to 192.168.100.1
4. In the *Username* field, type admin.
5. In the *Password* field, type the password associated with the admin account.

SSL deep inspection for site-based users

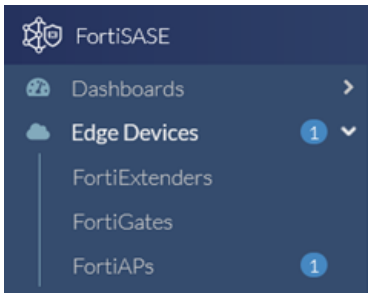
When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless proxy users and site-based edge device users. See Installing a certificate for deep inspection mode on page 317.

Viewing notifications for a new FortiAP

When a new FortiAP powers on, the bell icon in the header displays a notification about the new device.



In this example, the 1 beside *Network* in the left navigation pane also indicates the new device.



Configuring FortiAP as FortiSASE edge device

In *Operations* > *Connectivity* > *Edge devices* > *FortiAPs*, you can configure FortiAPs:

- Connecting a FortiAP to FortiSASE using FortiZTP on page 171
- Managing FortiAPs on page 173
- Editing a FortiAP profile on page 177
- Creating a FortiAP profile and applying it to a FortiAP on page 181
- Creating an SSID on page 181
- Troubleshooting a FortiAP that FortiSASE does not see on page 184

Typically, the configuration workflow for a FortiAP as a FortiSASE edge device is as follows:

1. Connect the FortiAP to FortiSASE using FortiZTP.
2. Log into FortiSASE and view notifications confirming that FortiSASE sees the FortiAP.
3. Authorize the FortiAP. If needed, FortiSASE will automatically upgrade the FortiAP device firmware to the latest supported version.
4. Create an SSID for your wireless network.
5. Edit the default FortiAP profile to configure desired radio settings, including whether the radio will apply to all SSIDs or selected SSIDs.

Connecting a FortiAP to FortiSASE using FortiZTP

This section requires the FortiAP device to run a supported firmware version. See SIA for FortiAP site-based remote users.

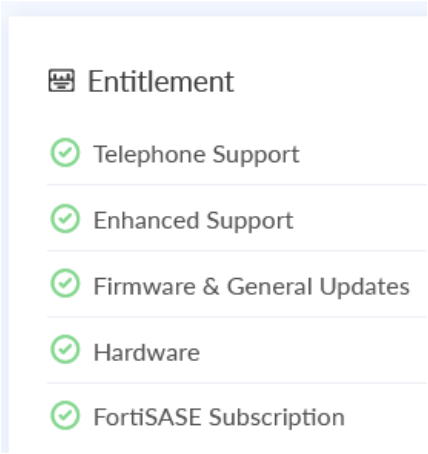
If the FortiAP device runs an unsupported version, then it must be upgraded to a supported version first. See Upgrading to a supported FortiAP firmware version using alternative connection methods on page 187.

The following configuration workflow is required for connecting a FortiAP to FortiSASE:

1. Register FortiAP and FortiSASE license on FortiCloud.
2. Provision a FortiAP to FortiSASE using FortiZTP.

To register FortiAP and FortiSASE subscription on FortiCloud:

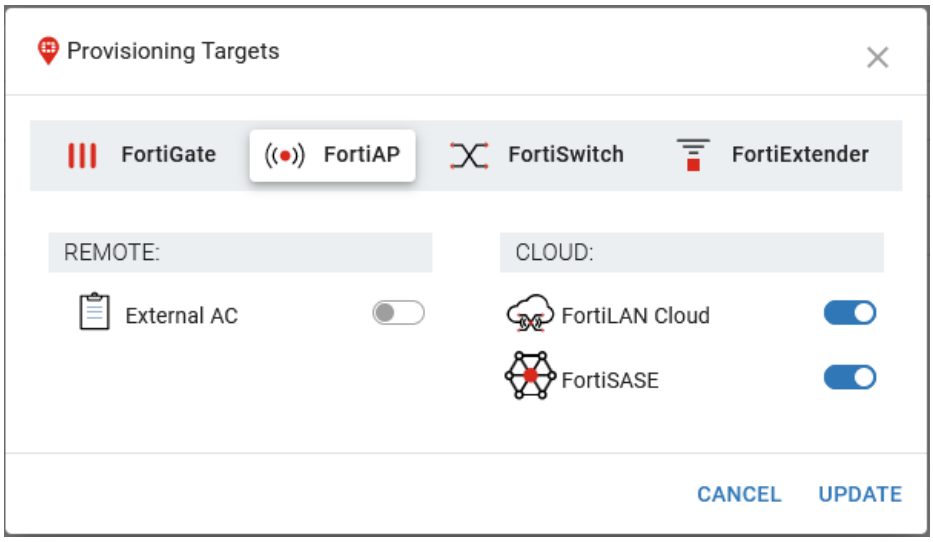
1. Sign in to your FortiCloud account.
2. Go to *Products* and click *Register More*.
3. In the *Register Product* dialog, in the *Registration Code* field, enter the FortiAP serial number and follow the dialogs to complete registering it. You require physical access to the FortiAP device because registration requires the cloud key on the back label. See Registering assets.
4. Repeat step 3 with the FortiSASE Subscription registration code.
5. Go to *Products* and *Product List* to confirm that you registered the FortiAP device. Click the FortiAP serial number. Ensure that *Entitlement* lists *FortiSASE Subscription*.



To provision a FortiAP to FortiSASE using FortiZTP:

1. In FortiSASE, click *Services*. Under *Cloud Services*, click *FortiZTP*. You perform the remaining steps in FortiZTP.
2. In FortiZTP, click *Setting*.

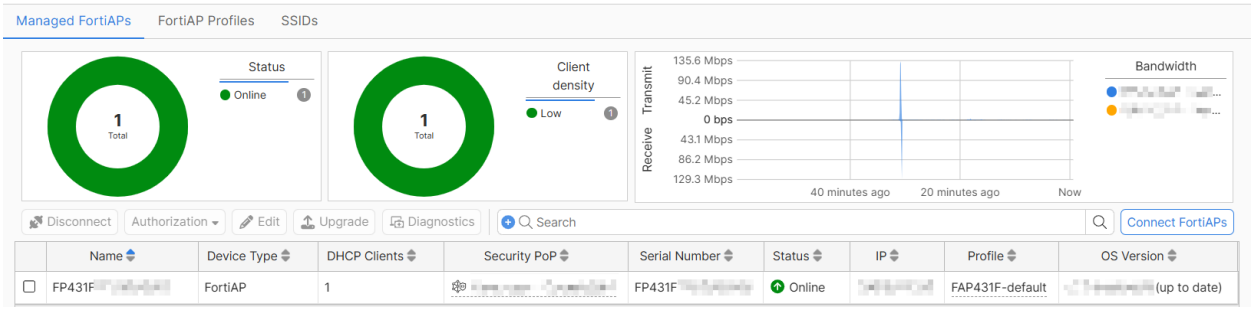
3. On the *FortiAP* tab, ensure that *FortiSASE* is enabled.



4. Click *UPDATE*.
5. On the *UNPROVISIONED* tab, do the following:
   - To provision a single FortiAP, click *Provision*.
   - To provision multiple FortiAPs, select the checkboxes for the desired FortiAPs, then click *PROVISION*.
6. Under *TARGET LOCATION* in the *Provision devices* dialog, select *FortiSASE*. Only options that you have configured in *Provisioning Settings* appear in this dialog.
7. Click *PROVISION NOW*.
8. In the prompt that mentions the provision process started for devices, click *OK*.

Managing FortiAPs

You can manage a FortiAP device from *Operations* > *Connectivity* > *Edge devices* > *FortiAPs* in the *Managed FortiAPs* tab.



The *Managed FortiAPs* tab presents these charts for monitoring:

- Usage chart with a summary of FortiAP device status
- Usage chart with a summary of FortiAP devices based on client load based on the number of clients connected (supported FortiAP devices have two Wi-Fi radios):
  - High: more than 110 clients
  - Average: 60-110 clients
  - Low: fewer than 60 clients

- Bandwidth chart displaying inbound FortiAP edge device traffic per SSID and security PoP

> FortiSASE does not recommend firmware versions for FortiAP G-series edge devices or indicate whether the installed FortiAP OS version for these devices is up to date.

From this page, you can perform these tasks:

Authorizing a FortiAP and upgrading to a supported FortiAP firmware version

To authorize a FortiAP:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiAPs* and click the *Managed FortiAPs* tab at the top.
2. Select the desired FortiAP.
3. Do one of the following:
   - Under *Authorization*, click the *Authorize* button.
   - Right-click the device and select *Authorization* > *Authorize*.
4. After authorization, FortiSASE displays the FortiAP status as *Offline*. Refresh the *FortiAPs* page. The FortiAP device status changes to *Online*. If needed, upon device authorization, FortiSASE automatically upgrades the FortiAP edge device to the latest supported FortiAP firmware release. The device must be authorized and online for the upgrade to take place.
   - The device must be running an older FortiAP firmware release than the latest supported version.
   - The device will need to reboot as part of the upgrade. Wireless endpoints already connected to the device may experience a temporary loss of connectivity.
   - It takes around 15-20 minutes before an upgrade is performed.
5. After 15-20 minutes, go to the *Managed FortiAPs* tab and observe the *OS Version* field reflects the latest FortiAP firmware version that the device was upgraded to.

Considerations

- If FortiSASE does not find a FortiSASE subscription, it disables the *Authorization* > *Authorize* button and hovering over the *Authorize* button displays *No authorization entitlements for this Device*. Therefore, you can only authorize licensed FortiAPs. Ensure you apply a FortiSASE subscription to each FortiAP for FortiSASE to manage.
- If needed, the FortiAP automatically upgrades to the latest FortiAP firmware version. The FortiAP must reboot as part of the upgrade. Wireless endpoints already connected to the FortiAP may experience temporary connectivity loss.
- FortiSASE does not recommend firmware versions for FortiAP G-series edge devices or indicate whether the installed FortiAP OS version for these devices is up to date.

Deauthorizing a FortiAP

To deauthorize a FortiAP:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiAPs* and click the *Managed FortiAPs* tab at the top.
2. Select the desired FortiAP.
3. Do one of the following:
   - Under *Authorization*, click the *Deauthorize* button.
   - Right-click the device and select *Authorization* > *Deauthorize*.

After deauthorization, FortiSASE displays the FortiAP status as *FortiCare Registered*.

Disconnecting a FortiAP

If a FortiAP device has been deregistered from the FortiCloud account, then disconnecting this device will remove the listed device from the FortiSASE *Operations* > *Connectivity* > *Edge devices* > *FortiAPs* page.

To disconnect a FortiAP:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiAPs* and click the *Managed FortiAPs* tab at the top..
2. Select the desired FortiAP.
3. Do one of the following:
   a. Click the *Disconnect* button.
   b. Right-click the device and select *Disconnect*.

Editing a FortiAP

From *Operations* > *Connectivity* > *Edge devices* > *FortiAPs* under the *Managed FortiAPs* tab, by selecting a FortiAP device and clicking *Edit*, you can edit these settings:

Field	Description
Name	Enter a name for the FortiAP.
Authorized	Authorization state of the FortiAP.
FortiAP Profile	FortiAP profile applied to this FortiAP.
Enable LEDs	Select if you want LEDs on the FortiAP to be enabled (default) or disabled.
Login Password	Select if you want set a new AP login password or leave the password unchanged.

Upgrading to the latest supported FortiAP firmware version after authorization

This procedure describes how to upgrade the FortiAP to the latest supported firmware version after the initial authorization.

To upgrade to a supported FortiAP firmware version after authorization:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiAPs* > *Managed FortiAPs*.
2. Select the desired FortiAP.
3. Do one of the following:
   - Click *Upgrade*.
   - Right-click the device and select *Upgrade*.
4. FortiSASE displays a prompt warning of a FortiAP reboot and temporary connectivity loss for wireless endpoints already connected to the FortiAP, and lists the FortiAP firmware version to be upgraded to. Click *OK* to continue with the FortiAP firmware upgrade.
5. Observe the message at the top-right of the screen: *Request to upgrade the FortiAP to latest firmware successful*.
   - The device must be running an older FortiAP firmware release than the latest supported version.
   - The device will need to reboot as part of the upgrade. Wireless endpoints already connected to the device may experience a temporary loss of connectivity.
   - It takes around 15-20 minutes before an upgrade is performed.
6. After 15-20 minutes, go to the *Managed FortiAPs* tab and observe the *OS Version* field reflects the latest FortiAP firmware version that the device was upgraded to.

Prerequisites and considerations

Prerequisites

The FortiAP device must be authorized and online for the upgrade to take place. The FortiAP must reboot as part of the upgrade. Wireless endpoints already connected to the FortiAP may experience a temporary connectivity loss.

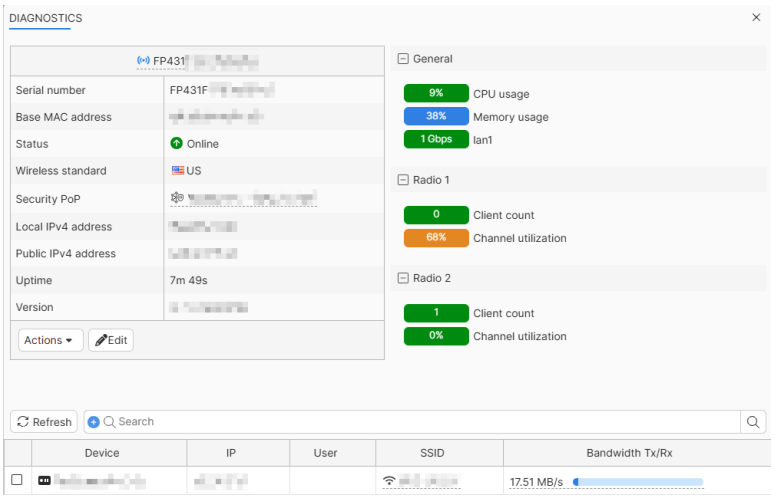
Considerations

FortiSASE does not recommend firmware versions for FortiAP G-series edge devices or indicate whether the installed FortiAP OS version for these devices is up to date.

Diagnostics

From the *Operations* > *Connectivity* > *Edge devices* > *FortiAPs* page, in the *Managed FortiAPs* tab, you can view FortiAP diagnostics by selecting a FortiAP device and clicking *Diagnostics*. These diagnostics can be use to assist with troubleshooting FortiAP device or wireless client issues.

The *Diagnostics* pane appears as follows:



The top part of the page focuses on FortiAP device diagnostics.

The bottom part of the page lists wireless clients connected to the FortiAP device. By right-clicking on a wireless client, you can choose *Show in FortiView*.

For wireless client views, the *User* column is only available if the SSID is configured with the following WiFi Security Modes and the user has been authenticated by these modes:

- *WPA2 Enterprise*
- *WPA3 Enterprise Only*
- *Captive Portal Only*

Editing a FortiAP profile

When you authorize a FortiAP, it is configured by default to use the default FortiAP profile, which the model determines. The FortiAP profile defines the entire configuration for the AP.

From *Operations* > *Connectivity* > *Edge devices* > *FortiAPs* under the *FortiAP profiles* tab, you can create a new FortiAP profile or edit an existing default FortiAP profile.

Typically, you edit an existing default FortiAP profile by selecting the profile and clicking *Edit*.

General FortiAP profile options

Field	Description
Name	Enter a name for the FortiAP profile
Model	Select the FortiAP model to which this profile applies. For a list of supported FortiAP devices and firmware versions, see SIA for FortiAP site-based remote users.
Platform Mode	If you selected a WiFi 6E capable model, select a platform mode: • *Single 5G*: only one radio operates on the 5GHz 802.11ax/ac/n/a band. • *Dual 5G*: two radios operate on the 5GHz 802.11ax/ac/n/a band and dedicated scanning is always disabled.

Field	Description
Deployment Location	Select where the FortiAP is being installed: indoor or outdoor. You can override the default designation of the FortiAP to change the available channels based on your region.
Wireless standard	Select the country or region to apply the country code for where you will use the FortiAP.
Login Password	Select *Set* if you want set a new AP login password or leave the password unchanged.
Client Load Balancing	Select a handoff type as needed. See Wireless client load balancing for high-density deployments.
802.1x Authentication	Enable if you want to configure the FortiAP to act as a 802.1x supplicant to authenticate against the server using EAP-FAST, EAP-TLS, or EAP-PEAP (see Configuring 802.1X supplicant on LAN).
UNII-4 5GHz band channels	Enable to enable configuring UNII-4 5 GHz bands in the radio-specific profile options. This resets radio 2 channel lists and UNII-5 and UNII-6 6 GHz band channels will be unavailable for selection.

Radio-specific profile options

For FortiAP devices with 6 GHz support via Radio 3, when *Single 5G* platform mode and 802.11ax are configured, you can use only SSIDs configured with WPA3 Enterprise as the *WiFi Security Mode* with Radio 3.

Field	Description
Mode	Select the type of mode: • *Disabled*: radio is disabled. • *Access Point*: platform is an access point.
Band	Select the wireless protocols that you want to support. The available choices depend on the radio's capabilities.
Channel Width	Select channel width for 802.11ax or 802.11n on 5 GHz. For optimal performance on supported radios, *Channel Width* is selected as 80 MHz by default for the default profile and for new profiles.
Channel Plan	For 2.4 GHz radios, select if you want to automatically configure a Channel plan or if want to select custom channels. • *Three Channels*: automatically selects channel 1, 6, and 11. • *Four Channels*: automatically selects channels 1, 4, 8, and 11. • *Custom*: select custom channels.
Channels	Select the channel or channels to include. The available channels depend on which IEEE wireless protocol you selected in *Band*. By default, for 5 GHz radios all available channels are enabled.
Short Guard Interval	Select to enable the short guard interval for 802.11ax or 802.11n on 5 GHz.
Transmit Power Mode	Select how you want to determine transmit power:

Field	Description
	• *Percent*: transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device. • *dB*m: transmit power is setting using a dBm value. • *Auto*: set a range of dBm values and the power is set automatically.
Transmit Power	Specify either the minimum and maximum Transmit power levels in dBm or as a percentage.
SSIDs	Select SSIDs to use for this radio either *All* or *Specify* with selected SSIDs added to a list. If SSIDs is configured to *All* for a radio, then click on *View Enabled SSIDs* to display a slide-in listing *Enabled SSIDs*. You may *Create*, *Edit*, or *Delete* SSIDs from this slide-in.
Monitor Channel Utilization	Select to enable monitoring channel utilization.

LAN port options for FortiAP 23JF

For FortiAP 23JF devices, unlike with other FortiAP devices, you do not need to configure `WANLAN_MODE=WAN-LAN` on the device to support the LAN port configuration from the FortiAP profile in FortiSASE.

Field	Description
	Select the LAN port configuration type: • *All*: applies to all LAN ports • *Custom*: each LAN port has a custom LAN port configuration.
All Ports	When *All* is set, specify the function of all LAN ports: • *Offline* (default): port is offline • *Default*: bridge LAN port to WAN port • *Bridge to SSID*: bridge LAN port to specified SSID
Port 1 *Port 2* *Port 3*	When *Custom* is set, specify the function of each LAN port on the FortiAP device. The configuration available for each LAN port is the same as for the *All ports* field (*Online*, *Default*, *Bridge to SSID*).

LAN port options for FortiAP devices other than the FortiAP 23JF

For FortiAP devices other than the FortiAP 23JF, *Port 1* refers to the next available LAN port after the first LAN port labeled port 1 on the device, which in most cases is the LAN port labeled port 2 on the device.

For these FortiAP devices, the first LAN port is used as the WAN port, or the uplink, used to provide wired internet access to the device and management traffic to and from FortiSASE.

For FortiAP devices other than the FortiAP 23JF, before configuring LAN ports from FortiSASE through a FortiAP profile and before authorizing the FortiAP device in FortiSASE, you must configure these commands on the device by accessing the FortiAP CLI. See FortiAP CLI access:

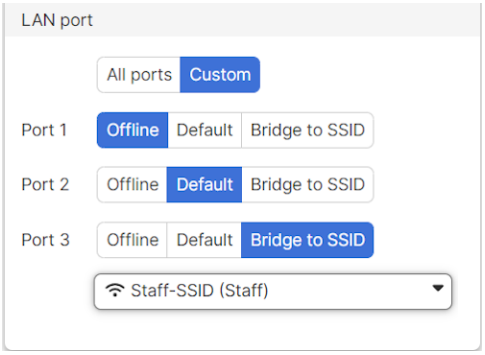
```
cfg -a WANLAN_MODE=WAN-LAN
cfg -c
```

Field	Description
Port 1	When *All* is set, specify the function of all LAN ports: • *Offline* (default): port is offline • *Default*: bridge LAN port to WAN port • *Bridge to SSID*: bridge LAN port to specified SSID

Example: Configure LAN ports for a FortiAP device

To configure LAN ports for a FortiAP 23JF device:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiAPs*.
2. In the *SSIDs* tab, configure an SSID. See Example: Configuring an SSID using WPA2 Enterprise with a local user group on page 182 or Example: Configuring a captive portal only SSID for FortiAP on page 191.
3. In the *FortiAP profiles* tab, create a new FortiAP 23JF profile or edit an existing default FortiAP 23JF profile.
4. Configure the general and radio-specific options in the FortiAP profile.
5. In the FortiAP profile page, in *LAN Port*, configure *Custom* and select the LAN port settings for each of the LAN ports.



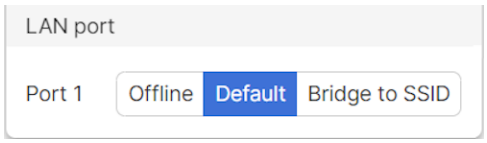
In the example above, the following custom configuration was made:

- Port 1 is set to *Offline* and cannot be used.
- Port 2 is set to *Default* and is bridged to the WAN/uplink port.
- Port 3 is set to *Bridge to SSID* and is bridged to the SSID *Staff-SSID*. In other words, the LAN port is in the same subnet and layer 2 network as the SSID.

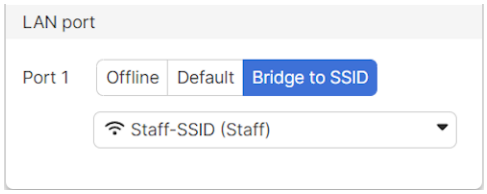
To configure LAN ports for a FortiAP device other than a FortiAP 23JF device:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiAPs*.
2. In the SSIDs tab, configure an SSID. See Example: Configuring an SSID using WPA2 Enterprise with a local user group on page 182 or Example: Configuring a captive portal only SSID for FortiAP on page 191.
3. In the *FortiAP Profiles* tab, create a new FortiAP profile or edit an existing default FortiAP profile for your specific FortiAP device.
4. Configure the general and radio-specific options in the FortiAP profile.

5. In the FortiAP profile page, in *LAN Port*, for the *Port 1* field, select the LAN port settings for each of the LAN ports.
   a. If *Offline* is set, then the port labeled Port 2 on the device cannot be used.
   b. If *Default* is set, then the port labeled Port 2 on the device is bridged to the WAN/uplink port, that is, the port labelled Port 1.



   c. If *Bridge to SSID* is set, then the port labeled Port 2 on the device is bridged to the specified SSID.



Creating a FortiAP profile and applying it to a FortiAP

You can also choose to create new FortiAP profiles by clicking *Create* for the purpose of overriding specific settings for individual FortiAPs. You cannot update the name, model, and country/region of a profile once you save it.

To assign a newly created FortiAP profile:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiAPs*.
2. On the *Managed FortiAPs* tab, select a FortiAP device and click *Edit*.
3. For the *FortiAP profile* field, from the dropdown list, select the desired FortiAP profile to apply to this FortiAP.

Creating an SSID

You can configure your wireless network by defining one or more SSIDs to which your users can connect. FortiSASE uses IP address management (IPAM) to automatically configure IP/Netmask settings for an SSID.

General SSID settings

Field	Description
Name	Enter a name for the SSID interface.
Traffic Mode	*Tunnel* — (Tunnel to Wireless Controller) Data for WLAN passes through WiFi Controller. This is the default. FortiSASE only supports this mode.
Status	SSID interface status.

WiFi Settings

Field	Description
SSID	Enter the SSID.
Client Limit	Limit the number of clients allowed in the SSID.
Broadcast SSID	Disable broadcast of SSID. By default, the SSID is not broadcast.

WiFi Security

Field	Description
Mode	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. • *WPA2 Personal*: WPA2 is WiFi Protected Access version 2. Users use a preshared key (password) to obtain access. • *WPA2 Enterprise*: similar to WPA2 Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password. See Example: Configuring an SSID using WPA2 Enterprise with a local user group on page 182. • *WPA3 Enterprise Only*: WPA3 enterprise with Protected Management Frames (PMF) mandatory. Best used for enterprise networks. Each user is separately authenticated by user name and password. • *Captive Portal Only*: enforced based on the user groups specified in *Security Groups*. To avoid captive portal, ensure you have a policy for this SSID which exempts captive portal authentication. See Example: Configuring a captive portal only SSID for FortiAP on page 191.
Pre-shared Key	Available only when *Mode* is *WPA2 Personal*. Preshared key must be 8 to 63 characters long.
Authentication	Available only when *Mode* is *WPA2 Enterprise* or *WPA3 Enterprise Only*. Select one of the following: • *RADIUS Server*: select the RADIUS server that will authenticate the clients. • *User Groups*: select the local user group(s) that can authenticate.

Example: Configuring an SSID using WPA2 Enterprise with a local user group

This example configures a Staff SSID with WPA2 Enterprise and a local user group for user authentication of staff users. This example requires a FortiAP edge device to already be connected to and authorized within FortiSASE. You can use this example to configure WPA3 Enterprise Only instead of WPA2 Enterprise.

The configuration workflow is as follows:

1. Create local users.
2. Create a local user group.
3. Create an SSID to use WPA2 Enterprise with the local user group.
4. Verify WPA2 Enterprise user authentication upon connecting to the SSID.

To create local users:

1. Go to *Access & authentication > Access > Users and groups*.
2. Click *Create*.
3. Select *User*, then click *Next*.
4. Enter the *Email* of the new user. This will be the username of the new user.
5. Click *OK*. The new user will receive an email prompting them to activate the new account and to set a new password.
6. Repeat the process to add more local users.

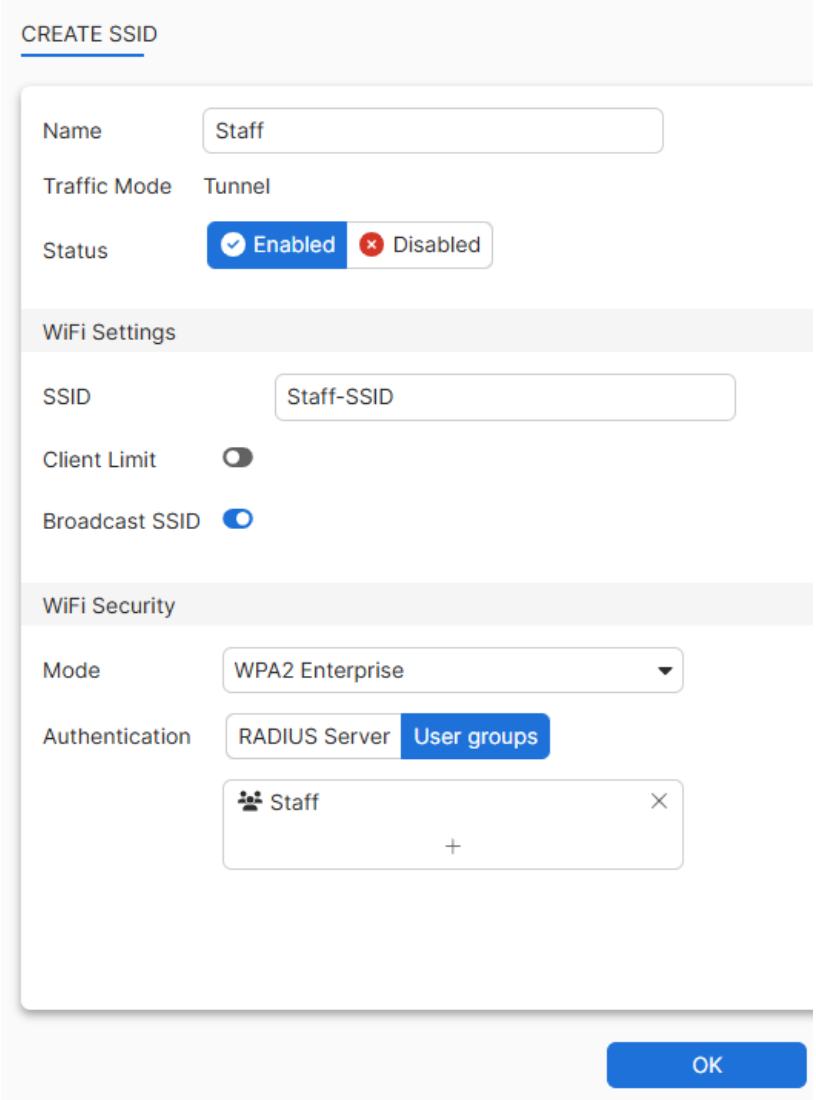
To create a local user group:

1. Go to *Access & authentication > Access > Users and groups*.
2. Click *Create*.
3. Select *User group*, then click *Next*.
4. Enter the *Name* of the new user group, for example, *Staff*.
5. For *Users*, click *+* and in the slide-in select the newly created local users to add to the local user group. Click *Close*.
6. Click *OK*.

To create an SSID to use WPA2 Enterprise with the local user group:

1. Go to *Operations > Connectivity > Edge devices > FortiAPs*.
2. On the *SSIDs* tab, click *Create*.
3. In the *Create SSID* page, do the following:
   a. Enter the *Name* of the SSID used for identifying the SSID in FortiSASE, for example, *Staff*.
   b. In *WiFi Settings*, configure the following:
      i. Enter the *SSID* name to be seen by wireless clients, for example, *Staff-SSID*.
      ii. Enable *Broadcast SSID*, if desired.
   c. In *WiFi Security*, configure the following:
      i. For *Mode*, select *WPA2 Enterprise*.
      ii. For *Authentication*, select *User groups*.
      iii. Click *+*. In the slide-in, select the local user group created previously. In this example, it is *Staff*.

d. Click *OK*.



To verify WPA2 Enterprise user authentication upon connecting to the SSID:

1. On a wireless client device, connect to the SSID, for example, *Staff-SSID*.
2. When prompted to continue connecting, click *Connect* to proceed.
3. Upon connection, you are prompted to enter your username and password. If you are using Windows, deselect *Use my Windows user account* and enter one of the local usernames and passwords to proceed.
4. Click *OK*.
5. Click *Connect*. Once connected, you should see *Connected, Secured* next to the SSID if you are using Windows. You should now be able to securely access the internet through the SSID and FortiAP edge device that FortiSASE manages.

Troubleshooting a FortiAP that FortiSASE does not see

If after configuring the FortiAP, FortiSASE does not see it, take the following troubleshooting steps.

To troubleshoot a FortiAP that FortiSASE does not see:

1. Ensure that the FortiAP is registered in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 169.
2. Ensure that the FortiAP is registered with a FortiSASE subscription in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 169.
3. Ensure that after you connect the FortiAP to a wired network that it is getting a valid IP address, can access the internet, and can connect to the FortiSASE wireless controller. By default, the FortiAP obtains a LAN IP using DHCP. You can connect to the FortiAP CLI using a serial console connection and serial terminal software to perform these steps:
   a. Check the FortiAP LAN IP address and netmask, and default gateway, respectively, using these commands:

      ```
      ifconfig br0
      route
      ```

   b. Ping the FortiSASE domain name using `ping <FortiSASE domain name>` and then cancel it using Ctrl+C.
   c. Check the FortiAP has a valid CAPWAP connection to the wireless controller using this command:

      ```
      FortiAP-431F # cw_diag -c acs
      WTP Configuration
          name                 : FortiAP-431F
          loc                  : N/A
          ap mode              : thin AP
          ...
      ACS 0 info
          wcha info            : mode=0 max=10 wait=10 peer_cnt=0
          acPri                : 1
          fsm-state            : RUN 768
          ac-ip-addr           : 154.52.4.72:5246,5247        DNS
          ac-name              : FGVMABCD00000EFG
          ...
          data-chan-sec-oper   : ipsec-sn
          ...

      ACS 1 info
          wcha info            : mode=0 max=0 wait=0 peer_cnt=0
          acPri                : 2
          fsm-state            : START 796
          ac-ip-addr           : 0.0.0.0:0,0        UNKNOWN
          ac-name              :
          ...
      ```

4. For additional troubleshooting steps, refer to these topics as a reference only:
   a. Connecting a FortiAP to FortiSASE using alternative connection methods on page 186
   b. Upgrading to a supported FortiAP firmware version using alternative connection methods on page 187

Connecting a FortiAP to FortiSASE using alternative connection methods

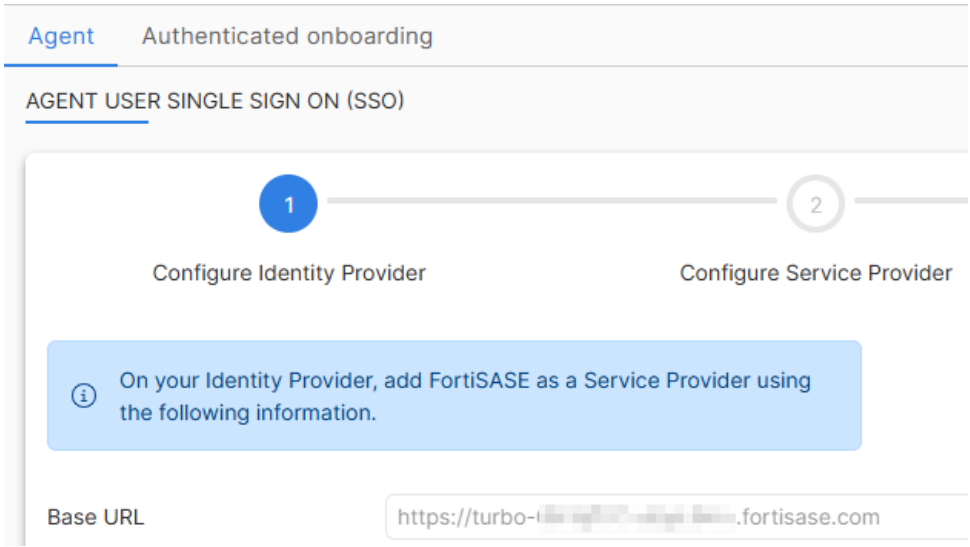
You can connect a FortiAP to FortiSASE using alternative connection methods, namely, using the FortiAP GUI or CLI.

> For ease of configuration, following Connecting a FortiAP to FortiSASE using FortiZTP on page 171 is recommended.
>
> As a reference only, this section describes alternative connection methods other than using FortiZTP.

Before using the FortiAP GUI or CLI steps, you must obtain the FortiSASE domain name from FortiSASE.

To obtain the FortiSASE domain name from FortiSASE:

1. Go to *Access & authentication* > *SSO*.
2. View the URL in the *Base URL* field and note the FortiSASE domain name after the https:// string. In the example, the FortiSASE domain name is turbo-a1p0hv3p.edge.prod.fortisase.com.



To connect a FortiAP to FortiSASE via the GUI:

1. Log in to the FortiAP GUI.
2. Go to *Settings* > *Local Configuration*.
3. For *AC Discovery Type*, select *DNS*.
4. For *AC Host Name 1*, copy and paste the FortiSASE domain name that you obtained.
5. Click *OK*.
6. If you are using FortiAP Configuration mode, do the following:
   a. To exit this mode, go to the admin menu at the top-right corner and click *Reboot*.
   b. Click *Yes*. Configuration changes take effect after the FortiAP reboots.
7. Connect the FortiAP port to a wired network with internet access. The FortiAP connects to FortiSASE using the domain name configured.

To connect a FortiAP to FortiSASE via the CLI:

1. Connect to FortiAP by starting one of the following:
   a. SSH session with the FortiAP IP address
   b. Console session if your FortiAP has a console port
2. Log in to the FortiAP CLI.
3. Enter these configuration commands:

```
cfg -a AC_DISCOVERY_TYPE=3
cfg -a AC_HOSTNAME_1=<FortiSASE domain name>
cfg -c
```

4. If you are using FortiAP Configuration mode, enter `reboot` to exit this mode. Configuration changes take effect after the FortiAP reboots.
5. Connect the FortiAP port to a wired network with internet access. The FortiAP connects to FortiSASE using the domain name configured.

Upgrading to a supported FortiAP firmware version using alternative connection methods



For ease of configuration, following Considerations on page 174 or Prerequisites and considerations on page 176 is recommended.

As a reference only, this section describes FortiAP firmware upgrades using alternative connection methods other than the recommended methods.

If the FortiAP runs an unsupported firmware version, prior to connecting a FortiAP to FortiSASE, you generally must perform these preliminary steps on the FortiAP to ensure proper connectivity:

1. Upgrade the FortiAP to the latest firmware version known to work with FortiSASE using the FortiAP upgrade path. You will save one or more the firmware files locally to your computer and upload the firmware to the device using the FortiAP GUI. See SIA for FortiAP site-based remote users.
2. Factory reset the FortiAP device. For this step, you will use the FortiAP CLI and an SSH client to ensure no prior configuration remains on the device.

To upgrade the FortiAP firmware to the latest version using the FortiAP upgrade path:

1. Connect and log in to the FortiAP GUI as follows:
   a. Connect the FortiAP unit from the LAN 1 port to a separate private switch or hub via a straight-through Ethernet cable or directly connect from the LAN 1 port to your computer Ethernet port via a crossover cable.
   b. Change your computer IP address to 192.168.1.3.
   c. Using a web browser on your computer, connect to https://192.168.1.2. This IP address is overwritten if the FortiAP is connected to a DHCP environment. Ensure that the FortiAP unit is in a private network with no DHCP server.
   d. Log in with the username *admin* and no password.
2. Check the current firmware version on the FortiAP GUI from *Information > Dashboard* and in the *Firmware* widget by noting the *Firmware Version* field. Note the four-digit number after build. For example, if you see build0001, 0001 is the build number.

3. Review Supported Upgrade Paths, which lists the FortiAP firmware upgrade path required to upgrade to the supported FortiAP firmware version:
   a. In the *Build #* column, find the build number matching the current firmware version.
   b. In the *Path* column, note the other firmware versions needed. There may be one or more firmware versions required in the upgrade path to upgrade to the supported firmware version. You will need to download the firmware image files for these versions corresponding to your FortiAP device model from the Fortinet Support Site.
4. From the Fortinet Support Site, download the FortiAP firmware image files in the supported upgrade path corresponding to the FortiAP device model, saving them locally to your computer. The firmware image files will be uploaded to the FortiAP device using the FortiAP GUI.
5. From admin dropdown on the top-right, click *Upload/Upgrade*.
6. In the dropdown, select *Image*, click *Image File*, and select the desired firmware image file location saved locally on your computer.
7. Click *Upload* to start the upgrade. You see an *Uploading* dialog as the file upload proceeds. FortiAP reboots automatically to complete the firmware upgrade.
8. Reconnect and log into the FortiAP GUI and confirm the firmware version updated as desired.
9. If necessary, repeat steps 5-8 for each firmware in the supported upgrade path until all the steps in the path are complete.

To factory reset the FortiAP device:

1. Connect the FortiAP unit from the LAN 1 port to a separate private switch or hub via a straight-through Ethernet cable or directly connect from the LAN 1 port to your computer Ethernet port via a cross-over cable.
2. Change your computer IP address to 192.168.1.3.
3. Using an SSH client on your computer, connect to 192.168.1.2 . You may need to download and install an SSH client if it has not been previously installed on your computer.
4. Enter the following FortiAP CLI command to factory reset the device: `factoryreset`
5. Confirm the factory reset when prompted by entering `y`:

```
FortiAP # factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n)y
```

A reboot occurs as part of the factory reset process.

Captive portal

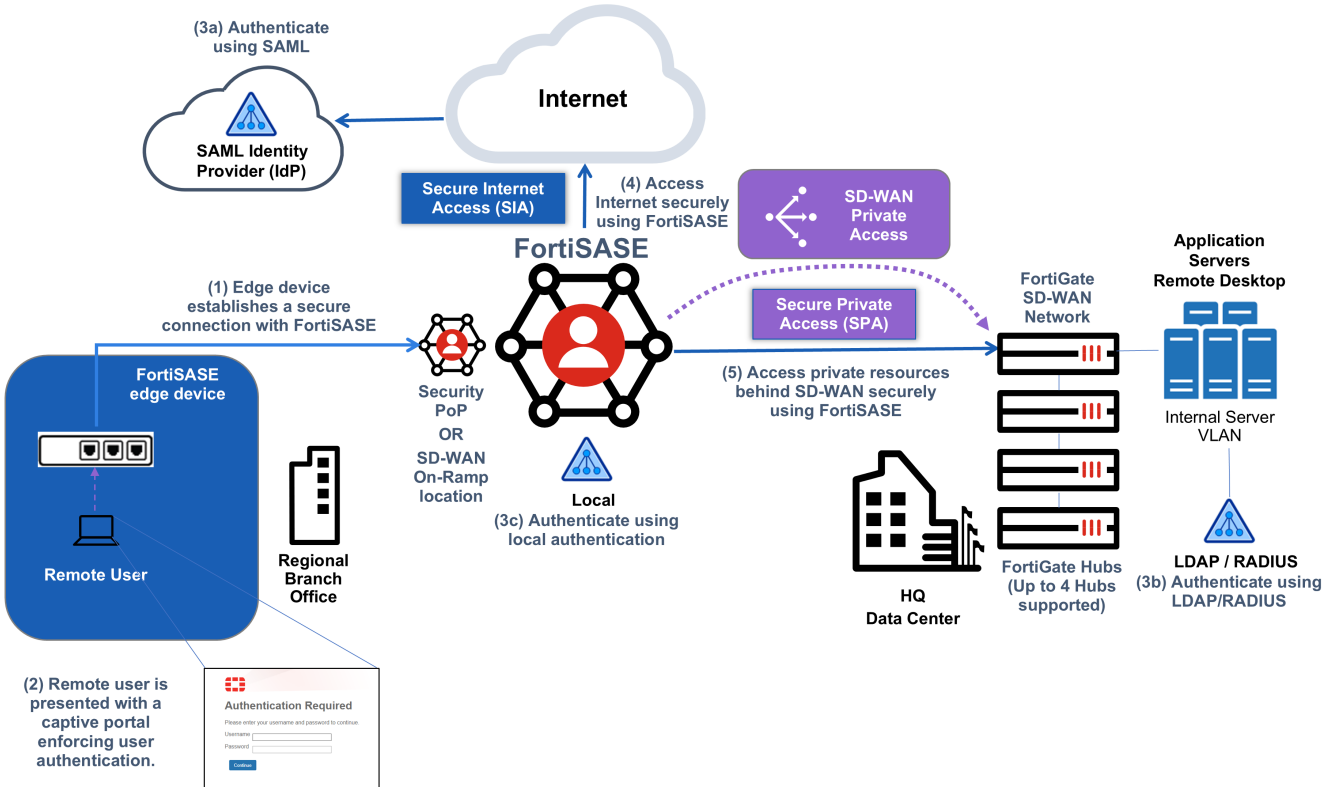
FortiSASE supports a captive portal that enforces user authentication for endpoints connected behind edge devices that attempt to access the Internet or private access resources.

User authentication for the captive portal can be achieved through the following authentication servers and sources:

- Local users
- LDAP users
- RADIUS users

- SSO authentication via SAML IdP

The workflow for captive portal authentication is illustrated below:



Considerations

- With the addition of support for identity-based policies for edge devices in FortiSASE 24.3.a, the behaviour of edge device traffic based on policies has changed in existing FortiSASE instances:
  - Any policies you created before FortiSASE 24.3.a, specifically for edge devices, namely, policies with *Source Scope* set to *Edge Devices* will have *User* set to *Captive Portal Exempt*.
  - Any policies you created before FortiSASE 24.3.a with *Source Scope* set to *All* will not be modified. Therefore, any edge devices whose traffic matched an *All* allow policy before will now have authentication enforced using the captive portal. You must explicitly create a new exemption policy and place it above any *All* allow policies to avoid captive portal authentication for any impacted edge devices. See Configuring an exemption policy for SSO authentication for Entra ID on page 190.
- When SSO authentication is used with the captive portal for edge devices, you must add an exemption policy for the SAML IdP URLs specified using hosts or infrastructure selections for the *Destination* field to allow SSO authentication traffic destined for the IdP to bypass the captive portal. See Configuring an exemption policy for SSO authentication for Entra ID on page 190.

Configuring an exemption policy for SSO authentication for Entra ID

When using single sign on (SSO) authentication with captive portal for edge devices, you must add an exemption policy for the SAML identity provider (IdP) URLs specified using hosts or infrastructure selections for the *Destination* field to allow SSO authentication traffic destined for the IdP to bypass the captive portal.

> This example configures an exemption policy for SSO authentication when Microsoft Entra ID SSO has been configured. Therefore, a prerequisite for this topic is to have configured an SSO authentication source in *Access & authentication > SSO*. See Configuring FortiSASE with Microsoft Entra ID SSO in FortiClient agent-based mode on page 517.

To configure an exemption policy for SSO authentication for Entra ID:

1. Go to *Security > Traffic > Policies*.
2. Click *Create* to create a new policy.
3. In the *New Policy* page, configure these settings:

Field	Value
Name	SSO-exempt
Source Scope	*Edge device*
Source	*All Edge Devices* or *Specify* with specific edge devices selected, depending on your requirements
User	*Captive Portal Exempt*
Destination	*Specify* Click + and select *Infrastructure* in the dropdown. Search for Azure in the search field and press `Enter`. Select *Microsoft-Azure* and *Microsoft.AD*. Click *Close*.
Profile Group	*Default* or *Specify* (depending on your requirements)
Basic Certificate Inspection Override	Disabled
Action	*Accept*
Status	Enabled
Log Allowed Traffic	Enabled *Security Events* or *All Sessions* (depending on your requirements).

4. Click *OK*.
5. Ensure you move the exemption policy above the Allow-All policy.

Configuring an exemption policy for an edge device

For troubleshooting purposes or to fulfill your requirements, you may need to exempt endpoints behind a specific edge device from captive portal authentication. Follow these steps to configure an exemption policy for an edge device.

> This example configures an exemption policy for a FortiAP edge device with an SSID configured. With *Source Scope* set to *Edge Device*, configure a different edge device as *Source* as applicable to your current deployment.

To configure an exemption policy for an edge device:

1. Go to *Security* > *Traffic* > *Policies*.
2. Click *Create* to create a new policy.
3. In the *New Policy* page, configure these settings:

Field	Value
Name	FAP-Captive-Portal-Exemption
Source Scope	*Edge Device*
Source	Click *Specify*, then select the specific edge device. This example selects the SSID FM-STAFF.
User	*Captive Portal Exempt*
Destination	*All Internet Traffic*
Service	*ALL*
Profile Group	*Default* or *Specify* (depending on your requirements)
Basic Certificate Inspection Override	Disabled
Action	*Accept*
Status	Enabled
Log Allowed Traffic	Enabled *Security Events* or *All Sessions* (depending on your requirements)

4. Click *OK*.
5. Ensure you move the exemption policy above the Allow-All policy.

Example: Configuring a captive portal only SSID for FortiAP

This example configures a captive portal using the WiFi Security Mode configured within an SSID for a FortiAP edge device. The FortiAP edge device has already been registered and authorized in FortiSASE.

If you require a WPA2 Personal protected SSID for FortiAP, substitute the appropriate steps in the following procedure to configure WPA2 Personal as the WiFi Security Mode instead and use a passphrase with your wireless endpoint to connect to the SSID.

By default, without a captive portal exemption policy that applies to specific SSID or for all edge devices, a WPA2 Personal-protected SSID and SSIDs of other WiFi security modes for FortiAP are subject to captive portal authentication.

The configuration workflow is as follows:

1. Create local users.
2. Create a local user group.
3. Create an SSID to use Captive Portal Only with the local user group.
4. (Optional) Customize messages that display to the user in browser for captive portal.
5. Verify captive portal user authentication upon connecting to the SSID.

To create local users:

1. Go to *Access & authentication* > *Access* > *Users and groups*.
2. Click *Create*.
3. Select *User*.
4. Enter the *Email* of the new user. This will be the username of the new user.
5. Click *OK*. The new user will receive an email prompting them to activate the new account and to set a new password.
6. Repeat steps 1 to 4 to add more local users.

To create a local user group:

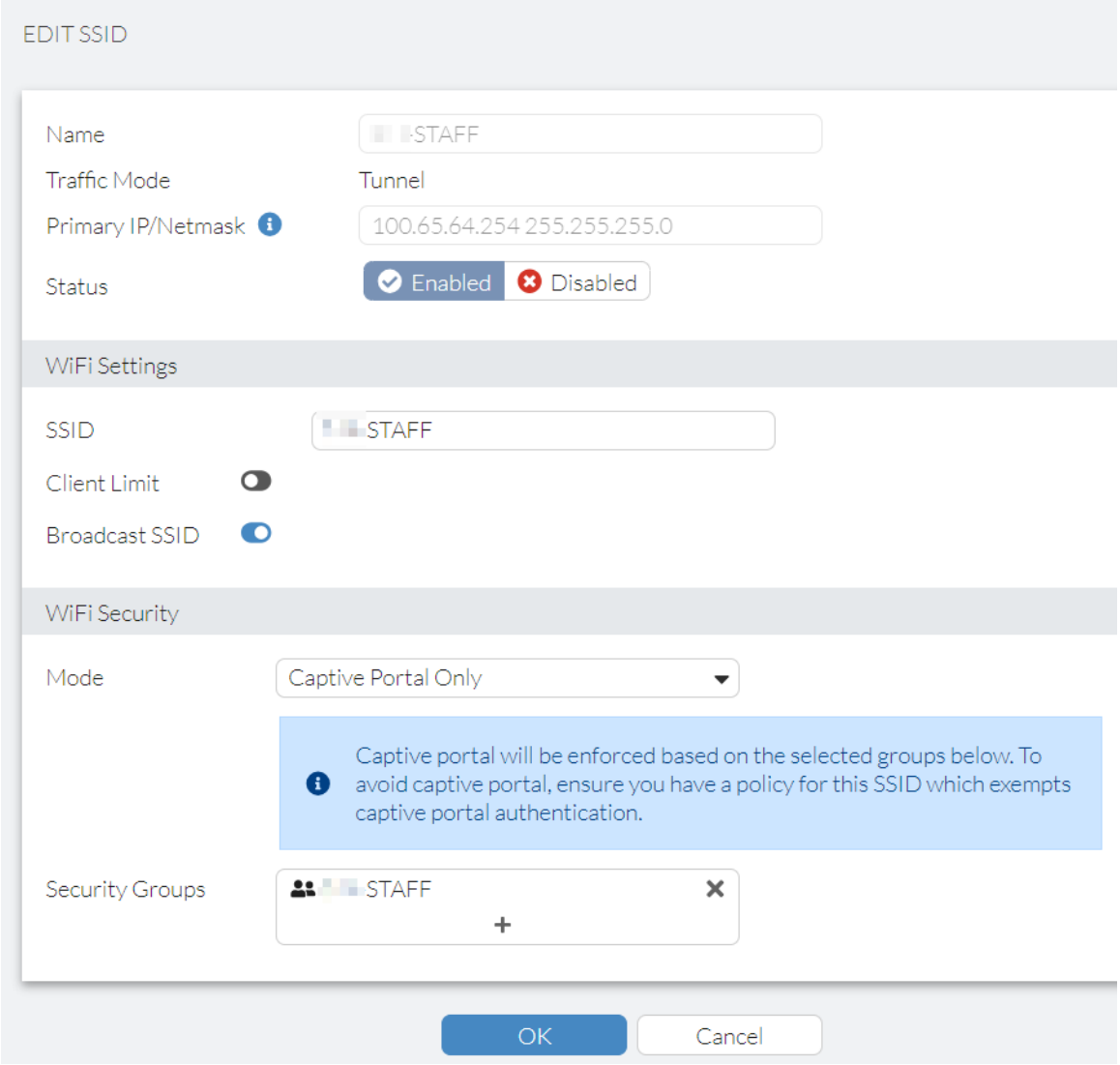
1. Go to *Access & authentication* > *Access* > *Users and groups*.
2. Click *Create*.
3. Select *User group*.
4. Enter the *Name* of the new user group, for example, Staff.
5. For *Users*, click + and in the slide-in select the newly created local users to add to the local user group. Click *Close*.
6. Click *OK*.

To create an SSID to use Captive Portal Only with the local user group:

1. Go to *Operations* > *Connectivity* > *Edge devices* > *FortiAPs*.
2. On the *SSIDs* tab, click *Create*.
3. In the *Create SSID* page, do the following:
   a. Enter the *Name* of the SSID used for identifying the SSID in FortiSASE, for example, STAFF.
   b. In *WiFi Settings*, configure the following:
      i. Enter the *SSID* name to be seen by wireless clients, for example, STAFF.
      ii. Enable *Broadcast SSID*, if desired.

c. In *WiFi Security*, configure the following:
   i. For *Mode*, select *Captive Portal Only*.
   ii. For *Security Groups*, click *+*. In the slide-in, select the local user group created previously. In this example, it is STAFF.

d. Click *OK*.

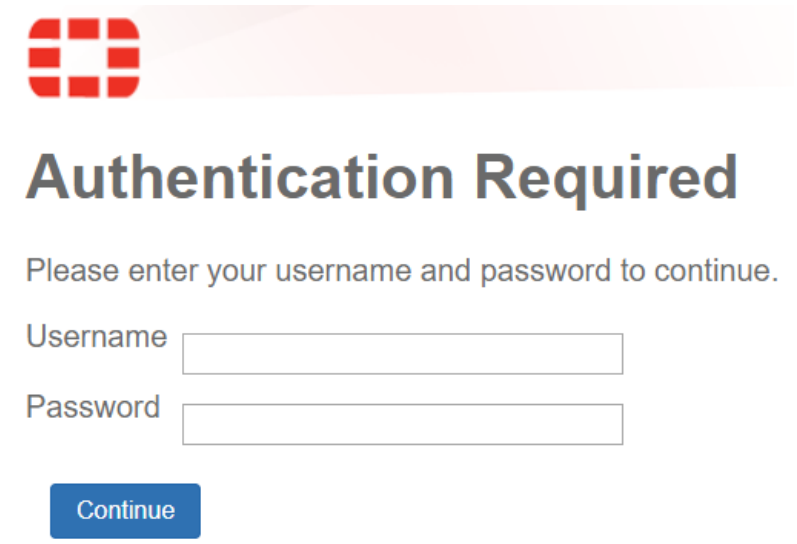


To customize messages that display to the user in browser for captive portal:

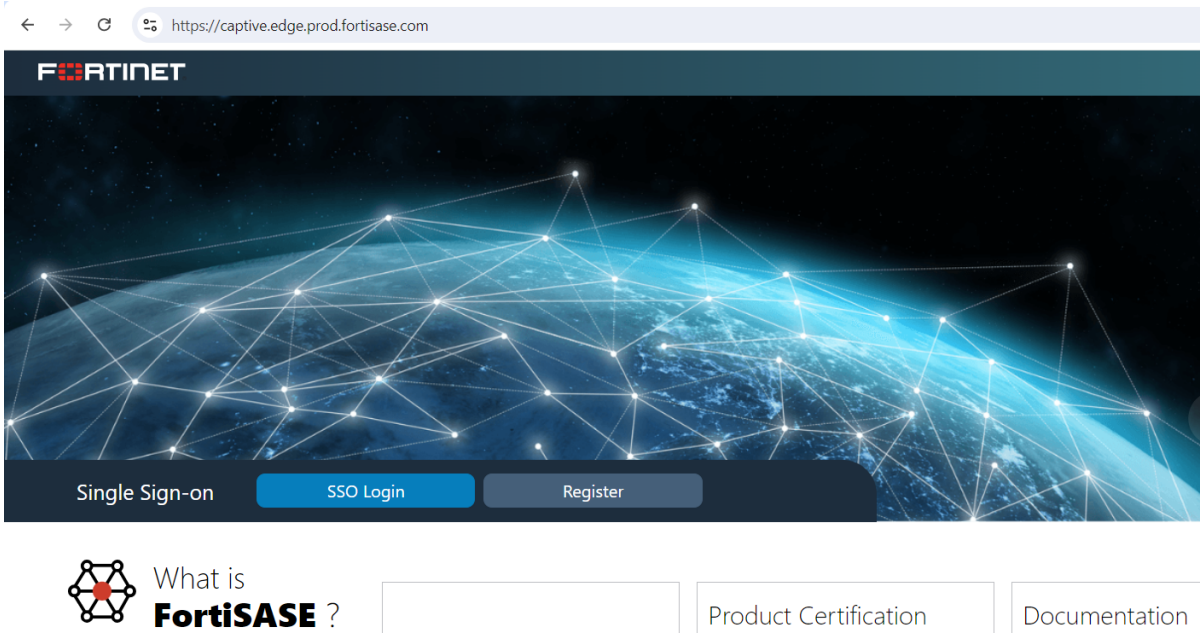
You can customize messages that display to the user in browser for captive portal if desired. See HTML templates on page 589.

To verify Captive Portal Only user authentication upon connecting to the SSID:

1. On a wireless client device, connect to the SSID, for example, STAFF.
2. A web browser should appear prompting you to authenticate using the captive portal page. If you customized this message, confirm that it displays as per your configuration. Enter a local user name and password and click *Continue*.



Upon successful authentication, your web browser redirects to the FortiSASE page. The endpoint should be able to access the internet, as desired.



Example: Configuring a captive portal for FortiExtender

This example configures a captive portal for a FortiExtender edge device. The

FortiExtender edge device has already been registered and authorized in FortiSASE.

> By default, without a captive portal exemption policy that applies for a specific edge device or for all edge devices, any endpoints behind an edge device including FortiExtender, FortiGate as LAN extension, and Branch On-ramp will be subject to captive portal authentication.

The configuration workflow is as follows:

1. Create local users.
2. Create a local user group.
3. (Optional) Customize messages that display to the user in browser for captive portal.
4. Verify captive portal user authentication when using FortiExtender as a default gateway.

To create local users:

1. Go to *Access & authentication > Access > Users and groups*.
2. Click *Create*.
3. Select *User*.
4. Enter the *Email* of the new user. This will be the username of the new user.
5. Click *OK*. The new user will receive an email prompting them to activate the new account and to set a new password.
6. Repeat steps to add more local users.

To create a local user group:

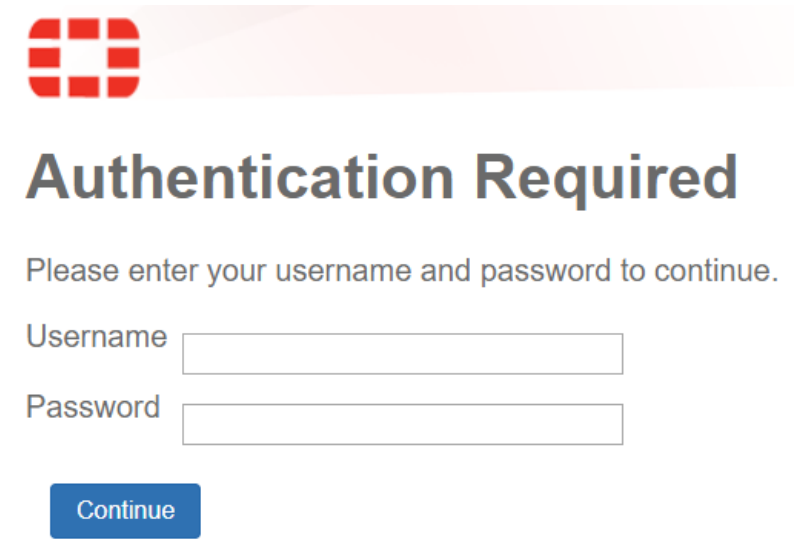
1. Go to *Access & authentication > Access > Users and groups*.
2. Click *Create*.
3. Select *User Group*.
4. Enter the *Name* of the new user group, for example, Staff.
5. For *Users*, click *+* and in the slide-in select the newly created local users to add to the local user group. Click *Close*.
6. Click *OK*.

To customize messages that display to the user in browser for captive portal:

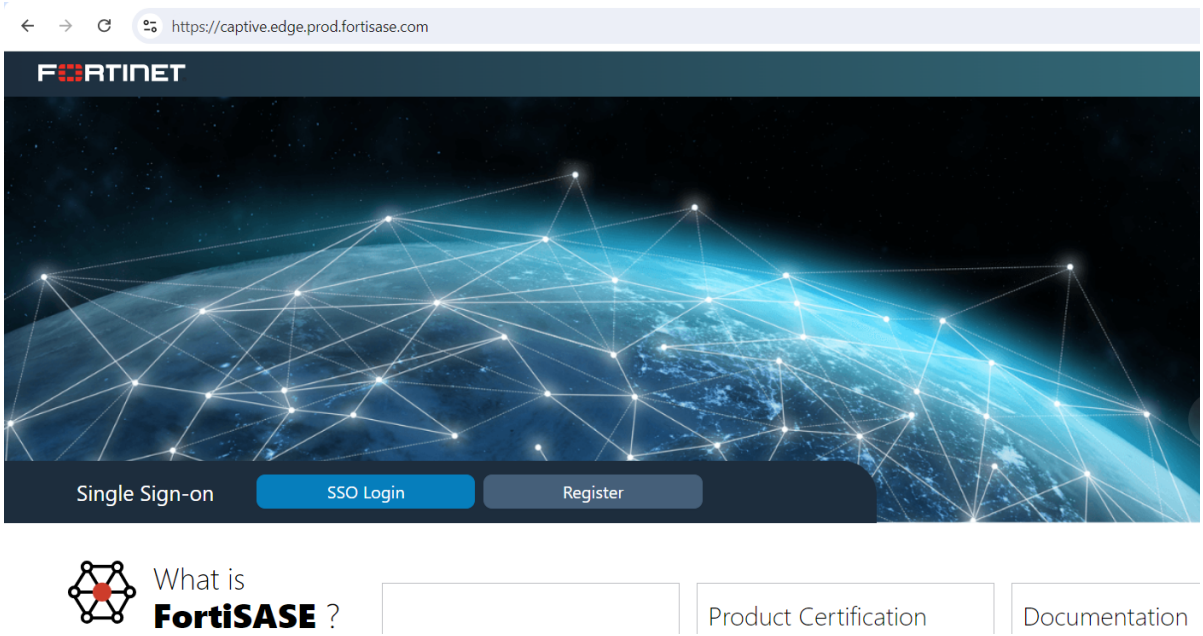
You can customize messages that display to the user in browser for captive portal if desired. See HTML templates on page 589.

To verify Captive Portal Only user authentication when using FortiExtender as a default gateway:

1. On an endpoint device using the FortiExtender as a default gateway, attempt to connect to the Internet. In some cases, the device is already trying to access the Internet through software updates so this should trigger the captive portal. In either case, the traffic should be matching the default Allow-All policy which enforces captive portal authentication.
2. A web browser should appear prompting you to authenticate using the captive portal page. If you customized this message, confirm that it displays as per your configuration. Enter a local user name and password and click *Continue*.



Upon successful authentication, your web browser will be redirected to the FortiSASE page. The endpoint should be able to access the Internet, as desired.

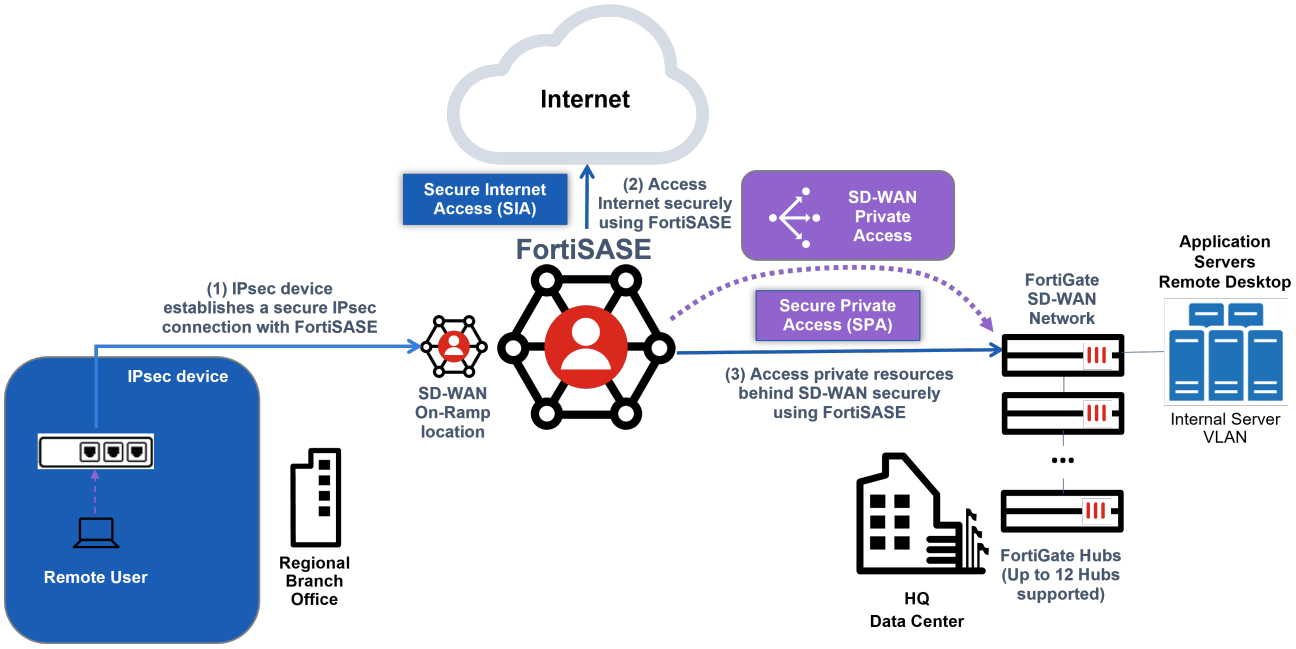


On-ramp tunnel

You can configure an IPsec device for Branch On-ramp by setting up an IPsec tunnel between the IPsec device located at the branch and a FortiSASE Branch On-ramp security PoP. In this use case, because the IPsec device is responsible for centralizing its remote users' site connectivity to the FortiSASE firewall-as-a-service (FWaaS), the endpoints only need to be configured in their IP settings to forward traffic to the IPsec branch device as the default gateway.

Multiple IPsec branch devices can establish IPsec connections with the Branch On-ramp security PoP.

Therefore, for this use case, individual workstation or device setup is minimized because FortiClient does not need to be installed on endpoints and web browser-based endpoints do not require explicit web proxy settings to be configured.



Configuration workflow

1. Configuring IPsec device as Branch On-ramp on page 200
2. Configuring profile groups and policies to control traffic flow from branch devices on page 207
3. Configure a device to establish IPsec connection to FortiSASE:
   a. Configuring a FortiGate IPsec connection to FortiSASE on page 208
   b. Configuring a third-party IPsec connection to FortiSASE on page 226

Prerequisites and considerations

See Prerequisites and considerations on page 197.

Prerequisites and considerations

Prerequisites

This section covers prerequisites to using Branch On-ramp in FortiSASE:

- Supported models and firmware on page 198
- FortiCloud account prerequisites on page 198

- Network topology on page 199
- SSL deep inspection for site-based users on page 200

In addition to configuring FortiSASE Branch On-ramp IPsec settings, you must still configure the FortiGate or third-party branch device itself with the corresponding IPsec settings.

Considerations

- Implementing dedicated public IP addresses impacts the operation of the FortiSASE instance. It is a fully automated end-to-end process and cannot be reverted as it involves architectural and configuration changes for the tenant. Fortinet recommends that you raise a request to implement dedicated public IP address use cases with ample time in advance before onboarding any remote users or implementing features such as edge device support to avoid service disruption.
- When using FortiGate branch devices, the Branch On-ramp and secure private access (SPA) features share the BGP configuration.
  - You must configure the SPA network configuration first before deploying an Branch On-ramp Security PoP but you can create SPA service connections after deploying an Branch On-ramp Security PoP.
  - For this use case, only iBGP is supported between the FortiGate branch devices and Branch On-ramp Security PoP.
- Since BGP is not supported when using third-party branch devices, static routing must be configured on the branch device.
- In *Current on-ramp resources* listed in *Deploy Security PoP* or *Edit Security PoP*, the *Connections* value reflects the number of connections in use based on On-Ramp subscriptions and does not reflect the number of active connections in use.
- When a Branch On-ramp security PoP is configured with multiple IPsec tunnels for third-party branch devices, to ensure correct tunnel matching you must configure each tunnel with a unique peer ID and set the local ID on each branch device to match the corresponding peer ID.
- When a Branch On-ramp security PoP is configured with multiple IPsec tunnels for FortiGate branch devices, to ensure correct tunnel matching you must configure each tunnel with a unique network ID, which is a Fortinet proprietary feature.

Supported models and firmware

For a list of model and firmware version prerequisites, see SIA for Branch On-ramp site-based remote users.

FortiCloud account prerequisites

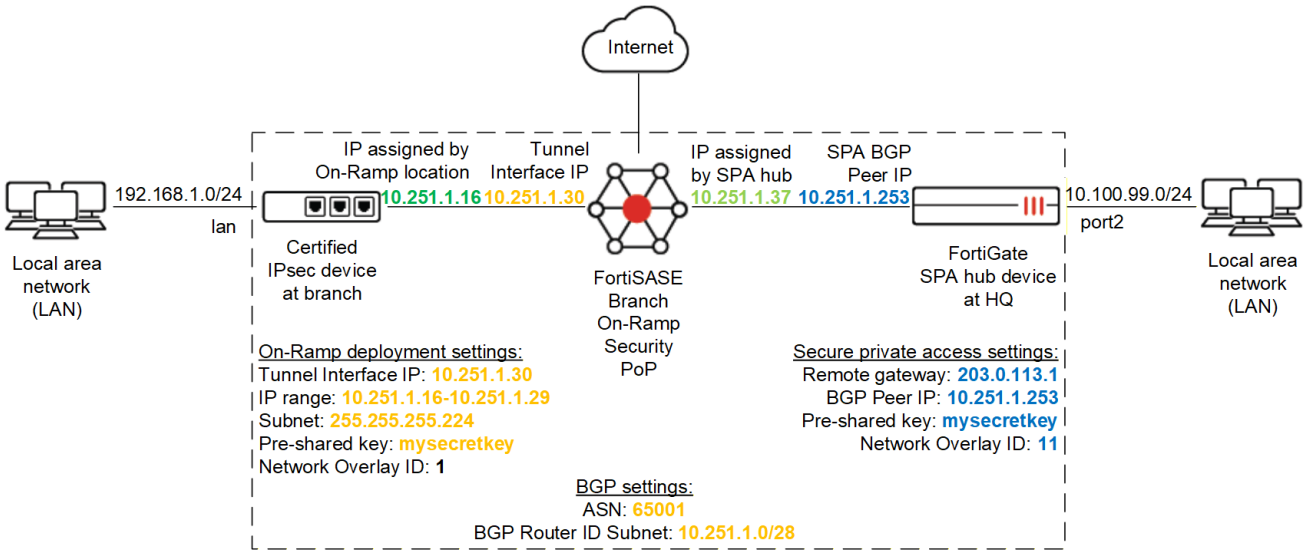
- Branch On-ramp requires a FortiSASE instance with a Standard, Advanced, or a Comprehensive subscription applied and a separate FortiSASE On-Ramp Location subscription.
- The FortiSASE subscription restricts the number of On-Ramp security PoPs that you can deploy based on the number of seats (2 to 20) that the subscription specifies. Contact your Fortinet sales/partner representative to purchase a FortiSASE subscription for each certified IPsec device.
- When upgrading your instance from a Standard subscription to an Advanced or Comprehensive subscription, as a prerequisite for Branch On-ramp, you must explicitly request the enablement of dedicated public IP addresses your FortiSASE instances. See Subscriptions on page 786.

See SIA for Branch On-ramp site-based remote users or the FortiSASE Ordering Guide.

For details on registering products, see Registering assets.

Network topology

The following diagram depicts an example network topology that an IPsec device uses for FortiSASE Branch On-ramp:



An IPsec tunnel is established between the IPsec device and a FortiSASE Branch On-ramp security PoP.

When using FortiGate branch devices, BGP AS and router ID subnet configuration settings are shared between the Branch On-ramp and secure private access (SPA) features.

- You must configure the BGP network configuration first before deploying a Branch On-ramp Security PoP but you can create SPA service connections after deploying a Branch On-ramp Security PoP.
  - Either BGP per overlay or BGP on loopback routing designs can be used for BGP peering between the FortiSASE Branch On-Ramp Security PoP and FortiGate SPA hub.
  - This example uses BGP per overlay to demonstrate the configuration.
- For this use case, only iBGP, specifically, BGP per overlay routing design, is supported between the FortiGate branch devices and Branch On-ramp Security PoP.
- Between the FortiGate branch devices and On-Ramp Security PoP, iBGP (BGP per overlay only) is used to ensure FortiSASE can access branch local subnets for secure internet access (SIA) reply traffic.
- Using iBGP, the branch local subnets are advertised to the SPA hub but the SPA hub local subnets are not advertised to the branch device.
- Since BGP is not supported when using third-party branch devices, static routing must be configured on the branch device.

Multiple branch devices can establish IPsec connections with the Branch On-ramp security PoP.

- When a Branch On-ramp security PoP is configured with multiple IPsec tunnels for third-party branch devices, to ensure correct tunnel matching you must configure each tunnel with a unique peer ID and set the local ID on each branch device to match the corresponding peer ID.

- When a Branch On-ramp security PoP is configured with multiple IPsec tunnels for FortiGate branch devices, to ensure correct tunnel matching you must configure each tunnel with a unique network ID, which is a Fortinet proprietary feature.

> Example values for branch on-ramp and SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

The example network topology uses the following settings configured in FortiSASE when the IPsec device at the branch is a FortiGate device:

Configuration setting	Value used in example network topology
On-Ramp deployment settings	
Tunnel Interface IP	10.251.1.30
IP range	10.251.1.16-10.251.1.29
Subnet	255.255.255.240
Pre-shared key	mysecretkey
Network Overlay ID	1
Secure private access settings	
Remote gateway	203.0.113.1
BGP Peer IP	10.251.1.253
Pre-shared key	mysecretkey
Network Overlay ID	11

The BGP router ID subnet must not overlap with the On-ramp tunnel IP range. Otherwise, the BGP peering between the branch devices and the On-Ramp Security PoP will not be established because of IP conflicts.

For additional networking considerations specific to FortiGate branch devices see BGP, SD-WAN, and routing configuration on page 210.

SSL deep inspection for site-based users

When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless proxy users and site-based edge device users. See Installing a certificate for deep inspection mode on page 317.

Configuring IPsec device as Branch On-ramp

> Ensure that you are aware of Branch On-ramp Prerequisites and considerations on page 197.

In *Operations* > *Connectivity* > *On-ramp tunnel*, you can configure the IPsec settings used by FortiGate or third-party IPsec branch devices to connect to FortiSASE.

In addition to configuring FortiSASE Branch On-ramp IPsec settings, you must still configure the FortiGate or third-party branch device itself with the corresponding IPsec settings.

- Configuring BGP on page 201
- Configuring On-Ramp security PoPs on page 203

Configuring BGP

Ensure that you are aware of Branch On-ramp Prerequisites and considerations on page 197.

Example values for branch on-ramp and SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

To configure BGP settings for Branch On-ramp:

1. Go to *Network* > *BGP*.
2. Configure the following BGP settings:

Network attributes	Description	Example
BGP Routing Design	FortiSASE supports these main routing design methods: • BGP per overlay (default) • BGP on loopback You can use only a single BGP routing design method for all hubs and spokes. You cannot mix them. **Considerations:** • This setting only configures the BGP routing design between the FortiSASE Branch On-Ramp Security PoP and FortiGate SPA hub. • Only BGP per overlay routing design is supported between the FortiGate branch devices and Branch On-ramp Security PoP.	BGP per overlay

Network attributes	Description	Example
BGP Router ID subnet	Define the subnet from which loopback interface IP addresses will be assigned to the entitled FortiSASE security PoPs. The loopback interface IP address assigned from this subnet will be used as the BGP router ID on the FortiSASE security PoPs. Each security PoP will receive one IP address in this subnet. /28 is the minimum subnet size. Note that a subnet larger than /28 may be required if the number of entitled security PoPs exceeds 16 and/or if any entitled security PoPs have been provisioned to exceed the default maximum number of remote agents per region of 4096 (/20). This BGP setting is shared between the Branch On-ramp and secure private access (SPA) features.	10.251.1.0/28
SPA hubs belong to	If all SPA hub(s) are in the same BGP autonomous system number (ASN) as FortiSASE, select *FortiSASE autonomous system*. This option enables iBGP peering between FortiSASE and the SPA hub(s). If the SPA hub(s) are distributed across both the same and different BGP autonomous system numbers (ASNs) relative to FortiSASE, select *Different autonomous systems*. This configuration enables eBGP peering with SPA hubs in different ASNs and iBGP peering with those in the same ASN as FortiSASE.	FortiSASE autonomous system
FortiSASE ASN	BGP autonomous system (AS) number of your hubs. This BGP setting is shared between the Branch On-ramp and secure private access (SPA) features.	65001
Hub Selection Method	Method by which FortiSASE selects hub. By default, FortiSASE uses hub health and priority: • **Hub health and priority**: periodically obtain jitter, latency, and packet loss measurements for each hub via the health check IP address. FortiSASE selects the highest priority hub within each security PoP that meets SLA	Hub health and priority

Network attributes	Description	Example
	requirements. A hub can be assigned a different priority level in different security PoPs. This method is not available when support for configuring multi-ASN is enabled using *SPA hubs belongs to* setting. • **BGP MED**: BGP multi-exit discriminator (MED) is an attribute that an autonomous system advertising routes to another peer sets. FortiSASE learns MED from the configured hubs. See BGP multi-exit discriminator.	
Health Check IP	The health check IP is used to periodically obtain jitter, latency and packet loss measurements per service connection. While it is option for the BGP MED hub selection method, the health check IP provides insight into the service connection health.	10.11.11.11
Endpoint-to-endpoint Traffic	Traffic can travel directly between endpoints by traversing secure private access hubs. Once enabled, additional configuration is required to re-announce subnets learned from FortiSASE spokes and to resolve any conflicts that may arise between on-prem and FortiSASE subnets.	Disabled
Advertise Hub Priorities	Advertise hub priorities through BGP communities to steer traffic from external peers.	Disabled
BGP Recursive Routing	Enabling the BGP recursive routing setting allows for interhub connectivity and redundancy to networks behind the active hub if each hub has a physical connection to the others for cases when connectivity between a FortiSASE security PoP and the active hub fails.	Disabled

3. Click *Save*.

Configuring On-Ramp security PoPs



Ensure that you are aware of Branch On-ramp Prerequisites and considerations on page 197.

This section describes steps to configure on-ramp security PoPs:

- Deploying a Branch On-ramp security PoP on page 204
- Configuring an IPsec tunnel for the FortiGate device type on page 204
- Configuring an IPsec tunnel for the custom device type on page 205

Deploying a Branch On-ramp security PoP

To deploy a Branch On-ramp Security PoP:

1. Go to *Operations* > *Connectivity* > *On-ramp tunnel*.
2. Click the *Security PoP* tab.
3. Click *Deploy security PoP*.
4. Configure the following settings in the Deploy Security PoP page:

Setting	Description	Example
Deploy security PoPs and connections per PoP		
Security PoP and Connections	Datacenter to deploy as Branch On-ramp Security PoP.	Vancouver - Canada
	Number of connections per Security PoP	10

5. Click *+* to add more Security PoPs and connections as your FortiSASE Branch On-ramp subscription allows.
6. Click *OK*. In *Security PoP*, observe the *Status* begins as *Pending* and the *FQDN* field has a corresponding value. After some time the *Status* changes to *Running*. Note the *FQDN* field, which will be used for IPsec device configuration.

Configuring an IPsec tunnel for the FortiGate device type

In addition to configuring FortiSASE Branch On-ramp IPsec settings, you must still configure the FortiGate branch device itself with the corresponding IPsec settings. See Configuring a FortiGate IPsec connection to FortiSASE on page 208 .

Example values for branch on-ramp and SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

To configure an IPsec tunnel for the FortiGate device type:

1. Go to *Operations* > *Connectivity* > *On-ramp tunnel*.
2. Click the *On-ramp security PoPs* tab.
3. Select the security PoP, then click *Edit*.
4. In *IPsec tunnel*, click *Create*.
5. Configure the following settings in *Create New IPsec Tunnel*:

Setting	Description	Example
Name	Name of the IPsec tunnel	FortiGateCorp

Setting	Description	Example
Device type	Branch device type, either FortiGate or Custom for third-party devices.	FortiGate
Remote device		
Tunnel interface IP	IP address defined on the IPsec tunnel interface for the Security PoP	10.251.1.30
IP range	IP address range that the Security PoP uses for assigning tunnel interface IP addresses for IPsec devices using mode configuration.	10.251.1.16-10.251.1.29
Subnet mask	Subnet mask corresponding to the IP address range that the Security PoP uses for IP address assignment.	255.255.255.224
Pre-shared key	IPsec device authenticates with the Security PoP using preshared key (PSK). Define the PSK.	mysecretkey
Network ID	Define a unique network ID for each remote device. Ensure that the IPsec tunnels towards each remote device have different network IDs.	11

6. Click *OK*. Note the *Tunnel interface IP*, which will be used for IPsec device configuration.

Configuring an IPsec tunnel for the custom device type

In addition to configuring FortiSASE Branch On-ramp IPsec settings, you must still configure the third-party branch device itself with the corresponding IPsec settings. For an example on configuring a third-party IPsec device as an IPsec IKEv2 dialup client, see Configuring a third-party IPsec connection to FortiSASE on page 226.

Since BGP is not supported when using third-party branch devices, static routing must be configured on the branch device.

Multiple branch devices can establish IPsec connections with the Branch On-ramp security PoP.

- When a Branch On-ramp security PoP is configured with multiple IPsec tunnels for third-party branch devices, to ensure correct tunnel matching you must configure each tunnel with a unique peer ID and set the local ID on each branch device to match the corresponding peer ID.
- When a Branch On-ramp security PoP is configured with multiple IPsec tunnels for FortiGate branch devices, to ensure correct tunnel matching you must configure each tunnel with a unique network ID, which is a Fortinet proprietary feature.

Example values for branch on-ramp and SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

To configure an IPsec tunnel for the Custom device type:

1. Go to *Operations* > *Connectivity* > *On-ramp tunnel*.
2. Click the *On-ramp security PoPs* tab.
3. Select the security PoP, then click *Edit*.
4. In *IPsec tunnel*, click *Create*.

Setting	Description	Example
Name	Name of the IPsec tunnel	CorpDevice
Device type	Branch device type, either FortiGate or Custom for third-party devices.	Custom
Network		
Tunnel interface IP	IP address defined on the IPsec tunnel interface for the security PoP	10.251.1.30
Mode config	Toggle whether the security PoP uses mode configuration to assign tunnel interface IP addresses for IPsec devices	Enabled
IP assignment	The IP address range that the security PoP uses for assigning tunnel interface IP addresses for IPsec devices.	10.251.1.16-10.251.1.29
Subnet mask	When *IP assignment* is enabled, subnet mask corresponding to the IP address range that the security PoP uses for IP address assignment.	255.255.255.224
Pre-shared key	IPsec device authenticates with the security PoP using preshared key (PSK). Define the PSK.	mysecretkey
IKE	IKE version used for IPsec	IKEv2
Peer ID	Options to authenticate VPN peers or clients • *Any*: accept the local ID of any remote VPN peer • *From dial-up group*: accept peer ID in dialup group • *Specify*: accept the specified peer ID	*Specify* *8000v-99*
Phase 1		
Encryption - authentication	Choose encryption algorithm and message digest for the phase 1 proposal(s). Use + to add additional proposals.	SHA256 - AES256
Diffie-Helman groups	Asymmetric key algorithms used for public key cryptography. Select one or more from groups 1, 2, 5, and 14 through 32.	14, 19
Local ID	Optional setting. This value must match the peer ID value given for the remote VPN peer's peer options.	CorpDevice001
Phase 2		
Remote subnet (s)	Enter the destination subnet using network ID and subnet mask that corresponds to the recipients or networks behind the Branch device. Use + to add additional subnets.	192.168.30.0/255.255.255.0

Setting	Description	Example
Automatically create static routes	Create static routes on the Branch On-ramp security PoP to reach networks behind the Branch device.	Enabled
Encryption - authentication	Choose encryption algorithm and message digest for the Phase 2 proposal(s). Use + to add additional proposals.	SHA256 - AES256
Diffie-Helman groups	Asymmetric key algorithms used for public key cryptography. Select one or more from groups 1, 2, 5, and 14 through 32.	14, 19
Perfect Forward Secrecy	Perfect forward secrecy improves security by forcing a new DH exchange whenever keylife expires.	Enabled

5. Click *OK*.

Configuring profile groups and policies to control traffic flow from branch devices

In FortiSASE you can configure profile groups with security features enabled, hosts, and policies to control traffic flow as desired.

For example, the following devices can establish IPsec connections with a deployed Branch On-ramp security PoP:

- Branch 1 FortiGate with a local subnet of 192.168.1.0/24
- Branch 2 FortiGate with a local subnet of 192.168.10.0/24

In FortiSASE, you can configure the following:

1. Create profile groups and configure security features and settings in *Security* that are specific to each branch device.
2. Configure hosts in *Security* > *Hosts*, namely, IPv4 hosts of the *Subnet* type for each local subnet.
3. (Optional) Configure a policy to exempt the branch device and endpoints connected to it from using a captive portal if this matches your requirements and use case. See Configuring an exemption policy for an edge device on page 191.
4. Configure a policy for each branch with these settings in *Security* > *Profiles*:
   a. *Source Scope*: *Specify*
   b. Select the host created for the branch local subnet
   c. *Action*: *Accept*
   d. *Profile Group*: Specify and select the profile group created for the branch

See Security profile groups on page 313 and Configuring a policy to allow traffic from an Edge device to FortiSASE on page 299.

Configuring a FortiGate IPsec connection to FortiSASE

Ensure that you are aware of Branch On-ramp Prerequisites and considerations on page 197.

After deploying a Branch On-ramp security PoP in FortiSASE and configuring an IPsec tunnel for the FortiGate device type, you can configure the FortiGate as an IPsec branch device to establish an IPsec connection to FortiSASE:

- Connecting and logging into the FortiGate
- IPsec configuration using IPsec wizard and CLI
- BGP per overlay configuration
- Verifying and troubleshooting the IPsec connection
- Verifying and troubleshooting BGP and static routing

Connect and logging into the FortiGate

For details on connecting and logging into the FortiGate GUI, see Connecting using a web browser.

For details on connecting and logging into the FortiGate CLI, see Connecting to the CLI.

IPsec configuration using IPsec wizard and CLI

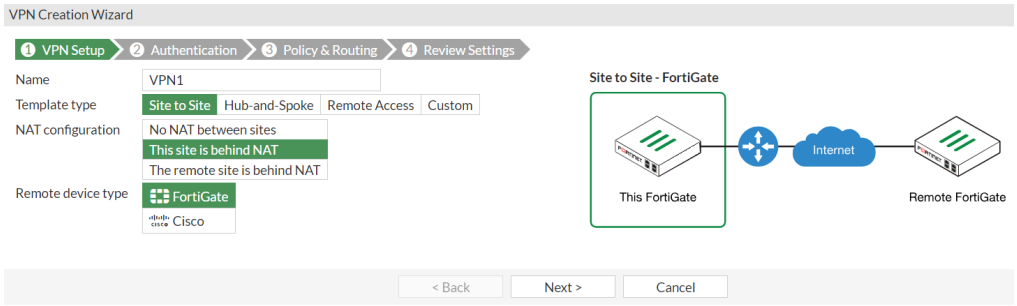
The FortiGate as an IPsec device for Branch On-ramp requires the following IPsec settings:

- IKEv2
- Branch device configured as an IPsec dialup client. Your branch device connects to the FortiSASE Branch On-ramp security PoP, which acts as a remote site.
- You must enable the mode config setting. Each FortiSASE Branch On-ramp security PoP assigns IP addresses, and the branch device automatically configures its tunnel interfaces IP address with the acquired IP address. You also use this IP address to set up BGP peering.
- On branches, remote gateway(s) where one overlay tunnel should be established per underlay even though multiple WAN underlays exist
  Use network overlay IDs for each overlay tunnel configuring set network-overlay enable and set network-id <n>
- Pre-shared key for each overlay tunnel
- Phase 1 and 2 proposals and settings:
  - For IPsec phase 1:
    - Proposals: Only aes256-sha256 is supported.
    - DH groups: 5, 14
  - For IPsec phase 2:
    - Proposals: Only aes256-sha256 is supported.
    - DH groups: 5, 14

The following settings are only examples. Do not consider them as recommended settings.

To configure an IPsec using the GUI and IPsec wizard:

1. On the FortiGate, go to *VPN > IPsec Wizard*. The *VPN Creation Wizard* displays.
2. Configure the following *VPN Setup* options:
   a. In the *Name* field, enter VPN1.
   b. For *Template type*, select *Site to Site*.
   c. For *NAT configuration*, select the option that corresponds to your network topology.
   d. For *Remote device type*, select *FortiGate*.
   e. Click *Next*.



3. Configure the following *Authentication* options:
   a. For *Remote device*, select *Dynamic DNS*.
   b. For *FQDN*, paste the *FQDN* from the *Security PoP* tab in *Operations > Connectivity > On-ramp tunnel* page. Notice that the FortiGate displays *Resolved to < IP address >*. Make note of this IP address since it will be used later.
   c. From the *Outgoing Interface* dropdown list, select the WAN interface that the hub will listen on for VPN peer connections. For example, you could select *wan1*.
   d. For *Authentication method*, select *Pre-shared Key*.
   e. In the *Pre-shared key* field, enter the desired key in alphanumeric characters. Click *Next*.
4. Configure the following *Tunnel Interface* options:
   a. In the *Tunnel IP* field, enter 10.251.1.1.
   b. In the *Remote IP/netmask* field, enter 10.251.1.30/27. Click *Next*.
   The tunnel interface IP address is assigned by mode configuration. However, this step simply configures placeholder values to allow the IPsec wizard to proceed.
5. Configure the following *Policy & Routing* options:
   a. Set *Local interface* to the desired LAN interface(s).
   b. Observe that the *Local subnets* are automatically detected based on the LAN interface(s) selected.
   c. For *Remote Subnets* since there are no specific destinations, enter 0.0.0.0/0
   d. For *Internet access*, select *None*. Click *Next*.
6. Configure the following settings using the CLI. The IPsec wizard does not configure these settings. Replace VPN1 with your actual IPsec phase 1 name:
   a. Enable IKEv2
   b. Enable network overlays
   c. Set the VPN gateway network ID to a unique ID. For example, you can use a network ID of 11.
   d. Enable mode config in Phase 1 and configure DH groups 5, 14 for Phase 1 and Phase 2.

```
config vpn ipsec phase2-interface
   delete VPN1
end
config vpn ipsec phase1-interface
   edit VPN1
      set ike-version 2
      set network-overlay enable
      set network-id 11
      set mode-cfg enable
      set proposal aes256-sha256
      set dhgrp 14 5
   next
end
config vpn ipsec phase2-interface
   edit "VPN1"
      set phase1name "VPN1"
      set proposal aes256-sha256
      set dhgrp 14 5
   next
end
```

7. Remove the statically assigned tunnel interface IP addresses configured from the IPsec wizard using these CLI commands:

```
config system interface
    edit VPN1
       unset ip
       unset remote-ip
    next
end
```

BGP, SD-WAN, and routing configuration

Once the IPsec tunnel establishes, you must configure routing settings on the branch FortiGate to ensure the following operation:

1. Ensuring FortiSASE can access branch local subnets for secure internet access (SIA) reply traffic
2. Outgoing routing to FortiSASE for SIA
3. Outgoing routing to WAN connection for direct internet access, if applicable

You can use iBGP (BGP per overlay) or static routing with source NAT to achieve the first objective. You can use static routing alone or static routing with SD-WAN for traffic steering to achieve the second and third objectives.

The example demonstrates the following configuration:

- iBGP (BGP per overlay) for the first objective.
- Static routing with SD-WAN for traffic steering for the second and third objectives

This topic covers the following:

- BGP configuration considerations on page 211
- Static routing and SD-WAN configuration considerations on page 211
- BGP per overlay configuration on page 212

- Static routing with SD-WAN configuration on page 212

BGP configuration considerations

The branch FortiGate connects to the FortiSASE Branch On-ramp security PoP and establishes an iBGP peering with it. Using iBGP, the FortiSASE Branch On-ramp security PoP can learn routes to your network.

The branch FortiGate requires the following BGP settings:

- AS number
- Router ID
- Using iBGP for dynamic routing via overlays (BGP per overlay routing design)
- BGP neighbor IP address for Branch On-ramp security PoP
- One BGP session per overlay between the branch and the Branch On-ramp security PoP

This section describes BGP settings that you must configure since the IPsec wizard creates does not include them.

Branch On-ramp supports routing design using BGP per overlay to learn routes to your local networks behind the branch FortiGate. With this routing design, the On-Ramp security PoP can see the source IP address of the client connected behind the IPsec device.

To use static routing on the branch FortiGate for your routing design, you must configure source NAT on the branch FortiGate firewall policy destined for the On-Ramp security PoP for reply traffic from the On-Ramp security PoP to be routed back to the branch FortiGate. With this routing design, the On-Ramp security PoP only sees the tunnel interface IP address of the FortiGate IPsec device and not the source IP address of the client connected behind the IPsec device.

Static routing and SD-WAN configuration considerations

The administrative distance of the static route using the IPsec tunnel interface varies depending on how IPsec was configured on the branch FortiGate:

- When using the IPsec wizard on the branch FortiGate, a static route to the peer local subnet, 0.0.0.0/0 in the example configuration, using the IPsec tunnel interface is created with a default administrative distance of 10.
- If you configure IPsec on the branch FortiGate as a custom tunnel, then with *set add-route enable* by default, FortiGate dynamic IPsec route control will add a static route to peer destination selector with a default administrative distance of 15. If the peer destination selector is set to 0.0.0.0/0 then the default static route has an administrative distance of 15.

For routing configuration on the branch FortiGate, you have the following options for routing traffic through the IPsec tunnel acting as a full tunnel to the Branch On-ramp security PoP:

1. Configure the existing default route using the WAN interface to have the same administrative distance as the default route using the IPsec tunnel interface. Then configure SD-WAN for traffic steering.
2. Configure the existing default route using the WAN interface to have a greater distance (making this the less preferred route) than the static route using the IPsec tunnel interface and just leverage this latter route.

When configuring the static default route for full tunneling, the FortiGate routing table includes connected routes for locally connected subnets. A local DNS server that is directly connected to one of these subnets is accessible without further configuration.

However, if your branch device uses a local DNS server that is on a subnet different than a local interface, then you must configure a new static route for that DNS server to ensure that DNS traffic does not mistakenly route to FortiSASE instead.

This topic gives an example of static routing with SD-WAN for traffic steering.

BGP per overlay configuration

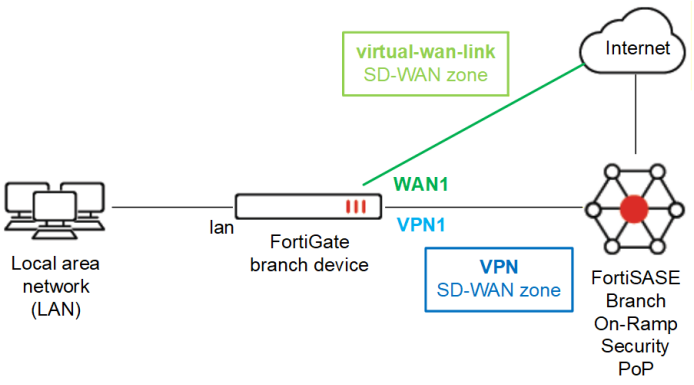
To configure BGP per overlay using the GUI:

1. On the FortiGate, go to *Network* > *BGP*. If you cannot view *Network* > *BGP*, go to *System* > *Feature Visibility* and enable *Advanced Routing* in the *Core Features* column.
2. Confirm that the *Local AS* field is set to 65001.
3. In the *Router ID* field, enter 192.168.1.99, which corresponds to the highest interface IP address on the FortiGate; in this case, the LAN IP of the port2 interface.
4. Under *Neighbors*, click *+ Create New*.
   a. For *IP*, enter *Tunnel interface IP* from the *Edge Devices* > *SD-WAN On-Ramp* > *On-Ramp locations* page.
   b. For *Remote AS*, enter 65001.
   c. In the options, enable *Soft reconfiguration* and *Capability: route refresh*.
   d. Click *OK*.
5. Under *Networks*, add the LAN subnets in the *IP/Netmask* field. Click *+* to add more subnets, if necessary.
6. Click *Apply*.

Static routing with SD-WAN configuration

The following network topology and configuration provide a basic SD-WAN example applied to branch FortiGate use cases for direct internet access and SIA with FortiSASE. For details and other use cases, see SD-WAN quick start, SD-WAN members and zones, Performance SLA, and SD-WAN rules.

The following network topology is used for the static routing and SD-WAN configuration:



For this topology, we have a single underlay interface *WAN1* and single overlay interface *VPN1*, and corresponding *virtual-wan-link* and *VPN* SD-WAN zones, respectively. The *virtual-wan-link* SD-WAN zone is used for direct Internet access for critical, latency-sensitive traffic that bypasses FortiSASE and the VPN SD-WAN zone is used for secure Internet access through FortiSASE. In example, traffic to example.com is considered critical and latency sensitive.

To configure static routing in preparation for SD-WAN:

1. On the FortiGate, go to *Network* > *Static Routes*.
2. Click to select the route with the *Destination* of *0.0.0.0/0* and *Interface* set to the WAN interface.
3. Click *Edit in CLI*.
   a. If the IPsec wizard was previously used, enter these CLI commands to configure distance equal to the static route created by the wizard (note that this step can be skipped if a default static route was manually created for the WAN interface previously since static routes default to a distance of 10):

   ```
   set distance 10
   show
   end
   ```

   b. If the IPsec Custom tunnel option was used, enter these CLI commands to configure distance equal to the static route added by dynamic IP route control:

   ```
   set distance 15
   show
   end
   ```

4. Go to *Dashboard* > *Network* and in the *Routing* widget click *Expand* to full screen. By default, the *Static & Dynamic* view should be selected from the dropdown at the top-right.
5. Confirm that both the route for the WAN interface and the route for the IPsec tunnel interface as visible as two separate entries in the routing table:

   Route for WAN interface:

Field	Value
Network	0.0.0.0/0
Gateway IP	<Default gateway corresponding to WAN interface>
Interfaces	<Name of WAN interface>
Distance	10 if IPsec wizard previously used 15 if IPsec Custom tunnel previously used
Type	Static

   Route for IPsec tunnel interface:

Field	Value
Network	0.0.0.0/0
Gateway IP	<Blank>
Interfaces	<Name of IPsec tunnel interface>
Distance	10 if IPsec wizard previously used 15 if IPsec Custom tunnel previously used
Type	Static

To configure SD-WAN for traffic steering:

1. On the FortiGate, go to *Policy & Objects > Firewall Policy*.
2. Select any firewall policies where the WAN or IPsec tunnel interfaces are either configured as source or destination interfaces by holding CTRL and clicking on policies. Click on Delete to delete them. This is required to select these interfaces as SD-WAN members.
3. Create a new VPN zone and assign member interfaces to SD-WAN zones.
   a. Go to *Network > SD-WAN* and select the *SD-WAN Zones* tab.
   b. Select *virtual-wan-link* and click *Edit*.
      i. Set the *Interface members* to *wan1*.
      ii. Click *OK*.
   c. Click *Create New > SD-WAN Zone*.
      i. Enter the *Name* as *VPN*.
      ii. Set the *Interface members* to *VPN1*.
      iii. Click *OK*.
4. Create a new performance SLA to detect latency.
   a. Go to *Network > SD-WAN* and select the *Performance SLAs* tab.
   b. Click *Create New*.
   c. In the *New Performance SLA* page, enter these values (leave unspecified values to default values):

Field	Value
Name	Internet
Probe mode	Active
Protocol	Ping
Server	8.8.8.8
Participants	1. Click *Specify*. 2. Select *VPN1*, then *wan1*, and click *Close*.
SLA Target	Enabled
Latency threshold	Enabled Set to 170 ms.
Jitter threshold	Disabled
Packet loss threshold	Disabled
Actions when Inactive > Update static route	Disabled

   d. Click *OK*.
5. Create an SD-WAN rule for critical direct Internet access traffic only. In this example, any traffic to example.com will bypass FortiSASE and will use the branch FortiGate WAN interface directly.
   a. Go to *Network > SD-WAN* and select the *SD-WAN Rules* tab.
   b. Click *Create new*.
   c. In the *Priority Rule* page, enter the following values. Leave unspecified values to default values.

Field	Value
Name	Critical-DIA
Status	Enabled
Source	
Address	all
Destination	
Address	1. Click on *+*. 2. Click *+Create*. 3. Click *+Firewall Address*. 4. Create a *New Address*. 5. Set the *Name* as *example.com*. 6. Set the *Type* as *FQDN*. 7. Set *FQDN* as *example.com*. 8. Set the *Interface* as *any*. 9. Set the *Static route configuration* as *Disabled*. 10. Click *OK*. 11. The newly created FQDN should be selected. Click *Close*.
Protocol number	ANY
Interface selection strategy	Lowest cost (SLA)
Interface preference	1. Select *wan1* and then *VPN1*. 2. Click *Close*.
Required SLA target	Internet#1

d. Click *OK*.

6. Create an SD-WAN rule low priority secure Internet access traffic only.

a. Go to *Network > SD-WAN* and select the *SD-WAN Rules* tab.

b. Click *Create new*.

c. In the *Priority Rule* page, enter the following values. Leave unspecified values to default values.

Field	Value
Name	Low-Priority-SIA
Status	Enabled
Source	
Address	all
Destination	
Address	all

Field	Value
Protocol number	ANY
Interface selection strategy	Lowest cost (SLA)
Interface preference	1. Select *VPN1* and then *wan1*. 2. Click *Close*.
Required SLA target	Internet#1

d. Click *OK*.

7. Create a firewall policy to allow direct Internet access traffic:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create new*.
   c. In the *New Policy* page, enter the following values. Leave unspecified values to default values.

Field	Value
Name	Direct Internet Access
Incoming Interface	lan
Outgoing Interface	virtual-wan-link
Source	all
Destination	all
Service	ALL
NAT	Enabled
IP Pool Configuration	Use Outgoing Interface Address
Log Allowed Traffic	Enabled Select *All Sessions*.

   d. Click *OK*.

8. Create a firewall policy to allow secure Internet access traffic:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create new*.
   c. In the *New Policy* page, enter the following values. Leave unspecified values to default values.

Field	Value
Name	Secure Internet Access
Incoming Interface	lan
Outgoing Interface	VPN
Source	all
Destination	all

Field	Value
Service	ALL
NAT	Disabled
Log Allowed Traffic	Enabled Select *All Sessions*.

d. Click *OK*.

IPsec, BGP, SD-WAN, and routing configuration through CLI-only configuration

This topic covers the CLI-only configuration for the example configuration described in these sections:

- IPsec configuration using IPsec wizard and CLI on page 208
- BGP, SD-WAN, and routing configuration on page 210

The steps provided in this topic are recommended for administrators who are familiar and comfortable with the FortiGate CLI.

Add IPsec Phase 1 and Phase 2 configuration settings:

```
config vpn ipsec phase1-interface
    edit "VPN1"
        set type ddns
        set interface "<WAN interface>"
        set ike-version 2
        set peertype any
        set net-device enable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set dhgrp 14 5
        set idle-timeout enable
        set network-overlay enable
        set network-id 11
        set remotegw-ddns <FQDN for on-ramp location>
        set psksecret mysecretkey
    next
end
config vpn ipsec phase2-interface
    edit "VPN1"
        set phase1name "VPN1"
        set proposal aes256-sha256
        set dhgrp 14 5
        set auto-negotiate enable
    next
end
```

Create firewall policies required for branch device to initiate an IPsec connection (temporary only for testing IPsec connection and BGP peering relationship):

```
config firewall policy
    edit 0
        set name "toVPN1"
        set srcintf "<LAN interface>"
        set dstintf "VPN1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 0
        set name "fromVPN1"
        set srcintf "VPN1"
        set dstintf "<LAN interface>"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 0
        set name "InternetAccess"
        set srcintf "<LAN interface>"
        set dstintf "<WAN interface>"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end
```

After entering this configuration, you should validate that the IPsec connection on the FortiGate is established with the on-ramp security PoP. See Verifying and troubleshooting IPsec connection on page 222.

Add BGP configuration:

```
config router bgp
    set as 65001
    set router-id 192.168.1.99
    config neighbor
        edit "10.251.1.30"
            set advertisement-interval 1
            set capability-graceful-restart enable
```

```
            set link-down-failover enable
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
    config redistribute "connected"
    end
    config redistribute "rip"
    end
    config redistribute "ospf"
    end
    config redistribute "static"
    end
    config redistribute "isis"
    end
    config redistribute6 "connected"
    end
    config redistribute6 "rip"
    end
    config redistribute6 "ospf"
    end
    config redistribute6 "static"
    end
    config redistribute6 "isis"
    end
end
```

Static routing configuration:

```
config router static
    edit 1
        set gateway 172.19.50.1
        set device "<WAN interface>"
    next
    edit 2
        set device "VPN1"
    next
end
```

After entering this configuration, you should validate that the BGP peering relationship on the FortiGate is established with the on-ramp security PoP. See Verifying and troubleshooting BGP and static routing with SD-WAN on page 224.

Delete firewall policies used for testing IPsec connection and BGP peering relationship:

```
config firewall policy
delete 1
delete 2
delete 3
```

SD-WAN zones, performance SLA, and SD-WAN rules configuration:

```
config firewall address
    edit "example.com"
        set type fqdn
        set fqdn "example.com"
        set allow-routing disable
    next
end
config system sdwan
    set status enable
    config zone
        edit "VPN"
        next
    end
    config members
        edit 1
            set interface "< WAN interface >"
                   set zone "virtual-wan-link"
        next
        edit 2
            set interface "VPN1"
                    set zone "VPN"
        next
       end
    config health-check
        edit "Internet"
            set server 8.8.8.8
            set protocol ping
            set detect-mode active
            set update-static-route disable
            config sla
                edit 1
                    set latency-threshold 170
                next
            end
        next
    end
    config service
        edit 1
            set name "Critical-DIA"
            set status enable
            set src "all"
            set dst "example.com"
            set protocol 0
```

```
            set mode sla
            config sla
                edit "Internet"
                    set id 1
                next
            end
            set priority-member 1 2
        next
        edit 2
            set name "Low-Priority-SIA"
            set status enable
            set src "all"
            set dst "all"
            set protocol 0
            set mode sla
            config sla
                edit "Internet"
                    set id 1
                next
            end
            set priority-member 1 2
        next
    end
end
```

Create firewall policies for direct Internet access and secure Internet access traffic, respectively:

```
config firewall policy
    edit 0
        set name "Direct Internet Access"
        set srcintf "port2"
        set dstintf "virtual-wan-link"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set action accept
        set nat enable
        set logtraffic all
        set schedule always
    next
    edit 0
        set name "Secure Internet Access"
        set srcintf "port2"
        set dstintf "VPN"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set action accept
        set nat disable
        set logtraffic all
        set schedule always
```

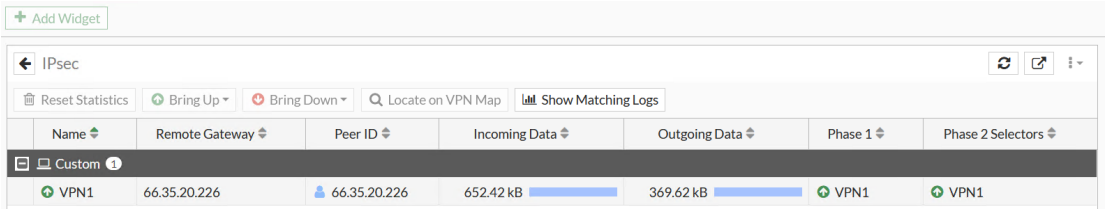
```
    next
end
```

After entering this configuration, you should validate SD-WAN on a branch FortiGate using a client computer works. See Verifying and troubleshooting BGP and static routing with SD-WAN on page 224.

Verifying and troubleshooting IPsec connection

To verify the IPsec tunnel on a branch FortiGate:

1. Go to *Dashboard* > *Network* and click the *IPsec* widget to expand it.
2. Verify the IPsec tunnel that is established with the Branch On-ramp security PoP.



To verify Internet traffic is forwarded to FortiSASE:

1. In the FortiGate CLI, check the Public/WAN IP address:

```
Branch1 # diag sys waninfo ipify
Try to get my public IP through https://api.ipify.org with src_ip=0.0.0.0 device=unspecified
vfid=0(root) ...

Public/WAN IP: 66.35.20.126
...
```

2. In FortiSASE, go to *Operations* > *Connectivity* > *On-ramp tunnel* > *Security PoP* and copy the FQDN for the On-Ramp security PoP.
3. Confirm that the Public/WAN IP address corresponds to the FortiSASE Branch On-ramp security PoP by pinging the FQDN used for the On-Ramp security PoP on the FortiGate:

```
Branch1 # exec ping ipsec-be68qi9e-sjc-f1.stage.fortisase.com
PING ipsec-be68qi9e-sjc-f1.stage.fortisase.com (66.35.20.226): 56 data bytes
64 bytes from 66.35.20.126: icmp_seq=0 ttl=243 time=23.2 ms
64 bytes from 66.35.20.126: icmp_seq=1 ttl=243 time=22.6 ms
64 bytes from 66.35.20.126: icmp_seq=2 ttl=243 time=22.6 ms
64 bytes from 66.35.20.126: icmp_seq=3 ttl=243 time=22.6 ms
64 bytes from 66.35.20.126: icmp_seq=4 ttl=243 time=22.5 ms

--- ipsec-be68qi9e-sjc-f1.stage.fortisase.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 22.5/22.7/23.2 ms
```

To troubleshoot the IPsec tunnel on a branch FortiGate:

If after configuring the FortiGate, the IPsec tunnel is not established, then perform the following troubleshooting steps.

1. On the branch FortiGate, run this CLI command to ensure the Branch On-ramp security PoP FQDN is responding to pings:
   `exec ping <FQDN>`
   If these pings time out, then ensure that the On-Ramp security PoP in *Operations > Connectivity > On-ramp tunnel > On-ramp security PoPs* has a *Status* of *Running*.
   If the *Status* says *Running* and you just finished deploying the On-Ramp security PoP, then you may need to wait a few minutes before the FQDN responds to pings.
2. On the branch FortiGate, run these CLI commands to capture IKE debug messages:

   ```
   diag debug console timestamp enable
   diag debug application ike -1
   diag debug enable
   ```

   Wait for a few messages to be displayed then disable them by running this command:

   ```
   diag debug disable
   ```

   If you see these error messages:

   ```
   ike 0:VPN1:765: negotiation timeout, deleting
   ike 0:VPN1: connection expiring due to phase1 down
   ike 0:VPN1: deleting
   ```

   Verify the IPsec Phase 1 configuration settings are correct on the branch FortiGate from the GUI:
   a. Go to *VPN > IPsec Tunnels*.
   b. Select the tunnel and click *Edit*.
   c. Click *Convert To Custom Tunnel*.
   d. Verify the following settings match with the deployed Branch On-ramp security PoP:
      i. In *Network*, ensure the *Dynamic DNS* field has the correct FQDN from the *Operations > Connectivity > On-ramp tunnel > On-ramp security PoPs* page.
      ii. In *IKE*, ensure *Version* is set to *2*.
      iii. In *Authentication*, ensure the *Pre-shared Key* has the correct value. Since you cannot view the *Pre-shared Key* value in plaintext, you may need to re-enter this value.
   e. In the CLI, run this command:

      ```
      show vpn ipsec phase1-interface
      ```

      Ensure these CLI commands are configured:

      ```
      set network-overlay enable
      set network-id 11
      ```

Verifying and troubleshooting BGP and static routing with SD-WAN

To verify BGP routing on a branch FortiGate:

1. In the CLI, check the BGP peering status:

```
Branch1 # get router info bgp summary

VRF 0 BGP router identifier 192.168.1.99, local AS number 65001
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.251.1.30 4      65001     731     758        1    0    0 00:35:00        0

Total number of neighbors 1
```

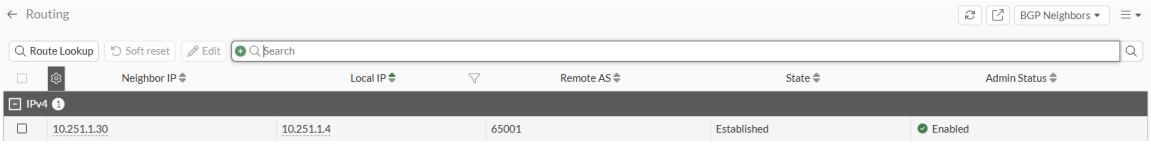
2. Check the BGP advertised routes:

```
Branch1 # get router info bgp neighbor 10.251.1.30 advertised-routes
VRF 0 BGP table version is 1, local router ID is 192.168.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i192.168.1.0      10.251.1.4                        100  32768        0 i <-/->

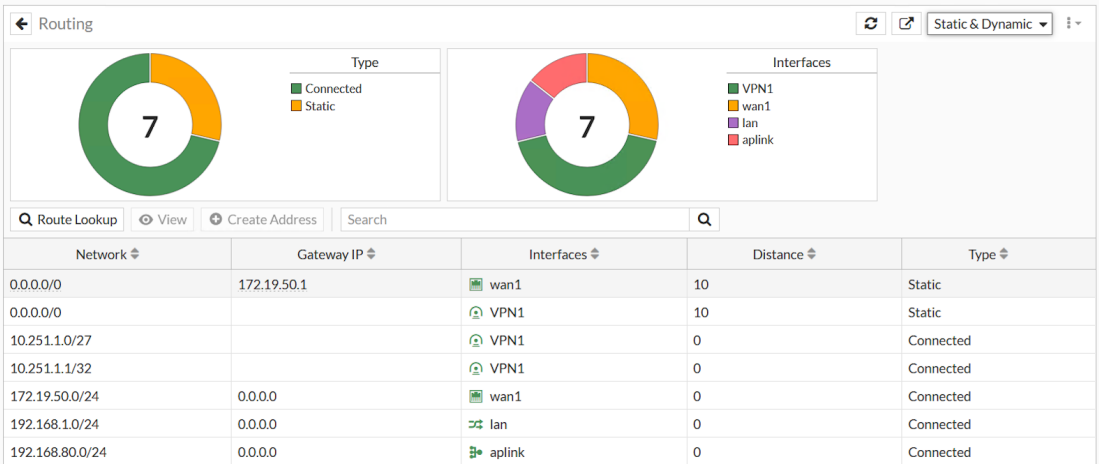
Total number of prefixes 1
```

3. In the GUI, go to *Dashboard* > *Network* and click the *Routing* widget to expand it.
4. In the dropdown, select *BGP Neighbors*.



To verify static routing with SD-WAN on a branch FortiGate:

1. In the GUI, go to *Dashboard* > *Network* and click the *Routing* widget to expand it.
2. In the dropdown, select *Static & Dynamic*.
3. Observe that default static routes to wan1 and VPN1 interfaces have the same distance and both exist in the routing table.



To verify SD-WAN on a branch FortiGate using a client computer:

1. On a client computer, enter the following in a Windows Command Prompt:

```
C:\> ping example.com

Pinging example.com [93.184.215.14] with 32 bytes of data:
Reply from 93.184.215.14: bytes=32 time=4ms TTL=55
Reply from 93.184.215.14: bytes=32 time=4ms TTL=55
Reply from 93.184.215.14: bytes=32 time=20ms TTL=55
Reply from 93.184.215.14: bytes=32 time=4ms TTL=55

Ping statistics for 93.184.215.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 20ms, Average = 8ms
```

2. On the branch FortiGate, go to *Log & Report > Forward Traffic* and confirm the ping traffic for example.com goes through the *Direct Internet Access* policy.
3. On a client computer, enter the following in a Windows Command Prompt:

```
C:\> ping google.com

Pinging google.com [142.250.191.46] with 32 bytes of data:
Reply from 142.250.191.46: bytes=32 time=25ms TTL=113
Reply from 142.250.191.46: bytes=32 time=24ms TTL=113
Reply from 142.250.191.46: bytes=32 time=24ms TTL=113
Reply from 142.250.191.46: bytes=32 time=24ms TTL=113

Ping statistics for 142.250.191.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 25ms, Average = 24ms
```

4. On the branch FortiGate, go to *Log & Report > Forward Traffic* and confirm the ping traffic for google.com goes through the *Secure Internet Access* policy.

To troubleshoot BGP routing on a branch FortiGate:

If after configuring the FortiGate, the BGP peering is not established, perform the following troubleshooting steps.

1. In the CLI, check the BGP peering status:

   ```
   get router info bgp summary
   ```

   If the command returns empty, then confirm these BGP settings from *Network* > *BGP* as correctly configured:
   a. *Local AS*
   b. *Router ID*
   c. *Neighbor*
      i. *IP*
      ii. *Remote AS*
2. Check the BGP advertised routes:

   ```
   get router info bgp neighbor <neighbor IP address> advertised-routes
   ```

   If the command returns empty, then confirm from *Network* > *BGP* that the branch FortiGate LAN subnet is configured in *Networks* with the correct *IP/Netmask*.

To troubleshoot static routing with SD-WAN on a branch FortiGate:

If after configuring the FortiGate, full tunnel operation does not occur because of an issue with static routing, perform the following troubleshooting steps. Check the static routes on the branch FortiGate:

1. In the GUI, go to *Dashboard* > *Network* and click the *Routing* widget to expand it.
2. In the dropdown, select *Static & Dynamic*.
3. Confirm that the following routes display:
   - Default static route through the VPN tunnel:
     - *Network*: 0.0.0.0
     - *Interface*: <Tunnel interface>
   - Default static route through WAN interface:
     - *Network*: 0.0.0.0
     - *Interface*: < WAN interface >
4. If these routes are not displayed, then carefully review the steps in To configure static routing in preparation for SD-WAN: on page 213.
5. If these routes are displayed, then carefully review the steps in To configure SD-WAN for traffic steering: on page 214.

Configuring a third-party IPsec connection to FortiSASE



Ensure that you are aware of the Branch On-Ramp Prerequisites and considerations on page 197.

After deploying a Branch On-ramp security PoP in FortiSASE and configuring an IPsec tunnel for the custom device type, you can configure the third-party IPsec device as an IPsec branch device to establish an IPsec connection to FortiSASE.

This section provides generic steps for configuring a third-party IPsec device:

- Configuring IPsec on the third-party IPsec device on page 227
- Configuring static routing on the third-party IPsec device on page 229
- Verifying and troubleshooting the IPsec connection and static routing on page 230

Configuring IPsec on the third-party IPsec device

The third-party IPsec device for Branch On-ramp requires the following IPsec settings:

- IKEv2
- Branch device configured as an IPsec dialup client. Your branch device connects to the FortiSASE Branch On-ramp security PoP, which acts as a remote site.
- (Optional) If supported by the Branch device, you can enable the `mode config` setting on the FortiSASE side and the Branch device side.
  - If enabled, each FortiSASE Branch On-ramp security PoP assigns IP addresses, and the branch device automatically configures its tunnel interfaces IP address with the acquired IP address.
  - If the Branch device does not support this feature, ensure the *Network > Mode config* setting is set to *Disabled* when configuring an IPsec connection for a custom device type.
- On branches, remote gateways should establish one overlay tunnel per underlay even though multiple WAN underlays exist
- Pre-shared key for each overlay tunnel
- Phase 1 and 2 proposals and settings
  - For IPsec phase 1, only aes256-sha256 is supported.
  - For IPsec phase 2, only aes256-sha256 is supported.
- FQDN of the Branch On-ramp Security PoP from the *Security PoP* tab in *Operations > Connectivity > On-ramp tunnel*.
  - You will need to ping this FQDN from another device to determine the corresponding remote peer IP address used in the third-party device IPsec configuration.

The following settings are only examples. Do not consider them as recommended settings.

For this example, a Cisco Catalyst 8000v is used as the third-party IPsec device and is configured using CLI commands. In this case, the device supports the IKEv2 `mode config` setting.

To configure IPsec on a Cisco Catalyst 8000v device as a third-party IPsec device for Branch On-Ramp:

1. Configure settings for the IKEv2 remote peer accepts connections from any client peer IP address:

```
crypto ikev2 keyring hub-keyring
    peer hub-fss
        address 0.0.0.0 0.0.0.0
```

```
        pre-shared-key local mysecretkey
        pre-shared-key remote mysecretkey
```

2. Configure the IKEv2 Phase 1 settings:

```
crypto ikev2 profile fss-profile
    match identity remote key-id CorpDevice001
    identity local key-id 8000v-99
    authentication remote pre-share
    authentication local pre-share
    keyring local hub-keyring
!
crypto ikev2 proposal fss-proposal
    encryption aes-cbc-256
    integrity sha256
    group 19 14
!
crypto ikev2 policy fss-policy
    proposal fss-proposal
```

3. Configure the IKEv2 Phase 2 settings:

```
crypto ipsec transform-set hub-transform-set esp-aes 256 esp-sha256-hmac
    mode tunnel
!
crypto ipsec profile hub-ipsec-profile
    set transform-set hub-transform-set
    set ikev2-profile fss-profile
```

4. Configure the tunnel interface to negotiate an IP address via IKEv2 mode configuration:

```
interface Tunnel10
    ip address negotiated
    tunnel source GigabitEthernet1
    tunnel mode ipsec ipv4
    tunnel destination 203.0.113.1
    tunnel protection ipsec profile hub-ipsec-profile
```

Replace 203.0.113.1 with the IP address that resolves from a ping of the FQDN of the Branch On-ramp Security PoP from the *Security PoP* tab in *Operations > Connectivity > On-ramp tunnel*. See Deploying a Branch On-ramp security PoP on page 204.

5. Configure a loopback interface as a ping source with an unused/reserved IP address within the IP assignment range configured in FortiSASE to simulate a host within the IPsec device local subnet:

```
interface Loopback0
    ip address 192.168.30.100 255.255.255.255
end
```

Configuring static routing on the third-party IPsec device

Once the IPsec tunnel is established, you must configure routing settings on the branch third-party IPsec device to ensure the following operation:

1. Ensuring FortiSASE can access branch local subnets for secure internet access (SIA) reply traffic.
   - Configuring the correct Phase 2 remote subnets in the FortiSASE custom device type IPsec configuration achieves this first objective.
2. Outgoing routing to FortiSASE for SIA.
   - Configuring a static route with the tunnel interface on the third-party IPsec device achieves this second objective.

The example demonstrates a Cisco Catalyst 8000v as the third-party IPsec device and is configured using static routing CLI commands.

To configure static routing on a Cisco Catalyst 8000v device as a third-party IPsec device for Branch On-Ramp:

1. On the branch device, ensure that you already have a static route to the Branch On-ramp Security PoP IP address via the WAN underlay interface.
   - This static route ensures that the IPsec tunnel can be established with the Branch On-ramp Security PoP.
   - Recall, this IP address is resolved from the FQDN of the Branch On-ramp Security PoP from the *Security PoP* tab in *Operations > Connectivity > On-ramp tunnel*. See Deploying a Branch On-ramp security PoP on page 204.

   For example, if the WAN underlay interface is GigabitEthernet1 and the Branch On-ramp Security PoP IP address is `203.0.113.1` with subnet mask `255.255.255.252` then you should have a static route configured as follows:

   ```
   ip route 203.0.113.1 255.255.255.252 GigabitEthernet1
   ```

   For devices where the WAN underlay interface uses DHCP, then a default static route is added automatically and this step can be omitted.
2. To steer branch device traffic to FortiSASE:
   - If the WAN underlay interface uses a static route configured, configure a default static route using the tunnel interface as a default gateway:

     ```
     ip route 0.0.0.0 0.0.0.0 Tunnel10
     ```

     This static route only takes effect when the IPsec tunnel is up, that is when the tunnel is established and steers all traffic to FortiSASE though the IPsec tunnel.
   - If the WAN underlay interface uses DHCP, there are multiple options for steering traffic to FortiSASE:
     - Configure specific destinations through static routes to use the tunnel interface. For example, for 1.1.1.1/32:

       ```
       ip route 1.1.1.1 255.255.255.255 Tunnel10
       ```

     - Configure an ACL and route map to steer only selected source traffic through the tunnel interface. For example, for steering all traffic to FortiSASE from sources in the 192.168.30.0/24 subnet:

i. Create an access control list for the desired subnet to steer to FortiSASE:

```
ip access-list extended FSS_STEER_ACL
    permit ip 192.168.30.0 0.0.0.255 any
```

ii. Create a route map that matches using the access control list just created and associate it with the tunnel interface:

```
route-map FSS_STEER_MAP permit 10
    match ip address FSS_STEER_ACL
    set ip next-hop 10.251.1.30
```

iii. Define a policy-based route using the route map and the WAN underlay interface:

```
interface GigabitEthernet1
    ip policy route-map FSS_STEER_MAP
```

- (For local ping test only) Define a policy-based route for locally generated traffic:

```
ip local policy route-map FSS_STEER_MAP
```

Verifying and troubleshooting the IPsec connection and static routing

Typically, each third-party branch device will have either GUI or CLI features to view the status of the IPsec connection. When Phase 1 and Phase2 of the IPsec connection succeed, then you should be able to view details about that connection using the device's features.

This topic demonstrates how to verify and troubleshoot the IPsec connection on a Cisco Catalyst 3000v device.

To verify the IPsec tunnel on a third-party branch device:

1. In the device CLI, verify the tunnel status using these commands:

```
show crypto ikev2 sa
show crypto ipsec sa
show interface Tunnel10
```

2. When the IPSec tunnel is successfully established, the show `crypto ikev2 sa` command should display `Status: READY`.

```
8000v-99#show crypto ikev2 sa
    IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         172.16.8.5/4500       203.0.113.1/4500     none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth
verify: PSK
      Life/Active Time: 86400/2276 sec
      CE id: 43214, Session-id: 60
      Local spi: ADEF545BD3B655C1       Remote spi: 2D4D0BB48DBD05DB
```

```
       IPv6 Crypto IKEv2  SA
```

If you see `Status: ACTIVE(ACTIVE)` and non-zero packet counters, the IPsec tunnel is up and passing traffic.

```
8000v-99#show crypto ipsec sa
interface: Tunnel10
    Crypto map tag: Tunnel10-head-0, local addr 172.16.8.5

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 203.0.113.1 port 4500
        PERMIT, flags={origin_is_acl,}
    #pkts encaps: 330, #pkts encrypt: 330, #pkts digest: 330
    #pkts decaps: 173, #pkts decrypt: 173, #pkts verify: 173
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

...

     inbound esp sas:
      spi: 0xF9199FAB(4179206059)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 2120, flow_id: CSR:120, sibling_flags FFFFFFFF80004048, crypto map: Tunnel10-
head-0, initiator : True
            sa timing: remaining key lifetime (k/sec): (4607825/859)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:
     inbound pcp sas:

     outbound esp sas:
      spi: 0xC9F416D5(3388217045)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 2119, flow_id: CSR:119, sibling_flags FFFFFFFF80004048, crypto map: Tunnel10-
head-0, initiator : True
            sa timing: remaining key lifetime (k/sec): (4607828/859)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:
```

3. Using `show interface Tunnel10`, confirm the following:

- To confirm the tunnel interface is operational check:
  - Tunnel10 is up
  - Line protocol is up
- To confirm that IKEv2 `mode config` works, check that the Internet address is within the IP assignment range (10.251.1.16-10.251.1.29).
- To confirm that IPsec is applied correctly, verify `Tunnel protection via IPsec` is shown.

```
8000v-99#show interfaces Tunnel10
Tunnel10 is up, line protocol is up
    Hardware is Tunnel
    Internet address is 10.251.1.16/19
    MTU 9922 bytes, BW 100 Kbit/sec, DLY 50000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation TUNNEL, loopback not set
    Keepalive not set
    Tunnel linestate evaluation up
    Tunnel source 172.16.8.5 (GigabitEthernet1), destination 203.0.113.1
    Tunnel Subblocks:
        src-track:
            Tunnel10 source tracking subblock associated with GigabitEthernet1
            Set of tunnels with source GigabitEthernet1, 1 member (includes iterat
                                                                            ors), on
interface <OK>
    Tunnel protocol/transport IPSEC/IP
    Tunnel TTL 255
    Tunnel transport MTU 1422 bytes
    Tunnel transmit bandwidth 8000 (kbps)
    Tunnel receive bandwidth 8000 (kbps)
    Tunnel protection via IPSec (profile "hub-ipsec-profile")
    Last input 00:18:48, output 00:18:49, output hang never
    Last clearing of "show interface" counters 2d23h
    Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/0 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
        350 packets input, 335008 bytes, 0 no buffer
        Received 0 broadcasts (0 IP multicasts)
        0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        625 packets output, 344140 bytes, 0 underruns
        Output 0 broadcasts (0 IP multicasts)
        0 output errors, 0 collisions, 0 interface resets
        0 unknown protocol drops
        0 output buffer failures, 0 output buffers swapped out
```

To verify Internet traffic is steered to FortiSASE:

For testing that traffic is steered to FortiSASE, use the destination 1.1.1.1.

1. Check the static routing table using `show ip route 1.1.1.1` that destination 1.1.1.1 uses the Tunnel0 interface:

```
8000v-99#show ip route 1.1.1.1
Routing entry for 0.0.0.0/0
    Known via "static", distance 1, metric 0 (connected)
    Routing Descriptor Blocks:
    * directly connected, via Tunnel10
        Route metric is 0, traffic share count is 1
```

2. Run a ping to 1.1.1.1 using the source loopback interface from within the CLI:

```
8000v-99# ping 1.1.1.1 source 192.168.30.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.100
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 61/69/100 ms
```

To troubleshoot the IPsec tunnel and static routing on a third-party branch device:

1. On the branch device, run this CLI command to ensure the Branch On-ramp security PoP FQDN is responding to pings:

```
ping <FQDN>
```

   If these pings time out, then ensure that the On-Ramp security PoP in *Operations > Connectivity > On-ramp tunnel > On-ramp security PoPs* has a *Status* of *Running*.

   If the *Status* says *Running* and you just finished deploying the On-Ramp security PoP, then you may need to wait a few minutes before the FQDN responds to pings.

2. Run show `crypto ikev2 sa` and observe the `Status`.
   a. If you observe `Status: IN-NEG`, the negotiation is still in progress or has failed; the tunnel is not yet active.
   b. If you observe `Status: DOWN` or zero packet count, further troubleshooting is needed.
3. Using `show running-config all` on the branch device:
   a. Verify the IPsec Phase 1 configuration settings are correct:

```
crypto ikev2 keyring <keyring_name>
crypto ikev2 profile <profile_name>
crypto ikev2 proposal <proposal_name>
crypto ikev2 policy <policy_name>
```

   b. Verify the IPsec Phase 2 configuration settings are correct:

```
crypto ipsec transform-set <transform-set-name> ...
crypto ipsec profile <profile_name>
```

   c. Verify the tunnel interface configuration settings are correct:

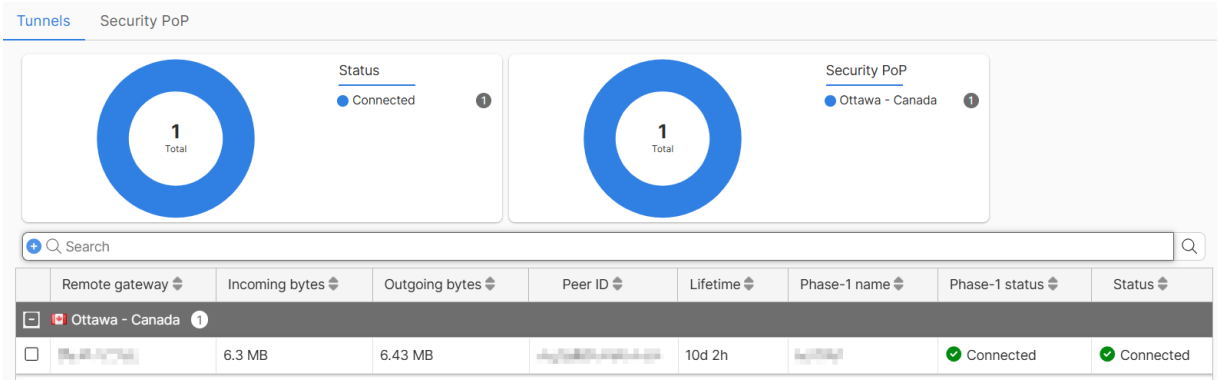
```
interface <tunnel_interface_name>
```

   d. Verify the static routes configured are correct:

```
ip route …
```

Viewing IPsec connections

In *Operations* > *Connectivity* > *On-ramp tunnel*, in the *Connections* tab, you can monitor the IPsec connections established between the IPsec devices and the deployed Branch On-ramp security PoPs.



Reports

You can generate data reports from logs by using the Reports feature. You can configure FortiSASE to regularly run reports at scheduled intervals, and manually run reports when desired.

Scheduling a report

To create an email group used for sending emails of scheduled reports:

1. Go to *Operations* > *Reports* > *Scheduled reports*.
2. Click *Manage email groups*.
3. Click *+Create*.
4. In the *New email group* slide-in, set the *Name*, *Subject*, *Body*, and *Description* accordingly. For *Recipients*, enter the email addresses that will receive the scheduled report that the email group will be configured with in the following steps.
5. Click *Close*.

To edit a report schedule:

1. Go to *Operations* > *Reports* > *Scheduled reports*.
2. Select the desired report. Click *Customize report* at the top and a slide-in window appears.
3. Set *Status* to *Enabled* to enable scheduling reports.
4. Set *Time period* to the desired time, indicating the timeframe from which FortiSASE uses logs to generate reports.

For instances provisioned after the FortiSASE 25.3.a release, you can configure a maximum time period of seven days.

For instances provisioned prior to the FortiSASE 25.3.a release, you can configure a longer time period.

5. In the *Schedule* section, set the *Interval*, *Start time* (your local time), and optionally *End time* (your local time) for the report. FortiSASE generates the first report at the configured *Start time*. After the first generation, FortiSASE generates the report eternally at regular periods based on the configured *Interval* unless you configure an *End time*.
6. In *Output*, for *Send report to*, select the email group to send this report to.
7. Click *OK*.
8. When FortiSASE completes generating the report, view it in *Operations* > *Reports* > *Generated reports*.

Manually running a report

To manually run a report:

1. Go to *Operations* > *Reports* > *Scheduled reports*.
2. Select the desired report.
3. Click *Run report* at the top.
4. When FortiSASE completes generating the report, view it in *Operations* > *Reports* > *Generated reports*.
5. You can download a report in PDF, HTML, XML, and CSV formats from *Operations* > *Reports* > *Generated reports*. Click the report and select the *Download* dropdown list to download it in the desired format.

Report types

Each report type has FortiSASE configuration dependencies that you must have configured in your FortiSASE instance to obtain valid data for the report.

You can view the configuration dependencies in *Operations* > *Reports* > *Scheduled reports* by following one of these steps:

- Scrolling to the right and viewing them in the *Dependencies* column
- Selecting the report, clicking *Customize report*, and viewing them in the *Dependencies* section under *Report*

For those reports with Application Control as a configuration dependency, Application Control With Inline-CASB features are not guaranteed to work when other security features are disabled. Enabling one of the following security features is recommended: Antivirus, File filter, DLP, Web filter, or DNS filter.

The following lists the report types that you can generate in FortiSASE:

Title	Description
Application	
Application Risk and Control	Risks that applications introduce on endpoints and efforts to control those risks. The report organizes applications into categories and includes information such as high-risk application, high-risk application by bandwidth, web categories, vulnerability exploits, virus, botnet, adware malicious attacks, zero day, and file transfers.
Bandwidth and Applications Report	Traffic, bandwidth, and sessions that users and applications use on endpoints. Also includes a summary of destinations that the user and applications accessed.
Cyber-Bullying Indicators Report	Users exhibiting behavior that aligns with common cyberbullying indicators, such as use of offensive phrases on social media.
High Bandwidth Application Usage Report	Applications with high bandwidth usage that may affect network performance. This report focuses on the following application types: • Peer-to-peer, such as BitTorrent, Xunlei, Gnutella, and Filetopia • File sharing and storage applications, such as Onebox, Google Drive, Dropbox, and Apple Cloud • Voice or video applications, such as YouTube, Skype, Spotify, Vimeo, and Netflix
Self-Harm and Risk Indicators Report	Users exhibiting behavior that aligns with common self-harm and risk indicators, such as use of risky terms on social media.
Shadow IT Report	Summarizes the usage of SaaS apps compared to all applications, sanctioned vs unsanctioned SaaS applications, and total bandwidth by SaaS Sanctioned and Unsanctioned apps. This report does not support the Top 10 inline CASB applications by occurrences section.
Security	
Cloud Security Usage Report	This report summarizes user connections and bandwidth by different regions. It includes the total number of users and number of users per PoP, the number of sessions, and total traffic. Average hourly underlay activity is reported by security PoP. Top authentication failures are listed by region and originating IP address.
Cyber Threat Assessment	Risk of applications on endpoints to cyber threats. Includes a review of application visibility and control, threat detection, threat prevention, and recommended actions.
Endpoint Vulnerability Report	This report summarizes vulnerabilities detected through FortiClient scans throughout the network.
Security Events and Incidents Summary	Security-related events or incidents that FortiSASE collected.

Title	Description
Threat Report	Malware and botnet attempts on endpoints. Includes detected malware and botnets. Also includes blocked intrusions, sources, and a timeline of the attempted intrusions as well as the blocked intrusion's severity rating.
VPN Report	Tunnel traffic on endpoints, including authenticated and failed user logins as well as top agents. Identifies remote tunnels and users as well as web mode by bandwidth and duration.
Web Usage Summary Report	Web usage on endpoints and a bandwidth summary. Includes top active users and bandwidth usage. Also identifies users who are blocked the most from websites.
System	
SPA Report	This report summarizes SD-WAN performance SLAs, health of each connected SPA hub, and the traffic through popular hubs.

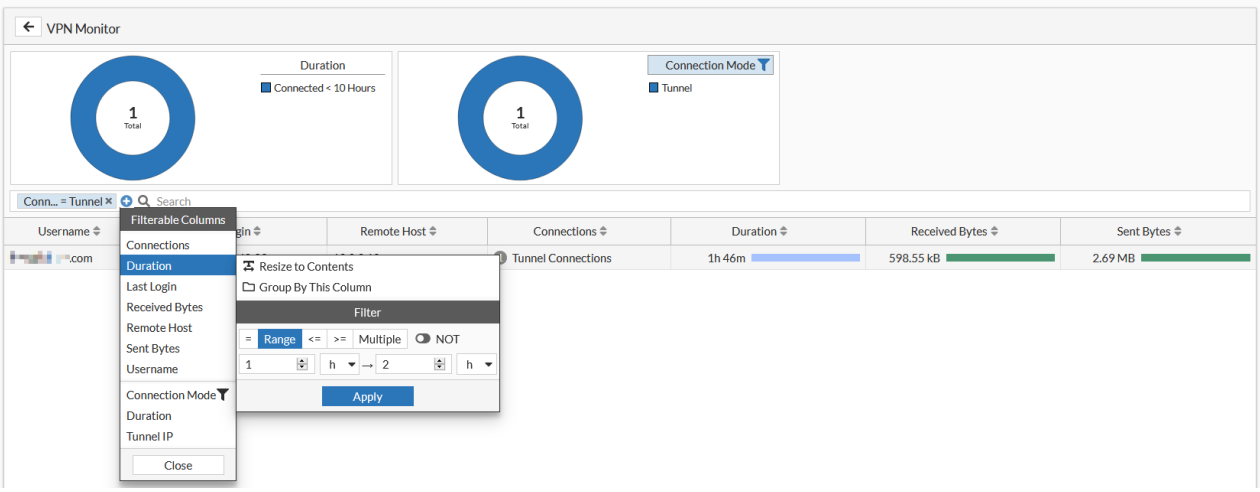
Logs

Logging and monitoring are useful components to help you understand what is happening on your network and to inform you about network activities, such as a virus detection, visit to an invalid website, intrusion, failed login attempt, and others.

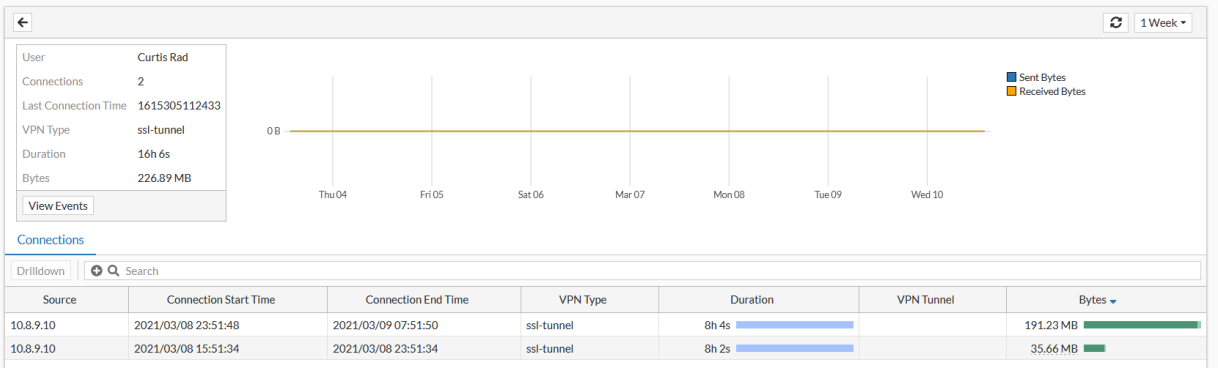
When downloading logs, the maximum number of logs for each log download attempt is 100000 log entries. When exporting logs, only currently visible entries are exported.

To find a connected user and drill down on logs:

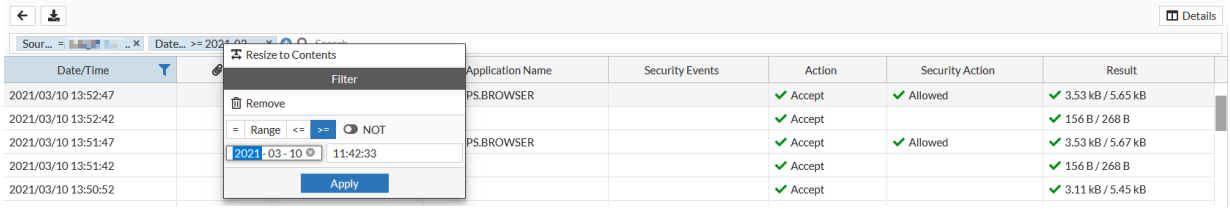
1. Go to *Monitoring* > *Dashboards* > *Status*. Expand the *User connection monitor* widget.
2. The User connection monitor displays currently connected agents. If desired, apply filters to the list of users displayed. For example, you can apply the *Duration* filter to only view users who have been connected for one to two hours:



3. Right-click the user that you want to drill down on. Select one of the following options:
   - *Show In FortiView*: goes to the *FortiView VPN* dashboard, which displays real-time tunnel connection information for the selected user. To view historical data for the user, select *1 Day* or *1 Week* from the dropdown list in the top right corner.



   - *Show Matching Traffic Logs*: displays real-time traffic logs for the selected user. To view historical data for the user, select the applied *Date* filter. Apply a new filter for the desired timerange.



Forwarding logs to an external server

You can configure FortiSASE to forward logs to external servers, such as FortiAnalyzer. FortiSASE supports forwarding logs to two, independent external servers.

FortiSASE supports forwarding the following logs to an external server, regardless of remote server type:

Log type	Log type description	Sub type	Subtype description
traffic	Records security PoP traffic flow information, such as an HTTP/HTTPS request and its response, if any.	*forward*	Forward traffic logs

Log type	Log type description	Sub type	Subtype description
event	Records security PoP system and administrative events.	*vpn*	Tunnel agent events
		user	User authentication events
		sase	FortiSASE administrator events
		endpoint	Endpoint management events: • Agent tunnel events • Scan events • Malware events (antiexploit, antiransomware, antivirus) • Sandbox detection events • Removable media events • FortiClient traffic events • FortiClient system events • FortiClient security events
utm	Records security PoP security profile events.	*virus*	AntiVirus event
		webfilter	Web Filter With Inline-CASB event
		ips	Intrusion Prevention event
		dlp	Data Loss Prevention event
		app-ctrl	Application Control With Inline-CASB event
		dns	DNS Filter event
		ssl	SSL inspection or certificate handling event
		file-filter	File Filter event

To forward logs to an external server:

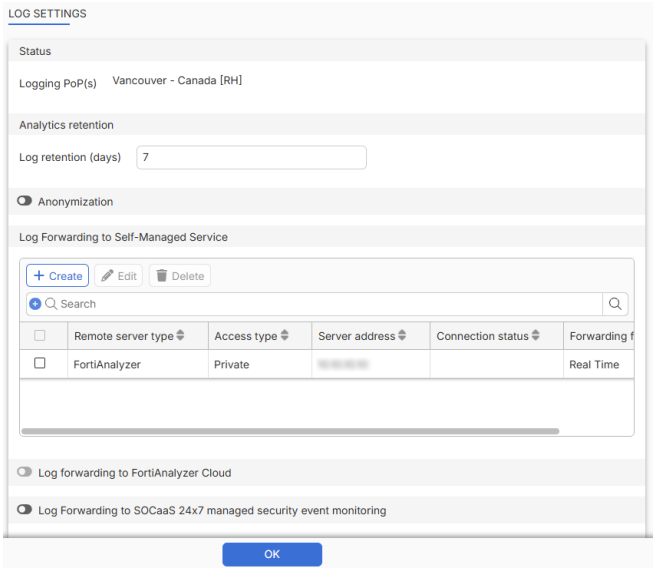
1. Go to *Operations* > *Logs* > *Settings*.
2. Configure the first external server:
   a. In *Log Forwarding to Self-Managed Service*, click *Create*.
   b. In *Remote Server Type*, select *FortiAnalyzer*, *Syslog*, or *Common Event Format (CEF)*.
   c. For *Access type*, select one of the following:
      - *Public* if the self-managed service is publicly accessible on the internet.
      - *Private* if the self-managed service is behind a secure private access FortiGate hub.
   d. In the *Server address* field and *Server Port* field (shown for *Syslog* and *CEF* types only), enter the desired address and port for FortiSASE to communicate with the server:
      - If you selected *Public* for *Access type*, then the *Server address* field should be the public IP address or FQDN of the self-managed service.

- If you selected *Private* for *Access type*, then the *Server address* field should be the private IP address or FQDN of the self-managed service.

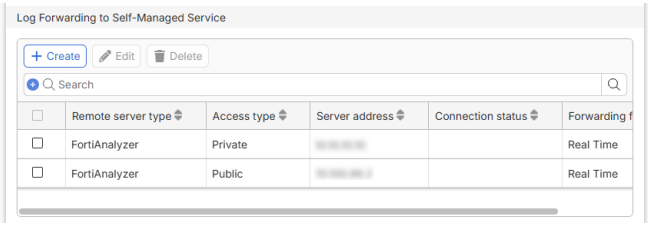
e. Enable *Reliable connection* to use TCP for log forwarding instead of UDP.

f. For *Forwarding frequency*, select *Real Time*, *Every Minute*, or *Every 5 Minutes* for log forwarding frequency from FortiSASE to the self-managed service.

g. Click *OK*.



3. Repeat step two to configure a secondary log forwarding server.

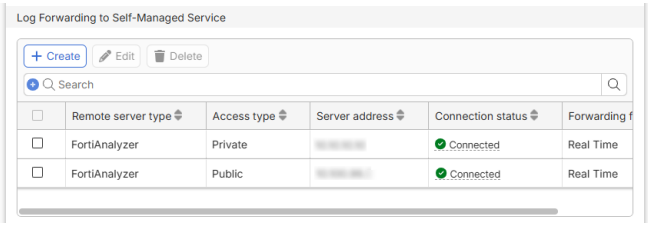


FortiSASE supports the following combination of external server access types:

- Two *Public* servers
- One *Public* server and one *Private* server

If the primary server is set to *Private*, the secondary server must be *Public*. *Private* servers require secure private access (SPA). See SPA on page 101.

4. Click *OK*. After submitting the changes, the *Connection status* changes from *Connecting* to *Connected*.



To forward logs securely using TLS to an external syslog server:

1. Go to *Operations* > *Logs* > *Settings*.
2. In *Log Forwarding to Self-Managed Service*, click *Create*.
   a. In *Remote Server Type*, select *Syslog*.
   b. In the *Server Address* and *Server Port* fields, enter the desired address and port for FortiSASE to communicate with the syslog server.
   c. Observe that *Reliable Connection* is enabled by default. Enabling this option enables TCP for log forwarding instead of UDP.
   d. Observe that *Secure Connection* is enabled by default. Enabling this option enables TLS for log forwarding and requires *Reliable Connection* to be enabled.

      When hovering over the information icon, ensure the appropriate remote CA certificate for the external syslog server is uploaded for the TLS connection to succeed by clicking *Certificates*. Alternatively, go to *System* > *Certificates*.
      - For details on importing a remote CA certificate, see Certificates on page 592.
      - For details on the cipher suites that a secure external syslog server supports, see Supported cipher suites for secure external syslog server.

      > You must import the remote CA certificate for the external syslog server to FortiSASE to establish trust with the external syslog server. Otherwise, the TLS connection fails and the external syslog server cannot read the forwarded logs.

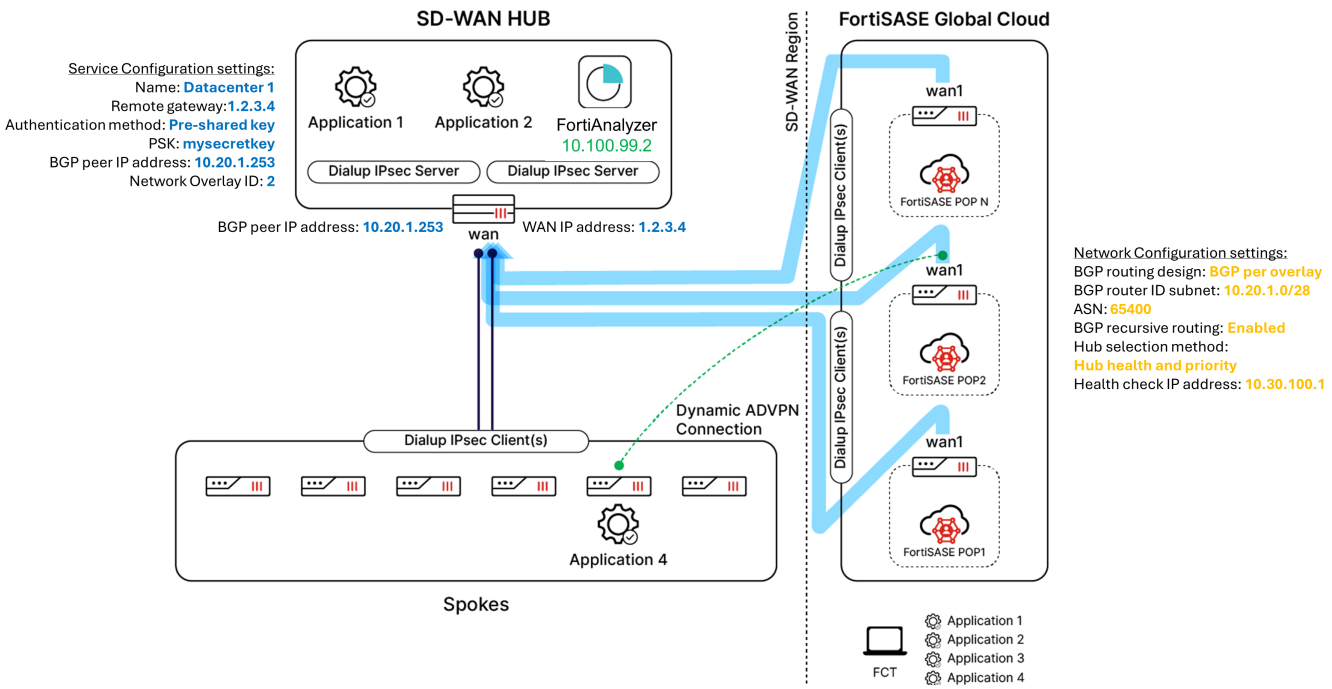
   e. Click *OK*.
3. Click *OK*.

Example: Forwarding logs to an on-premise FortiAnalyzer in an SPA hub network

This example demonstrates how to configure forwarding logs to an on-premise FortiAnalyzer in an SPA hub network using the *Log Forwarding to Self-Managed Service* setting with the *Access Type* set to *Private*.

> This example uses BGP per overlay as the BGP routing design because that is the default setting. The example also applies to the BGP on loopback BGP routing design.

In this example, we have the following SPA hub network topology using BGP per overlay as the BGP routing design:

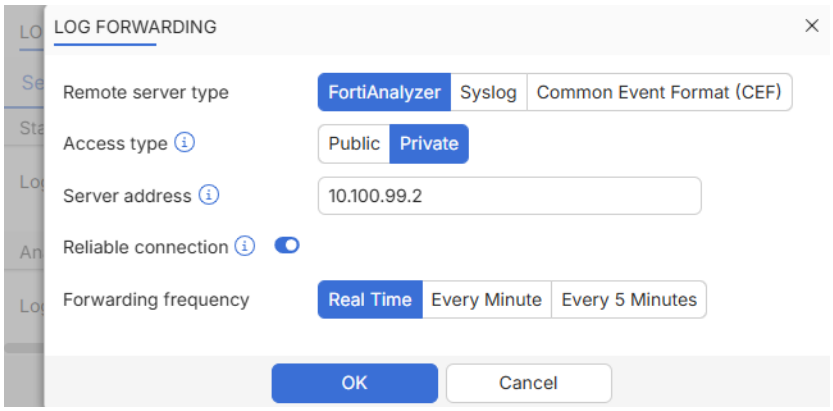


The FortiAnalyzer is in the SPA hub network with an IP address of 10.100.99.2.

For this example, you will configure FortiSASE to forward logs to the FortiAnalyzer using its private IP address on the SPA hub local network. Then you will authorize the FortiSASE security PoPs on the FortiAnalyzer to allow FortiSASE to forward logs to the FortiAnalyzer. Lastly, you will verify that the logs from FortiSASE are forwarded to the FortiAnalyzer.

To configure forwarding logs to an on-premise FortiAnalyzer in an SPA hub network:

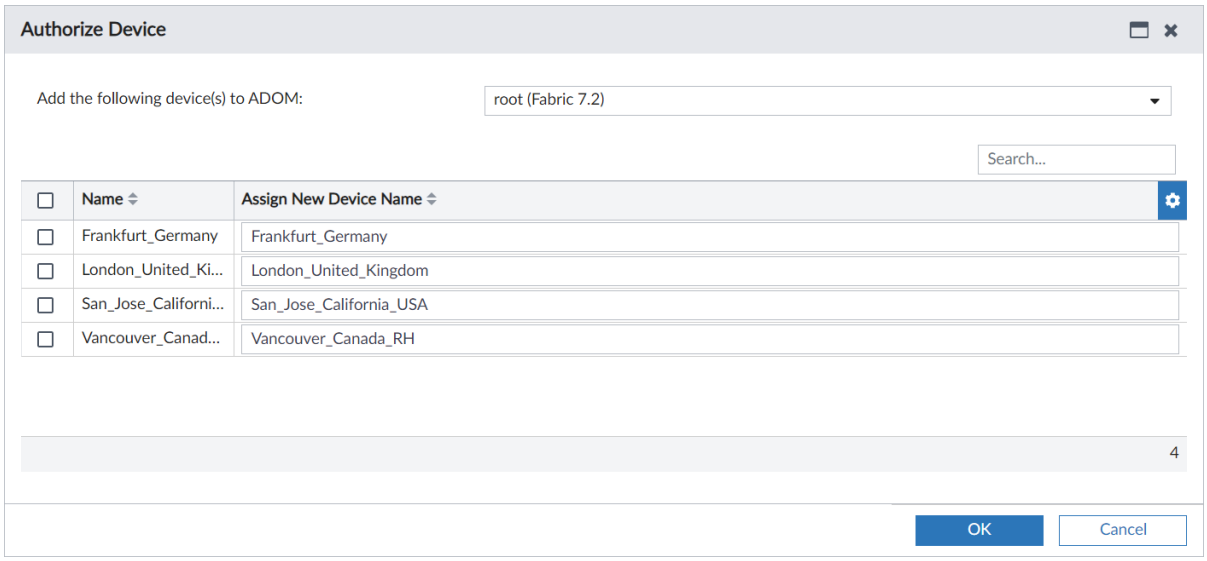
1. Go to *Operations* > *Logs* > *Settings*.
2. In *Log Forwarding to Self-Managed Service*, click *Create*.
   a. For *Remote server type*, select *FortiAnalyzer*.
   b. For *Access type*, select *Private* because the self-managed service (on-premise FortiAnalyzer) is behind a Secure Private Access (SPA) FortiGate hub.
   c. In the *Server address* field, enter 10.100.99.2, which is the private IP address of the self-managed service.
   d. Enable *Reliable connection* to use TCP for log forwarding instead of UDP.
   e. For *Forwarding frequency*, select *Real Time*.
   f. Click *OK*.



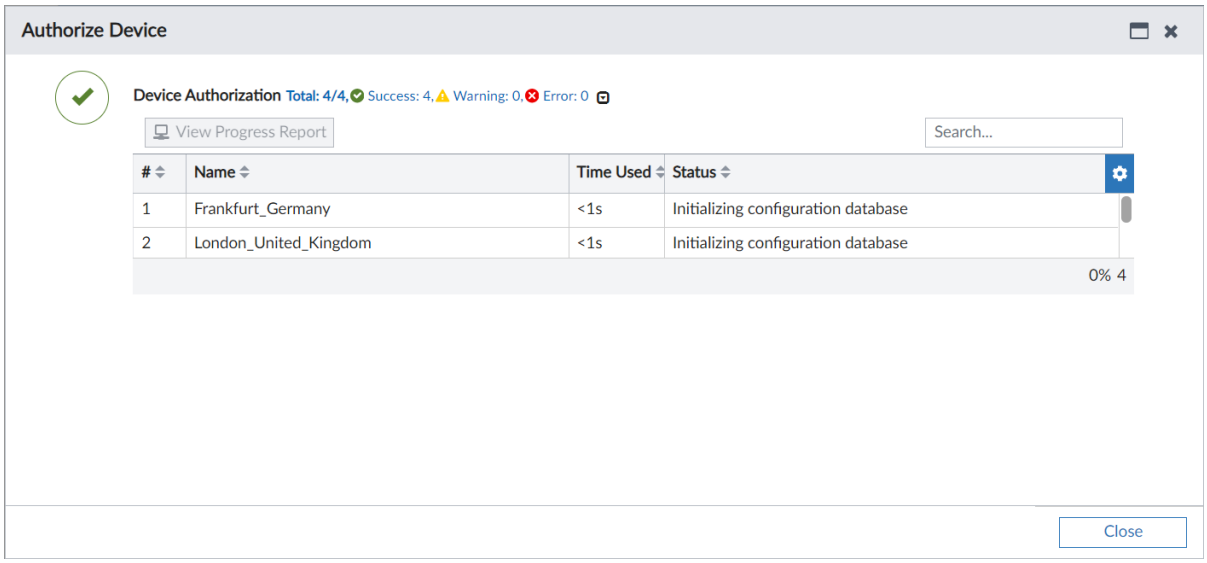
3. Click *OK*. After submitting the changes, the *Connection status* changes from *Connecting* to *Connected*.

To authorize the FortiSASE security PoPs on the FortiAnalyzer to allow FortiSASE to forward logs to the FortiAnalyzer:

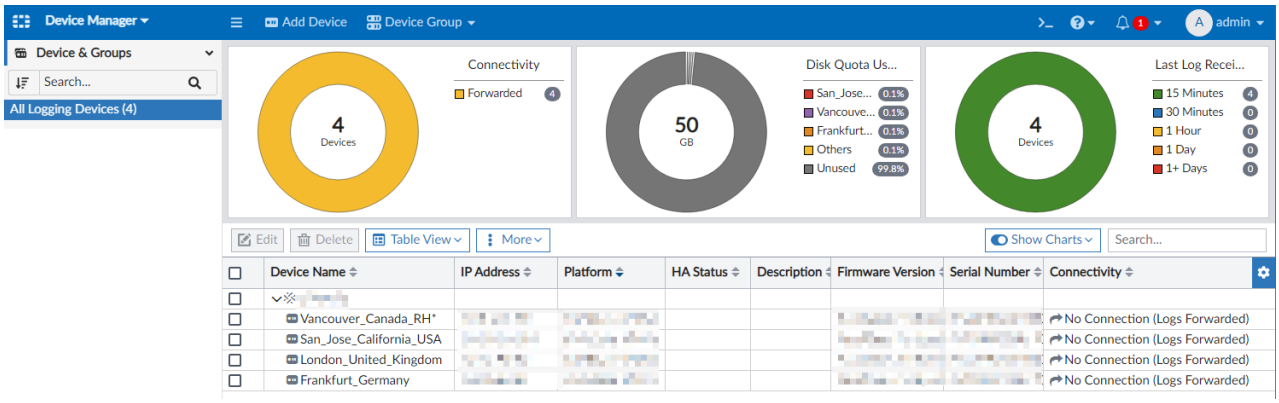
1. Log on to the FortiAnalyzer GUI.
2. Go to the *Device Manager*.
3. In the *Device Manager*, under *Unauthorized Devices* observe the FortiSASE security PoPs attempt to connect to FortiAnalyzer. Select all devices and click on *Authorize*.
4. In the *Authorize Device* wizard, select all the devices, add them to the root ADOM, and click *OK*.



5. Observe *Device Authorization* succeeds for 4/4 devices. Click *Close*.

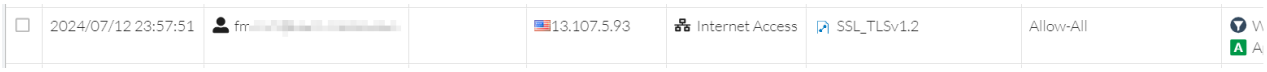


6. In the *Device Manager* page, wait for one minute and notice the *Connectivity* as *No Connection (Logs Forwarded)* as desired.



To verify that the logs from FortiSASE are forwarded to the FortiAnalyzer:

1. In FortiSASE, go to *Operations* > *Logs* > *Traffic*.
2. Select *All Internet & Private Access Traffic*.
3. Observe one of the log entries with user fm to destination IP address 13.107.5.93:



4. In FortiAnalyzer, go to *Log View*.
5. Go to *FortiGate* > *Traffic* to view the corresponding traffic log entries forwarded from FortiSASE.
6. In FortiAnalyzer, observe the log entry corresponding to the log entry observed in FortiSASE:



Administrator Events

Administrator Events logs under *Operations > Logs > Events* provide granular logs that are useful to monitor and audit administrator activities such as login, MSSP portal access, configuration changes made by normal Identity & Access Management (IAM)/single sign on (SSO)/API user accounts or impersonated SSO/IAM accounts, and configuration change logs contributing to effective auditing and compliance management. FortiSASE stores Administrator Events logs for the number of days that you specify in the log retention policy. See Log retention policy on page 251.



Configuration change logs can be enabled in *System > Administration*. See Administration on page 587.

Currently, in FortiSASE, administrator event logs are displayed after some delay. Therefore, different timestamp fields are available for administrator events only to distinguish between the event's actual occurrence time and the time that the log was exported to FortiSASE.

Administrator Events log type	Timestamp field for actual event time (Unix timestamp in seconds)	Timestamp field for log export time to FortiSASE (Unix timestamp in nanoseconds)
FortiSASE Log Detail Window	Date/Time	Log Event Original Timestamp
Log forwarding to self-managed syslog or FortiSASE Downloaded Log File	audittime	eventtime
Log forwarding to self-managed FortiAnalyzer	Security Rating Time	Event Time

To view an Administrator Events log:

1. Go to *Operations > Logs > Events*.
2. Click *Administrator Events*.
3. Double-click the desired log. A slide in window appears where you can view the log in detail.

Endpoint management

To increase endpoint visibility, FortiSASE supports displaying detailed logs for these FortiClient events:

- Tunnel connection
- Scan
- Malware
- Sandbox detection
- Removable media
- Traffic
- System

FortiClient event logs are not forwarded from endpoints to FortiSASE when an agent policy to deny all internet traffic has been configured using one of these methods:

- Disabling the default Allow-All Internet Access policy, which causes traffic to be matched by the Implicit Deny policy.
- Creating an Internet Access policy that denies all internet traffic with *Service* set to *ALL* and *Destination* set to *All Internet Traffic* and placed above the default Allow-All policy.

If your FortiSASE instance requires an agent policy that denies all internet traffic and you want to use this feature, contact FortiCare Support to open a ticket to apply a known workaround to your instance.

Forwarding logs to SOCaaS

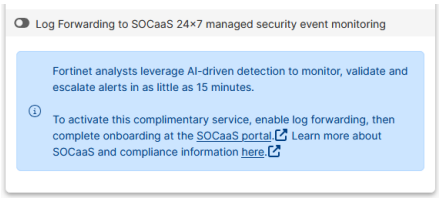
SOC-as-a-Service (SOCaaS) can analyze security events generated by FortiSASE, perform alert triage, and escalate verified threat notifications to your security team. For information on the benefits and capabilities of SOCaaS, see the SOCaaS User Guide.

To provide integration with FortiGuard SOCaaS, FortiSASE supports the ability to configure log forwarding from FortiSASE to a SOCaaS collector using *Log Forwarding to SOCaaS 24x7 managed security event monitoring* in *Operations > Logs > Settings*. When log forwarding to SOCaaS is enabled, all traffic and event logs from FortiSASE are forwarded to SOCaaS.

To be configurable, *Log Forwarding to SOCaaS 24x7 managed security event monitoring* requires an Advanced or Comprehensive remote users FortiSASE subscription. Otherwise, FortiSASE grays out this option in *Operations > Logs > Settings*. See the FortiSASE Ordering Guide.

To configure log forwarding to SOCaaS:

1. Go to *Operations > Logs > Settings*.



2. Enable *Log Forwarding to SOCaaS 24x7 managed security event monitoring*.
3. Click *OK*.
4. Once FortiSASE enables this feature, observe the following:
   a. A prompt instructs you to *Start Onboarding*. If you click *Start Onboarding*, a browser window opens for the SOCaaS portal to complete onboarding. Once you complete onboarding, FortiSASE sends a service request to the SOCaaS team. Completing onboarding on the SOCaaS portal is important for this feature to work as intended.
   b. In *Status*, *Logging Location(s)* displays a *SOCaaS Collector Region*.
   c. Under *Log Forwarding to SOCaaS*, *Connection Status* displays *Connected* with a green checkmark. Hovering over the *Connection Status* value shows the rate at which FortiSASE forwards logs.

Currently, you cannot disable the *Log Forwarding to SOCaaS 24x7 managed security event monitoring* feature from *Operations > Logs > Settings* once you have enabled it because the toggle is grayed out. To disable this feature, you must create a new FortiCare ticket.

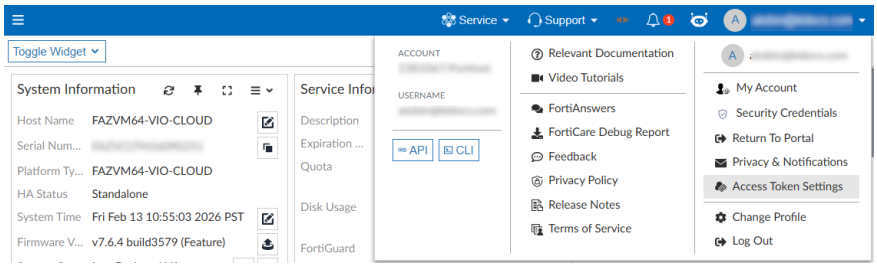
Forwarding logs to FortiAnalyzer Cloud

FortiAnalyzer Cloud is a cloud-based logging platform based on FortiAnalyzer. It is designed for system health monitoring and alerting using event logs, security logs, and IOC scans. FortiAnalyzer Cloud can receive traffic, UTM, and other logs. For information on the benefits and capabilities of SOCaaS, see the FortiAnalyzer Cloud Deployment guide.

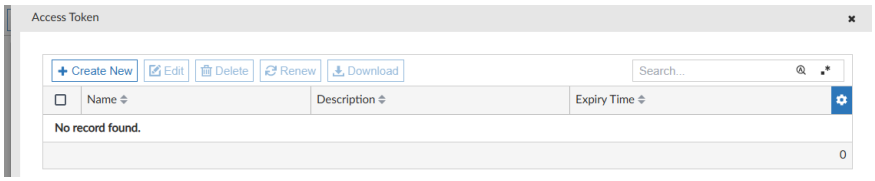
FortiSASE supports the ability to configure log forwarding from FortiSASE to a FortiAnalyzer Cloud instance using *Log forwarding to FortiAnalyzer Cloud* in *Operations > Logs > Settings*. When log forwarding is enabled and connected through the use of a FortiAnalyzer Cloud token, all traffic and event logs from FortiSASE are forwarded to FortiAnalyzer Cloud.

To forward logs to FortiAnalyzer Cloud:

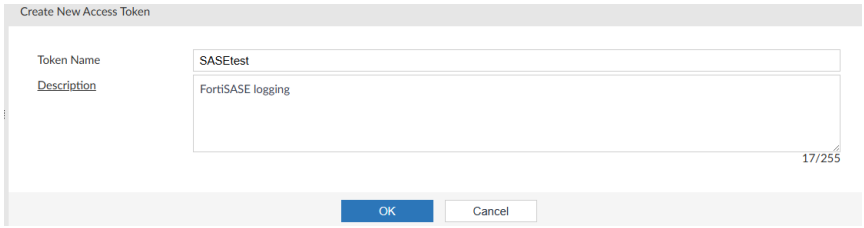
1. Configure a FortiAnalyzer Cloud token:
   a. In the FortiAnalyzer Cloud instance, open the portal toolbar menu.



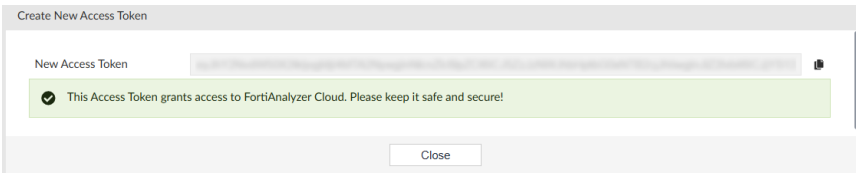
   b. Click *Access Token Settings*.



   c. Click *Create New*.
   d. Configure the *Token Name* and *Description*.



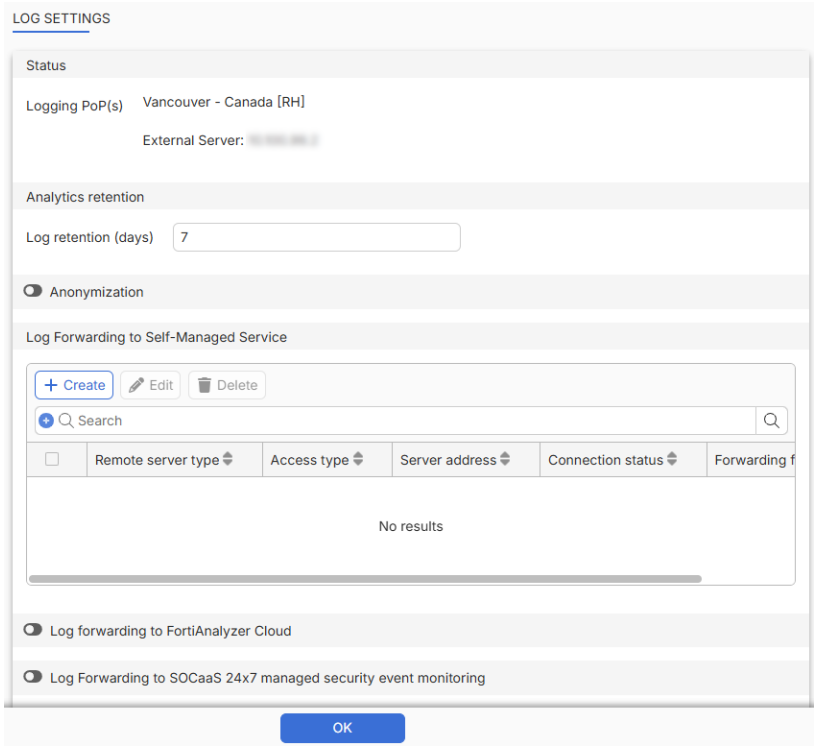
   e. Click *OK*. The token information is displayed.



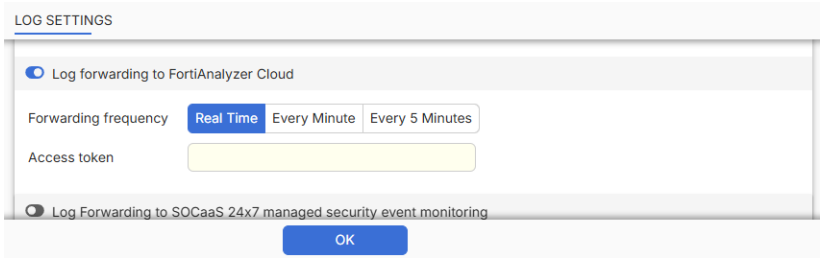
f. Copy the token. You will need this to connect to FortiSASE.

For more information, see Managing access tokens.

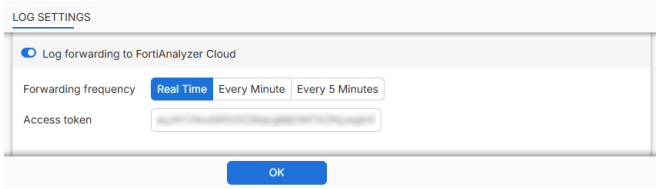
2. In FortiSASE, go to *Operations* > *Logs* > *Settings*.



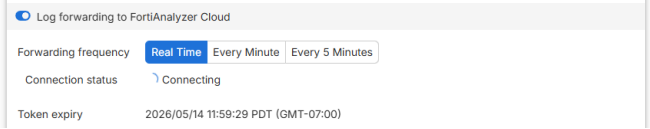
3. Enable *Log forwarding to FortiAnalyzer Cloud*.



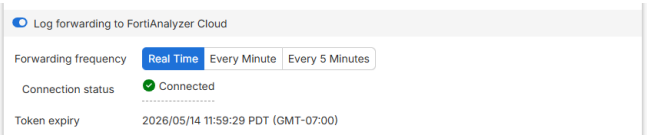
4. Select the *Forwarding frequency* for sending logs to FortiAnalyzer Cloud.
5. Enter the *Access token* copied from FortiAnalyzer Cloud.



6. Click *OK*. After submitting the changes, *Connection status* will appear as *Connecting*.



7. In the FortiAnalyzer Cloud instance, go to Device Manager and authorize the FortiSASE instance.
   Once log forwarding is successfully configured, the FortiSASE instance's *Connection status* will be updated to *Connected*.



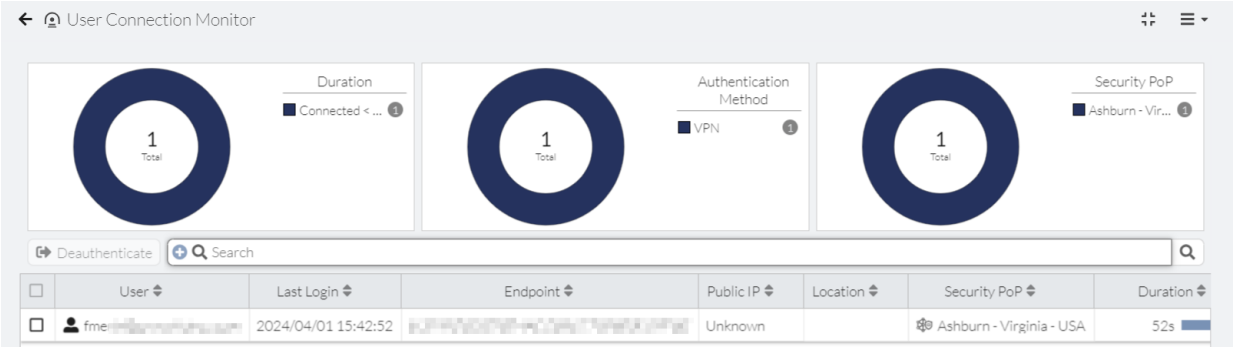
Prerequisites

- This feature requires the FortiAnalyzer Cloud Storage Add-On License subscription and FortiAnalyzer 7.6.3 or later. If there is no FortiAnalyzer Cloud Storage Add-On License, token generations will not be successful. See the FortiAnalyzer Ordering Guide for more information.
- A FortiAnalyzer Cloud instance must be created in the same FortiCloud Services account as the FortiSASE instance. For information on configuring a FortiAnalyzer Cloud instance, see Deploying a FortiAnalyzer Cloud instance.

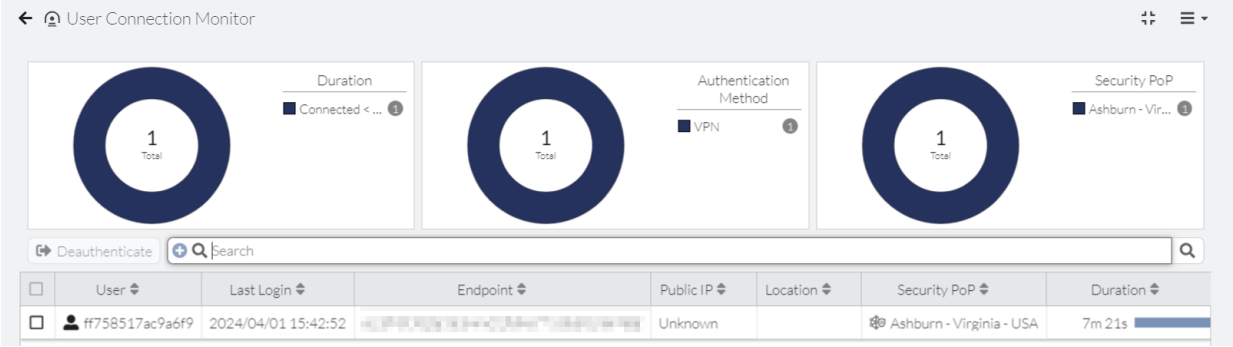
Log anonymization

Log anonymization allows you to hide personally identifiable user information, such as their username, in Dashboard widgets, logs, and other areas of FortiSASE.

The following shows the *Connected Users* page when log anonymization is disabled. The username information in the *User* field is visible.

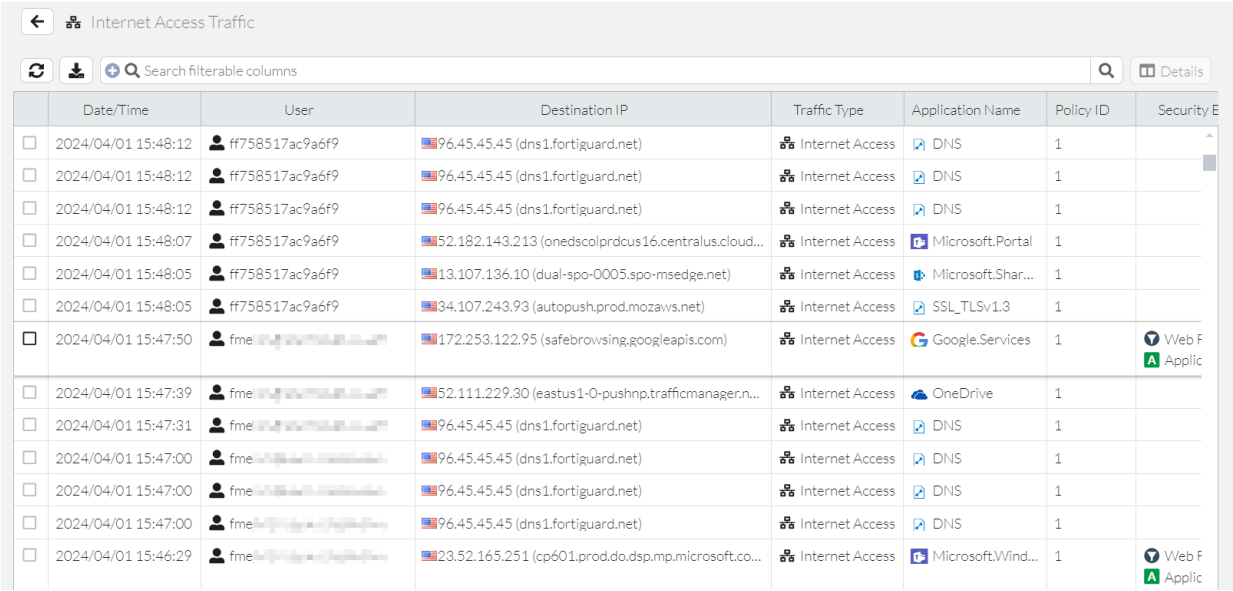


The following shows the *Connected Users* page when log anonymization is enabled. The username information in the *User* field is anonymized.

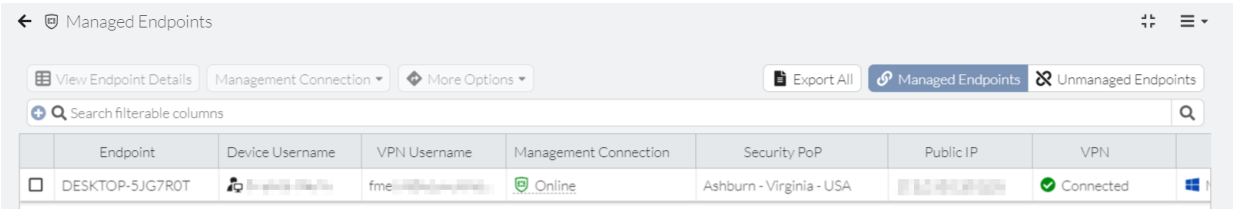


The following shows log anonymization's effect on *Operations > Logs > Traffic*. In the following example, all logs are from the same source (user fme) and log anonymization was enabled at 15:48. All logs for traffic that occurred before 15:48 show the source information. All logs that occurred after 15:48 have the source information anonymized.

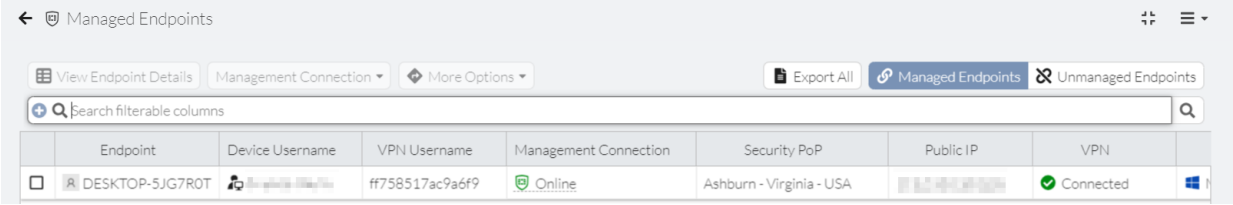
You cannot retroactively anonymize or deanonymize source information by enabling or disabling anonymization. The source information remains anonymized or not anonymized based on whether log anonymization was enabled or disabled when the traffic occurred.



The following shows the *Managed Endpoints* page when log anonymization is disabled. The username information is visible.



The following shows the *Managed Endpoints* page when log anonymization is enabled. The username is anonymized.



When log anonymization is enabled, reports may be less useful, as personally identifiable information will be anonymized.

To enable log anonymization:

1. Go to *Operations* > *Logs* > *Settings*.
2. Enable *Anonymization*.
3. In the *Salt* field, enter the desired username anonymization hash salt. FortiSASE generates a hash based on the username and salt value and uses this to anonymize log information.

Log retention policy

Log storage is fixed and log storage usage depends on factors such as number of users, number of policies with logging enabled, and logging type selected (security events, all sessions) for such policies. If log rotation occurs ahead of the configured log retention period, open a FortiCare support ticket to request a log storage increase for your instance.

You can configure FortiSASE to store logs up to a certain number of days that you specify as the log retention policy. FortiSASE automatically deletes logs that are older than the specified log retention (days).

All FortiSASE instances have log retention enabled. The log retention period behavior differs depending on whether the instance was provisioned (initialized with security PoPs) before or after 25.3.a (See Provisioning):

FortiSASE instance type	Default log retention period	Configurable log retention policy range
Provisioned before 25.3.a	30 days	2 to 30 days
Provisioned after 25.3.a	7 days	2 to 7 days

If you attempt to set *Log Retention (days)* to 30 days and it is not supported in your instance you will see the error message *Failed to update security log retention*. This can be used to confirm whether or not your instances has been provisioned in 25.3.a or later.

The log retention policy applies to traffic, security, and event logs.

To store logs for a longer duration, configuring log forwarding to an external server is advised. See Forwarding logs to an external server on page 238.

To configure log retention policy:

1. Go to *Operations* > *Logs* > *Settings*.
2. Under *Analytics Retention*, set *Log Retention (days)* to the required number of days.
3. Click *OK* to save the changes.

Administration

You can perform FortiSASE administrative tasks using these Administration features:

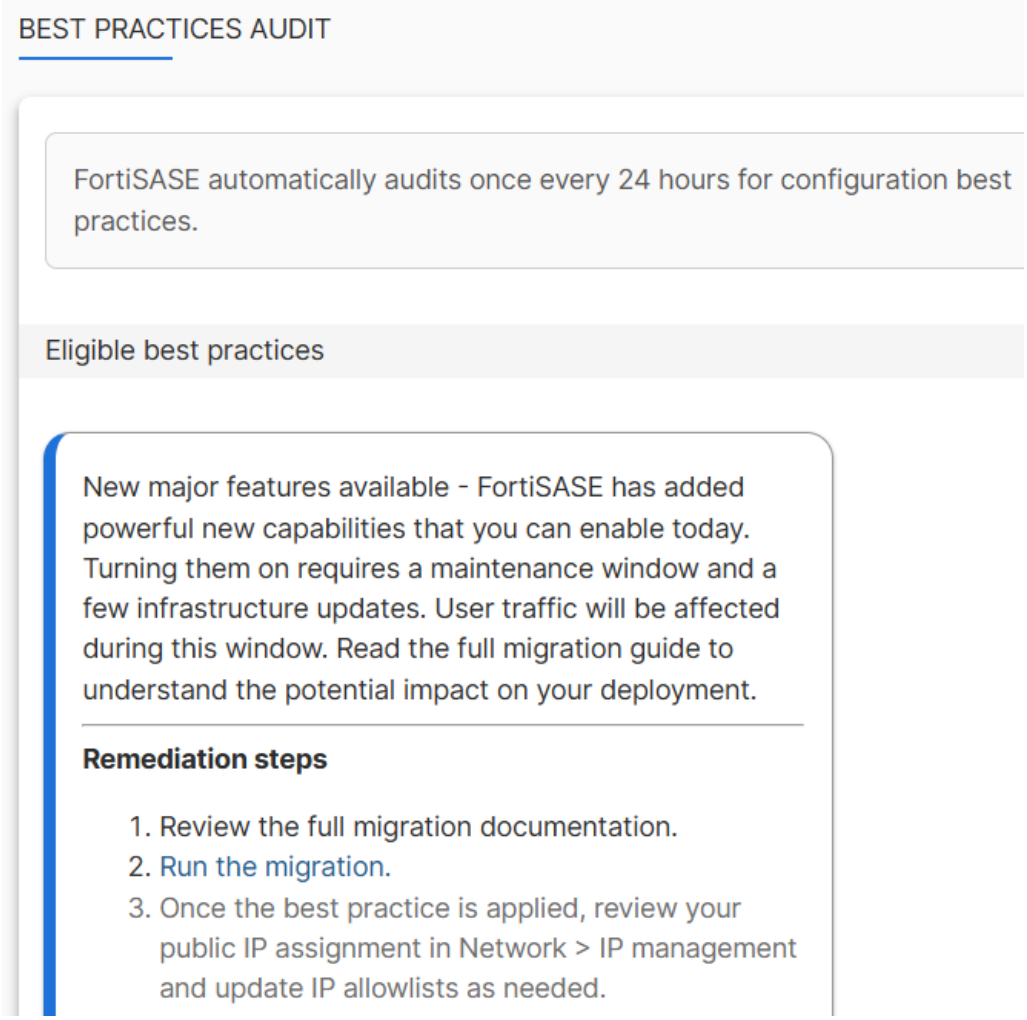
- Software audit & version on page 252
- Automation on page 259

Software audit & version

FortiSASE includes a software audit & version page that provides configuration best practice recommendations regarding your instance, its configuration, and selecting a preferred maintenance window for FortiSASE upgrades. You can access this page in *Operations* > *Software audit & version*.

Any eligible best practices appear below *Eligible best practices* in the *Audit* tab, such as new major features and SOCaaS log forwarding.

Fortinet will occasionally prioritize certain best practices and will strongly encourage administrators to run them through prompts and notifications within the FortiSASE portal.



To select a preferred maintenance window for FortiSASE upgrade:

1. Go to *Operations* > *Software Audit & Version*, and select the *Version* tab.
2. From the *Preferred maintenance window* dropdown, select a suitable upgrade time slot. The selection determines the upgrade window for the upcoming FortiSASE release. Based on your chosen time slot, a corresponding maintenance window day for upgrade is automatically selected. To view which maintenance day aligns with each time slot, see *Monthly Maintenance*.
3. Click *OK* to save your changes.

Considerations

- FortiSASE automatically performs an audit once every 24 hours for configuration best practices.
- Best practice steps start immediately once initiated through *Operations* > *Software audit & version* under the *Audit* tab.
- Some best practice steps have operations that may involve temporary network disruption, including user sessions.

- Once initiated, pausing and rollbacks are not possible.
- Proceed only after completing all prerequisites for an operation and only if a maintenance window is acceptable at the time of initiating the best practice steps through *Operations* > *Software audit & version* under the *Audit* tab.
- For these operations, you must acknowledge the potential impact by clicking a checkbox in the audit page dialog before the best practice steps can continue.

- A maintenance window of 22:00-06:00 JST (13:00 - 21:00 UTC) is available that is more suitable for customers whose instances have Japanese security PoPs selected.
  - For new instances with a Japanese security PoP selected, their maintenance windows will be automatically assigned to this new window.
  - For existing instances with a Japanese security PoP selected, administrators can select this new window from *Software audit & version* > *Version*.

SSL to IPsec transition mode

The *FortiSASE Cloud Security tunnel - SSL to IPsec transition mode* best practice option appears in the audit page once available for your tenant. This best practice is only available for SSL VPN instances to support the one-way transition from SSL to IPsec remote user connectivity.

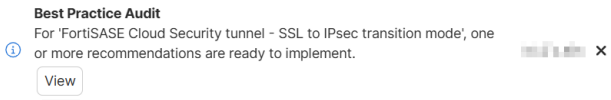
For greater performance and security, instances with FortiSASE Cloud Security SSL tunnels will be migrated one-way to IPsec in 2027. Get a head start and enable transition mode to test SSL and IPsec side-by-side that is available as an opt-in feature for SSL VPN instances through the *Operations* > *Administration* > *Software audit & version* page's best practices. This provides the opportunity to verify if additional configuration changes are needed before migrating with confidence.

Before enabling this transition mode, carefully review the IPsec and SSL VPN supported features in these topics:

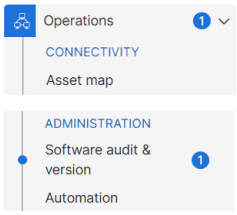
- Supported FortiClient 7.4.6 features
- Supported FortiClient 7.2.14 features

Prior to enabling this transition mode, the FortiSASE portal displays several notifications about the SSL to IPsec transition mode being available:

- In the header, a bell icon *Best Practice Audit* notification for this mode is displayed. Clicking *View* in the notification redirects to *Operations* > *Administration* > *Software audit & version*.



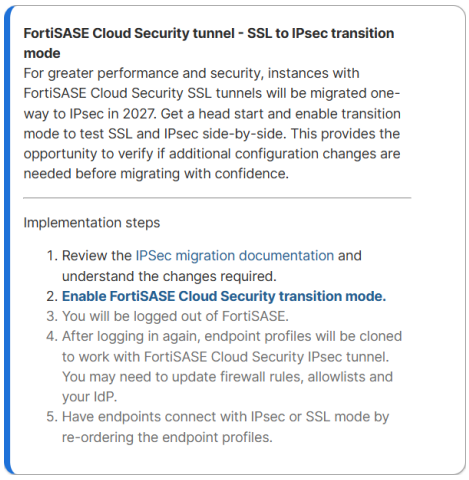
- In the navigation bar, notifications appear in the *Operations* menu and in the *Administration* > *Software audit & version* item, respectively. Hovering over any of these notifications presents a tooltip.



- Dismissing the bell icon notification in the header also dismisses the notifications in the navigation bar.

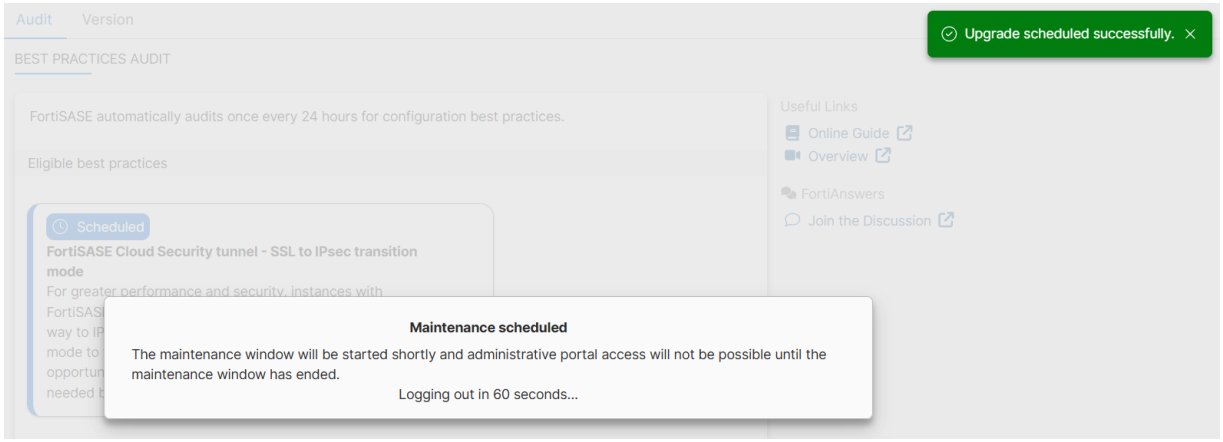
To enable SSL to IPsec transition mode:

1. In *Eligible best practices*, the *FortiSASE Cloud Security tunnel – SSL to IPsec transition mode* option appears.

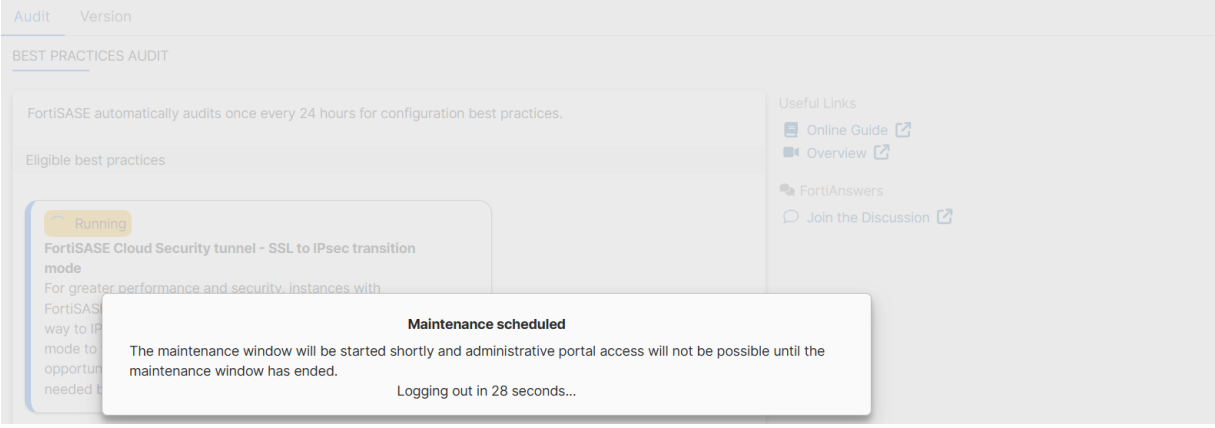


2. Review the steps carefully before proceeding.
   a. Click the hyperlinked text *IPsec migration documentation* which opens this current document.
   b. Determine a maintenance window when temporary network disruption, including user sessions, is acceptable. Once initiated, pausing and rollbacks will not be possible.
   c. When ready, click the hyperlinked text *Enable FortiSASE Cloud Security transition mode*.
3. An *Acknowledgment required* window appears. Review the window carefully before proceeding. Once ready, click *I understand the potential impact and would like to continue* and click *Continue*.

   You see the *Upgrade scheduled successfully* message and the best practice appears as *Scheduled*. A countdown timer appears in the *Maintenance scheduled* window before the portal logs you out.



   After some time, the best practice appears as *Running*.



As part of the best practice process, the current portal session is logged out.



4. After a successful upgrade:
   a. Log back into the FortiSASE portal.
   b. In the header, a *Best Practice Audit* notification displays *Successfully implemented the best practice for 'FortiSASE Cloud Security tunnel - SSL to IPsec transition mode'*.

Best practice considerations

This section outlines considerations to understand before proceeding with enabling the SSL to IPsec transition mode on your instance. It also outlines the considerations to understand after proceeding with the best practice.

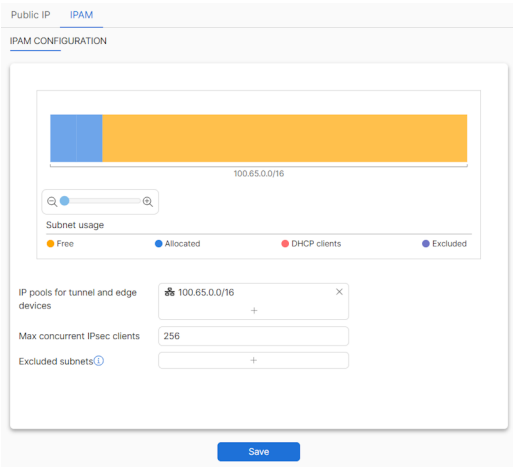
> ⚠ You must review all considerations carefully prior to applying the best practice to ensure you understand the potential impact of implementing it on your deployment.

Considerations before applying the best practice

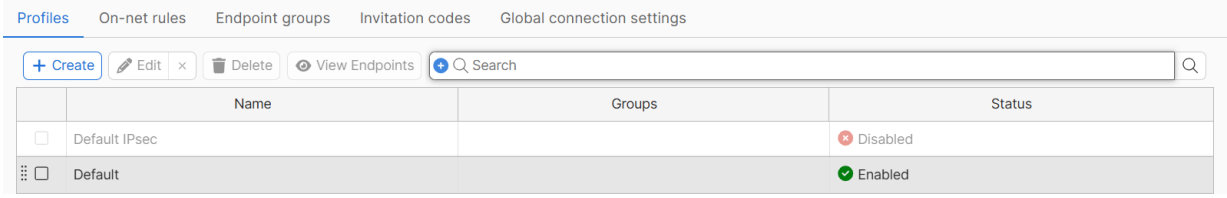
- Once the option to enable SSL to IPsec transition mode is available for your tenant and is visible in the audit page, as part of this option, the security PoPs for the affected instance will have their remote user tunneling configuration updated to add support for IPsec clients as follows:
  - Before implementing the best practice, there was a previously allocated range of 4096 IP addresses for SSL clients. After implementing the best practice, a range of 256 IP addresses will be allocated to IPsec clients as a subset within the existing range.
  - The *Default IPsec* endpoint management profile will be created and disabled by default.
  - Separate Agent SSO settings for IPsec with SP configuration appended with port 11443 will be created.
  - The following existing settings will be updated to allow Agent SSO settings for IPsec:
    - Allow-All traffic policies
    - User groups with SAML SSO configured as a remote server
  - The following existing settings prior to implementing the best practice will remain unchanged:
    - SSL tunneling settings
    - Agent SSO settings configured and used with SSL tunneling

Considerations after applying the best practice

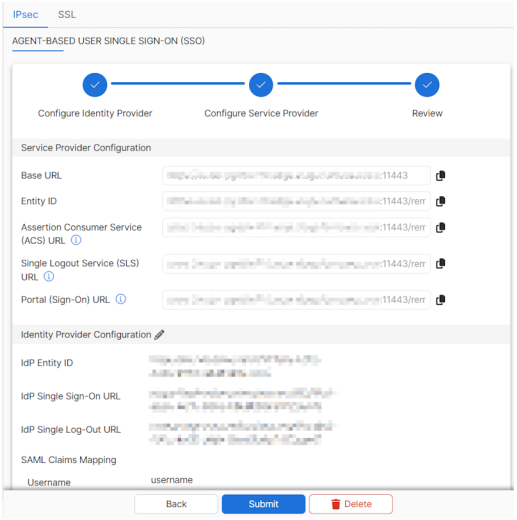
- Within the *IP pools for tunnel and edge devices* range in *Network > IP management > IPAM*, a range of 256 IP addresses will be allocated to IPsec clients. This is achieved by setting the *Max concurrent IPsec clients* to 256.



  - Before implementing the best practice, there was a previously allocated range of 4096 IP addresses for SSL clients. After implementing the best practice, a range of 256 IP addresses will be allocated to IPsec clients as a subset within the existing range.
  - After implementing the best practice, since the IP addresses for both IPsec and SSL tunneling clients share IP addresses allocated to SSL client previously. Therefore, in most cases you do not need to update firewall rules or allowlists.
  - The *Max concurrent IPsec clients* value must be within the range of 256 and 3840 (default value is 256).
    - After updating this value in the FortiSASE portal, it will take 10 to 15 minutes for this change to take effect on all Security PoPs selected for your FortiSASE instance.
- The *Default IPsec* endpoint management profile is created and disabled by default.

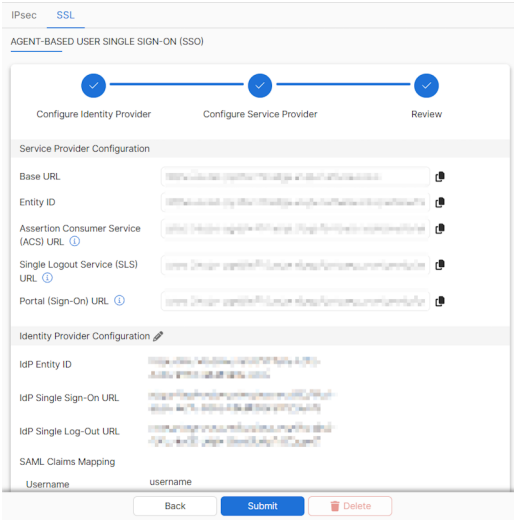


  - You must enable this profile to allow agents to connect to FortiSASE using IPsec tunneling.
    - In the *Groups & AD Users* tab, you must configure AD users, non-AD groups, or AD groups to assign the endpoint profile to. See Groups & AD Users on page 469.
  - While migrating users from SSL to IPsec, you can enable this profile together with the *Default* profile or any other profiles using the *SSL* type.
  - You may need to reorder this *Default IPsec* profile before the *Default* profile to ensure endpoints connect with the IPsec mode.
- FortiSASE maintains separate Agent SSO settings for IPsec and SSL types that can be viewed and edited via IPsec and SSL tabs, respectively, in *Access & authentication > Authentication sources > SSO*.
  - For IPsec, FortiSASE copies the SSO settings for SSL and appends port 11443 to the *Service Provider Configuration*.

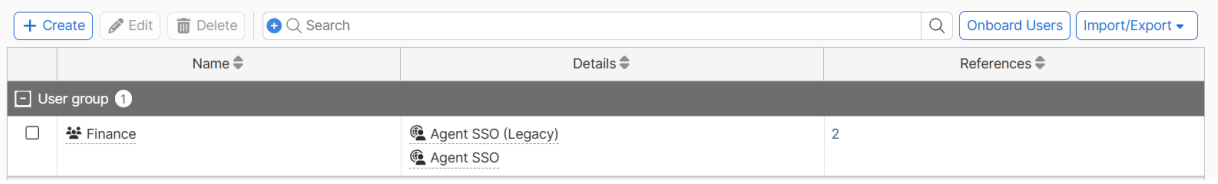


- It is still necessary to configure corresponding SP settings on the IdP side to account for the updated SP configuration on the FortiSASE side, that is, those settings appended with port 11443.
- For an SSO configuration example using Entra ID, see Configuring FortiSASE with Microsoft Entra ID SSO in FortiClient agent-based mode on page 517.

- For SSL, the SSO settings remain unchanged. Therefore, FortiSASE continues to use the previously configured SSO IdP.



- FortiSASE maintains separate SSO settings that are selectable in *Add group match* > *Remote Server* as follows:
  - SSL: *Agent SSO (Legacy)*
  - IPsec: *Agent SSO*



Therefore, you must either update existing groups or create new groups to use the *Agent SSO* as the *Remote Server* for IPsec tunnel authentication to work.

Consequently, in *Security* > *Traffic* > *Policies* you must update existing policies or create new policies to use groups using *Agent SSO* to control IPsec tunnel access accordingly.

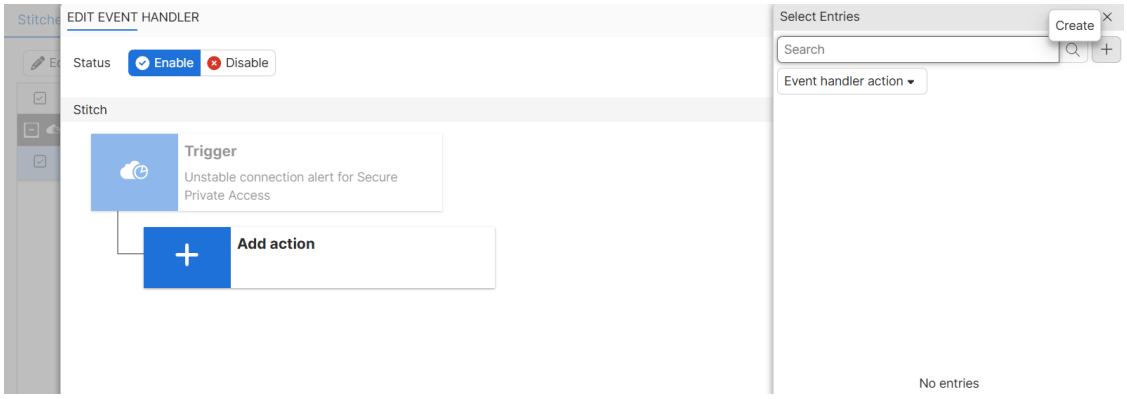
Automation

In the *Operation* > *Administration* > *Automation* page, FortiSASE allows configuring of actions, such as sending alert emails, based on predefined triggers to proactively notify administrators of events.

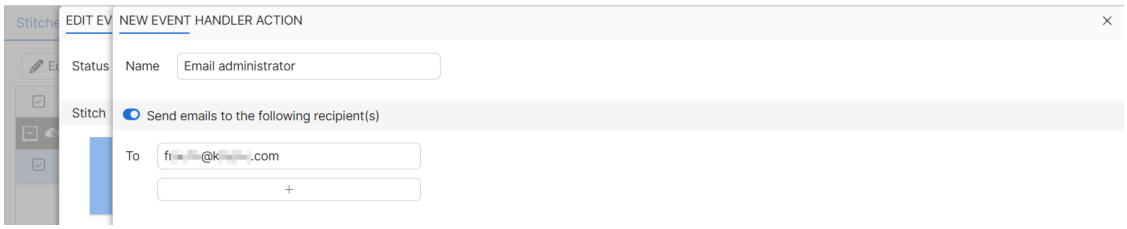
Currently, an alert email can be triggered for an unstable Secure Private Access (SPA) connection only when SLA failures, routing changes, and BGP neighbor status changes all occur. The example below demonstrates how to configure such an alert email and trigger. For this example, you must have proper SPA licensing and configuration already in place for your instance and a FortiGate as an SPA hub must have been setup already. For details, see SPA on page 101.

To configure alert emails triggered on unstable Secure Private Access (SPA) connections:

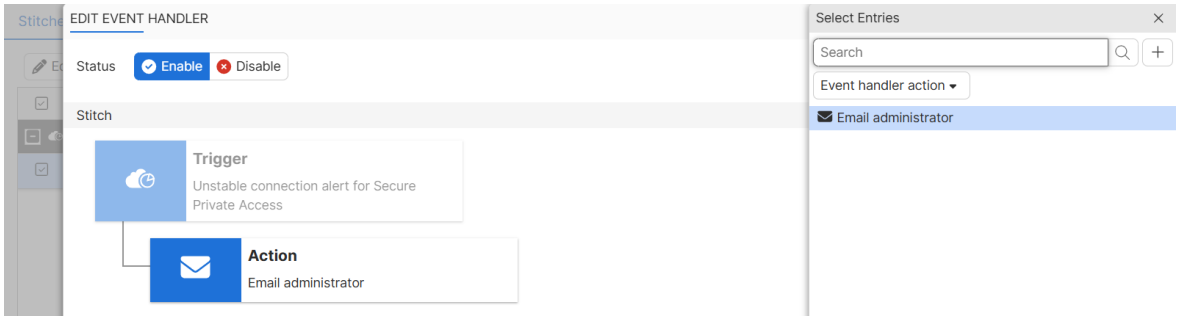
1. Go to *Operations* > *Administration* > *Automation*.
2. By default, the *Stitches* tab is displayed. In *Analytics event handlers*, select *Unstable connection alert for Secure Private Access* and click *Edit*.
3. In the *Edit Event Handler* pane:
   a. Observe that the *Status* is set to *Enable*, by default.
   b. In the *Stitch* section, click *+Add action*.
      i. In the *Select Entries* pane, click *+* to create a new event handler action.
         - Alternatively, you can also create a new event handler action from the *Operations* > *Automation* > *Actions* tab by clicking *+Create*.



      ii. In the *New Event Handler Action* pane:
         i. Enter the desired *Name*.
         ii. Observe the *Send emails to the following recipient(s)* is enabled, by default.
         iii. Enter a valid email address for the first recipient
         iv. Click *+* to add email addresses for additional recipients.
         v. Click *OK* to save the new event handler action.

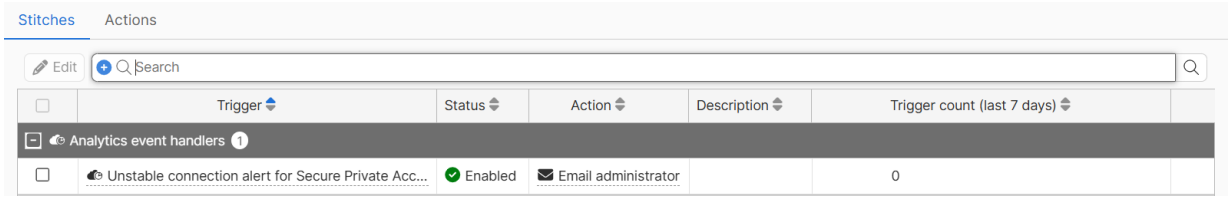


iii. Click *OK* to select the new event handler action entry.



c. Click *Close* then *OK* to finish editing the event handler.

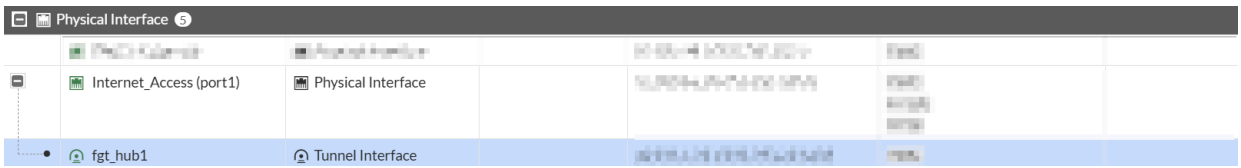
4. Observe the event handler is now associated with an email action.



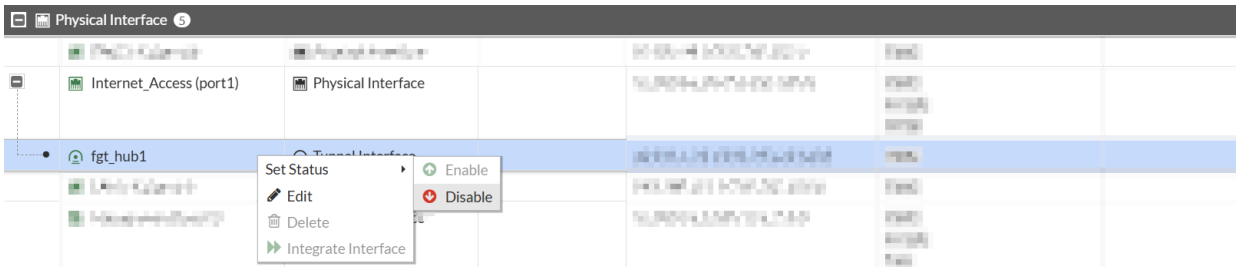
To simulate an unstable SPA connection on the FortiGate SPA hub:

1. Log into the GUI of the FortiGate configured as an SPA hub.
2. From *Network* > *Interface*, locate the WAN interface and collapse it to display the IPsec tunnel interface configured for the SPA hub.

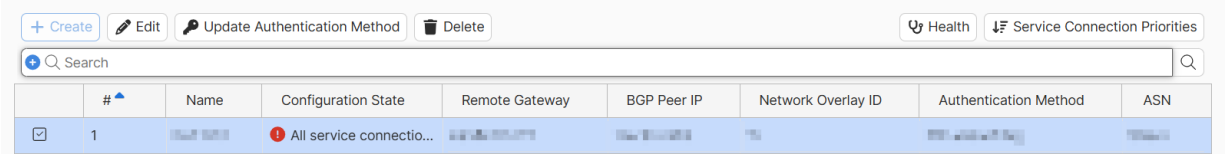
   In this example, the WAN interface is port1 and the tunnel interface is *fgt_hub1*.



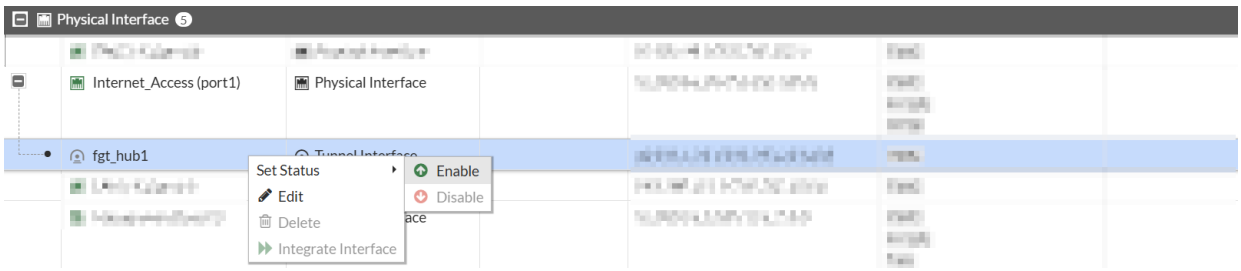
3. Right-click the tunnel interface and click *Set Status* > *Disable*. The interface color should change from green to grey.



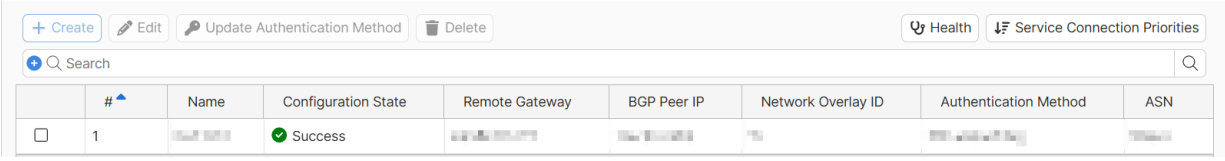
4. In FortiSASE, in *Operations* > *Connectivity* > *Secure private access*, the corresponding SPA service connection should display a *Configuration State* of *All service connections have issues*.



5. Keep the tunnel interface down for about 2 minutes.
6. After 2 minutes, right-click the tunnel interface and click *Set Status* > *Enable*. The interface color should change from grey back to green.

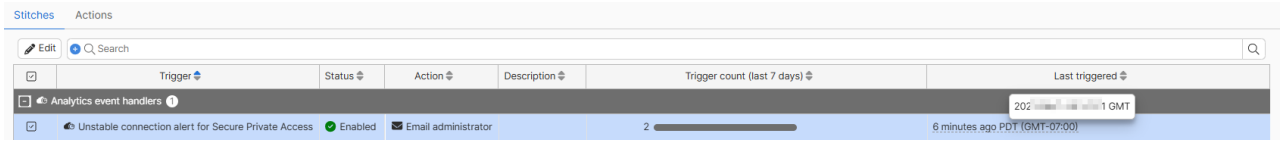


7. In FortiSASE, in *Operations* > *Connectivity* > *Secure private access*, the corresponding SPA service connection should display a *Configuration State* of *Success*.

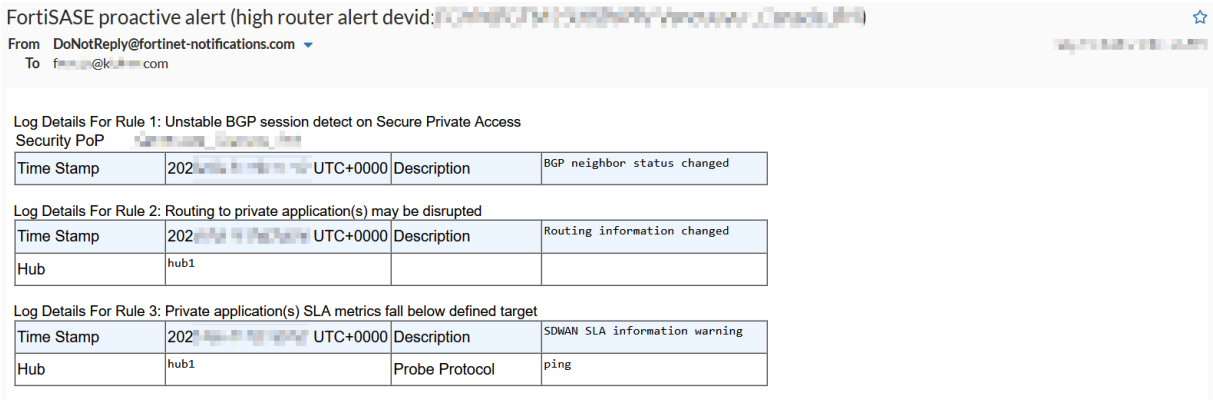


To validate alert emails triggered on unstable Secure Private Access (SPA) connections:

1. Go to *Operations* > *Administration* > *Automation*.
2. By default, the *Stitches* tab is displayed. In *Analytics event handlers*, observe the following updates to the display for *Unstable connection alert for Secure Private Access*:
   - *Trigger count* (last 7 days) is a non-zero value.
   - *Last triggered* is populated with a last triggered time duration (actual time stamp is displayed when hovering the mouse over the time duration).



3. Verify that alert emails were received at the email address specified in the event handler action.



FortiSASE proactive alert (high router alert devid:[redacted])

From DoNotReply@fortinet-notifications.com
To [redacted]@[redacted]com

Log Details For Rule 1: Unstable BGP session detect on Secure Private Access
Security PoP [redacted]

Time Stamp	202[redacted] UTC+0000	Description	BGP neighbor status changed

Log Details For Rule 2: Routing to private application(s) may be disrupted

Time Stamp	202[redacted] UTC+0000	Description	Routing information changed
Hub	hub1		

Log Details For Rule 3: Private application(s) SLA metrics fall below defined target

Time Stamp	202[redacted] UTC+0000	Description	SDWAN SLA information warning
Hub	hub1	Probe Protocol	ping

You will receive an email for each security PoP configured with your FortiSASE instance.

Network

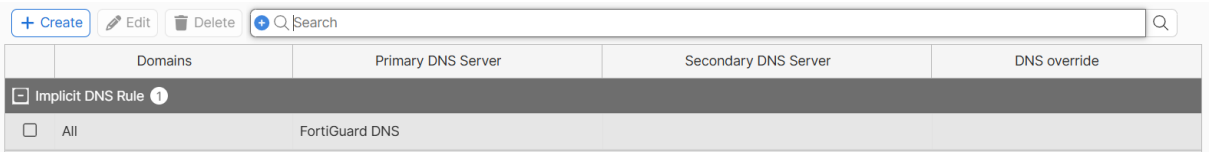
In *Network*, you can access various features so that you can easily monitor your network.

DNS

Remote users use the DNS server in FortiSASE under *Network > DNS* to resolve hostnames for internal and external domains.

Agent and agentless endpoints and endpoints connected to authorized Edge devices forward their DNS traffic to FortiSASE. FortiSASE performs transparent DNS redirection to redirect DNS traffic conditionally as desired.

- Implicit DNS rules are predefined for agents and users connected to authorized Edge devices. FortiSASE uses these rules for resolving hostnames for external domains.
- You can create split DNS or DNS redirection rules by clicking *Create*. FortiSASE uses these rules for resolving hostnames for internal domains. See DNS redirection rules on page 265.



By default, FortiSASE deployments use FortiGuard DNS as the default DNS server for the *All* implicit DNS rule. You can select any implicit DNS rule and click *Edit* to change the default DNS server.

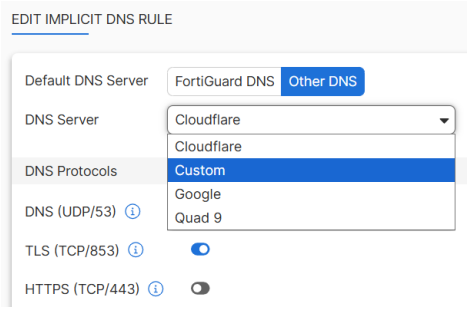
You can configure *Default DNS Server* with one of the following options, then click *OK* to save the change:

DNS Server	Description	Primary and Secondary DNS Server IP Address
FortiGuard DNS	Use FortiGuard DNS	96.45.45.45 96.45.46.46
Other DNS	Use a public DNS server other than FortiGuard DNS	IP addresses specific to public DNS server
CloudFlare	Use the CloudFlare public DNS server	1.1.1.1 1.0.0.1
Custom	Enable to specify your own custom primary and secondary DNS servers.	Specify IP address of primary and secondary DNS.
Google	Use the Google public DNS server	8.8.8.8 8.8.4.4
Quad 9	Use the Quad 9 public DNS server	9.9.9.9 149.112.112.112

For example, you can edit the implicit DNS rule to use a custom DNS server as follows:

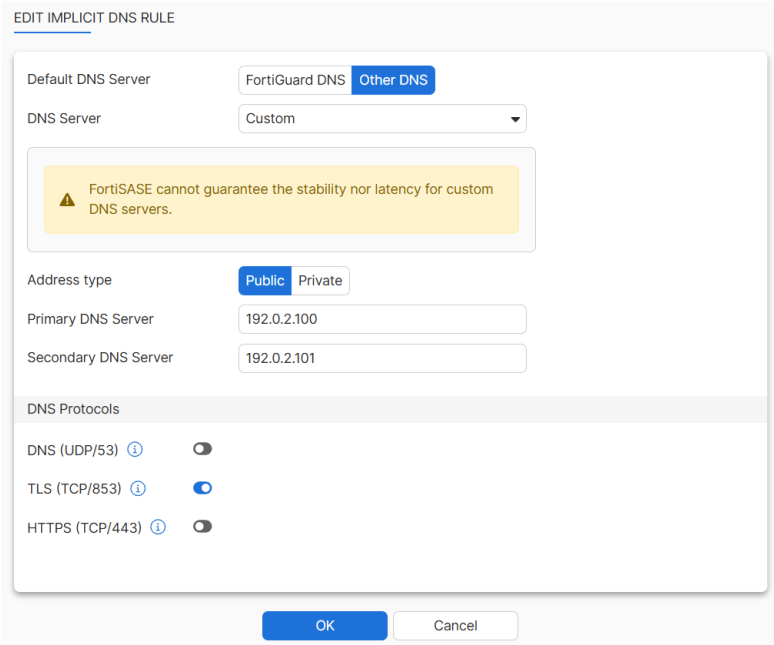
To configure a custom DNS server:

1. Go to *Network* > *DNS*, select the *All* implicit DNS rule, and click *Edit*.
2. In the *Edit Implicit DNS Rule* page, for *Default DNS Server*, select *Other DNS*.
3. From the *DNS Server* dropdown, select *Custom*.



4. In the *Primary DNS Server* and *Secondary DNS Server* fields, enter the respective IP addresses for the servers of your choice.

> The screenshot uses IP addresses for documentation and should not be used in a production environment.



5. Click *OK*.

Using FortiGuard DNS or another public DNS service is sufficient for most secure internet access (SIA) use cases that simply require remote users to resolve hostnames for external domains.

Considerations

- The *All* Implicit DNS rule does not apply to Proxy users. Proxy users always use FortiGuard DNS servers.
- FortiGuard DNS servers do not support DNS over TCP. If you require DNS over TCP, edit implicit DNS rules from the default FortiGuard DNS server to other DNS servers that support DNS over TCP.
- FortiSASE cannot guarantee the stability nor latency for custom DNS servers. These factors must be considered by the customer or provider maintaining the custom DNS servers.
- FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs in the DNS, RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with any BGP routing design.
  - Implicit and DNS redirection rules for agent traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.
  - When the SPA hub has been configured with BGP on loopback, you will also need to set *Access Type* to *Private* in the DNS, RADIUS or LDAP server settings.
  - Ensure that your FortiSASE remote users have access to the internal DNS server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.
- For edge devices, additional configuration is required to support DNS redirection rules and DNS filter functionality:
  a. Go to *Security* > *Traffic* > *Policies*.
  b. In the *Custom* section, edit the *Captive portal DNS traffic exemption (captive-dns-exempt)* policy.
  c. For *Profile Group*, select *Default* or select *Specify* and select a profile group with the DNS filter enabled.
  d. Click *OK* to save the policy changes.

DNS redirection rules

FortiSASE users often must resolve internal hostnames that public DNS servers cannot resolve in scenarios including but not limited to:

- Agent-based users are located within the organization's local network, also known as being on-net, and users must use an internal DNS server instead of a public DNS server.
- Agent-based, agentless, or Edge device users are located remotely, FortiSASE Private Access has been configured with secure private access (SPA) hubs, and users must use an internal DNS server behind the SPA hub.

To support these scenarios, you can configure FortiSASE DNS settings for DNS redirection using DNS redirection rules.

DNS redirection works as follows:

- Agent and agentless endpoints and endpoints connected to authorized edge devices forward all their DNS traffic to FortiSASE.
- FortiSASE performs transparent DNS redirection to redirect DNS traffic conditionally as desired.
- Selectively use an internal DNS server only when it is necessary to resolve hostnames for the specified internal domain(s). If you have multiple internal DNS servers in different geographical locations, you can configure remote users to use the internal DNS server that is closest to their region using *PoP DNS override*, which enhances the DNS response time.

- Resolve all other hostnames for external domains using the implicit DNS rule.

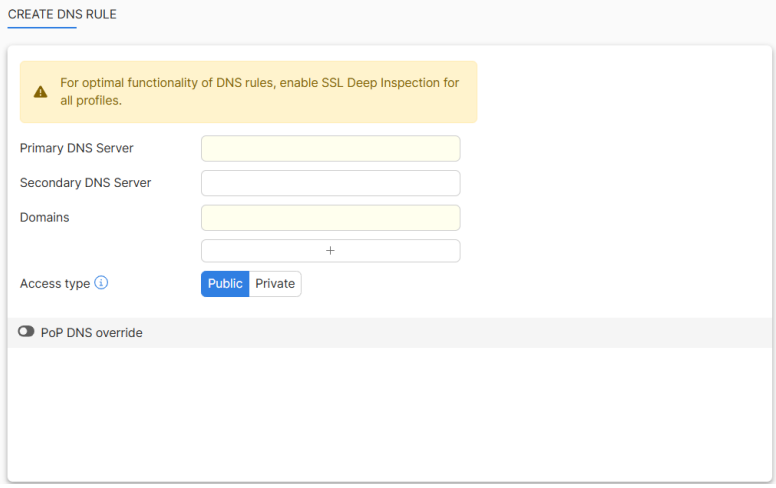
DNS redirection is more efficient than sending all DNS requests to DNS servers defined in the implicit DNS rules because it reduces any potential latency and downtime with using these DNS servers for resolving public hostnames if any issues arise with these limited availability and limited resource DNS server deployments. For resolving hostnames for external domains, DNS redirection can leverage the redundancy, extensive resources, and geographical coverage of public DNS servers with anycast capabilities.

To secure DNS requests, the DNS-over-HTTPS (DoH) protocol secures DNS requests and replies sent and received over HTTPS and works with public DNS servers that support this protocol. DoH is enabled by default on modern web browsers including Chrome, Edge, and Firefox and is supported by Google's public DNS servers, which is the default for upgraded FortiSASE deployments. Therefore, for DNS redirection rules to work with DNS servers that support DoH, you must enable SSL deep inspection for agent-based remote users on FortiSASE.

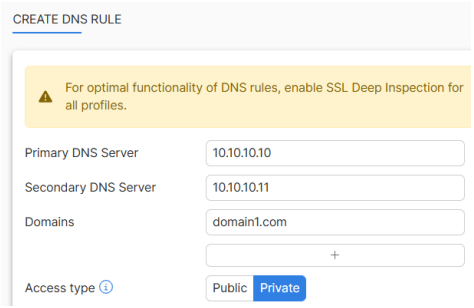
Configuring DNS redirection rules

To configure DNS redirection rules:

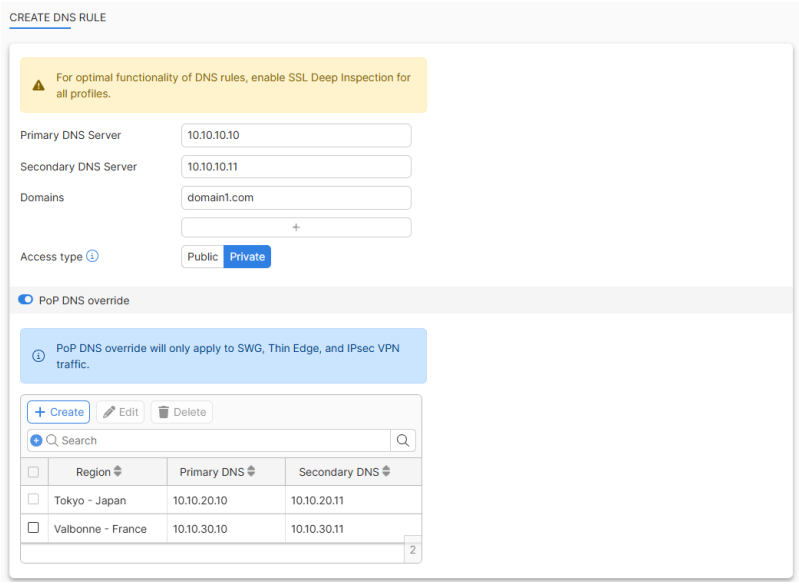
1. Go to *Network* > *DNS*.
2. Click *Create*.



3. In the *Create DNS Rule* pane, do the following:
   a. Enter the *Primary DNS Server*, (optional) *Secondary DNS Server*, and one or more *Domains*.
   b. (Optional) Click *+* to add more fields to enter in additional domains.
   c. The *Access type* field is only visible and required if you have SPA configured using *BGP on loopback* BGP routing design under *Network* > *BGP*. If the specified DNS server(s) are reachable via SPA, set *Access type* to *Private*. If the DNS servers are publicly accessible and not routed via SPA, set *Access type* to *Public*.



4. If you have multiple internal DNS servers spread geographically, enable *PoP DNS override* for remote endpoints to use geographically closest DNS server to them:
   a. Click *Create*.
   b. Select the *PoP* region using dropdown and specify the *Primary DNS Server* and (optional) *Secondary DNS Server*.
   c. Click *Submit*.
   d. Perform the same steps to configure different DNS server(s) per region. As shown, the remote endpoint closest to Tokyo-Japan region will use 10.10.20.10 and 10.10.20.11 as its DNS server, whereas remote endpoints closest to Valbonne-France region will use 10.10.30.10 and 10.10.30.11 as its DNS server, to resolve the domain domain1.com.



   Only two internal DNS servers are configurable per region for each domain. If the region does not appear in the list of security PoPs to use, the remote endpoint users uses the main *Primary* and/or *Secondary DNS Server* i.e. 10.10.10.10 and 10.10.10.11 to resolve the domain.
   e. Click *OK* to save the DNS redirection rule.
5. Observe that the DNS redirection rule has been created and displays in the table.

Prerequisites and considerations

Prerequisites

- DNS redirection requires enabling SSL deep inspection on FortiSASE so that FortiSASE can intercept the DNS traffic.
  - To confirm that you enabled SSL deep inspection, go to *Security > Security profiles* and at the top of the security profile group page, in the *SSL Inspection* section, confirm that it displays *SSL inspection: Deep inspection mode*.
  - To enable SSL deep inspection, go to *Security > Security profiles* and at the top of the security profile group page, in the *SSL Inspection* section, click *Configure SSL*. In the *SSL Inspection* pane, select *Deep inspection* and click *OK*.

  See Certificate and deep inspection modes on page 315.
- With deep inspection enabled, FortiSASE proxies traffic from the client. While being proxied, connections using secure protocols like HTTPS have their certificates replaced and signed by FortiSASE. To avoid seeing warnings and errors, the client must trust the signing certificate authority (CA) and have a valid certificate chain back to the root CA. Therefore, installing FortiSASE's CA certificate on the client's trusted certificate store is important.
  - FortiSASE supports automatically installing the FortiSASE CA certificate for agent-based users with FortiClient installed on their endpoints.
  - The FortiSASE CA certificate must be manually installed on endpoints for Proxy users and edge device users.
    - For Proxy users, installing this CA certificate is part of the Proxy onboarding process.
    - For endpoints using an edge device, installing this CA certificate is an additional step that they must perform.

  See Installing a certificate for deep inspection mode on page 317 for installing the FortiSASE CA certificate.
- Ensure that your FortiSASE remote users have access to the internal DNS server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.

Considerations

- For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring DNS redirection using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE will yield inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that DNS redirection is configured using an internal DNS server with a public IP address.
- DNS redirection supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.
- FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.
- Implicit and DNS redirection rules for agent traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.
- If you are using DNS redirection to resolve local domains using an internal DNS server with an SPA hub configured, to ensure access to the internal DNS server from FortiClient remote users you must have a Private Access policy configured that allows DNS requests to that specific server.

- Security PoP DNS override will only apply to Proxy, Thin Edge (edge device), and IPsec traffic.
- If you are using DNS redirection to resolve local domains using an internal DNS server with an SPA hub configured, then the Web Filter or DNS Filter blocks access to these local domains from FortiClient remote users if the Newly Observed Domain category is set to Block in the respective security component. In this case, you must create URL Filter entries for the Web Filter or Domain Filter entries for the DNS Filter to allow access to these local domains.
- For edge devices, additional configuration is required to support DNS redirection rules and DNS filter functionality:
  a. Go to *Security* > *Traffic* > *Policies*.
  b. In the *Custom* section, edit the *Captive portal DNS traffic exemption (captive-dns-exempt)* policy.
  c. For *Profile Group*, select *Default* or select *Specify* and select a profile group with the DNS filter enabled.
  d. Click *OK* to save the policy changes.
- FortiSASE supports DNS redirection (formerly known as split DNS) for SSL tunnels. With this feature, specific domains are resolved by the DNS servers assigned through the tunnel, while all other domains continue to be resolved by the DNS server configured in the FortiSASE portal in the *All Implicit DNS Rule*.
  - If DNS requests must be sent to a public DNS server that is not part of the VPN configuration, a steering bypass rule using a *Subnet* match type must be applied to allow those queries outside the VPN tunnel.
  - If DNS requests must be sent to an internal DNS server accessible via SPA, a split DNS rule with the domain and the internal DNS server must be configured in FortiSASE.
- DNS queries via agent tunnel are only possible to DNS servers explicitly assigned during the SSL tunnel connection.

Geofencing

You can configure FortiSASE to allow or block all remote user connections and edge device connectivity to FortiSASE's security point of presence (PoP) if they are initiated from specified countries/regions or infrastructures by configuring *Regional access to FortiSASE* under *Network* > *Geofencing*.

By default, with *Country/regions* set to *Allow all*, FortiSASE enforces no restrictions.

Before configuring *Regional access to FortiSASE*, you must configure geography hosts in *Security* > *Resources* > *Hosts*.

To configure a geography host:

1. Go to *Security* > *Resources* > *Hosts*.
2. Click *Create* > *Host*.
3. Configure these fields:

Field	Value
Location	Select a location for the host: • *Ingress*: internal hosts located within your organization's network. • *Internet*: external hosts located outside of your organization's network • *Private Access Hub*: hosts located within a secure private access hub

Field	Value
	• *Unspecified*: no specified location
Category	*IPv4 Host*
Name	Enter a unique host name.
Type	*Geography*
Country	Select a country.

4. Click *OK*.

To configure Regional access to FortiSASE:

1. Go to *Network* > *Geofencing*.
2. On the *Regional access to FortiSASE* tab, for *Country/regions*, select one of these options:

Option	Description
Allow all (default)	Allow remote and edge connections to FortiSASE for all countries or regions.
Allow specified	Allow remote and edge connections to FortiSASE initiated from specified countries/regions only. Otherwise, deny connections initiated from all other countries or regions.
Deny specified	Block remote and edge connections to FortiSASE initiated from specified countries/regions only. Otherwise, allow connections initiated from all other countries or regions.

3. If you selected *Allow specified* or *Deny specified*, click + to add a country or region.
4. In the *Select Entries* slide-in, only hosts with the *Geography* type display. Select one or more locations to apply the restriction to.
5. Click *Close*.
6. Click *Submit*.

Regional compliance

Regional compliance rules configurable in *Network* > *Geofencing* under the *Regional compliance* tab allow you to control and prioritize routing a remote user's tunnel connection attempts to the following connection types

Connection type	Description
On-premise device	On-premise device (gateway). FortiSASE does not manage this device's configuration. Either FortiSASE instances enabled with SSL remote user support or IPsec remote user support are supported. For IPsec, the pre-shared key must be configured the same for the FortiSASE Cloud Security tunnel and for the on-premise FortiGate gateway used for regional compliance.
Security PoP	A security PoP is FortiSASE's managed security PoP in a specific region.

Connection type	Description
	Successful connection to this connection type establishes secure internet access (SIA).

Tunnel connection workflow

FortiSASE follows the following workflow to enable remote users to establish a tunnel connection to an on-premise device or security PoP connection:

1. **Determine country or region**: FortiSASE identifies the remote user's originating country or region based on their public IP address.

   > ⚠ Adding countries/regions to a regional compliance rule involves backend updates that take time to propagate and take effect. Therefore, ensure you select only the countries/regions required for your regional compliance rules.

2. **Check Regional access to FortiSASE**: FortiSASE verifies whether the settings configured in *Network > Geofencing* under the *Regional access to FortiSASE* tab permits the detected country or region.
3. **Select a Regional compliance rule**: If settings configured in *Network > Geofencing* under the *Regional access to FortiSASE* tab allow the detected country or region, FortiSASE selects a rule from the rule list configured in *Network > Geofencing* under *Regional compliance*. FortiSASE selects the rule by matching the remote user's originating country or region with the *Source countries/regions* specified in regional compliance rules.
4. One of the following occurs:
   - **Attempt to establish a tunnel connection**: if FortiSASE selects a regional compliance rule, FortiClient attempts to establish a tunnel connection to the specified tunnel connection type, on-premise device or security PoP, defined within the rule. FortiClient attempts connecting to connections listed under the *Permitted connections & priority* table in the order that they are listed, preferring connections higher on the list to those lower down. If a connection attempt fails, FortiClient proceeds to the next tunnel connection in the priority list. This repeats in a round robin fashion until FortiClient establishes a connection.
   - **Fallback to default FortiSASE security PoP**: if FortiSASE does not select a regional compliance rule, the remote user tries to connect to their closest FortiSASE security PoP. See Security PoPs on page 791.

> 💡 A remote user from a country or region specified in a regional compliance rule only attempts to connect to the tunnel connections explicitly defined in the rule. There is no automatic fallback to the geographically closest security PoP unless the rule explicitly includes those alternative security PoPs.

Health check and failover

To ensure the availability of connections of type *On-prem device*, FortiSASE continuously performs health checks every one to two minutes via ICMP or ping probes directed at the remote gateway IP address configured for the device.

Ensure that the on-premise device allows ICMP or ping probes so that FortiSASE can successfully perform health checks.

If an on-premise device becomes unavailable or unresponsive to health checks, FortiSASE automatically updates the DNS record for its domain. The DNS update ensures that the remote user's tunnel connection attempts resolve and direct to the next available connection under the *Permitted connections & priority* table.

The time required for a remote endpoint to failover to the next available connection varies and depends on the following factors:

Factor	Description
On-premise device failure detection	FortiSASE identifies an on-premise device as being down within one to three minutes based on the results of the ICMP and ping probes.
DNS cache	The A record for FortiSASE's domain name has a TTL of 300 seconds (5 minutes). Thus, endpoints transition to the updated DNS record once the old cache expires.

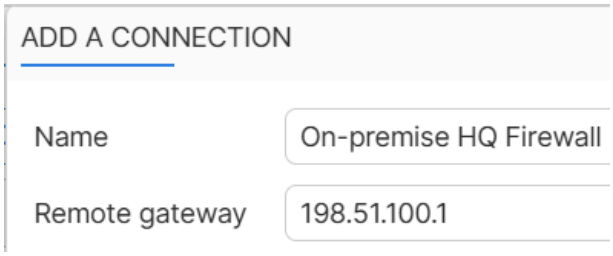
Therefore, the entire failover process typically takes between three to eight minutes to occur.

To determine the FortiSASE domain used for your FortiSASE instance, do the following:

1. Go to *Access & authentication > SSO*.
2. View the URL in the *Base URL* field and note the domain name after the https:// string.

To configure Regional compliance rules per source country or region:

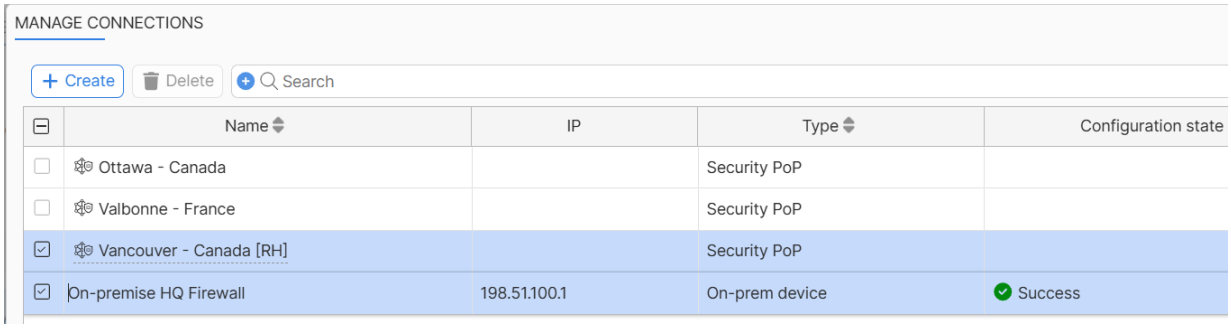
1. Go to *Network > Geofencing*.
2. Under the *Regional compliance* tab, click *Create*.
3. Enter a suitable *Name* for the *Regional compliance rule*.
4. For *Countries/regions*, click *+* and select the desired countries and regions. This compliance rule applies only to remote users whose public IP address is in a selected country or region.
5. Under *Permitted connections & priority*, click *Manage connections* to add an on-premise device or security PoP connection:
   a. Review the available security PoP tunnel connections for each selected country or region.
   b. To create an on-premise device connection, do the following:
      i. Click *Create*.
      ii. Enter the desired name.
      iii. In the *Remote gateway* field, enter the on-premise device (i.e. gateway)'s public IP address.



      iv. Click *OK*. The new connection displays on the *Manage connections* slide-in with *On-prem device* as its value in the *Type* column.

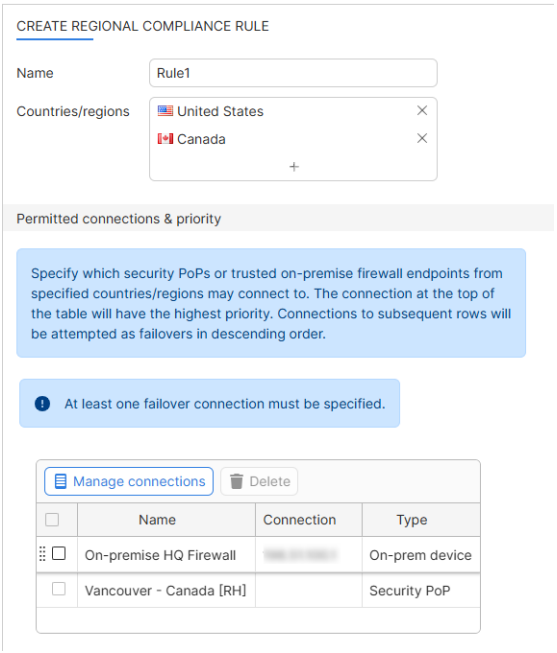
v. (Optional) Repeat these steps to add more on-premise device connections.

c. Select the desired tunnel connections that remote users from the specified countries and regions must attempt connection to.

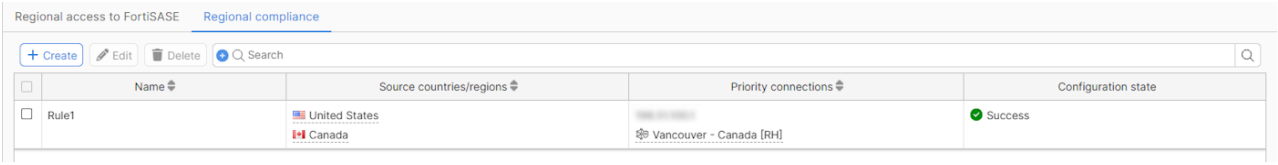


d. Click *Add selected*. The selected tunnel connections display under the *Permitted connections & priority* table.

6. Review the sequence of connections listed under the *Permitted connections & priority* table. A remote user whose public IP address is from a specified country or region attempts the tunnel connections in the table from top to down. To reprioritize the connections, use the drag-and-drop feature beside the checkbox in the left column.



7. Click *OK*. FortiSASE takes a few seconds to apply the configuration. The *Configuration state* changes from *Updating* to *Success*.



8. Create other *Regional compliance* rules for other source countries and regions as desired. For a remote user whose country or region does not have an associated *Regional compliance* rule, FortiClient attempts to connect to their closest FortiSASE security PoP. See Security PoPs on page 791.

Default tunnel settings

If FortiSASE is configured to use single sign on (SSO) for user authentication to connect to a security PoP connection (i.e. SIA), then you must enable SSO on their on-premise device(s).

The tunnel settings for SSL VPN that FortiSASE uses are as follows:

- FortiClient versions that FortiSASE supports use SSL on TCP port 443 to connect to security PoP connections such as SIA. You must configure the SSL port on your on-premise device as TCP port 443.
- This feature uses the same turbo URL to connect to on-premise device and security PoP connections. To view the turbo URL used for your FortiSASE instance, go to *Access & authentication > Authentication Sources > SSO > Agent* and note the URL in *Base URL*. To prevent any SSL certificate warnings on endpoints when FortiClient attempts to connect to on-premise device connections, do the following:
  a. Go to *Endpoint management > Endpoint profiles*.
  b. Select desired endpoint profile and click *Edit*.
  c. Under *Connection*, click *SSL-VPN settings*.
  d. Enable *Accept invalid server certificate*.
  e. Click *OK*.

Prerequisites and considerations

Prerequisites

- Configuring regional compliance rules requires an Advanced or Comprehensive FortiSASE remote users subscription. See the FortiSASE Ordering Guide.
- When upgrading your instance from a Standard subscription to an Advanced or Comprehensive subscription, you must explicitly request the enablement of dedicated public IP addresses on your FortiSASE. See Subscriptions on page 786.

Considerations

The FortiSASE portal does not allow:

- Creating new *Regional compliance* rules while *Configuration state* for other regional compliance rules is in an *Updating* state.
- Deleting multiple *Regional compliance* rules configured under the *Regional compliance* tab. If required, you can delete rules one at a time.

IP management

Network > IP management displays the following:

- *Public IP (Security PoP IP Addresses)*
- *IPAM*
- *Advanced*

Public IP

The Public IP (Security PoP IP Addresses) tab displays the following:

- Security Public IPs
- Analytics Public IPs
- Public IP Feed



Host or server destinations for FortiSASE remote user and edge device traffic can use these IP addresses for allowlisting or blocklisting.

Dedicated public IP addresses unique to the instance display and provided in the IP address feed for FortiSASE instances with dedicated public IP addresses, namely, instances with the Standard, Advanced or Comprehensive subscription.

See Dedicated public IP addresses on page 17.

For the *Public IPs* sections, a table of the Security PoP and its corresponding public IP addresses is shown.

For the *Public IP Feed*, you can use the listed URL as an REST API endpoint accessible via a GET request with a software tool such as Postman or curl. To access the IP feed you must use a FortiCloud IAM API user token. See API users. The public IP feed includes security PoP public IPs, analytics public IPs, and other infrastructural public IPs.

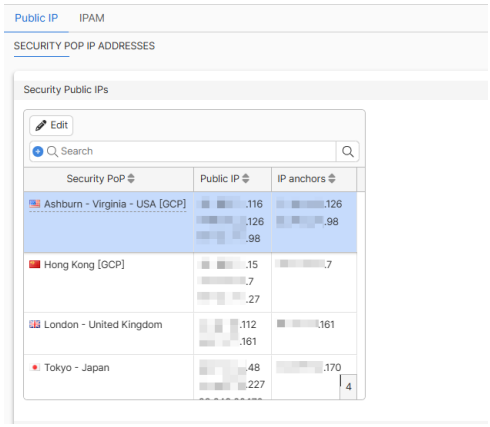
Editing security PoP public IP addresses

If your FortiSASE instance meets the prerequisites to support editing security PoP public IP addresses, you can edit the following from the FortiSASE portal:

- Geolocation tag for a security PoP public IP address
- Geolocation tag and source criteria (country/region and users/user groups only) for an IP anchor

To edit a geolocation tag for a security PoP public IP address:

1. Go to *Network* > *IP management*.
2. In *Security Public IPs*, select a security PoP and click *Edit*. The example selects the *Ashburn - Virginia - USA [GCP]* security PoP.



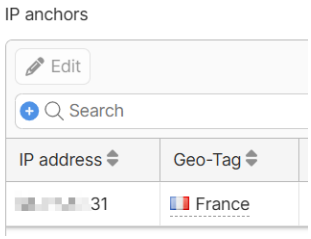
3. In *Edit Security PoP Public IP*, under the public IP address, notice the default country set under *Geolocation tag* for that public IP address. For example, for *Ashburn - Virginia - USA [GCP]*, the *Geolocation* tag is set to the *United States*. Thus, by default *Geolocation tag* is set to the same country/region as the Security PoP.



4. Use the dropdown menu to change the *Geolocation tag* and select the desired country.
5. Click *OK*.
6. Click *Save*.

To edit a geolocation tag and source criteria for an IP anchor:

1. Go to *Network > IP management*.
2. In *Security Public IPs*, select a security PoP and click *Edit*.
3. In *Edit Security PoP Public IP*, in *IP anchors*, select an IP anchor and click *Edit*. For example, select the *IP address* ending in *.31* with *Geolocation tag* set to France.



4. In the *Anchor IP* pane, observe the source criteria options of *Country/region* and *Users*.
5. Set the source criteria as follows:

Field	Value
Country	Select the source country of endpoint. For example, *Canada*.
Users	Select the desired users or user group. For example, *LDAP-grp*.
Geolocation tag	Canada

6. This configures the IP anchor for this instance such that remote user traffic from Canada egresses from the public IP ending in *.31* and configures the public IP ending in *.31* with a *Geolocation tag* of Canada.
7. Click *OK*.
8. Click *Save*.

To validate geolocation tag changes for a public IP:

After about one week (time can vary depending on the provider), you can validate a geolocation tag change for a public IP has taken effect by checking the current geolocation of the public IP using public sources such as the FortiGuard IP Geolocation Service.

To validate geolocation tag for an IP anchor:

Source criteria changes are applied immediately after being configured.

After about one week minimum (time can vary depending on the provider), you can check geolocation tag changes for an IP anchor have taken effect as follows:

1. With an endpoint whose security PoP matches the source criteria (country/region) for the updated IP anchor, establish a connection to FortiSASE.
2. Check the endpoint public IP by using the endpoint web browser to go to a public IP checking source such as IPinfo My IP or WhatIsMyIP.com.
   a. Validate that the public IP matches the Will egress from public IP configured in the IP anchor settings.
   b. Validate that the public IP current geolocation matches the geolocation tag configured in FortiSASE.

Prerequisites

This feature is only supported for an instance with these features enabled and subscriptions applied:

- Instance has been provisioned with Feature version support
- IPsec remote agent support
- Remote agent and edge device user identification
- Instance with a Standard, Advanced, or Comprehensive subscription
- For source IP anchoring, you must purchase another Dedicated Public IP add-on subscription with additional dedicated IP addresses beyond the initial number of dedicated IP addresses per PoP. The additional dedicated IP addresses can be allocated as desired for source IP anchoring rules such as all in a single security PoP, one per security PoP, or any combination in between.

Considerations

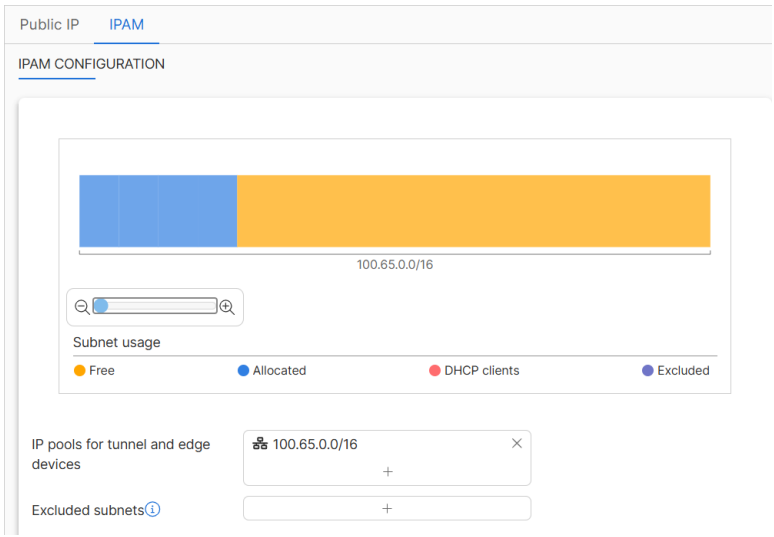
- Using this feature, geolocation tags for a specific public IP or IP anchor can be updated once every 30 days.
- Each geolocation tag change may take up to two weeks minimum (time can vary depending on the provider) to propagate and take effect. See Geolocation rules.
- By default, the Geolocation tag is set to the same country/region as the Security PoP.
- When using Microsoft Entra ID conditional access policies to restrict access to Entra ID cloud resources for remote users connected to a FortiSASE instance with dedicated IP addresses, defining the IPv4 address ranges of these dedicated IP addresses for these policies is recommended.

IPAM

The *IPAM* tab displays *IPAM configuration*.

With Remote agent and edge device user identification on page 24 enabled, a FortiSASE instance supports unique IP address ranges for remote agents and edge endpoints per FortiSASE security PoP using IP address management (IPAM) within the overall 100.65.0.0/16 range, by default.

FortiSASE automatically attempts IP conflict resolution as needed. Conflicts can also be minimized by excluding known utilized subnets, such as those assigned to on-premise networks.



You can view a chart representing IPAM subnet usage.

Subnet usage	Description
Free	Subnets managed by IPAM and unallocated
Allocated	Subnets managed by IPAM and allocated
DHCP clients	Subnets managed by IPAM and used by DHCP clients
Excluded	Subnets explicitly excluded from being managed by IPAM

Hovering the mouse over each subnet shows subnet details.

The chart can be enlarged as desired using the slider.

You can select subnets from the following private IP pools in the *IP pools for tunnel and edge devices* field:

- 100.65.0.0/16 (default)
- 10.0.0.0/8
- 100.64.0.0/10
- 172.16.0.0/12
- 192.168.0.0/16

You can specify *Excluded subnets*. FortiSASE does not assign agents and edge endpoints IP addresses within these address ranges.

Considerations

- After you update any IPAM configuration fields and save those changes for an instance, its remote agent and edge device users must manually disconnect and reconnect their user connections to FortiSASE. Otherwise, they experience internet and private access traffic disruptions. Therefore, consider configuring these IPAM configuration changes for scheduled maintenance windows outside of remote end users' typical work hours.
- While you select the private IP address pools from the aforementioned supernet subnets, with IPAM configured, the specific IP address allocations within the configured supernet subnets may vary based on

the FortiSASE components and configuration options enabled including SSL and IPsec, Thin Edge, and data center cloud type. The maximum number of SSL and IPsec remote agents per security PoP is 4096 (/20) by default. If you must exceed the specified IP address range due to allocation issues, open a FortiCare Support ticket.

- You must add a customer subnet that falls within the IPAM subnet as an entry in *Excluded subnets*. Otherwise, the customer subnet becomes inaccessible when you configure secure private access.
- *Excluded subnets* does not support /28 to /32 subnet masks.
- If allocating only 100.65.0.0/16 to restore the default subnet after having previously changed it to another subnet, please select 100.64.0.0/10 and exclude the following subnets:
  - 100.64.0.0/16
  - 100.66.0.0/15
  - 100.68.0.0/14
  - 100.72.0.0/13
  - 100.80.0.0/12
  - 100.96.0.0/11
- When excluding subnets from the IPAM pool, you must leave a /20 subnet mask free for each security PoP and a /24 subnet mask free for each Edge device. This ensures that there are sufficient IP addresses to assign to each security PoP and Edge device. With IPAM, you cannot control which /20 subnet mask is assigned to which security PoP.
- IPAM automatically allocates subnets to support remote users, edge device communication, and IP anchors. Each IP anchor configured for multiple security PoPs requires a dedicated private address space per security PoP, which can lead to rapid consumption of the available pool.
  - As more security PoPs, edge devices, or anchors are added, the available IP space may be exhausted. To accommodate additional resources, you must plan carefully and configure IPAM to use a larger address pool that provides greater subnetting capacity at the time of initial IPAM configuration. Any modification to the IP pools after initial IPAM configuration will introduce outages for endpoints of the FortiSASE instance.
  - If IP anchors are used, then either the 100.64.0.0/10 or 172.16.0.0/12 IP pools should be specified for an instance's IPAM configuration instead of the default IP pool of 100.65.0.0/16.
- FortiSASE uses IP address management (IPAM) to automatically configure IP address or netmask settings for clients connected to edge devices with a subnet within the specified IP pools for tunnel and edge devices which cannot be manually configured for each edge device and is allocated without VLAN capability.

Advanced

The *Advanced* tab displays the following:

- FortiExtender and LAN Extension control plane subnet:
  - After the 26.1.1 Feature release, FortiExtender devices will be assigned a management address from this subnet. This can be configured to avoid addressing conflicts with your on-prem network. This subnet defaults to 10.252.0.1/16.
    - Prior to customization, by default, the management subnet of 10.253.0.0/16 is reserved, in addition to the subnet that is visible on the page (default: 10.252.0.0/16).

    - Once a custom subnet has been configured, the previously reserved management subnet of 10.253.0.0/16 is also removed.
    - Currently, the custom FortiExtender and LAN Extension control plane subnet is overwritten back to the default of 10.252.0.0/16 when BGP configuration is saved. You must save the custom FortiExtender and LAN Extension control plane subnet again from *Network > IP management > Advanced*.
  - Before the 26.1.1 Feature release, the following management subnets were reserved and could not be configured through the portal:
    - 10.252.0.0/16
    - 10.253.0.0/16

BGP

In *Network > BGP*, you can configure BGP settings. BGP settings are used when you configure secure private access and on-ramp tunnel in FortiSASE. BGP settings are described in the relevant sections in this guide for these configurations:

- SPA on page 101
- On-ramp tunnel on page 196

Advertise Hub Priorities

When using multiple secure private access (SPA) Hubs in FortiSASE, intelligent hub selection is critical to ensure reliable and optimized traffic routing. The topic explains how a FortiSASE security PoP selects a hub and advertises its hub priority level using BGP community to influence routing decisions in network core.

Hub Health and Priority

One of the available hub selection methods is *Hub Health and Priority*, configurable under *Network > BGP*. If you configure multiple SPA hubs and set *Hub Selection Method* to *Hub Health and Priority*, the FortiSASE security PoPs selects a hub based on SLA compliance and the configured hub priority. The selection process is as follows:

1. The security PoP evaluates all service connections to the hubs to determine which ones meet the minimum SLA thresholds.
2. Among the connections that meet the minimum SLA thresholds, the security PoP selects the hub with the highest priority. A lower numeric hub priority value has a higher priority. For example, P1 is preferred over P2 is preferred over P3 and so on. To update the hub priority for a security PoP, see Updating service connection priorities on page 124. To edit the SLA threshold for a security PoP, see Editing SLA thresholds on page 121.

Encoding hub priority into BGP community

FortiSASE can advertise hub priorities and communicate a security PoP's SLA compliance status to its hub(s) by encoding it into BGP community strings. The format of the BGP community string advertised depends on the configured autonomous system number (ASN), the hub priority, and whether the SLAs are satisfied:

Are SLAs satisfied?	Format of BGP community string advertised
Yes	Consider that a security PoP is configured to use a hub priority of PX, where X is the priority value from 1 to 12, and the ASN is configured in *FortiSASE ASN* under *Network > BGP*.In this case, the BGP community that the security PoP advertises to the hubs follows this format: ASN:Y Where Y=5*X Therefore, when hub priorities range from 1 to 12, the value for Y is between 5 to 60 (5, 10, 15, ...60). For example, if FortiSASE belongs to AS 64512 and a security PoP has the hub priority of a Hub configured as P4, the equivalent encoded BGP community string advertised by the security PoP to that hub is 64512:20.
No	If the SLA threshold are not met, FortiSASE signals a degraded or non-preferred path by using a hub priority value of 9999. In this case, the BGP community that the security PoP advertises to the hub is: ASN:9999

Advertising hub priorities

FortiSASE security PoPs can advertise their configured hub priorities and SLA status to their associated hub(s) using BGP community. These BGP community values can be advertised further into a hub's network core to enable routing decisions in the network core using BGP community strings. To enable advertising the hub priority, enable *Advertise Hub Priorities* under *Network > BGP > Advanced BGP Settings*, and click *Save*.

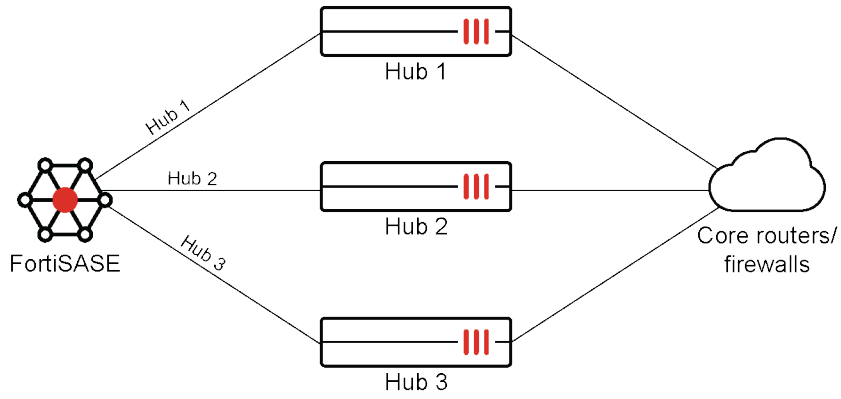
Once enabled, the following happens:

1. FortiSASE encodes each security PoP's configured hub priority into a BGP community string. See Encoding hub priority into BGP community on page 282.
2. This BGP community string is attached to the remote user pool prefix in the format ASN:Y when security PoPs advertise their remote user pool prefix to the hub(s).
3. FortiSASE monitors the SLA status of each security PoP. If the SLA is not satisfied, the security PoP signals a degraded or non-preferred path to the hub(s) by using BGP community string of ASN:9999. This signals the SLA failure to the hub and hub's network core.

The following diagram shows an example scenario. This scenario is as follows:

- ASN: 64512
- Security PoPs:
  - London
    - Service connection: Hub1
      - Hub priority: P1

    - Service connection: Hub2
        - Hub priority: P2
- Vancouver
    - Service connection: Hub1
        - Hub priority: P2
    - Service connection: Hub2
        - Hub priority: P1



The BGP community advertised to the hubs differ depending on whether the SLA is met or not met. The following table details the different possible BGP communities:

Hub	BGP community advertised			
	SLA is met	**SLA is not met on Vancouver security PoP**	**SLA is not met on London security PoP**	**SLA is not met on both Vancouver and London security PoPs**
Hub1	• London security PoP: 64512:5 • Vancouver security PoP: 64512:10	• London security PoP: 64512:5 • Vancouver security PoP: 64512:9999	• London security PoP: 64512:9999 • Vancouver security PoP: 64512:10	• London security PoP: 64512:9999 • Vancouver security PoP: 64512:9999
Hub2	• Londonsecurity PoP: 64512:10 • Vancouver security PoP: 64512:5	• London security PoP: 64512:10 • Vancouver security PoP: 64512:9999	• London security PoP: 64512:9999 • Vancouver security PoP: 64512:5	• London security PoP: 64512:9999 • Vancouver security PoP: 64512:9999

This mechanism allows FortiSASE security PoPs to signal a hub's priority and SLA status to upstream hubs by encoding it into specific BGP community values. This is of value in the following scenarios:

- The hub(s) advertise the received BGP communities from security PoPs to its BGP peers in its network core (e.g., data center or backbone routers), which you can then configure to prefer BGP neighbors (i.e. hubs)

advertising a higher priority community. This steers return traffic to a higher priority hub.
- Sending real-time priority signals in events when SLAs violations occur by using the BGP community string of ASN:9999, enabling the network core to react by deprioritizing the affected hub that advertises that BGP community. This steers return traffic to an SLA-compliant Hub instead.

Therefore, to leverage this feature, ensure that your network core routers are configured to recognize and match the BGP community strings based on the configured hub priority and to prefer a BGP peer (i.e. hub) that is most optimal for return traffic.

Prerequisites

- FortiSASE and SPA Hubs must operate within the same ASN. Therefore, you must configure SPA hubs to use the FortiSASE ASN. You must configure the setting that the SPA hubs belong to as the FortiSASE ASN under *Network > BGP*.
- This feature supports both BGP per overlay and BGP over loopback. This feature is available only when you configure *Hub Selection Method* as *Hub Health and Priority*.

BGP MED Setting

FortiSASE now supports enabling the BGP Multi-Exit Discriminator (MED) options always-compare-med and deterministic-med to improve route selection when multiple Secure Private Access (SPA) Hubs advertise the same prefix.

In multi-hub SPA deployments, particularly when receiving prefixes from SPA Hubs in different autonomous systems (ASes), the default BGP behavior may ignore MED values during prefix comparison to select a SPA Hub. This can lead to suboptimal path selection, where the preferred SPA Hub is not chosen based on MED priorities.

The following BGP MED options can be enabled or disabled.

- *Always Compare MED*: It forces BGP to evaluate MED values for routes received from different ASes, ensuring that MED is a consistent decision factor regardless of AS origin.
- *Deterministic MED*: It standardizes MED comparisons by grouping routes by their neighboring AS before selecting the best path, ensuring consistent and predictable results when multiple routes have the same prefix but different MED values.

To configure BGP MED Setting:

1. Navigate to *Network > BGP*.
2. Under *Advanced BGP settings > BGP MED Settings*, enable the required setting for your FortiSASE Security PoPs.
3. Click *Save*.

The *BGP MED Settings* options is a select availability feature and not visible in the FortiSASE portal by default. See Select availability features on page 39.

To enable this feature for a new or existing FortiSASE instance, submit a request to FortiCare Support by creating a new support ticket.

Proxy configuration

You can enable proxy. When you enable proxy, you can have end users configure their client software, such as a browser, to proxy all of its traffic through FortiSASE. You must manually send the proxy server information to end users. End users then configure their browser to send requests directly to the proxy server.

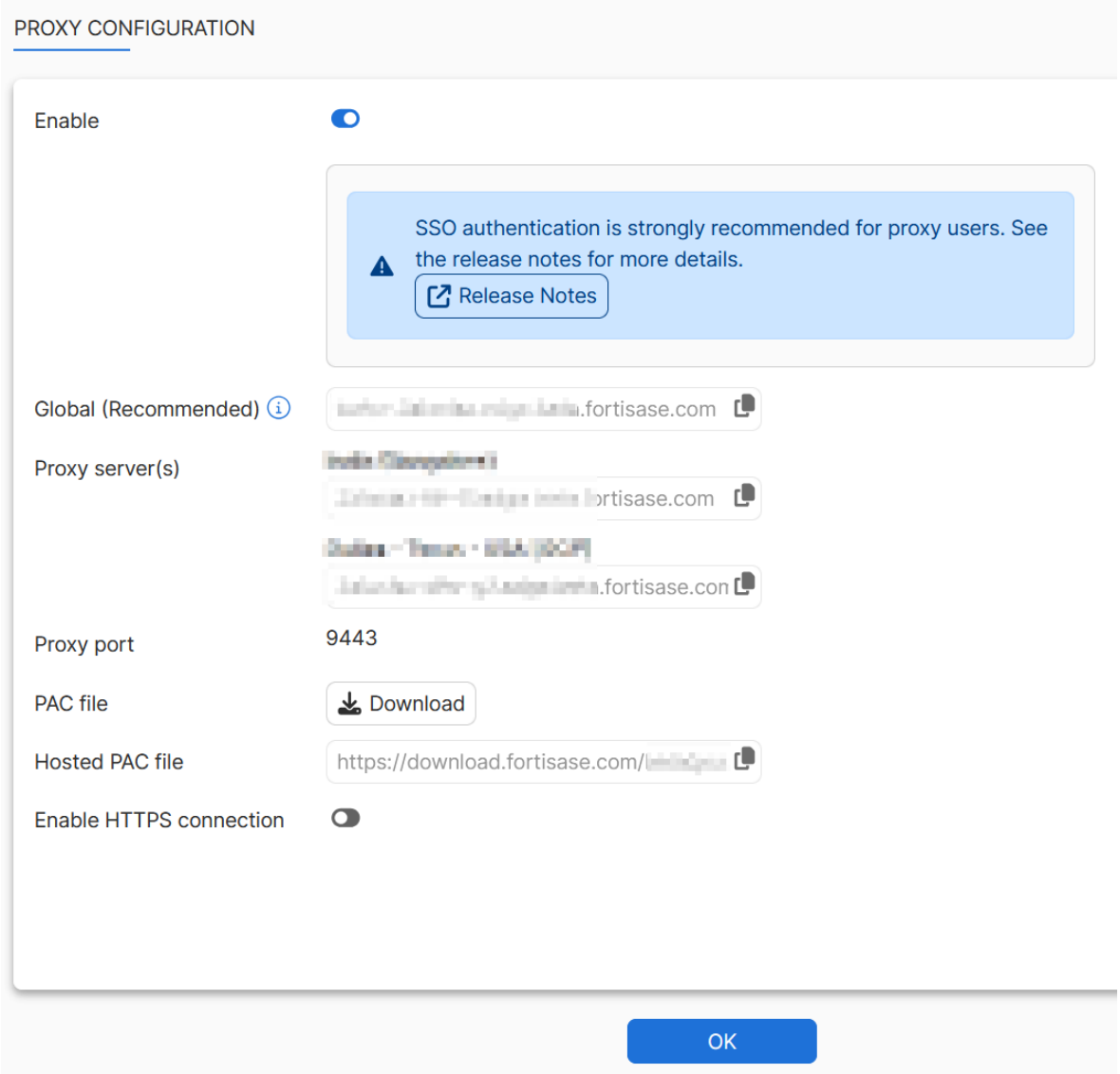
To enable proxy:

1. Go to *Network* > *Proxy configuration*.
2. Toggle *Enable* to on. Click *OK*. The GUI may take a few minutes to reload. Once the GUI finishes loading, you can view the *Hosted PAC file* URL, which users use to configure the proxy server on their endpoints. You can also view the default proxy policies and create custom ones in *Security* > *Traffic* > *Proxy policies*. See Proxy policies on page 302.
3. If you are using a FortiSASE instance provisioned after the 25.3.a release, Secure Proxy is enabled by default. With Secure Proxy, the browser established a secure HTTPS connection between the web client and FortiSASE and sends all HTTP requests to the proxy over HTTPS.

   The *Secure Proxy* best practice is recommended to be run in these cases:

   - If Proxy has been enabled without *Enable HTTPS connection* enabled before 25.3.c, then it is recommended to run the *Secure Proxy* best practice from the *Operations* > *Software audit & version* to migrate to using Secure Proxy.
   - If Proxy has been enabled with *Enable HTTPS connection* in either 25.3.a or 25.3.b, then it is recommended to run the *Secure Proxy (Refresh)* best practice from the *Operations* > *Software audit & version* to migrate the default PAC file for Secure Proxy.
   - After the best practice for *Secure Proxy*/*Secure Proxy (Refresh*) has been run, the *Enable HTTPS connection* option is hidden from the *Proxy configuration* page.

     See Secure proxy migration on page 293.



The above screenshot shows the *Enable HTTPS connection* option from 25.3.a. However, this option is hidden after running the best practice for secure proxy migration.

Prerequisites and considerations

Prerequisites

- For proxy single sign on (SSO) users, at least one proxy policy using SSO authentication must have deep inspection enabled in the configured security profile group. SSO authentication requires deep inspection to work.
  - Any traffic from proxy SSO users that is destined for hosts or URL categories defined as deep inspection exemptions does not work.
  - You must not configure proxy policies using SSO authentication with certificate inspection.

  - If a proxy policy requires certificate inspection, you must not configure SSO authentication in that policy.
- Possible intermittent network changes may be experienced when using a customized PAC file in these cases:
  - After enabling Secure Proxy
  - After refreshing Secure Proxy
  - When using a new FortiSASE instance provisioned after the 25.3.a release

  Therefore, to ensure proxy user connectivity with customized PAC files, you must perform these steps:

  a. Using the PAC editor in *Network* > *Proxy configuration* > *Hosted PAC files*:
    i. Edit the default PAC file as needed. By default, hosted PAC files include common SSO IdP destinations that must be excluded from being forwarded to the FortiSASE Proxy and go directly to the internet to ensure SSO authentication is functional.
    ii. Download it via *Download* > *Download directly*.

  b. You must deploy the PAC file by copying it to the self-hosted server and updating the proxy configuration of endpoints to refer to the self-hosted PAC file.

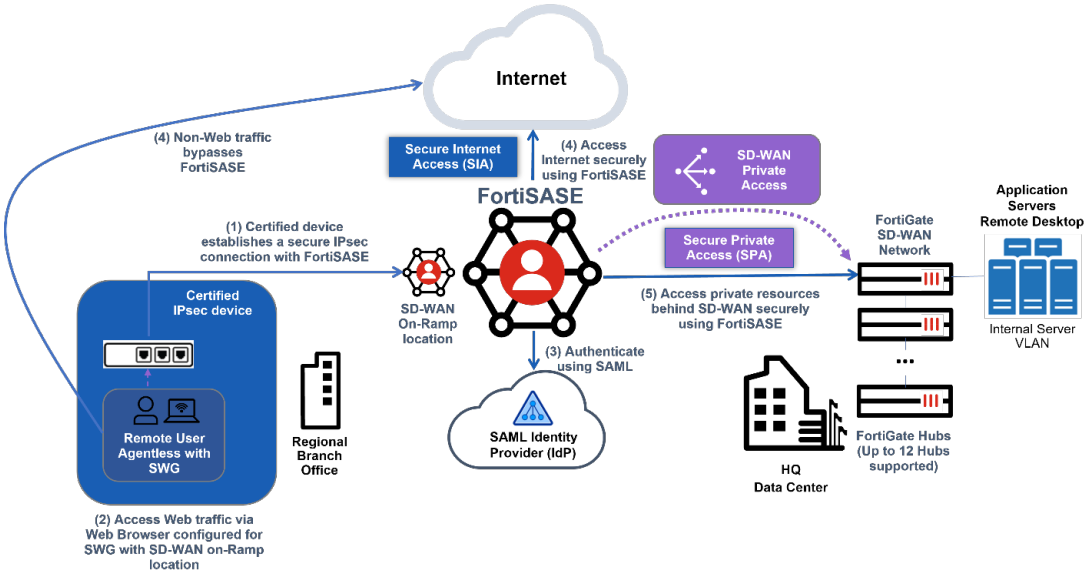
  See PAC file customization on page 737.

Considerations

- SSO authentication is strongly recommended for proxy users.
- Upon enabling a dedicated IP address for an instance, the proxy port number changes to 9443.
- Proxy mode does not support DNS filter.
- The *Secure Proxy* best practice is recommended to migrate instances with Proxy functionality previously enabled. See Secure proxy migration on page 293.
- After the best practice for Secure Proxy has been run, the *Enable HTTPS connection* option is hidden from the *Proxy configuration* page.
- For existing instances, Private Proxy using SSO authentication is not compatible with these configuration changes:
  - Secure proxy migration
  - Disable and then re-enable Proxy from *Network* > *Proxy configuration*
- Proxy mode is not supported on iOS devices.

Private proxy

FortiSASE supports private proxy. Similar to proxy, private proxy requires end users to configure their client software, such as a browser, to proxy all of its traffic through FortiSASE. With proxy, clients send proxied traffic to FortiSASE over the Internet. With private proxy, clients route their traffic to an on-premises Branch On-ramp device, which further routes traffic to an encapsulated and encrypted tunnel to FortiSASE. This configuration ensures traffic in transit between the proxy client and FortiSASE is secure.



Similar to proxy, private proxy allows users to access the Internet securely over HTTP and HTTPS protocols and to access private resources securely behind a FortiSASE SPA hub.

Prerequisites and considerations

See Prerequisites and considerations on page 288.

Prerequisites and considerations

Private proxy is essentially still a proxy configuration. Therefore, Prerequisites and considerations on page 286 for proxy still apply. The prerequisites and considerations listed below are specific to private proxy.

Prerequisites

Using private proxy requires the following:

- This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
- Branch On-ramp must be licensed and configured. Therefore, a dedicated IP address must be implemented for an instance and licensed accordingly. See Prerequisites and considerations on page 197 for Branch On-ramp.
- (Optional) If private resources must be accessed by private proxy users, then secure private access must be licensed and configured. See SPA on page 101.
- BGP configuration must be configured before enabling private proxy. No SPA license is required to perform this configuration.
- A supported Branch On-ramp IPsec device is on-premises, is configured, and is connected successfully to a Branch On-ramp security PoP.

- Each proxy client in the LAN environment of the On-Ramp IPsec device has a proxy configuration that uses the private proxy primary IP address in the manual proxy configuration or replacing the turbo URL in a PAC file.
- The FortiSASE administrator must choose and configure Primary and Secondary IP addresses that will serve as the private proxy server destinations on all On-Ramp nodes.

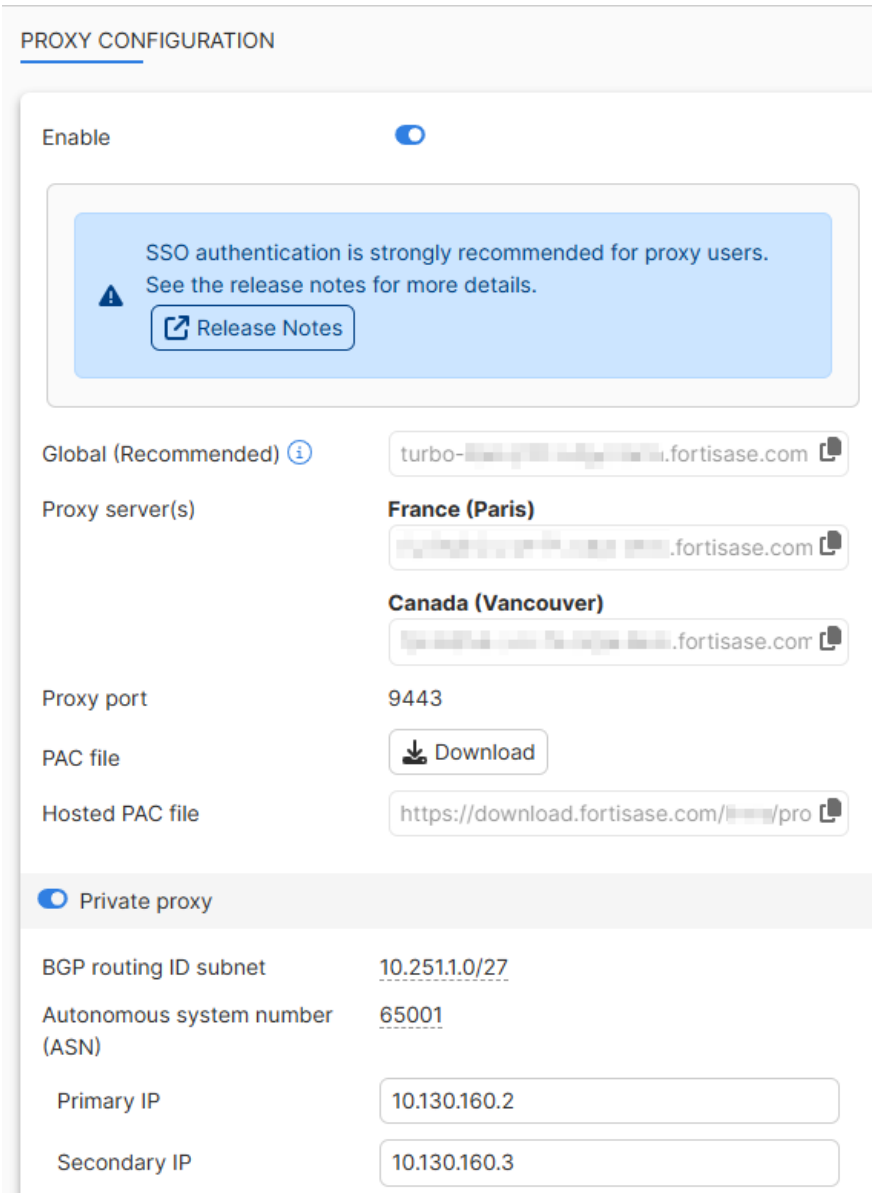
Considerations

- IP-based authentication for private proxy users is supported only when SSO authentication is configured and when NAT is disabled on the On-Ramp firewall policy on the On-Ramp IPsec device. With IP-based authentication, each client source IP is unique, which allows proxy users to be tracked in FortiSASE traffic and security event logs.
- For existing instances, Private Proxy using SSO authentication is not compatible with these configuration changes:
  - Secure proxy migration
  - Disable and then re-enable Proxy from *Network > Proxy configuration*

Configuration workflow

The workflow for configuring private proxy is as follows:

1. Enable proxy from *Network > Proxy configuration*. See Proxy configuration on page 285.
2. Enable SSO authentication for proxy users. For a configuration example, see Configuring FortiSASE with Entra ID SSO in proxy agentless mode on page 526.
3. Configure user groups for proxy users. See Users and groups on page 502.
4. Configure a security profile group with SSL deep inspection enabled. See Security profile groups on page 313.
5. Configure proxy policies according to your requirements. See Proxy policies on page 302.
6. Configure Branch On-ramp for the on-premises Branch On-ramp device and verify this functionality separately. See On-ramp tunnel on page 196.
7. (Optional) Configure SPA for the FortiGate device acting as an SPA hub and verify this functionality separately. See SPA on page 101.
8. Enable private proxy from *Network > Proxy configuration* and configure the *Primary IP* and *Secondary IP*.
   - The administrator provides the Primary and Secondary IP addresses, which must be unused private IP addresses.
   - Once private proxy settings are entered, clicking *OK* dynamically adds these IP addresses as new interfaces on the FortiSASE On-Ramp locations.
   - Private Proxy users should then direct their HTTP and HTTPS traffic to these Private Proxy IP addresses over their On-Ramp connection in subsequent steps.
   - The Secondary IP address is used for redundancy and must be configured on Private Proxy endpoints by users or other methods, such as Windows GPO.



9. Configure each proxy user client machine to forward its HTTP and HTTPS to the private proxy by specifying the *Primary IP* and port 9443 using one of these methods:
   a. Automatic proxy setup using a customized PAC file, replacing the turbo URL and port with the *Primary IP* and port 9443.
      For example, if the PAC file contains this line:

      ```
      return "PROXY turbo-hqwdvq17.edge.prod.fortisase.com:10925; DIRECT";
      ```

      Then if the *Primary IP* is 10.130.160.2, replace the line with:

      ```
      return "PROXY 10.130.160.2:9443; DIRECT";
      ```

   b. Manual proxy setup where the Primary IP and port 9443 are manually configured.

   In addition, with SSL deep inspection enabled, the CA certificate must be installed on each client machine to avoid certificate errors.

See Proxy client onboarding on page 737.

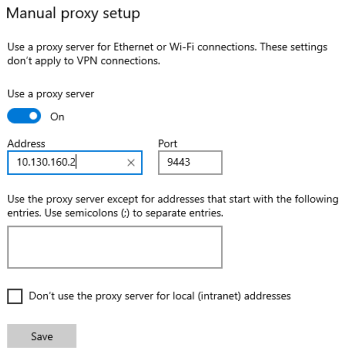
10. Verify private proxy access to the Internet and to desired private resources behind an SPA hub, if SPA is configured. See Verifying private proxy functionality on page 291.

Verifying private proxy functionality

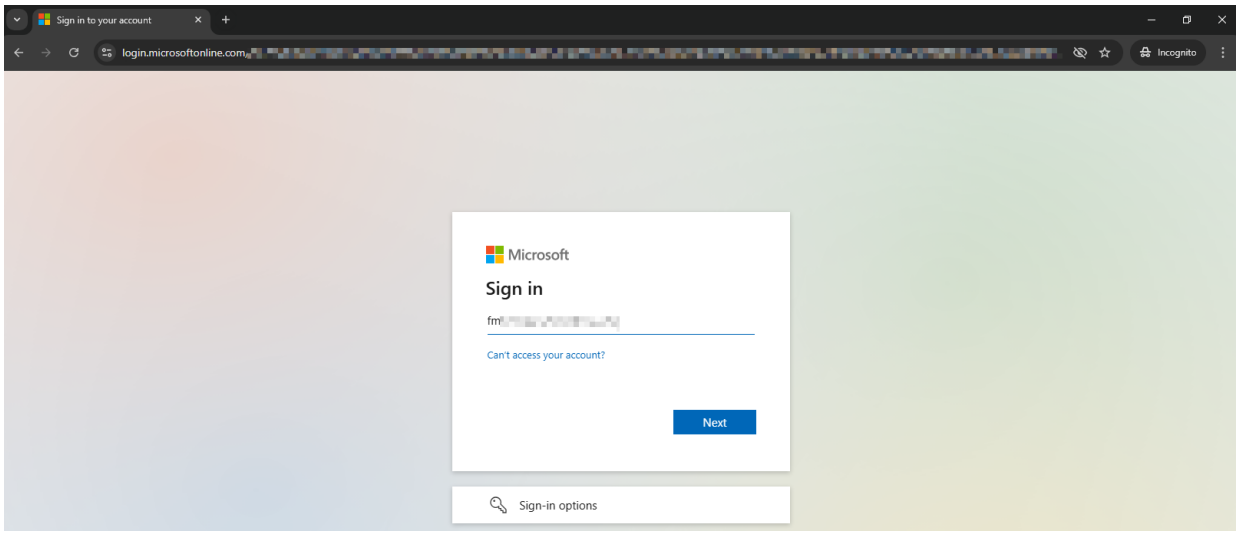
After following all the steps in Configuration workflow on page 289, you can proceed with verifying private proxy functionality.

To verify private proxy functionality:

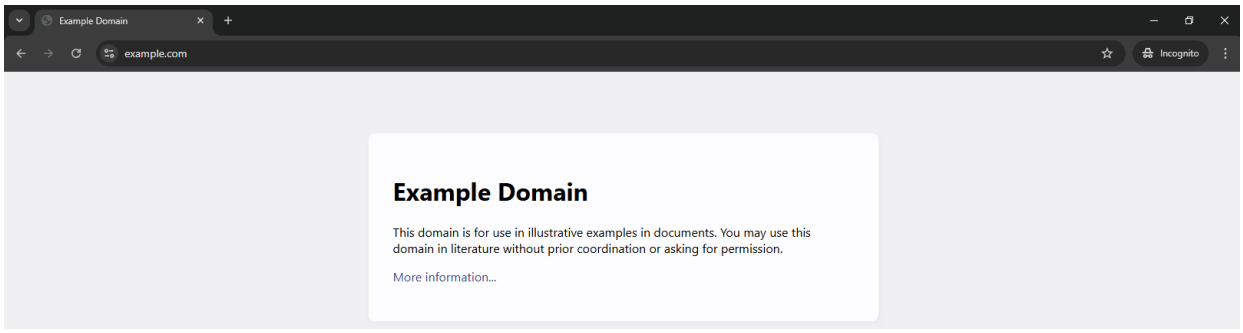
1. Configure the Proxy settings on the proxy user client machine. This example on a Windows machine configures manual proxy setup with the Primary IP of 10.130.160.2 and port 9443.



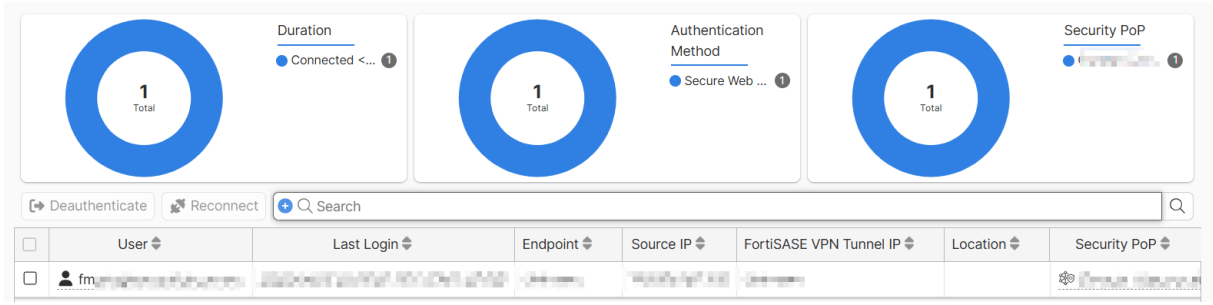
2. Using a web browser, access a desired Internet web site. For example, enter https://example.com.
3. With SSO configured, the configured SAML IdP will prompt for user authentication. Sign in using valid SSO user credentials.



4. After successfully authenticating, observe the desired Internet web site loads in the web browser. This access is confirmed in the traffic logs in a later step.

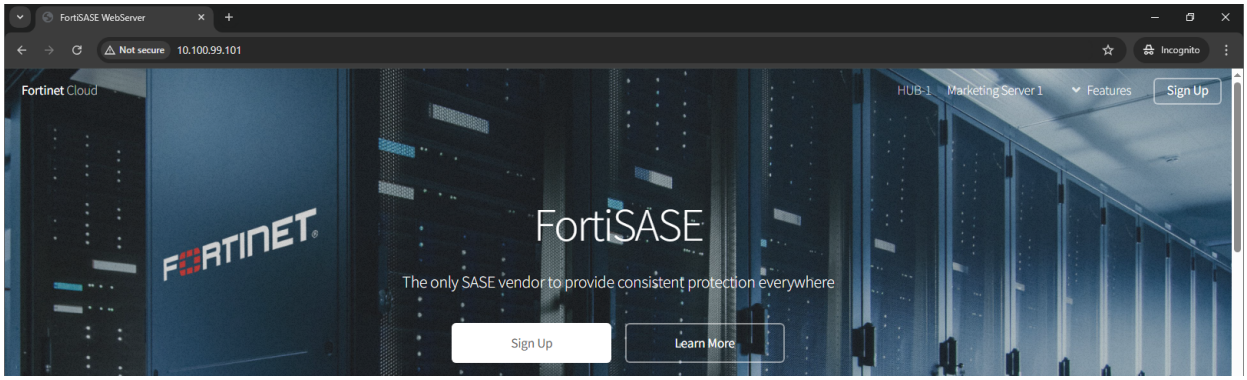


5. Go to *Operations* > *Connectivity* > *Connected users* and observe that the private proxy user is listed there with relevant data.

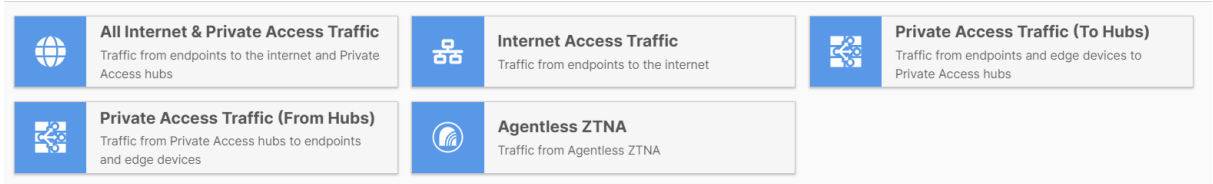


6. If an SPA hub and private resources have been configured, then using a web browser, access a desired private access resource. For example, enter http://10.100.99.101 to access an internal marketing server behind an SPA hub.

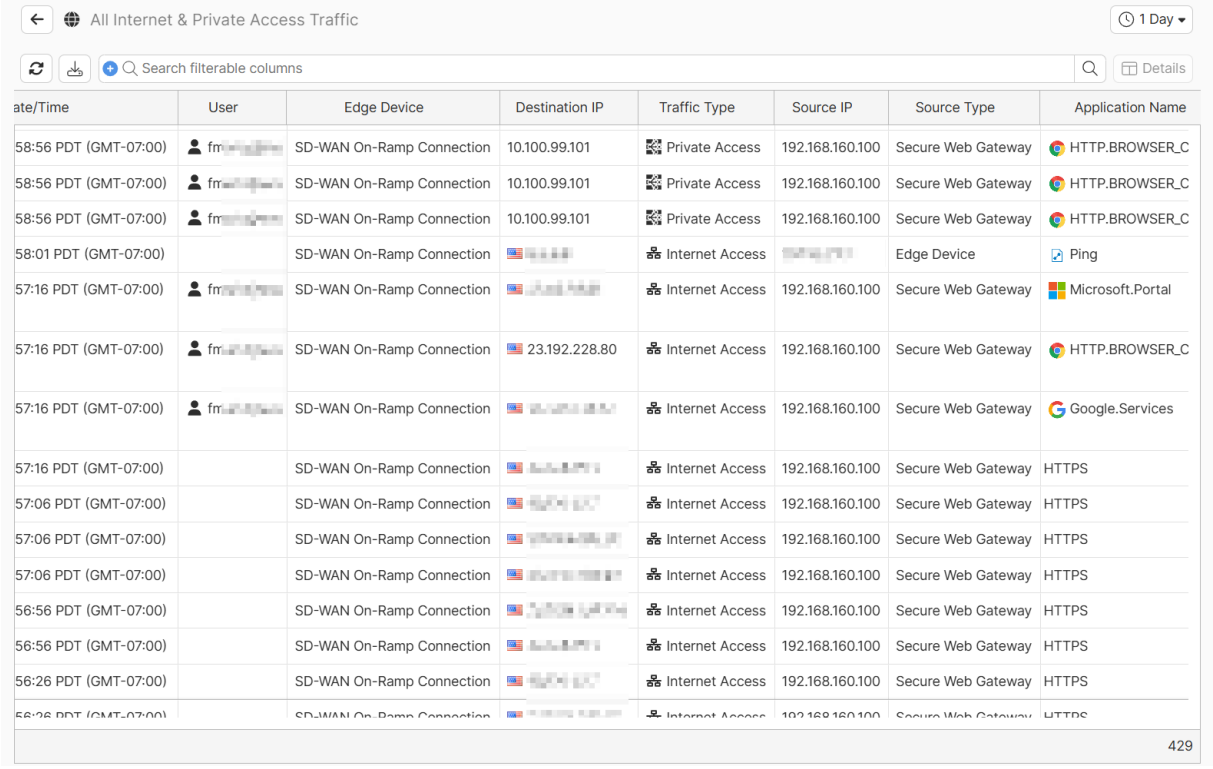
   Observe that you do not need to authenticate again since you have already done so previously and observe that the private server web site loads in the web browser.



7. Go to *Operations* > *Logs* > *Traffic* and click *All Internet & Private Access Traffic* to view the desired logs.



8. In the *All Internet Access & Private Access Traffic* logs, observe the traffic for web sites accessed previously.



Observe that:

a. Prior to SAML authentication, no user information is available.

b. *Edge Device* is listed with *SD-WAN On-Ramp Connection* and *Source Type* lists *Proxy*. A log entry with this combination verifies that private proxy is working as expected.

c. Traffic matching the *Destination IP* for Internet access and private access web sites is shown.

d. *Source IP* lists the IP address of the client machine in the LAN environment of the Branch On-ramp on-premises device.

Secure proxy migration

FortiSASE includes the best practice of migrating to Secure Proxy for an instance. With Secure Proxy, the browser establishes a secure HTTPS connection between the web client and FortiSASE and sends all HTTP requests to the proxy over HTTPS.

Prerequisites

- The Feature instance must have proxy enabled in its proxy configuration:
  - Tenants who previously enabled Secure Proxy in 25.3.a will be shown the best practice entitled *Secure Proxy (Refresh)*.
  - Tenants who have yet to enable Secure Proxy will be shown the best practice entitled *Secure Proxy*.

Considerations

- Proxy users will need to install the FortiSASE Default Certificate when SSL deep inspection is enabled.
- For users using a customized, self-hosted PAC file, possible intermittent network changes may be experienced after enabling Secure Proxy or refreshing Secure Proxy.
- If the PAC file deployment does not change after it has been redeployed as part of this best practice (i.e. server and port on which PAC file is hosted remains the same), then any customizations in the FortiSASE-hosted PAC file or self-hosted PAC file will be automatically picked up by the clients at a regular interval depending on the web browser implementation.
- For existing instances, Private Proxy using SSO authentication is not compatible with these configuration changes:
  - Secure proxy migration
  - Disable and then re-enable Proxy from *Network > Proxy configuration*

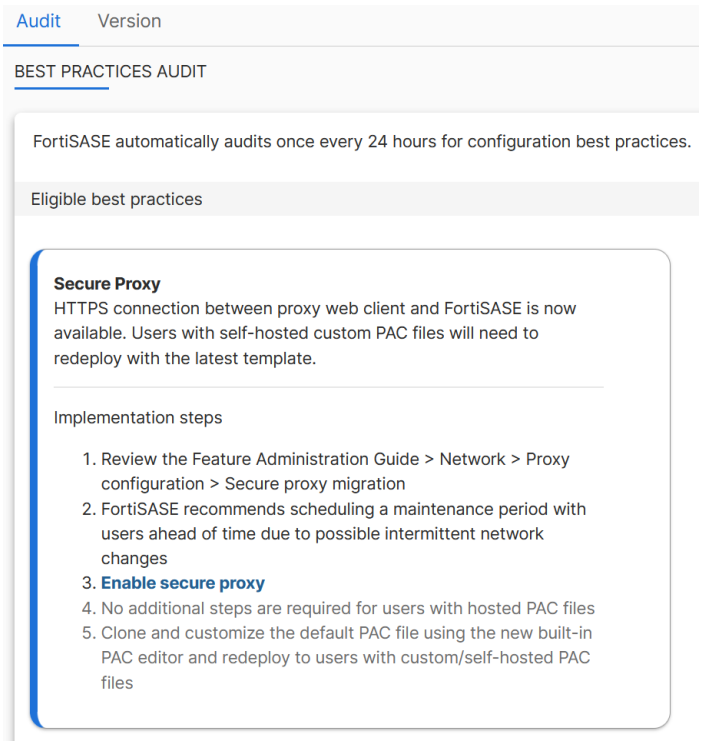
Detailed migration steps

To migrate to *Secure Proxy*/*Secure Proxy (Refresh)* using the associated best practice:

1. Schedule a maintenance period with users ahead of time due to possible intermittent network changes for users using custom/self-hosted PAC files.
2. If your users are using the default PAC file hosted by FortiSASE:
   a. Enable Secure Proxy or refresh Secure Proxy via the best practice page.
   b. No additional steps are required.
3. If your users are connecting via a customized, self-hosted PAC file:
   a. Note that possible intermittent network changes may be experienced after enabling Secure Proxy or refreshing Secure Proxy.
   b. Enable Secure Proxy or refresh Secure Proxy via the best practice page.
   c. After enabling Secure Proxy or refreshing Secure Proxy, you must perform the these steps:
      i. Using the PAC editor in *Network > Proxy configuration > Hosted PAC files*
         i. Edit the default PAC file as needed. By default, hosted PAC files include common SSO IdP destinations that must be excluded from being forwarded to the FortiSASE Proxy and go directly to the internet to ensure SSO authentication is functional
         ii. Download it via *Download > Download directly*.
      ii. Deploy the PAC file by copying it to the self-hosted server and updating the proxy configuration of endpoints to refer to the self-hosted PAC file.

   See PAC file customization on page 737.

Below is an example of an instance with the *Secure Proxy* best practice displayed:


Audit
Version
BEST PRACTICES AUDIT
FortiSASE automatically audits once every 24 hours for configuration best practices.
Eligible best practices
Secure Proxy
HTTPS connection between proxy web client and FortiSASE is now available. Users with self-hosted custom PAC files will need to redeploy with the latest template.
Implementation steps
1. Review the Feature Administration Guide > Network > Proxy configuration > Secure proxy migration
2. FortiSASE recommends scheduling a maintenance period with users ahead of time due to possible intermittent network changes
3. Enable secure proxy
4. No additional steps are required for users with hosted PAC files
5. Clone and customize the default PAC file using the new built-in PAC editor and redeploy to users with custom/self-hosted PAC files

Security

In *Security*, you can configure the following:

- Policies on page 296
- Proxy policies on page 302
- Bandwidth control on page 306
- Security profile groups on page 313
- ZTNA on page 388
- Hosts on page 405
- Schedules on page 407
- External feeds on page 408

Policies

For SSL remote agents, whenever changes are made to an existing policy, they take effect only after SSL agents reconnect to FortiSASE.

All traffic routed through FortiSASE must be associated with a policy. Policies define how FortiSASE handles the traffic including where it is forwarded, what security inspection is applied, and whether the traffic is allowed, blocked, or isolated.

When a session is initiated through the tunnel, FortiSASE inspects the connection and attempts to match it against the configured policies. The policy evaluation follows a top-down order, meaning FortiSASE starts from the top of the policy list and checks each policy sequentially until a match is found. Each policy contains matching criteria such as source, user, destination and more.

- If a matching policy is found and its action is *Accept*, FortiSASE allows the traffic and applies the associated security features, such as antivirus, web filtering, and data loss prevention etc.
- If the action is *Deny*, FortiSASE immediately blocks the traffic from passing through.
- If the action is *Isolate*, FortiSASE redirects the traffic to a secure remote browser session, isolating it from the endpoint while still rendering the content safely to the user.

Each policy has a unique and persistent *ID*, which is assigned at the time of creation. Policies are also assigned a *Sequence Number*, which determines their position in the top-down evaluation order and can be changed as needed to adjust policy precedence.

To display the Policy ID and Sequence Number in the policy table:

1. Go to *Security* > *Traffic* > *Policies*.
2. Hover over *Name* column on policy table and click the gear icon.
3. Move the *ID* and *Sequence Number* fields from the *Inactive Columns* section to the *Active Columns* section.

This allows you to easily view and manage policies based on their unique identifiers and evaluation order.

Default policies

FortiSASE is configured with the following default policies:

VPN policy	Description
Allow-All	Allows traffic for all services for all remote agents. You can edit and delete this policy.
Implicit Deny	Denies access to traffic that does not match another configured policy. You cannot edit or delete this agent policy.

With only these default agent policies and no custom configurations, FortiSASE allows traffic to pass through the Allow-All agent policy, and applies the enabled security components for scanning and processing.

Adding policies to perform granular firewall actions and inspection

For SSL remote agents, whenever changes are made to an existing policy, they take effect only after SSL agents reconnect to FortiSASE.

You can add multiple policies to perform granular firewall actions and inspection. This example configures a policy to allow a set of remote users to access *.fortinet.com and blocks the same remote users from accessing all traffic to *.netflix.com.

Policy name	Description
RemoteHomeOffice-DenyNetflix	Blocks remote employees (members of the Remote-Home-Office user group) from accessing *.netflix.com.
RemoteHomeOffice-AllowFortinet	Allows remote employees (members of the Remote-Home-Office user group) to access *.fortinet.com.

The following provides instructions for configuring the described policies. You may want to configure similar policies, modifying settings based on your environment.

To add policies to perform granular firewall actions and inspection:

1. Go to *Security* > *Traffic* > *Policies*.
2. Create the RemoteHomeOffice-DenyNetflix policy:
   a. Click *Create*.
   b. In the *Name* field, enter RemoteHomeOffice-DenyNetflix.
   c. For *Source Scope*, select *Agent users*.

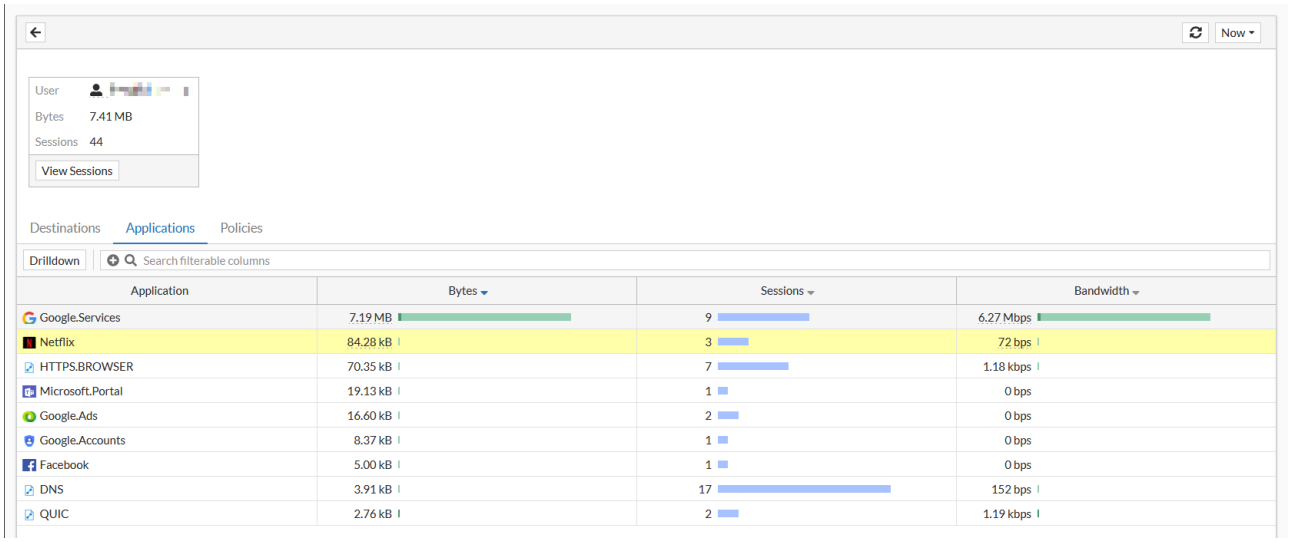
d. For *User*, select *Specify*: Click +, and select the *Remote-Home-Office* user group from the *Select Entries* pane.
e. In the *Destination* field, select *Specify*, click +, then do the following:
   i. Click *Create*.
   ii. Select *IPv4 Host*.
   iii. In the *Name* field, enter the desired name.
   iv. From the *Type* dropdown list, select *FQDN*.
   v. In the *FQDN* field, enter *.netflix.com. When using wildcard FQDNs, FortiSASE caches the FQDN address's IP addresses based on matching DNS responses.
   vi. Click *OK*.
   vii. Select the newly created Netflix host.
f. In the *Service* field, click +. On the *Select Entries* pane, select *ALL*.
g. In the *Schedule* field, select always, a recurring schedule, a schedule group, or create a new schedule by clicking +.
h. Leave all other fields at their default values.
i. Click *OK*.

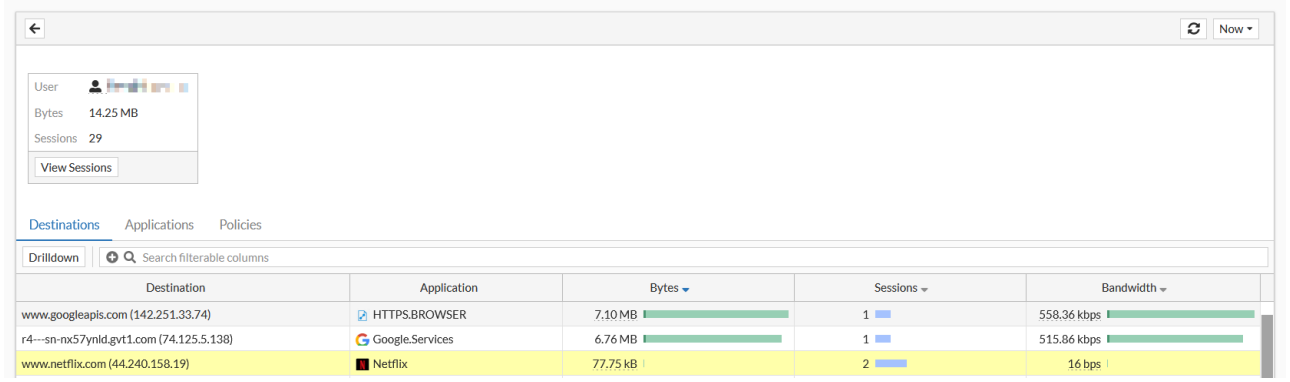
> In agent and proxy policies, when you select an infrastructure in the *Destination* field, you cannot select hosts and services, and vice-versa.

3. Create the RemoteHomeOffice-AllowFortinet policy:
   a. Click *Create*.
   b. In the *Name* field, enter RemoteHomeOffice-AllowFortinet policy.
   c. For *User*, select *Specify*. Click +, and select the *Remote-Home-Office* user group from the *Select Entries* pane.
   d. In the *Destination* field, click +, then do the following:
      i. Click *Create*.
      ii. Select *IPv4 Host*.
      iii. In the *Name* field, enter the desired name.
      iv. From the *Type* dropdown list, select *FQDN*.
      v. In the *FQDN* field, enter *.fortinet.com. When using wildcard FQDNs, FortiSASE caches the FQDN address's IP addresses based on matching DNS responses.
      vi. Click *OK*.
      vii. Select the newly created Fortinet host.
   e. In the *Service* field, click +. On the *Select Entries* pane, select *ALL*.
   f. For *Action*, select *Accept*.
   g. In the *Schedule* field, select always, a recurring schedule, a schedule group, or create a new schedule by clicking +.
   h. In the *Comments* field, enter comments up to the listed maximum number of characters.
   i. Leave all other fields at their default values. Click *OK*.
4. In *Security* > *Traffic* > *Policies*, ensure that you order the policies so that RemoteHomeOffice-DenyNetflix policy is before the RemoteHomeOffice-AllowFortinet policy, and that both those agent policies are before the Allow-All policy.

When a session is initiated through the tunnel, FortiSASE analyzes the connection and performs a policy match. FortiSASE performs the match from top down and compares the session with the configured policy parameters. For example, consider that a user who belongs to the Remote-Home-Office user group attempts to access www.fortinet.com. FortiSASE attempts to match the RemoteHomeOffice-DenyNetflix, but the traffic is not for *.netflix.com. Then, FortiSASE attempts to match the next policy, the RemoteHomeOffice-AllowFortinet policy, which matches. FortiSASE allows the user access to www.fortinet.com.

You can view data for access attempts on the FortiView sources dashboard. You can view the application, destination, and policy information.





Configuring a policy to allow traffic from an Edge device to FortiSASE

To configure a policy to allow traffic from an Edge device to FortiSASE for internet access:

1. Go to *Security* > *Traffic* > *Policies*.
2. Click *Create* to create a new policy.

3. Configure these fields:

Field	Value
Name	Enter a unique internet access policy name.
Source Scope	Select *Edge device*.
Source	• *All Edge Devices*: applies to all edge devices • *Specify*: specify selected authorized Edge devices if you selected *Edge device*.
User	• *All Users*: applies to all users • *Specify*: specify selected users and user groups for all source scopes • *Captive Portal Exempt*: exempt the edge device traffic from encountering a captive portal to determine the identity of a connected endpoint. By default, FortiSASE enforces a captive portal when edge device traffic matches policies with *Source Scope* set to *All*.
Destination	• *All Internet Traffic*: all internet access traffic • *Specify*: specify selected internet access hosts or host groups
Service	Click *+* and select services or service groups.
Action	*Accept* or *Deny*.
Profile Group	*Default* or *Specify* and select profile group.
Force Certificate Inspection	Enable or disable. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead use certificate inspection.
Schedule	Select *always* or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

With the addition of support for identity-based policies for edge devices in FortiSASE 24.3.a, the behavior of edge device traffic based on policies has changed in existing FortiSASE instances:

- Any policies you created before FortiSASE 24.3.a, specifically for edge devices, namely, policies with *Source Scope* set to *Edge device*, have *User* set to *Captive Portal Exempt*.
- Any policies you created before FortiSASE 24.3.a with *Source Scope* set to *All* are not modified. Therefore, any edge devices whose traffic matched an *All* allow policy before have captive portal authentication enforced. You must explicitly create a new exemption policy and place it above any *All* allow policies to avoid captive portal authentication for impacted edge devices. See Configuring an exemption policy for an edge device on page 191.

When using single sign on (SSO) authentication with captive portal for edge devices, you must add an exemption policy for the SAML identity provider (IdP) URLs specified using hosts or infrastructure selections for the *Destination* field to allow SSO authentication traffic destined for the IdP to bypass the captive portal. See Configuring an exemption policy for SSO authentication for Entra ID on page 190.

4. Click *OK*.

To configure a policy to allow traffic from an Edge device to FortiSASE for private access:

See Configuring a private access policy for client-to-server traffic on page 126.

Configuring a geography-based policy

You can configure a geography-based policy by specifying the source as one or more geography-based hosts and by specifying a customized security profile group. FortiSASE will inspect the public IP geolocation of remote users when matching this type of policy. Currently, this geography-based policy support is only supported with IPsec remote users.

To configure a geography-based policy to FortiSASE remote agents for internet access:

1. Go to *Security* > *Traffic* > *Policies*.
2. Click *Create* to create a new policy.
3. Configure these fields:

Field	Value
Name	Enter a unique internet access policy name.
Source Scope	Select *Specify*. **To specify scope:** 1. Click *+*. 2. In the *Select Entries* pane: • Select an existing geography-based host, or • Create a new geography-based host. See Hosts on page 405. i. Click *+*. ii. Select *+IPv4 Host*. iii. Configure these settings: • *Location*: Internet or Unspecified (default) • *Name*: <Name of geography-based host> • *Type*: Geography • *Country/Region*: <Country/Region of choice> iv. Click *OK*.

Field	Value
	v. Click *OK* to select the newly created host.
User	• *All Users*: applies to all users • *Specify*: specify selected users and user groups for all source scopes
Destination	• *All Internet Traffic*: all internet access traffic • *Specify*: specify selected internet access hosts or host groups
Service	Click + and select services or service groups.
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select profile group. For a geography-based policy, since a specific security policy is typically desired, you should create a custom security profile group to be used only by this policy. See Security profiles on page 312 .
Basic Certificate Inspection Override	Enable or disable. When this option is enabled, the SSL inspection profile in the selected profile group is replaced by a basic certificate-inspection profile. If you need more granular control over SSL certificate inspection, create and assign a new security profile group with custom settings.
Schedule	Select *always* or another recurring schedule.
Status	Enable or disable
Log Allowed Traffic	Enable or disable *Security Events*: log traffic that has a security profile applied to it. *All Sessions*: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

4. Click *OK*.

Proxy policies

You must associate any traffic going through FortiSASE with a policy. Proxy policies control where the traffic goes, how FortiSASE processes it, and whether or not FortiSASE allows it to pass through.

When a user's client software, such as a web browser, proxies traffic through FortiSASE, FortiSASE analyzes the connection and performs a proxy policy match. FortiSASE performs the match from top down and compares the session with the configured policy parameters. When there is a match and the action is *Accept*, FortiSASE applies the enabled security components to the traffic. If the action is *Deny*, FortiSASE blocks the traffic from proceeding. If the action is *Isolate*, FortiSASE isolates the traffic in a remote container with content rendered safely to the end user.

Each proxy policy has a unique and persistent ID, which is assigned at the time of creation. Policies are also assigned a Sequence Number, which determines their position in the top-down evaluation order and can be changed as needed to adjust policy precedence.

To display the Policy ID and Sequence Number in the policy table:

1. Go to *Security* > *Traffic* > *Proxy policies*.
2. Hover over *Name* column on policy table and click the gear icon.
3. Move the *ID* and *Sequence Number* fields from the *Inactive Columns* section to the *Active Columns* section.



The *Isolate* action is available only if you have enabled RBI on page 721.

You must first enable proxy configuration for the feature to be available in the GUI. See Proxy configuration on page 285.

Default proxy policies

FortiSASE is configured with the following default proxy policies:

Proxy policy	Description
Threat Feed Deny	Denies traffic to addresses from user-defined threat feeds for all proxy users. You cannot edit or delete this proxy policy.
Botnet Deny	Denies traffic to known botnet C&C servers for all proxy users. You cannot edit or delete this proxy policy.
Allow-All	Allows traffic for all services for all proxy users. You can edit and delete this proxy policy.
Implicit Deny	Denies access to traffic that does not match another configured proxy policy. You cannot edit or delete this proxy policy.

With only these default proxy policies and no custom configurations, FortiSASE blocks all traffic to addresses from user-defined threat feeds and known botnet C&C servers, allows all other traffic to pass through the Allow-All proxy policy, and applies the enabled security components for scanning and processing.

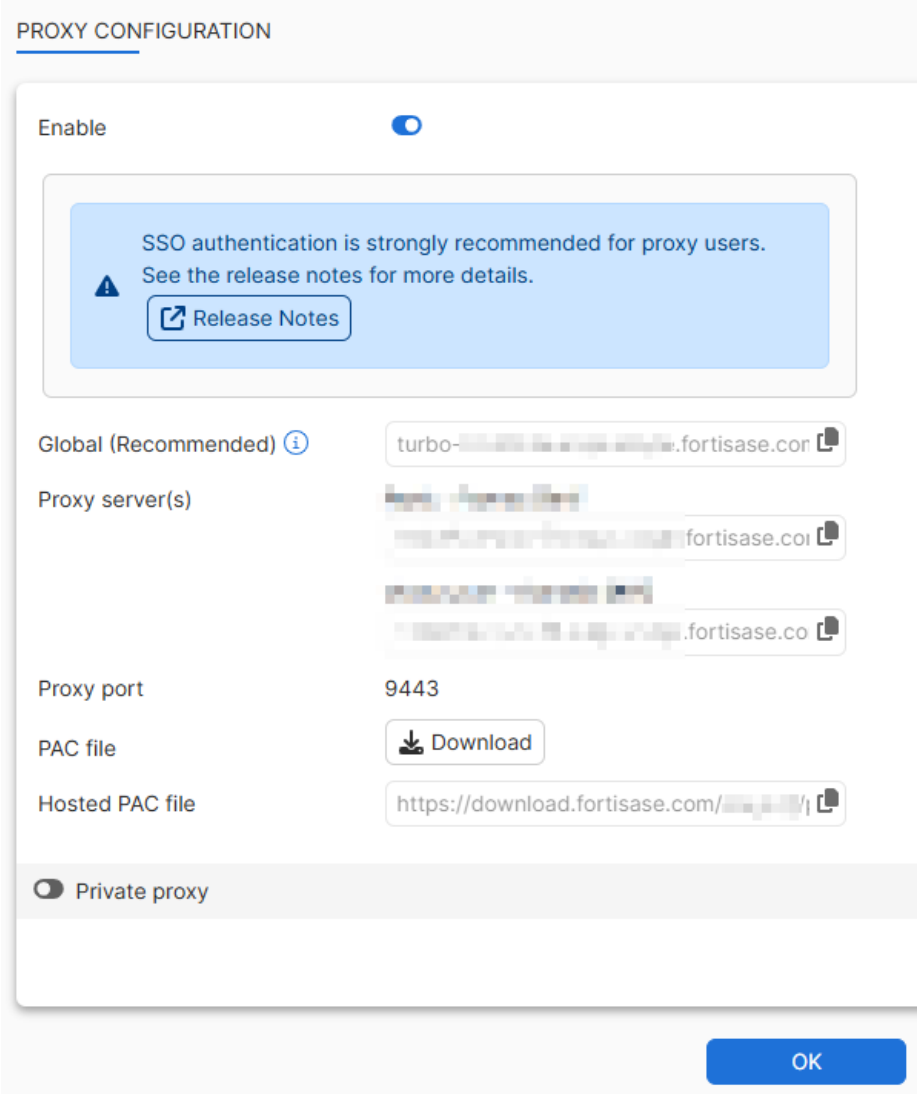
Configuring a proxy policy

This example configures a proxy policy to block all proxy users from accessing all traffic to *.netflix.com.

To configure a proxy policy:

1. Enable proxy configuration:
   a. Go to *Network* > *Proxy configuration*.
   b. Toggle *Enable* to on. The GUI may take a few minutes to reload. Once the GUI finishes loading, you can view the *Hosted PAC File* field. Endpoint users use this URL to configure connecting via the FortiSASE

proxy server.



c. On the right pane, click *Download proxy certificates*. You must distribute this certificate to end users to install on their endpoints to avoid untrusted certificate errors.

2. Create the Proxy-DenyNetflix proxy policy:
   a. Go to *Security* > *Traffic* > *Proxy policies*.
   b. Click *Create*.
   c. Configure the Proxy-DenyNetflix proxy policy:
      i. For *User*, select *All Proxy Users*.
      ii. In the *Destination* field, click *Specify*.
      iii. On the *Host* tab, click *Create*.
      iv. Select *IPv4 Host*. Configure the fields as follows:

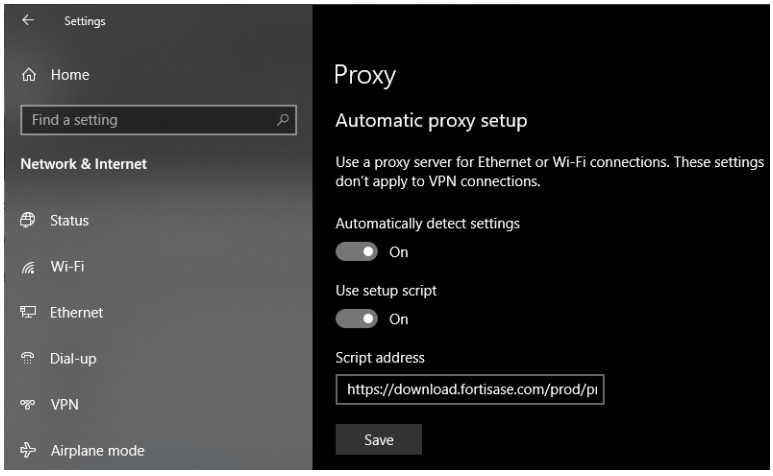
Field	Value
Name	Enter the desired name.

Field	Value
Type	i. Select *FQDN*.
FQDN	Enter *.netflix.com. When using wildcard FQDNs, FortiSASE caches the FQDN address's IP addresses based on matching DNS responses.

v. Click *OK*.
vi. Select the newly created Netflix host.
vii. In the *Schedule* field, select always, a recurring schedule, a schedule group, or create a new schedule by clicking +.
viii. In the *Comments* field, enter comments up to the listed maximum number of characters.
ix. Leave all other fields at their default values.
x. Click *OK*.

In agent and proxy policies, when you select an infrastructure in the *Destination* field, you cannot select hosts and services, and vice-versa.

3. In *Security* > *Traffic* > *Proxy policies*, ensure that you order the policies so that the Proxy-DenyNetflix policy is before the Allow-All policy.
4. Distribute the URL in the *Network* > *Proxy configuration* > *Hosted PAC File* field and the certificate downloaded from *Download proxy certificates* to end users.
5. The end user installs the certificate on their device.
6. The end user can configure proxy settings at the OS level or in a browser. Configuring proxy settings at the OS level applies them to all installed browsers. The following gives instructions for configuring proxy settings at the OS level on a Windows 10 device:
   a. In Windows, go to *Windows Settings* > *System* > *Proxy Settings*.
   b. Enable *Use setup script*.
   c. In the *Script address* field, enter the *Hosted PAC File* URL.



   d. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE user credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

When a session is initiated through the client browser, FortiSASE analyzes the connection and performs a proxy policy match. FortiSASE performs the match from top down and compares the session with the configured proxy policy parameters. For example, consider that a proxy user attempts to access www.netflix.com. FortiSASE attempts to match the Proxy-DenyNetflix policy, which matches. FortiSASE denies the user access to www.netflix.com.

Prerequisites and considerations

Prerequisites

For proxy SSO users, at least one proxy policy using SSO authentication must have deep inspection enabled in the configured security profile group. SSO authentication requires deep inspection to work.

- Any traffic from proxy SSO users that is destined for hosts or URL categories defined as deep inspection exemptions does not work.
- You must not configure proxy policies using SSO authentication with certificate inspection.
- If a proxy policy requires certificate inspection, you must not configure SSO authentication in that policy.

Considerations

SSO authentication is strongly recommended for proxy users.

Bandwidth control

FortiSASE provides bandwidth control of internet access and private access traffic by defining bandwidth policies and profiles.

FortiSASE delivers bandwidth control by policing, that is, when traffic exceeds the configured bandwidth limits, traffic is dropped.

To configure bandwidth control:

1. Create either a new shared profile or a per IP profile, or both. You can also choose to edit the configuration of any predefined shared profiles, if desired. See Shared profiles on page 307 and Per IP profiles on page 308.
2. Create a new bandwidth control policy, configuring the traffic matching conditions and which profiles to apply. See Bandwidth control policies on page 309.

For an example of configuring a bandwidth control profile and policy, see Example: Limiting YouTube speeds using bandwidth control on page 311.

Prerequisites

- Bandwidth control only applies to IPsec agent tunnel traffic matching bandwidth control policy conditions.

Considerations

- The bandwidth control policies must be placed in the correct order in the bandwidth control policy page to obtain the desired results. Policies are matched from top-down, so they should be arranged in a sequence that places the more granular policies above general policies.
- Shared profiles affect speed in the direction from source to destination. To limit the speed in the opposite direction, that is, from destination to source, in a bandwidth control policy, you would apply a shared profile using the *Reverse direction of shared profile* option.
- Per IP profiles apply the speed limit on operations in both directions.
- The *Apply shaper* option which applies a shared shaper either *Per policy* or to *All policies using this shaper* is only available with the predefined shared profiles.

Shared profiles

A shared profile is used in a bandwidth control policy to indicate the priority, and the guaranteed and maximum bandwidth for a specified type of traffic use. With this type of profile, all users share the set guaranteed and maximum bandwidths.

Using a predefined shared profile, you can apply bandwidth control per policy or for all bandwidth control policies. Using a newly-defined custom shared profile, you can only apply the profile to all bandwidth control policies.

To configure a shared profile:

1. Go to *Security > Traffic > Bandwidth control > Shared Profile*. You can select a predefined or existing shared profile and click *Edit* or create a new profile by clicking *+Create*.
2. Configure the following settings:

Setting	Description
Name	Enter the desired name of the shared profile.
Quality of service	
Traffic priority	Certain traffic can be prioritized as High, Medium, or Low. FortiSASE 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 business-critical services such as a web server. You should assign less important services a low priority.
Bandwidth unit	Configure the unit for specifying and measuring bandwidth. Choose from one of these units: • *Kilobits per second (Kbps)* • *Megabits per second (Mbps)* • *Gigabits per second (Gbps)*
Apply shaper	Configure how this shared profile should be applied:

Setting	Description
	• *Per policy* (default for predefined profiles): Apply shared profile to each bandwidth control policy individually. • *All policies using this shaper* (default for custom profiles): Apply shared profile evenly to all bandwidth control policies that use it, on a first-come, first-served basis. This setting is only configurable for predefined shared profiles.
Maximum bandwidth	When enabled, the specified bandwidth indicates the largest amount of traffic allowed depending on how the profile is applied. • *Per policy*: Maximum bandwidth per bandwidth control policy . • *All policies using this shaper*: Maximum bandwidth shared across all bandwidth control policies.
Guaranteed bandwidth	When enabled, the guaranteed bandwidth ensures that there is a consistent reserved bandwidth available.

3. Click *OK*.

Per IP profiles

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, FortiSASE allocates each user/IP address 1 Mbps of bandwidth.

- Even if the network consists of a single user, FortiSASE allocates them 1 Mbps.
- If there are ten users, each user gets 1 Mbps of bandwidth, totaling 10 Mbps of outgoing traffic.

To configure a Per IP profile:

1. Go to *Security > Traffic > Bandwidth control > Per IP Profile* and create a new profile by clicking *+Create*.
2. Configure the following settings:

Setting	Description
Name	Enter the desired name of the per IP profile.
Quality of service	
Bandwidth unit	Configure the unit for specifying and measuring bandwidth. Choose from one of these units: • *Kilobits per second (Kbps)* • *Megabits per second (Mbps)* • *Gigabits per second (Gbps)*

Setting	Description
Maximum bandwidth	When enabled, the specified bandwidth indicates the largest amount of traffic allowed per user.
Max concurrent connections	When enabled, each user can have up to the specified number of concurrent connections.
Max concurrent TCP connections	When enabled, each user can have up to the specified number of concurrent TCP connections.
Max concurrent UDP connections	When enabled, each user can have up to the specified number of concurrent UDP connections.

3. Click *OK*.

Bandwidth control policies

Bandwidth control policies are used to map traffic to a shared profile or to a per IP profile. A bandwidth control policy is a rule that matches traffic based on certain IP header fields and/or upper layer criteria. For example, it can match traffic based on source and destination IP, service, application, and URL category.

To configure a bandwidth control policy:

1. Go to *Security* > *Traffic* > *Bandwidth control* > *Bandwidth control policy* and create a new policy by clicking *+Create*.
2. Configure the following settings:

Setting	Description
Name	Enter the desired name of the bandwidth control policy.
Status	Set to *Enable* have the bandwidth control policy take effect.
Comments	(Optional) Add comments about the bandwidth control policy
If traffic matches	
Traffic type	Configure the traffic type that the bandwidth control policy applies to. • *Internet access*: Secure internet access using agent tunnels To private access hubs: When SPA is properly licensed and configured, traffic initiated from remote users (agent tunnels) to SPA hubs (or local networks behind SPA hubs). • *From private access hubs*: When SPA is properly licensed and configured, traffic initiated from SPA hub sources (local networks or connected spokes) to remote users (agent tunnels).
Source scope	Select the source scope: • *All* • *VPN users*: Remote agent tunnels
User	Select from: • *All Users*

Setting	Description
	• *Specify* Then, click *+* to select *User* or *User group*.
Destination	Select from: • *All destinations* • *Specify* Then, click *+* to select *Address* or *Internet service*.
Schedule	Select from: • *Always* • Custom defined recurring schedule
Service	Click *+* and select *ALL* or one or more specific services.
Application	Select one or more application control entries. See Prerequisites on page 310.
URL category	Select one or more URL categories. See Prerequisites on page 310.
Then apply the following profile	
Shared profile	When enabled, select the shared profile to apply in the source to destination direction.
Reverse direction of shared profile	When enabled, select the shared profile to apply in the destination to source (reverse) direction.
Per IP profile	When enabled, select the Per IP profile to apply in both directions.

3. Click *OK*.

Prerequisites

- If the *Application* setting is configured in a bandwidth control policy, then an application control profile must be configured in a policy to match the selected application.
- If the *URL category* setting is configured in a bandwidth control policy, then an web filter profile must be configured in a policy to match the selected URL category.

Considerations

- By default, an *Implicit Medium Control* bandwidth control policy has been predefine and matches all traffic types with a Medium-priority shared profile. It can neither be edited nor deleted.

Example: Limiting YouTube speeds using bandwidth control

The following example demonstrates how to limit YouTube speeds using bandwidth control.

To configure a shared profile:

1. Go to *Security > Traffic > Bandwidth control > Shared Profile* and create a new profile by clicking *+Create*.
2. Configure the following settings:

Setting	Description
Name	*custom-shared-1*
Quality of service	
Traffic priority	*High*
Bandwidth unit	*Kilobits per second (Kbps)*
Maximum bandwidth	*50*
Guaranteed bandwidth	*100*

3. Click *OK*.

To configure a bandwidth control policy:

1. Go to *Security > Traffic > Bandwidth control > Bandwidth control policy* and create a new policy by clicking *+Create*.
2. Configure the following settings:

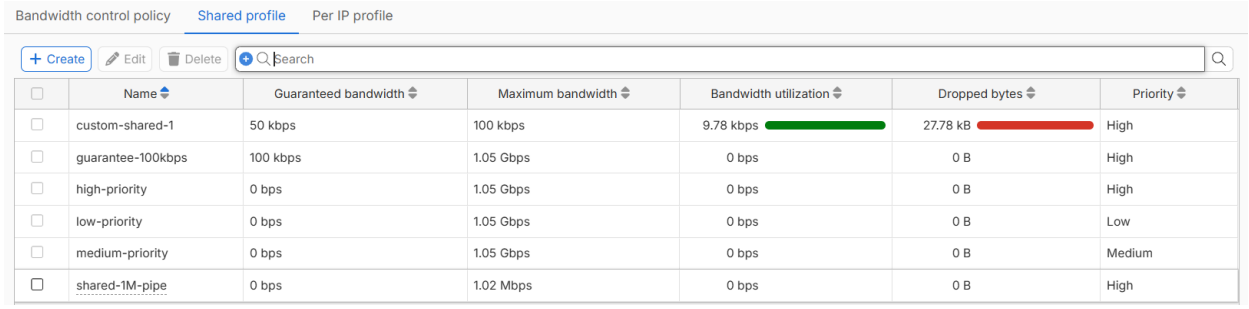
Setting	Description
Name	*Custom Control Policy 1*
Status	*Enable*
Comments	<Leave empty>
If traffic matches	
Traffic type	*Internet access*
Source scope	*All*
User	*Specify* `johnlocus@example.com`
Destination	*Specify* Create a new IPv4 FQDN host for **.youtube.com* named `wildcard.youtube.com`.

Setting	Description
Schedule	*Always*
Service	*ALL*
Application	None selected.
URL category	None selected.
Then apply the following profile	
Shared profile	*custom-shared-1*
Reverse direction of shared profile	Disabled
Per IP profile	Disabled

3. Click *OK*.

To validate the configured shared profile and bandwidth control policy:

1. Onboard an endpoint using the invitation code and connect to the *Secure Internet Access* tunnel by authenticating with the username johnlocus@example.com and corresponding password.
2. Open a browser, go to https://youtube.com and play several videos.
3. Go to *Security* > *Traffic* > *Bandwidth control* > *Shared Profile* and observe the non-zero values in *Bandwidth utilization* and *Dropped bytes* fields.



Security profiles

You can configure FortiSASE security components settings and view logs for each component in *Security* > *Traffic* > *Security profiles*. FortiSASE applies enabled security components to each Allow policy in *Policies*. You can configure some exemptions and overrides for some security components.

Decrypting and inspecting content in encrypted traffic for these FortiSASE security features requires deep inspection:

- Antivirus
- Web Filtering with Inline-CASB
- File Filter
- Data loss prevention
- Application Control with Inline-CASB
- Video Filter

Without deep inspection configured on FortiSASE and the corresponding certificate authority (CA) certificate automatically installed on the endpoint with FortiClient, the aforementioned features do not work as desired with encrypted traffic.

See Certificate and deep inspection modes on page 315.

Security profile groups

You can create security profile groups, which allow you to group different security profile settings together. You can then configure the profile group as part of a policy.

This topic covers the following use cases:

- Security profile groups for agents
- Security profile groups for proxy users
- Security profile groups for agentless ZTNA users

Security profile groups for agents

For example, consider the RemoteHomeOffice-AllowFortinet example policy from Adding policies to perform granular firewall actions and inspection on page 297, which allows remote employees (members of the Remote-Home-Office user group) to access *.fortinet.com. Consider that you also want to monitor these employees' access to Cloud/IT applications using Application Control With Inline-CASB, while disabling Application Control With Inline-CASB for all other employees. You can achieve this by creating a new security profile group with the desired Application Control With Inline-CASB settings, and configuring this profile group as part of the RemoteHomeOffice-AllowFortinet policy. Application Control With Inline-CASB remains disabled for policies that have another security profile group applied.

The following provides for configuring the described scenario.

To create a security profile group and configure it in an agent policy:

1. Go to *Security* > *Traffic* > *Security profiles*.
2. From the *Profile Group* dropdown list in the top right corner, click *Create*.
3. In the *Name* field, enter the desired name. This example uses "Cloud IT" as the group name.

4. In the *Initial Configuration* field, do one of the following:
   a. Select *Default* to configure the new group with the same settings as the default security profile group.
   b. Select *Based On* to configure the new group with the same settings as an existing non-default security profile group. From the dropdown list, select the desired group.
5. Click *OK*.
6. Configure Application Control With Inline-CASB to monitor employees' access of Cloud/IT applications by enabling Application Control With Inline-CASB. By default, once enabled, Application Control With Inline-CASB monitors access of Cloud/IT applications.
7. Configure the profile group in an agent policy:
   a. Go to *Security > Traffic > Policies*.
   b. Select the RemoteHomeOffice-AllowFortinet policy.
   c. In the *Profile Group* field, select *Specify*. From the dropdown list, select *Cloud IT*. The *Profile Group* field is only available for policies where the *Action* is configured as *Accept*.
   d. Click *OK*.

Security profile groups for proxy users

For proxy users, the process for configuring a security profile group and policy is similar to the process for configuring these settings for agents.

The only difference is that these steps are required if SSO authentication is used for proxy users:

- You must configure SSL inspection in *Configure SSL* ensuring that *Deep Inspection* is selected.
- You will need to download the CA certificate and install it on endpoints. See Installing a certificate for deep inspection mode on page 317.

Prerequisites and considerations

Prerequisites

For proxy SSO users, at least one proxy policy using SSO authentication must have deep inspection enabled in the configured security profile group. SSO authentication requires deep inspection to work.

- Any traffic from proxy SSO users that is destined for hosts or URL categories defined as deep inspection exemptions does not work.
- You must not configure proxy policies using SSO authentication with certificate inspection.
- If a proxy policy requires certificate inspection, you must not configure SSO authentication in that policy.

Considerations

SSO authentication is strongly recommended for proxy users.

Security profile groups for agentless ZTNA users

For agentless ZTNA users, the process for configuring a security profile group and policy is similar to the process for configuring these settings for proxy users, without the need to install a certificate for deep inspection.

For agentless ZTNA users, you must ensure that in *Security*, you select the *Private Access* tab in the top right corner. Only Private Access security groups are selectable from within agentless ZTNA application policies.

SSL Inspection

Secure sockets layer (SSL) inspection allows FortiSASE to inspect the SSL/TLS layer during certificate inspection and upper layers during deep inspection. This enables FortiSASE to filter and protect secured traffic that the various security profiles have processed. SSL inspection not only protects traffic over HTTPS, but also from other commonly used encrypted protocols such as SMTPS, POP3S, IMAPS, and FTPS. FortiSASE supports two SSL inspection types.

Certificate and deep inspection modes

These FortiSASE features require deep inspection to decrypt and inspect content in encrypted traffic:

- Split DNS
- Antivirus
- Web Filtering with Inline-CASB
- File Filter
- Data loss prevention
- Application Control with Inline-CASB

Without deep inspection configured on FortiSASE and the corresponding certificate authority certificate automatically installed on the endpoint with FortiClient, the aforementioned features do not work as desired with encrypted traffic.

You can configure FortiSASE SSL inspection to use certificate (default) or deep inspection or disable SSL inspection altogether.

Inspection mode	Description
Certificate	FortiSASE inspects only the header information up to the SSL/TLS layer. Certificate inspection verifies the web server identities by analyzing the SSL/TLS negotiations by looking at the server certificate and TLS connection parameters. Therefore web filter can perform FortiGuard category web filtering, URL filtering, and other filtering that does not require looking at the payload when you enable certificate inspection.
Deep	FortiSASE decrypts and inspects the content to find and block threats. It then reencrypts the content and sends it to the real recipient. You can configure exemptions for deep inspection. While HTTPS offers protection on the internet by applying SSL encryption to web traffic, malicious traffic can also use SSL encryption to get around your network's normal defenses.

Inspection mode	Description
	For example, you may download a file containing a virus during an e-commerce session or receive a phishing email containing a seemingly harmless download that, when launched, creates an encrypted session to a command and control (C&C) server and downloads malware onto your computer. You can use SSL inspection to protect the infiltration by scanning for malicious content in your HTTPS web traffic or identifying phishing content in encrypted mail exchanges. SSL inspection can also defend against the exfiltration process while an infected host calls home to a C&C server or loses company secrets over encrypted sessions. When you use deep inspection, FortiSASE serves as the intermediary to connect to the SSL server. It decrypts and inspect the content to find and block threats. The recipient is presented with the FortiSASE certificate or a custom certificate instead of the real server certificate. FortiClient receives the certificate automatically and endpoint users do not see any certificate browser warnings.
None	FortiSASE does not perform any SSL inspection. You can use this option to fully disable SSL inspection.

Configuring handling of unknown content types

When configuring certificate or deep inspection from *Security > Traffic > Security profiles > Configure security profile group settings*, FortiSASE allows you to configure its behavior when handling unknown content types.

You can configure the following actions for handling unknown content types:

Setting	When FortiSASE detects an unknown content type...
Block	Block the session.
Apply security profiles	Scan the session as plain text.
Allow	Bypass the session.

For cases where FortiSASE blocks downloads of legitimate files with specific unknown content types, you can configure this setting as *Apply security profiles* or *Allow*.

Exempting hosts and URL categories from deep inspection

In some scenarios, you may not want to perform SSL deep inspection and simply choose to trust the connections or the user initiating the connections. In this case, certificates of the hosts and URL categories are inspected but contents are not decrypted for inspection. Thus, security scanning of encrypted traffic for exempted hosts and websites matching exempted URL categories are not performed.

For example, for banking-related traffic, most end users do not want deep inspection applied out of privacy reasons. Similarly, traffic related to personal health and wellness may contain personal information that is too sensitive to scan. As such, when defining deep inspection, FortiSASE exempts the Finance and Banking and Health and Wellness categories by default.

In other cases, a user or user group may need to access websites without deep inspection. Exempting a host or hosts associated with a user or user group achieves this result.

To exempt hosts and URL categories from deep inspection:

1. Go to *Security > Traffic > Security profiles*.
2. At the top of the security profile group page, in the *SSL Inspection* section, click *Configure security profile group settings*.
3. Enable *Deep Inspection*.
4. In the *Hosts* and *URL Categories* fields, click *+*.
5. In the *Select Entries* pane, select the desired hosts and URL categories to exempt from deep inspection.
6. Click *OK*.

Uploading a certificate for deep inspection mode

By default, you can download the certificate authority (CA) certificate of the FortiSASE CA, Fortinet_CA_SSL, who signs the certificate used in encrypting SSL connections when performing deep inspection. If desired, you can upload a custom CA certificate and key to perform deep inspection.

To upload a certificate for deep inspection mode:

1. Go to *Security > Traffic > Security profiles*.
2. At the top of the security profile group page, in the *SSL Inspection* section, click *Configure security profile group settings*.
3. For *Inspection method*, select *Deep inspection*.
4. From the *CA certificate* dropdown list, select *+* to import a new local CA certificate and key for use with deep inspection.
5. Configure the fields and upload the certificate and key files as needed.
6. Click *OK*.

Installing a certificate for deep inspection mode

When users forward traffic to FortiSASE using agent-based mode, agentless proxy mode, or using an edge device, FortiSASE proxies traffic from the client. While being proxied, connections using secure protocols like HTTPS have their certificates replaced and signed by FortiSASE. To avoid seeing warnings and errors, the client must trust the signing certificate authority (CA) and have a valid certificate chain back to the root CA. Therefore, installing FortiSASE's CA certificate on the client's trusted certificate store is important.

With deep inspection enabled, FortiSASE supports automatically installing the FortiSASE CA certificate for agent-based users with FortiClient installed on their endpoints. Therefore, the following instructions are not required for agent-based users.

You must install the FortiSASE CA certificate on endpoints for agentless proxy users and site-based edge device users using the following instructions.

The following instructions demonstrate installing certificates on various operating systems:

- Windows on page 318
- macOS on page 318
- Chrome OS on page 319
- Managed Chromebook on page 319

First, you must download the CA certificate from FortiSASE prior to manually installing it on your endpoints.

To download the FortiSASE CA certificate:

1. Go to *Security > Traffic > Security profiles*.
2. From the *Profile Group* dropdown list, select the desired group.
3. At the top of the security profile group page, in the *SSL Inspection* section, click *Configure security profile group settings*.
4. Ensure *Deep inspection* is selected for *Inspection method*.
5. For *CA certificate*, select the certificate from the dropdown list. Typically, the default Fortinet_CA_SSL certificate can be used.
6. Click *Download* next to the dropdown list and save the CA certificate to your local computer. You use this CA certificate in one of the following sets of instructions.

Windows

To install the FortiSASE CA certificate on a Windows 10 device:

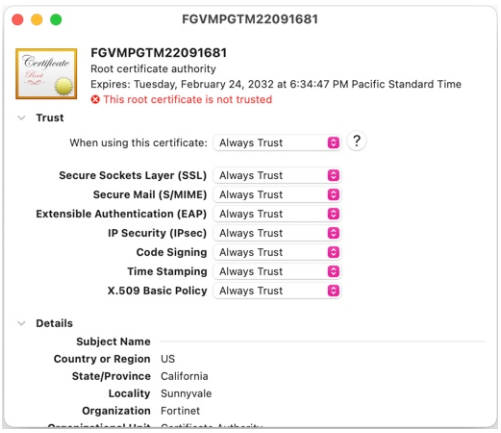
1. Double-click the FortiSASE certificate that the administrator provided during onboarding.
2. On the *General* tab, click *Install Certificate*.
3. You can install the certificate for the current user or local machine. Installing for the local machine requires administrator permissions. Select the desired option and click *Next*.
4. Choose where you want the certificate to be kept. To customize this, select *Place all certificates in the following store* and browse the store. Then select *Trusted Root Certification Authorities*. Click *Next*.
5. Review and click *Finish* to install the certificate.
6. You can upload and distribute CA certificates using a group policy on multiple Windows devices that are part of an Active Directory. See Distribute certificates to Windows devices by using Group Policy.

macOS

To properly browse any HTTPS websites, you must install the FortiSASE root certificate on the endpoint.

To upload the FortiSASE CA certificate on a mac:

1. Double-click the FortiSASE certificate that the administrator provided during onboarding.
2. From the *Keychain* dropdown list, select *System*, then click *Add*.
3. When you view the certificate, the root certificate appears as not trusted. Expand the *Trust* section. From the *When using this certificate* dropdown list, select *Always Trust*.

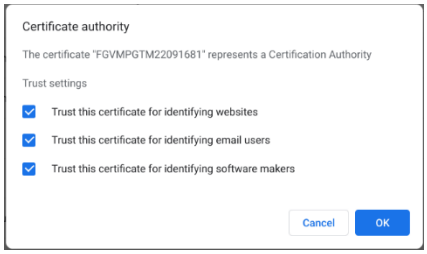


4. Save the configuration and add the certificate to the system keychain. You can connect to HTTPS websites without seeing a warning.

Chrome OS

To upload the FortiSASE CA certificate on a Chromebook:

1. In Chrome, open *Settings* from the menu or go to `chrome://settings`.
2. Go to *Privacy and security*. On the configuration page, click *Security*.
3. In the *Security settings* page, scroll to the bottom to find *Advanced* > *Manage certificates*. Click the right arrow.
4. In the *Manage certificate* page, select *Authorities*.
5. Click *Import* to import the FortiSASE certificate authority (CA) certificate.
6. If the Fortinet_CA_SSL.cer file does not appear, change the file selection page to show all files. Then select the Fortinet_CA_SSL.cer cert and click open.
7. The next screen asks for your trust settings for this certificate. Select all options, then click *OK*.



8. You have imported the FortiSASE CA certificate. Scroll down to see the org-Fortinet entry. Expand to see the certificate and view its details.

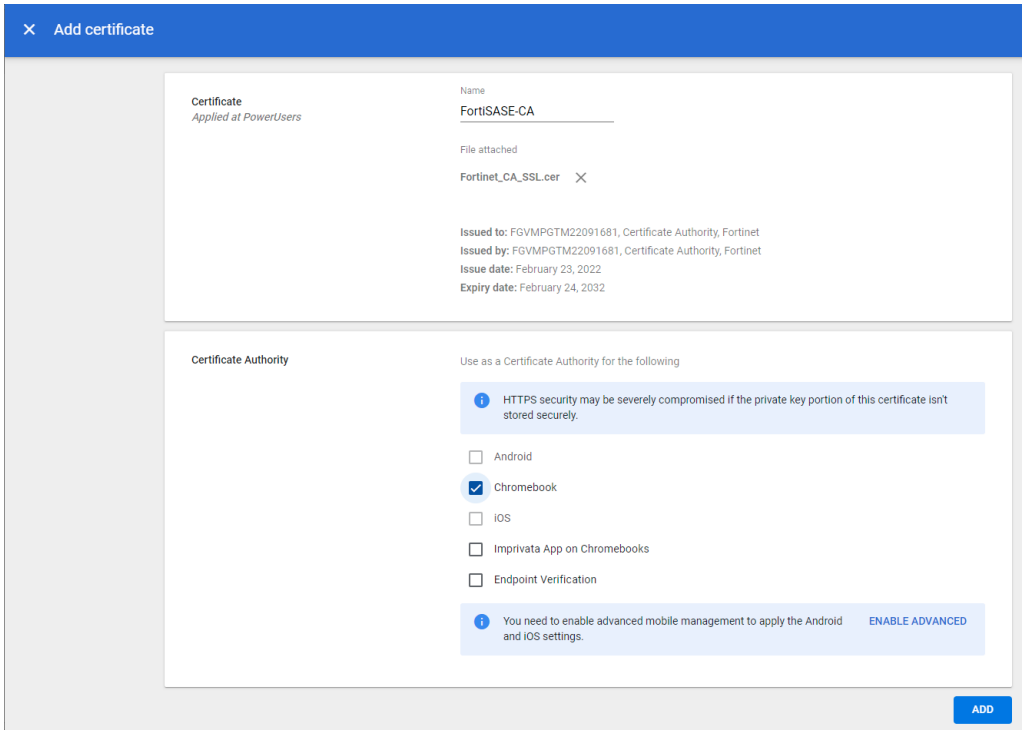
Managed Chromebook

If your organization manages Chromebooks using the Google Admin console, you can centrally install the FortiSASE certificate authority certificate on the Admin console and distribute it to each managed Chromebook.

To upload the FortiSASE CA certificate on Google Admin Console:

1. On the Google Admin console, go to *Device* > *Networks*.
2. Select the organizational unit in which to apply these settings.

3. Under *Certificates*, click *Create Certificate*.
4. Enter a name for this certificate entry, then click *Upload* to upload the Fortinet_CA_SSL.cer certificate.
5. Under *Certificate Authority*, select *Chromebook*. Click *ADD*.

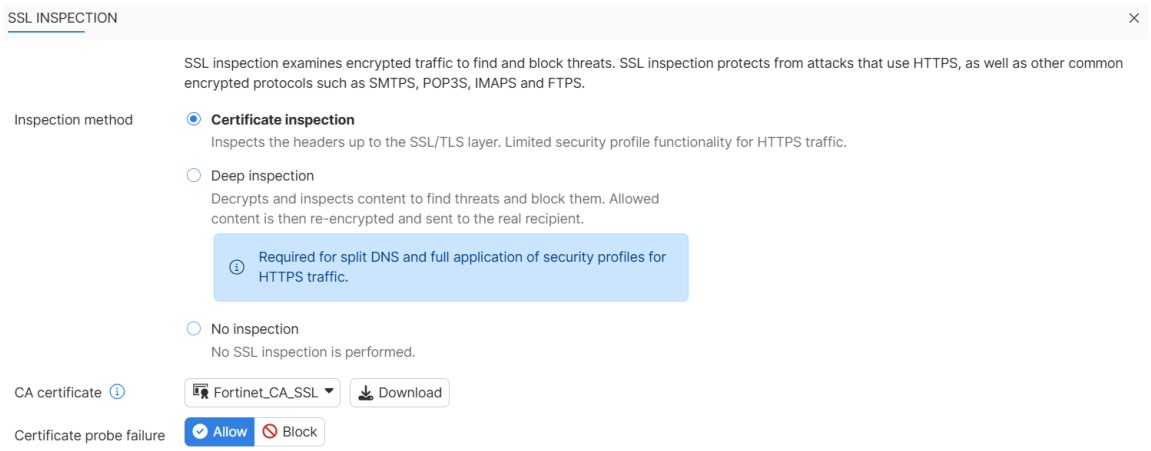


To verify the CA certificate is installed on a Chromebook:

1. In Chrome, open *Settings* from the menu or go to `chrome://settings`.
2. Go to *Privacy and security*. On the configuration page, click *Security*.
3. In the *Security settings* page, scroll to the bottom to find *Advanced* > *Manage certificates*. Click the right arrow.
4. In the *Manage certificate* page, select *Authorities*.
5. Scroll down to the org-Fortinet entry. Expand this entry. You see the certificate and an icon indicating that Google Admin console is managing it.

Configuring certificate probe failure option

When configuring either certificate inspection or deep inspection from *Security* > *Configure SSL*, FortiSASE allows you to configure its behavior when a certificate probe failure occurs.



FortiSASE checks a server certificate before a client-server HTTPS connection is established. Certificate probe failures can occur due to issues like handshake failures, misrouted traffic, or untrusted CAs. If a certificate is invalid, untrusted, or mismatched, then FortiSASE flags this as a certificate probe failure.

Certificate probe failure can be configured as either *Allow* (Default) or *Block*:

Setting	Description
Allow	FortiSASE bypasses the session when unable to retrieve server's certificate for inspection.
Block	FortiSASE blocks the session when unable to retrieve server's certificate for inspection.

For some cases requiring increased security requirements or stringent organization security policy, certificate probe failure may need to be configured to *Block*.

Configuring common options for invalid certificates

You can allow or block the passing of traffic with invalid SSL certificates by configuring common options for invalid certificates. For example, when publicly available web sites have expired certificates but users still need to access them, then the allow and keep untrusted action for expired certificates is the desired configuration.

You can configure these options when you configure certificate or deep inspection:

Option	Action to take when...	Default action
Expired certificates	Server certificate is expired.	Block
Revoked certificates	Server certificate is revoked.	
Validation timed-out certificates	Server certificate validation times out.	Allow and keep untrusted
Validation failed certificates	Server certificate validation fails.	Block

The aforementioned options have the following actions:

Action	Description
Allow	Allow the server certificate and keep it untrusted.
Block	Block the certificate.

To configure common options for invalid certificates:

1. Go to *Security* > *Traffic* > *Security profiles*.
2. At the top of the security profile group page, in the *SSL Inspection* section, click *Configure security profile group settings*.
3. Enable *Certificate Inspection* or *Deep Inspection* as desired.
4. Configure each common option as this topic describes, as desired.
5. Click *OK*.

Configuring performance optimization options

By default, FortiSASE optimizes performance by exempting oversized files from security profile inspection, that is, allowing FortiSASE to bypass sessions when it detects oversized files. FortiSASE performs security profile inspection scans for files where the size is below the oversized limit.

When configuring certificate or deep inspection from *Security* > *Traffic* > *Security profiles* > *Configure security profile group settings*, FortiSASE allows you to configure its behavior when handling oversized uncompressed and compressed files.

You can configure the following actions for handling oversized files:

Setting	When FortiSASE detects an oversized file...
Allow	Bypass the session (default).
Block	Block the session.

You can customize the threshold to consider a file as oversized within the range of 10-64 MB.

Setting	Description
Oversized, uncompressed files are larger than	FortiSASE does not scan sessions when uncompressed files are oversized, which is when they are larger than the specified file size in MB. Otherwise, FortiSASE scans the session. The file size ranges from 10-64 MB (default 10 MB).
Oversized, compressed files are larger than	FortiSASE does not scan sessions when compressed files are oversized, which is when they are larger than the specified file size in MB. Otherwise, FortiSASE scans the session. The file size ranges from 10-64 MB (default 10 MB).

Configuring an action for HTTP/3 (QUIC) traffic

FortiSASE supports SSL inspection of HTTP/3 traffic, which allows security features requiring such inspection to work without the need to block QUIC. You can configure an action for HTTP/3 (QUIC) traffic from within a

security profile group. This setting applies to agent and edge device traffic and does not apply to proxy policy traffic.

For proxy users, to ensure security features requiring SSL deep inspection work with HTTP/3 traffic, you can block QUIC (UDP 443) traffic to ensure fallback from QUIC to TLS 1.3 (HTTP/2 traffic) occurs. On proxy user endpoints, you can block QUIC traffic by disabling the corresponding web browser setting.

To configure an action for HTTP/3 (QUIC) traffic within a security profile group:

1. Go to *Security > Traffic > Security profiles*.
2. From the *Profile Group* dropdown list, select the desired group or create a new one.
3. Under *SSL inspection: Certificate inspection mode*, click *Configure security profile group settings*.
4. Under *Deep/certificate inspection settings*, configure an action for *HTTP/3 inspection*. This option is only available if you select *Certificate inspection* or *Deep inspection* for Inspection method:

Option	Description
Inspect	Allows and inspects HTTP/3 traffic. Other security features, such as Web Filter, inspect the HTTP/3 traffic.
Bypass	Allows HTTP/3 traffic.
Block	Blocks HTTP/3 traffic, causing the client to send HTTP/2 requests instead in most cases.

5. Click *OK*.

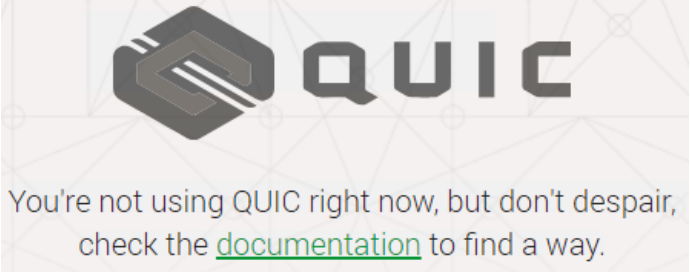
To block QUIC for proxy users in web browser settings and confirm it works:

On the endpoint machine, go to the web browser settings and disable QUIC as follows:

Browser	Action
Google Chrome	In the address bar, enter chrome://flags#enable-quic, and set *Experimental QUIC protocol* to *Disabled*.
Mozilla Firefox	In the address bar, enter about:config, search for *network.http.http3.enabled* and set it to *false*.
Microsoft Edge	In the address bar, enter edge://flags/#enable-quic, and set *experimental QUIC protocol* to *Disabled*.

After you have configured the web browser settings to block QUIC traffic, confirm it works as follows:

1. On an endpoint machine, open a web browser. For this example, Google Chrome is used.
2. Go to https://quic.nginx.org/. If QUIC traffic is blocked, you should see the following web site result:



AntiVirus

An AntiVirus (AV) profile allows you to configure FortiSASE to apply AV protection to traffic matching the following protocols:

- HTTP
- SMTP
- POP3
- IMAP
- FTP
- CIFS

AV inspection prevents potentially unwanted and malicious files from entering the network.

AV inspection supports content disarm and reconstruction (CDR), which sanitizes Microsoft Office documents and PDF files by removing potentially malicious and untrusted content from them (disarm) without affecting the integrity of its textual content (reconstruction). CDR does not support SMTP, FTP, and CIFS protocols.

Deep inspection is required for AV to decrypt and inspect content in encrypted traffic. See Certificate and deep inspection modes on page 315.

To apply AV protection to traffic matching certain protocols:

1. Go to *Security > Traffic > Security profiles*.
2. In the *AntiVirus* widget, click *Customize*.
3. Under *Inspected Protocols*, enable the toggle for the desired protocol.
4. Click *OK*.

To apply content disarm and reconstruction (CDR) to traffic matching supported protocols:

1. Go to *Security > Traffic > Security profiles*.
2. In the *AntiVirus* widget, click *Customize*.
3. Under *Inspected Protocols*, enable the toggle for protocols supported by CDR:
   a. HTTP
   b. POP3

c. IMAP

If SMTP, FTP, or CIFS are enabled, they will still be inspected by AV but will not have CDR applied to them.

4. Enable *Content disarm & reconstruction (CDR)* and configure these options:

Option	Description
Target file types	Supported file types for CDR. *Enable PDF* or *Office* as required.
Allow transmission if CDR error occurs	Configure the desired action when FortiSASE detects a CDR error: • *Enable* to allow the session • *Disable* to block the session

5. Click *OK*.

Intrusion prevention

Intrusion Prevention System (IPS) technology protects your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.

FortiSASE uses signature-based defense against known attacks or vulnerability exploits. These often involve an attacker attempting to gain access to your network. The attacker must communicate with the host in an attempt to gain access, and this communication includes commands or sequences of commands and variables. The IPS signatures include these command sequences, allowing FortiSASE to detect and stop the attack.

Intrusion prevention features are not guaranteed to work when other security features are disabled. It is recommended to enable one of these security features: Antivirus, File filter, DLP, Web filter, or DNS filter.

The following table describes the IPS profiles that you can select in FortiSASE:

	Recommended	Critical	Monitor
Protect client or server traffic	All (client and server)	All (client and server)	All (client and server)
Severity of the signatures	All severity levels: • Info • Low • Medium • High • Critical	• Low • Medium • High • Critical	All severity levels: • Info • Low • Medium • High • Critical
Protocols to be protected	All	All	All
Operating systems to be protected	All: • Windows • Linux • BSD • Solaris	All: • Windows • Linux • BSD • Solaris	All: • Windows • Linux • BSD • Solaris

	Recommended	Critical	Monitor
	• macOS	• macOS	• macOS
Applications to be protected	All	All	All
Action taken with traffic in which signatures are detected	Pass or drop matching traffic, depending on the signature default action, which FortiGuard IPS determines	• For signatures with medium, high, and critical severity: block or drop matching traffic. • For signatures with low severity: pass or drop matching traffic, depending on the signature default action, which FortiGuard IPS determines	Monitor, namely, pass or allow matching traffic while logging (monitoring) it.
Enable/disable logging of signatures included in filter	Enable	Enable	Enable

FortiSASE uses the IPS extended database for protection.

For a comprehensive list of protocols and applications protected by FortiGuard IPS signatures that FortiSASE uses, see the IPS database searchable by CVE lookup, ID lookup, or other keywords at Intrusion Prevention Service.

You can also configure custom IPS rules that use custom IPS signatures. To create custom IPS signatures using appropriate signature syntax, see Creating IPS and application control signatures.

To create, edit, and delete a custom IPS signature:

1. Go to *Security > Traffic > Security profiles*.
2. Select the *Profile resources* tab from the toolbar.
3. Select *Custom IPS signatures* to see all custom IPS signatures created across different security profile groups.
4. Do one of the following:
   - To create an IPS signature, click *Create > IPS Signature*. In the slide-in, specify *Tag*, *Comments*, and *Signature* using Creating IPS and application control signatures. Click *OK*. The newly created IPS signature is available to use in the *Intrusion Prevention* widget across different security profiles. These custom IPS signatures can be viewed in the *Custom IPS Signature* section of the *IPS signatures* table when the *Custom* profile is selected, when *IPS Signatures and Filters > Create* or *Edit* are selected, and when *Type* is selected as *Signature*.
   - To edit an IPS signature, select the desired IPS signature and click *Edit*. After making the required edits, click *OK*.
   - To delete, select the desired IPS signature available in the *Custom IPS signatures* list and click *Delete*. On the *Confirm delete* prompt, click *OK*.

To select an IPS profile and configure custom IPS rules to apply to traffic:

1. Go to *Security* > *Traffic* > *Security profiles* and switch to the *Profiles* tab from the toolbar.
2. In the *Intrusion Prevention* widget, click *Customize*.
3. Select a profile to apply to the traffic:

Profile	Description
Recommended (default)	Scans traffic for all known threats and applies the recommended action.
Critical	Scans traffic for critical threats and blocks them.
Monitor	Scans traffic for threats but does not apply any action. Primarily used for logging.
Custom	Allows for full customization of IPS signature and filter style rules.

4. To configure a custom profile, do the following:
   a. In the *IPS signatures and filters* section, click *Create*.
   b. In the *Add Custom IPS Filter* slide-n, configure the following:

Field	Description
Type	Choose the filter type by *Filter* criteria or by *Signature*.
Action	Action for matched IPS signatures to take. • *Allow*: Allow traffic to continue to its destination. • *Monitor*: Allow traffic to continue to its destination and log the activity. • *Block*: Drop traffic that matches the signature. • *Default*: Use the default action of the signature as defined in the FortiGuard database.
Packet logging	Enable packet logging to save a copy of the packets when they match the signature. Packet copies can be analyzed later.
Status	Define the signature status: • *Enable*: Enable the signature. • *Disable*: Disable the signature. • *Default*: Use the default status of the signature as defined in the FortiGuard database.
Filter	Define filter criteria used to select IPS signatures. Select the + to open the *Select Entries* field and select filter entries. There are different entry categories: • *Target*: Refers to the type of device targeted by the attack. • *Severity*: Refers to the level of the threat posed by the attack. • *Protocol*: Refers to the protocol that is the vector for the attack. • *OS*: Refers to the Operating System affected by the attack. • *Application*: Refers to the application affected by the attack.

5. Click *OK*.

6. (Optional) Create custom IPS signatures from the *Profile resources* tab. These custom IPS signatures can be viewed in the *Custom IPS Signature* section of the *IPS signatures* table when the *Custom* profile is selected, when *IPS Signatures and Filters* > *Create* or *Edit* are selected, and when *Type* is selected as *Signature*.

> The custom IPS rules are evaluated first before the configured IPS profile (i.e. recommended, critical, and monitor).
>
> You can use custom IPS rules to manage false positives by configuring a custom IPS signature with *Action* set to *Allow* or *Monitor* and using it in the rule.

File Filter

File Filter allows you to allow, block, or monitor specific file types. Inspection is based on file type only, not on file content.

> Deep inspection is required for File Filter to decrypt and inspect content in encrypted traffic. See Certificate and deep inspection modes on page 315.

To block traffic by file type:

1. Go to *Security* > *Traffic* > *Security profiles*.
2. In the *File Filter* widget, click *Customize*.
3. In the *File Types* table, select a file type and set the *Action* to *Allow* (default), *Monitor*, or *Block*.
4. In *Options*, select *Block password-protected files*. Password-protected files of the following types will be blocked when the *Action* is set to *Block* for these file types: 7z, MSOFFICE, MSOFFICEX, PDF, RAR, and ZIP.
5. Click *OK*.

Prerequisites and considerations

Prerequisites

Support for blocking password-protected files using File Filter is a select availability feature in FortiSASE that is not enabled by default on new instances and requires that the instance has been provisioned with Feature version support. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

Considerations

When File Filter configuration is synchronized using Central management, the *File Types* table only reflects the status of files that are not password-protected. See Configuring and applying a File Filter to block password-protected files on page 702.

DLP

FortiSASE data loss prevention (DLP) prevents sensitive data from leaving or entering your network by defining various sensitive data patterns, scanning for the patterns while inspecting traffic, and allowing, blocking, or logging only when traffic matches the patterns.

DLP rules specify how to handle traffic when a sensor or a file type is triggered. Sensors detect specific content types defined in dictionaries.

FortiSASE supports configuring predefined sensors and dictionaries managed by the FortiGuard DLP service.

DLP is configured based on the following components:

Component	Description
Data type	Define the type of pattern within data or content that DLP tries to match. DLP supports predefined types such as keyword, regular expressions, hex, credit card, and US social security number.
Data source type	Define the type of data source that DLP tries to match. DLP supports predefined types such as sensors, MPIP label, fingerprint, or none. With none, DLP matches using only file or message type and protocol as criteria.
Dictionary	Data type entry collections. When selecting a data type such as keyword, regular expressions, or hex, define the pattern that you are looking for. FortiSASE supports configuring custom dictionaries using built-in data types or configuring predefined dictionaries managed by the FortiGuard DLP service.
EDM template	An exact data match (EDM) template pairs the data from an external file, such as a data threat feed file, with FortiSASE DLP data types. The EDM template can link to a file on an external server to support dynamic updates, or the file can be uploaded to the EDM template.
Fingerprint	Indexed document matching (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.
MPIP Label	Labels are supported to help classify and protect sensitive information. MPIP labels are defined locally by configuring the Globally Unique Identifier (GUID).
Sensor	Define which dictionaries to check. You can match any dictionary or all dictionaries., or a special logical combination of the dictionaries. It can also count the number of dictionary matches to trigger the sensor. FortiSASE also supports configuring predefined sensors managed by the FortiGuard DLP service.
File pattern	Define file pattern groups based on predefined file types or define your own pattern to match the file name.
Rule	Define rules for matching a sensor based on a file type or a message, and the protocol type being used. It also allows you to choose the action to allow, block, or log only.

DLP requires deep inspection to decrypt and inspect content in encrypted traffic. See Certificate and deep inspection modes on page 315.

To create a DLP rule:

1. Go to *Security > Traffic > Security profiles*.
2. For *Profile Group*, select an existing profile group to edit or create a new profile group using *+* in the *Profile Group* dropdown list.
3. Disable all enabled security features (AntiVirus, Web Filter with Inline-CASB, Intrusion Prevention, DNS Filter) using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
4. In the *SSL inspection* section at the top of the page, ensure deep inspection is enabled:
   a. For *SSL inspection*, click *Configure SSL*.
   b. For *Inspection mode*, select *Deep inspection*.
   c. Click *OK*.
5. Create a DLP rule:
   a. In the *Data Loss Prevention (DLP)* widget, click the toggle button to enable this feature, and then click *Customize*.
   b. In the *Data Loss Prevention (DLP)* slide-in, click *Create* to create a new DLP rule.
   c. In the *New Rule* slide-in, configure these settings:

Field	Description
Name	Rule name.
Data Source Type	Select the type of data source that DLP tries to match. When you select *Sensors* or *MPIP Label*, you must select or create a new DLP sensor or sensitivity label, respectively.
Sensor	If you select *Sensors* for *Data Source Type*, select DLP sensors. You can either create a new DLP sensor and then select it or select a predefined sensor managed by the FortiGuard DLP service.
Sensitivity Label	If you select *MPIP Label* for *Data Source Type*, then select a sensitivity label. You must create a new sensitivity label and then select it.
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. You can either select a predefined file pattern table or create a new one by clicking *+* in the dropdown list.
Protocol	Check messages or files over one or more of these protocols.

6. Do one of the following:
   - If you selected *Sensors* for *Data Source Type*, do the following:
     i. Create a new sensor by clicking *+* next to *Sensor*. In the *Select Entries* slide-in, click *+* to the right to create a new sensor. In the *New DLP Sensor* slide-in, configure these settings:

Field	Description
Name	Sensor name.
Entry matches needed to trigger sensor	Logic used to apply to sensor entry matches to trigger sensor: • *All*: logical AND condition on matching entries • *Any*: logical OR condition on matching entries
Table of entries	Create one or more entries.

ii. Create a sensor entry by clicking *Create*. In the *New Entry* slide-in, configure these settings:

Field	Description
ID	Numerical ID for the sensor entry
Dictionary	Select the dictionary for this sensor entry. You can create a new dictionary and then select it or select a predefined dictionary managed by the FortiGuard DLP service.
Dictionary matches needed to consider traffic DLP risk	Number of dictionary matches to trigger sensor entry.
Status	Select whether the sensor entry is enabled or disabled.

iii. Create a dictionary by clicking the *Dictionary* field and click + to create a new DLP dictionary. In the *New DLP Dictionary* slide-in, configure these settings:

Field	Description
Name	Dictionary name.
Entries to evaluate	Logic used to apply to dictionary entry matches to trigger sensor: • *All*: logical AND condition on matching entries • *Any*: logical OR condition on matching entries
Table of dictionary entries	Create one or more dictionary entries.

iv. Create a new dictionary entry by clicking +. In the *New Entry* slide-in, configure these settings:

Field	Description
Type	Select a predefined *DLP Data Type* from the dropdown list.
Repeat	Enable or disable repeat matching of the selected *DLP Data Type*.
Status	Select whether the dictionary entry is *Enabled* or *Disabled*.

v. Click *OK* to create the new dictionary entry.
vi. Click *OK* to create the DLP dictionary. You will be prompted to select the newly created dictionary.
vii. Click *OK* to create the new sensor entry.
viii. Click *OK* to create the new sensor. You will be prompted to select the newly created sensor.
ix. Click *OK* to create the new DLP rule.

- If you selected *MPIP Label* for *Data Source Type*, do the following:
  i. Create a sensitivity label by clicking *+* next to *Sensitivity Label*.
  ii. In the *Create MPIP Sensitivity Label* slide-in, configure these settings:

Field	Description
Name	Sensitivity label name.
Sensitivity level GUID	Enter the globally unique identifier (GUID) for your sensitivity label. See Learn about sensitivity labels.

  iii. Click *OK*.
  iv. Click *OK* to create the sensitivity label. FortiSASE prompts you to select the newly created sensitivity label.
  v. Click *OK* to create the new DLP rule.

7. Click and drag the DLP rules in the desired order.

> Repeat any aforementioned step to create multiple entries for these settings:
> - Dictionary entries
> - DLP dictionaries
> - Sensor entries
> - Sensors
> - DLP rules

8. Configure the updated profile group in a policy:
   a. Go to *Security > Traffic > Policies*.
   b. Select an existing policy to apply the profile group to and click *Edit*. Alternatively, create a new policy to apply the profile group to.
   c. In the *Profile Group* field, select *Specify*. From the dropdown list, select the desired profile group. The *Profile Group* field is only available for policies where *Action* is configured as *Accept*.
   d. Click *OK*.

Blocking HTTPS upload traffic with credit card info example

This configuration blocks HTTPS upload traffic that includes credit card information. The predefined data type for credit card is used in the dictionary.

To configure blocking HTTPS upload traffic that includes credit card information:

1. Go to *Security > Traffic > Security profiles*.
2. For *Profile Group*, create a new profile group using *+* in the *Profile Group* dropdown list.
   a. In the *Create Profile Group* slide-in configure these settings:
      i. In the *Name* field, enter Custom-DLP-1.
      ii. For *Initial Configuration*, select *Basic*.
   b. Click *OK*.
   c. When prompted to select the new entry, click *OK*.

3. Disable all enabled security features (AntiVirus, Web Filter with Inline-CASB, Intrusion Prevention, DNS Filter, Application Control With Inline-CASB) using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
4. In the *SSL inspection* section at the top of the page, ensure deep inspection is enabled:
   a. For *SSL inspection*, click *Configure SSL*.
   b. For *Inspection mode*, select *Deep inspection*.
   c. Click *OK*.
5. Enable *Data Loss Prevention (DLP)*.
6. Create a DLP rule:
   a. In the *Data Loss Prevention (DLP)* widget, click *Customize*.
   b. In the DLP slide-in, click *Create* to create a new DLP rule.
   c. In the *New Rule* slide-in, configure these settings:

Field	Value
Name	dlp-case-1
Sensors	Select DLP sensors. You must create a new DLP sensor and then select it.
Severity	*Medium*
Action	*Block*
Type	*File*
File type	*builtin-patterns*
Protocol	*HTTP-GET, HTTP-POST*

   d. Create a new sensor:
      i. Create a new sensor by clicking *+* next to *Sensor*.
      ii. In the *Select Entries* slide-in, click *+ Create* to the right to create a new sensor.
      iii. In the *New Sensor* slide-in, configure these settings:

Field	Value
Name	sensor-case-1
Entry matches needed to trigger sensor	*Any*
Table of entries	Create a new entry.

   e. Create a sensor entry:
      i. Create a new sensor entry by clicking *+Create*.
      ii. In the *New Entry* slide-in, configure these settings:

Field	Value
ID	*1*

Field	Value
Dictionary	Select the dictionary for this sensor entry. You must create a new dictionary and then select it.
Dictionary matches needed to consider traffic DLP risk	*1*
Status	*Enabled*

f. Create a dictionary:

i. Click the *Dictionary* field and click *+Create* to create a new DLP dictionary.

ii. In the *New DLP Dictionary* slide-in, configure these settings:

Field	Value
Name	dl-case-1
Entry matches needed to trigger sensor	*Any*
Table of Dictionary Entries	Create one or more dictionary entries.

g. Create a dictionary entry:

i. Create a new dictionary entry by clicking *+Create*.

ii. In the *New Entry* slide-in, configure these settings:

Field	Value
Type	credit-card
Repeat	*Disable*
Status	*Enabled*

h. Click *OK* several times to complete the customization:

i. Click *OK* to create the new dictionary entry.

ii. Click *OK* to create the DLP dictionary. Click *OK* when prompted to select the newly created dictionary.

iii. Click *OK* to create the new sensor entry.

iv. Click *OK* to create the new sensor. Click *OK* when prompted to select the newly created sensor. Click *Close*.

v. Click *OK* to create the new DLP rule.

vi. Click *OK* to complete DLP configuration customization.

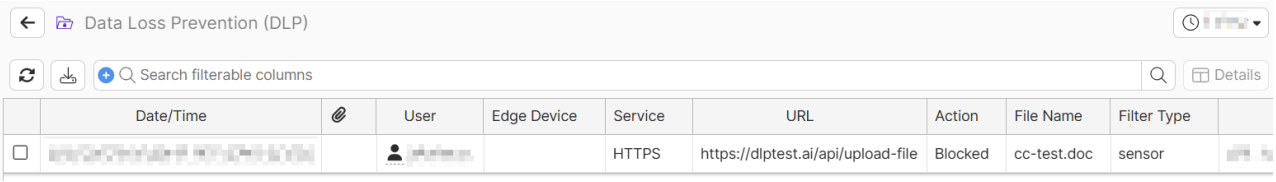
7. Configure the updated profile group in a policy:
   a. Go to *Security* > *Traffic* > *Policies*.
   b. Configure a new policy with these settings:

Field	Value
Name	Test-DLP-1
Source Scope	*Agent users*
Source	*All Traffic*
User	*All agent users*
Destination	*All Internet Traffic*
Service	*ALL*
Action	*Accept*
Profile Group	*Specify* Select *Custom-DLP-1*
Status	*Enable*
Log Allowed Traffic	*Enable* Select *All Sessions*

   c. Click *OK*.
8. Drag the *Test-DLP-1* to the top of the policy list. Ensure it is placed above *Allow-All*.

To verify blocking HTTPS upload traffic that includes credit card information is working:

1. Ensure that your endpoint with FortiClient installed is registered with FortiSASE Endpoint Management Service and that you have established a secure connection to FortiSASE.
2. On the connected endpoint, open the Chrome web browser in incognito mode.
3. In the web browser, go to https://dlptest.ai/sample-data.csv. Copy one of the credit card numbers from the file under the *CCN* column and paste it into a Word document. Save the document in .DOC format to your endpoint local drive as cc-test.doc.
4. Go to https://dlptest.ai. Under *File Upload*, select the .DOC file created and click *Submit*. Since HTTP POST traffic for the PDF file upload includes a credit card number, FortiSASE blocks the file and generates a DLP log.
5. In FortiSASE, go to *Operations* > *Logs* > *Security* > *Data Loss Prevention (DLP)* and confirm that FortiSASE generated a DLP block log entry that corresponds to your agent and cc-test.doc filename.



Blocking access to LLM applications using keywords and FQDN example

Applications like chatbots widely use large language models (LLMs), such as GPT, which are a type of Generative AI (GenAI).

This configuration blocks HTTPS upload traffic to the OpenAI ChatGPT, DeepSeek, and Gemini applications that includes a sensitive keyword using a message-based DLP rule. The predefined data type, keyword, is used in the DLP dictionary.

Web-based chatbot implementations are dynamic 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. See Restricting web usage using FortiGuard URL categories and URL filter on page 356.

Ensure you 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.

This example configures blocking QUIC so that the OpenAI server uses TLS 1.3 instead of QUIC. FortiSASE can inspect TLS 1.3 traffic using SSL deep inspection.

To configure blocking HTTPS upload traffic that includes sensitive keywords:

1. Go to *Security* > *Traffic* > *Security profiles*.
2. For *Profile Group*, create a new profile group using *+* in the *Profile Group* dropdown list.
   a. In the *Create Profile Group* slide-in configure these settings:
      i. In the *Name* field, enter llmapps.
      ii. For *Initial Configuration*, select *Basic*.
   b. Click *OK*.
   c. When prompted to select the new entry, click *OK*.
3. Disable AntiVirus, Web Filter with Inline-CASB, and DNS Filter using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
4. Observe that SSL inspection should already be enabled and is set to *Certificate Inspection*. Click *Configure SSL* and configure *Deep Inspection* using Fortinet_CA_SSL as the CA certificate accordingly.

5. Create a policy using the predefined QUIC service by going to *Security* > *Traffic* > *Policies*:
   a. Click *+Create*.
   b. In the *New Policy* page, configure the following:

Field	Value
Name	Block QUIC
Source Scope	*All*
Destination	*All Internet Traffic*
Service	Click *+*. Select *QUIC* under *Web Access*. Click *Close*.
Action	*Deny*
Status	*Enable*
Log Violation Traffic	*Enable*

   c. Click *OK*.
   d. Drag the newly created policy to the top of the policy list.
6. Enable *Data Loss Prevention (DLP)*.
7. Create a DLP rule:
   a. In the *Data Loss Prevention (DLP)* widget, click *Customize*.
   b. In the DLP slide-in, click *Create* to create a new DLP rule.
   c. In the *New Rule* slide-in, configure these settings:

Field	Value
Name	llmapps
Sensors	Select DLP sensors. You must create a new DLP sensor and then select it.
Severity	*Critical*
Action	*Block*
Type	*Message*
Protocol	*HTTP-POST*

   d. Create a new sensor:
      i. Create a new sensor by clicking *+* next to *Sensor*.
      ii. In the *Select Entries* slide-in, click *+ Create* to the right to create a new sensor.
      iii. In the *New Sensor* slide-in, configure these settings:

Field	Value
Name	llmapps

Field	Value
Entry matches needed to trigger sensor	*Any*
Table of entries	Create a new entry.

e. Create a sensor entry:

i. Create a new sensor entry by clicking *+Create*.

ii. In the *New Entry* slide-in, configure these settings:

Field	Value
ID	*1*
Dictionary	Select the dictionary for this sensor entry. You must create a new dictionary and then select it.
Dictionary matches needed to consider traffic DLP risk	*1*
Status	*Enabled*

f. Create a dictionary:

i. Click the *Dictionary* field and click *+Create* to create a new DLP dictionary.

ii. In the *New DLP Dictionary* slide-in, configure these settings:

Field	Value
Name	llmapps
Entry matches needed to trigger sensor	*All*
Table of Dictionary Entries	Create two dictionary entries as follows.

g. Create a dictionary entry with the *programming* keyword by doing the following:

i. Create a new dictionary entry by clicking *+Create*.

ii. In the *New Entry* slide-in, configure these settings:

Field	Value
Type	*keyword*
Pattern	programming
Case sensitive	Enable
Repeat	Disable
Status	Enabled

The configuration enables *Case sensitive* to enable ignoring letter case when pattern matching.

h. Create a dictionary entry with the *tips* keyword by doing the following:
   i. Create a new dictionary entry by clicking *+Create*.
   ii. In the *New Entry* slide-in, configure these settings:

Field	Value
Type	*keyword*
Pattern	tips
Case sensitive	Enable
Repeat	Disable
Status	Enabled

   The configuration enables *Case sensitive* to enable ignoring letter case when pattern matching.

i. Click *OK* several times to complete the customization:
   i. Click *OK* to create the new dictionary entry.
   ii. Click *OK* to create the DLP dictionary. Click *OK* when prompted to select the newly created dictionary.
   iii. Click *OK* to create the new sensor entry.
   iv. Click *OK* to create the new sensor. Click *OK* when prompted to select the newly created sensor. Click *Close*.
   v. Click *OK* to create the new DLP rule.
   vi. Click *OK* to complete DLP configuration customization.

8. Configure the updated profile group in a policy:
   a. Go to *Security* > *Traffic* > *Policies*.
   b. Configure a new policy with these settings:

Field	Value
Name	llmapps
Source Scope	*All*
Destination	*Specify:* 1. Click *+*. 2. In the *Select Entries* slide-in, click *+* and create new *+ IPv4 Host*. 3. In the *New Host* slide-in, configure these settings: a. *Location*: *Unspecified* b. *Name*: ChatGPT c. *Type*: *FQDN* d. *FQDN*: chatgpt.com 4. Click *OK* to create the new host. 5. Click *OK* when prompted to select the newly created host. 6. Click *Close*. 7. Repeat steps 1-6 for Gemini and DeepSeek. Create and use the following FQDNs: • **Gemini**: gemini.google.com

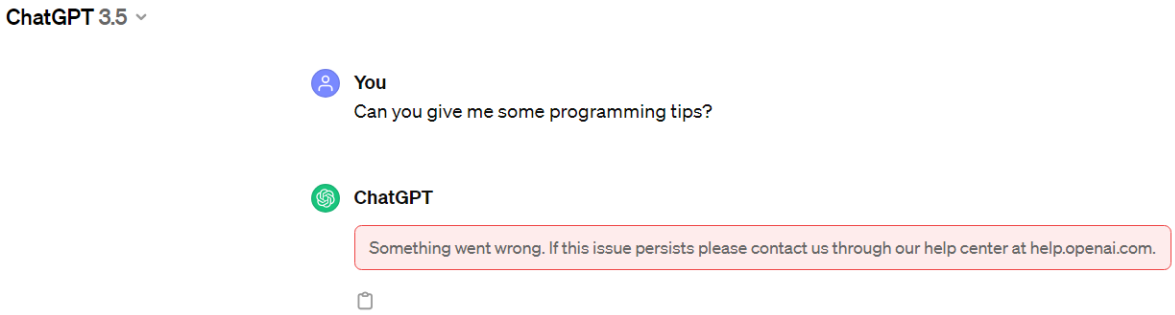
Field	Value
	• **DeepSeek**: chat.deepseek.com
Service	*ALL*
Action	*Accept*
Profile Group	*Specify* Select *llmapps*.
Status	*Enable*
Log Allowed Traffic	*Enable* Select *All Sessions*

c. Click *OK*.

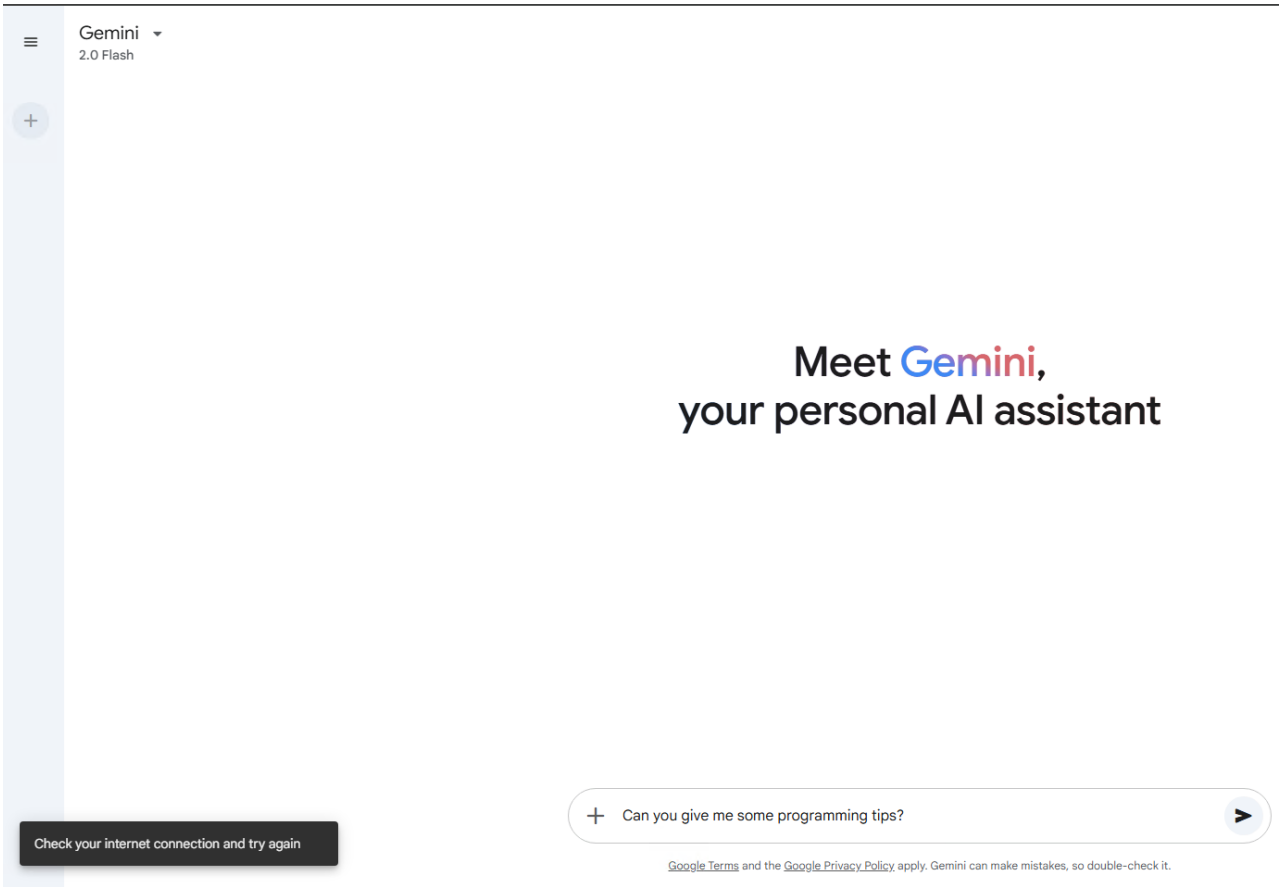
9. Drag the llmapps policy to the top of the policy list. Ensure it is placed above *Allow-All*.

To verify blocking HTTPS upload traffic that includes sensitive keywords is working:

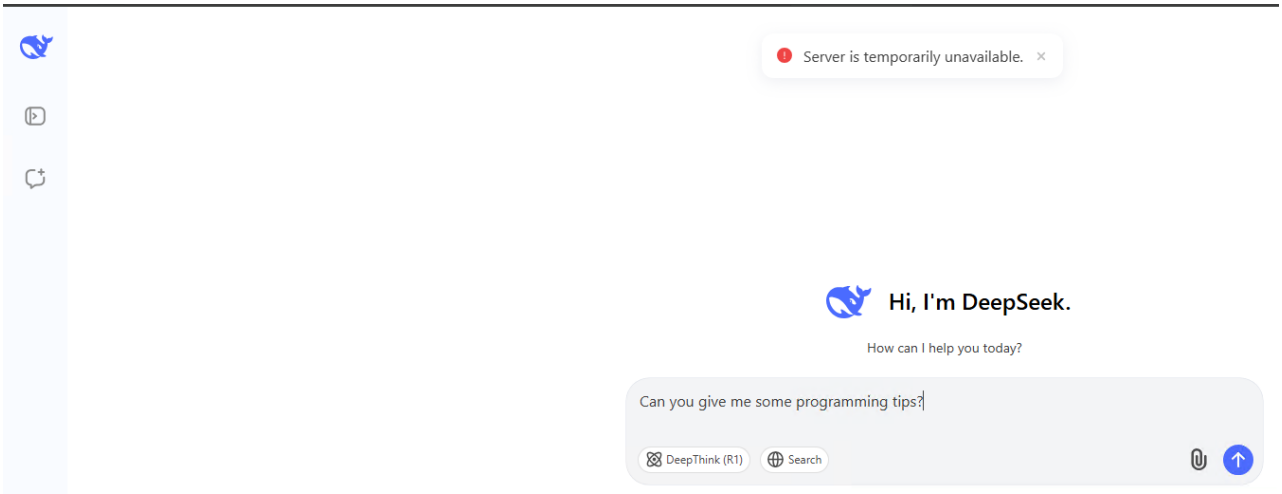
1. Ensure that your endpoint with FortiClient installed is registered with FortiSASE Endpoint Management Service and that you have established a secure connection to FortiSASE.
2. On the connected endpoint, open the Chrome web browser in incognito mode.
3. In the web browser, go to one of the following:
   - https://chatgpt.com
   - https://gemini.google.com
   - https://chat.deepseek.com
4. Search for any phrase that includes the keywords set up in the DLP dictionary. Since the phrase in HTTP POST traffic includes both sensitive keywords, FortiSASE blocks this traffic to ChatGPT and generates a DLP log. Verify the request fails and an error is generated.
   The following shows an example request failure in ChatGPT:



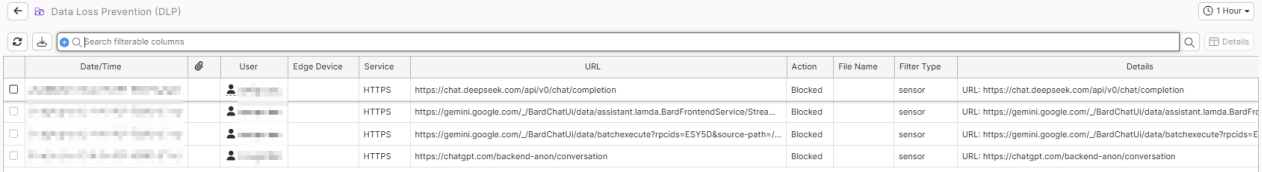
   The following shows an example request failure in Gemini:



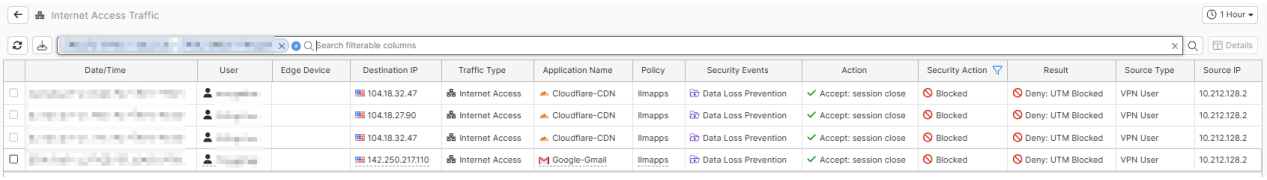
The following shows an example request failure in DeepSeek:



5. In FortiSASE, go to *Operations* > *Logs* > *Security* > *Data Loss Prevention (DLP)* and confirm that FortiSASE generated DLP block log entries that correspond to your agent and visiting the respective websites.



6. Go to *Operations* > *Logs* > *Traffic* > *Internet Access Traffic* and confirm that FortiSASE generated DLP block log entries that correspond to your agent and visiting the respective websites.



Blocking file with MPIP sensitivity label example

To safeguard your organization's data, you can employ labels as markers for sensitive information. Microsoft provides sensitivity labels, which act as identifiers emphasizing the importance of the data that they are associated with, thereby enhancing the security measures in place. See Protect your sensitive data with Microsoft Purview.

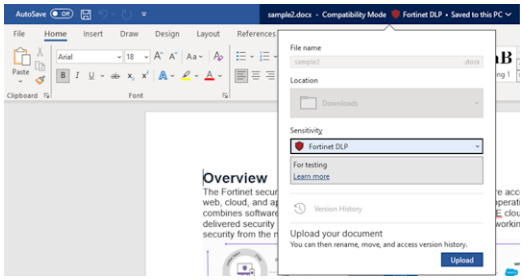
You can effectively manage any data traffic that includes a sensitivity label using FortiSASE. Usage of a predefined data source type, MPIP Label, specifically designed for matching MPIP sensitivity labels previously applied to files, makes this possible.

This configuration blocks HTTPS upload traffic that includes an MPIP sensitivity label.

To complete prerequisites:

Before configuring FortiSASE, complete the following steps:

1. Create and configure sensitivity labels and their policies. See Create sensitivity labels.
2. Apply a sensitivity label to content. See Apply sensitivity labels to your files and email. Once the sensitivity label is applied on a file, it displays on the sensitivity bar.



3. Obtain the globally unique identifier (GUID) for your sensitivity labels. See Search for documents by sensitivity label. The following shows a sample GUID:

```
PS C:\Windows\system32> Get-Label |Ft Name, Guid

Name                                Guid
----                                ----
Fortinet DLP                        ca51e4ff-0733-4744-bebb-d3e1eb6383f4
```

FortiSASE uses the GUID for label matching. The value of *Sensitivity level GUID* is configured to correspond to the label's GUID.

To configure blocking HTTPS upload traffic that includes an MPIP sensitivity label applied:

1. Go to *Security > Traffic > Security profiles*.
2. For *Profile Group*, select an existing profile group to edit or create a new profile group using *+* in the *Profile Group* dropdown list.
3. Disable all enabled security features (AntiVirus, Web Filter with Inline-CASB, Intrusion Prevention, DNS Filter) using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
4. In the *SSL Inspection* widget, ensure deep inspection is enabled:
   a. For *SSL inspection*, click *Customize*.
   b. Select *Deep Inspection*.
   c. Click *OK*.
5. Create a DLP rule:
   a. In the *Data Loss Prevention (DLP)* widget, click the toggle button to enable this feature, and then click *Customize*.
   b. In the *DLP* slide-in, click *Create* to create a new DLP rule.
   c. In the *New Rule* slide-in, configure these settings:

Field	Description
Name	Rule name.
Data Source Type	Select *MPIP Label*. You must select or create a new sensitivity label.
Sensitivity Label	Create a new sensitivity label and then select it.
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. You can either select a predefined file pattern table or create a new one by clicking *+* in the dropdown list.
Protocol	Check messages or files over one or more of these protocols.

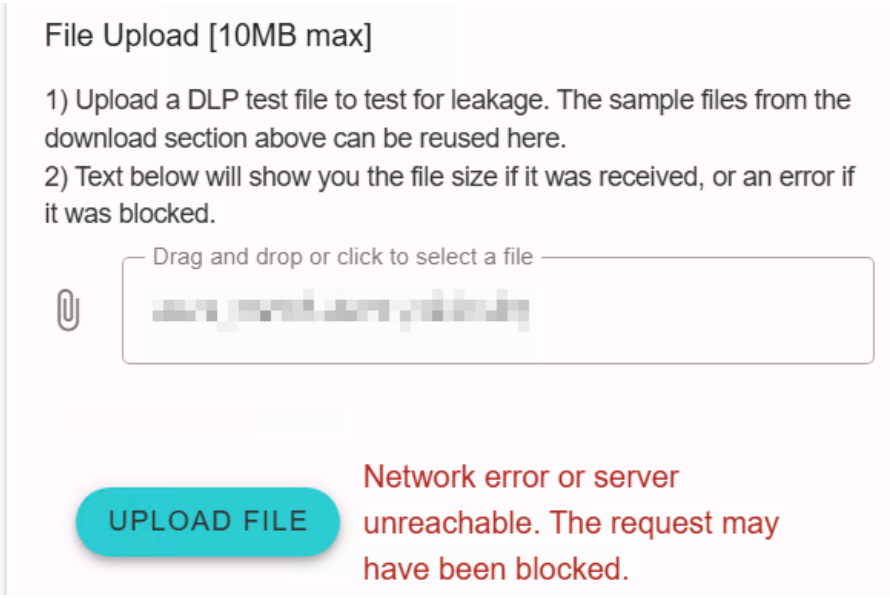
6. Create a new sensitivity label:
   a. Create a new sensitivity label by clicking *+* next to *Sensitivity Label*.
   b. In the *Create MPIP sensitivity label* slide-in, configure these settings:

Field	Description
Name	Sensitivity label name.
Sensitivity level GUID	Enter the globally unique identifier (GUID) for your sensitivity label. See To complete prerequisites: on page 342 for how to obtain the GUID for your sensitivity label.

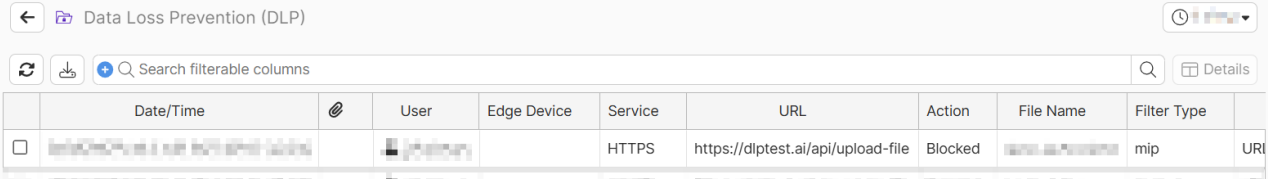
   c. Click *OK*.
7. Click *OK* twice to complete creating the DLP rule:
   a. Click *OK* to create the sensitivity label. You will be prompted to select the newly created sensitivity label.
   b. Click *OK* to create the new DLP rule.
8. Configure the updated profile group in a policy:
   a. Go to *Security* > *Traffic* > *Policies*.
   b. Select an existing policy to apply the profile group to and click *Edit*. Alternatively, create a new policy to apply the profile group to.
   c. In the *Profile Group* field, select *Specify*. From the dropdown list, select the desired profile group. The *Profile Group* field is only available for policies where *Action* is configured as *Accept*.
   d. Click *OK*.

To configure blocking HTTPS upload traffic that includes an MPIP sensitivity label applied is working:

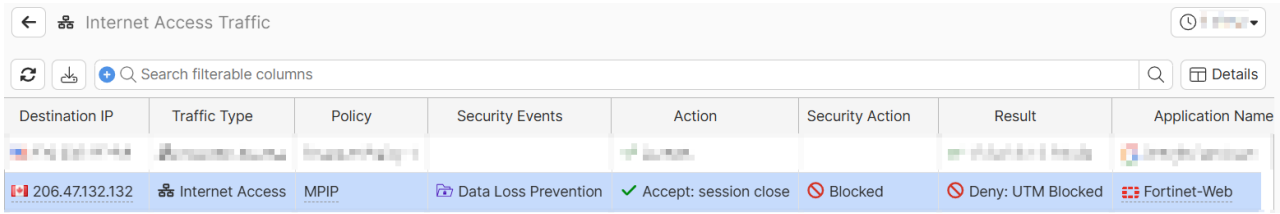
1. Ensure that your endpoint with FortiClient installed is registered with FortiSASE Endpoint Management Service and that you have established a secure connection to FortiSASE.
2. On the connected endpoint, open the Chrome web browser in incognito mode.
3. In the web browser, go to https://dlptest.ai
4. Upload a Word document file with an MPIP sensitivity label applied.
5. Observe that the file upload fails before and after file submission:



6. In FortiSASE, go to *Operations* > *Logs* > *Security* > *Data Loss Prevention (DLP)* and confirm that FortiSASE generated a DLP block log entry that corresponds to your agent and visiting https://dlptest.ai



7. Go to *Operations* > *Logs* > *Traffic* > *Internet Access Traffic* and confirm that FortiSASE generated a DLP block log entry that corresponds to your agent and visiting https://dlptest.ai



Blocking HTTPS upload traffic using EDM template example

Exact data matching (EDM) identifies particular data values within an indexed data source that require safeguarding. You can define a dataset in a CSV or TXT file on a server and point FortiSASE to this external resource or upload a CSV or TXT file directly to FortiSASE.

This configuration blocks HTTPS upload traffic that matches an EDM template.

To configure blocking HTTPS upload traffic using an EDM template:

1. Create a profile group:
   a. Go to *Security* > *Traffic* > *Security profiles*.
   b. For *Profile Group*, select an existing profile group to edit or create a new profile group using *+* in the *Profile Group* dropdown list.
   c. In the *Create Profile Group* slide-in, configure the following:
      i. In the *Name* field, enter DLP-EDM-Profile.
      ii. For *Initial Configuration*, select *Basic*.
      iii. Click *OK*. When prompted to select the new entry, click *OK*.
2. Disable all enabled security features (AntiVirus, Web Filter with Inline-CASB, DNS Filter) using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
3. In the *SSL inspection* section at the top of the page, ensure deep inspection is enabled:
   a. For *SSL inspection*, click *Configure SSL*.
   b. For *Inspection mode*, select *Deep inspection* and configure using Fortinet_CA_SSL as the CA certificate.
   c. Click *OK*.
4. Configure DLP:
   a. Create a DLP rule:
      i. In the *Data Loss Prevention (DLP)* widget, click the toggle button to enable this feature, and then click *Customize*.
      ii. In the *Data Loss Prevention (DLP)* slide-in, click *Create* to create a new DLP rule.

iii. In the *New Rule* slide-in, configure these settings:

Field	Description
Name	DLP-EDM-1
Data Source Type	*Sensors*
Sensor	*DLP sensors*. You must create a new DLP sensor and then select it.
Severity	*Critical*
Action	*Block*
Type	*Message*
Protocol	*HTTP-POST*

b. Create a new sensor by clicking *+* next to *Sensor*. In the *Select Entries* slide-in, click *+* to the right to create a new sensor. In the *New DLP Sensor* slide-in, configure these settings:

Field	Description
Name	DLP-EDM-1
Entry matches needed to trigger sensor	*Any*
Table of entries	Create one entry.

c. Create a sensor entry by clicking *Create*. In the *New Entry* slide-in, configure these settings:

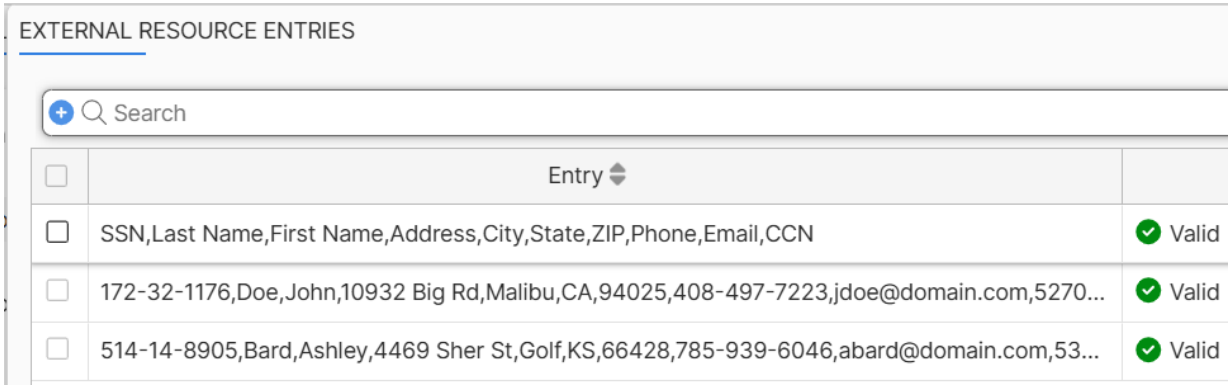
Field	Description
ID	1
Sensor	Select the EDM template for this sensor entry. You must create a new EDM template and then select it.
Dictionary matches needed to consider traffic DLP risk	1
Status	Enabled

d. Create an EDM template by clicking the *Sensor Entry* field, click *+*, and select *Create New* > *+DLP EDM Template*. In the *New DLP EDM Template* slide-in, configure these settings:

Field	Description
Name	DLP-EDM-T1
Resource settings	
Resource type	*File upload*
Upload file	Upload the customer_data.csv file by clicking to select the file or dropping the file into area provided
Match criteria	

Field	Description
+All of these fields	Selected: • Column index: *1*, Data type: `ssn-us`
+Any of these fields	Selected • Minimum number of fields matched: *1* • Column index: *3*, Data type: *edm-keyword* • Column index: *9*, Data type: *edm-keyword*

e. Click *View Entries* to view the data entries imported from the CSV file.



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.

f. Click OK several times to complete the configuration:

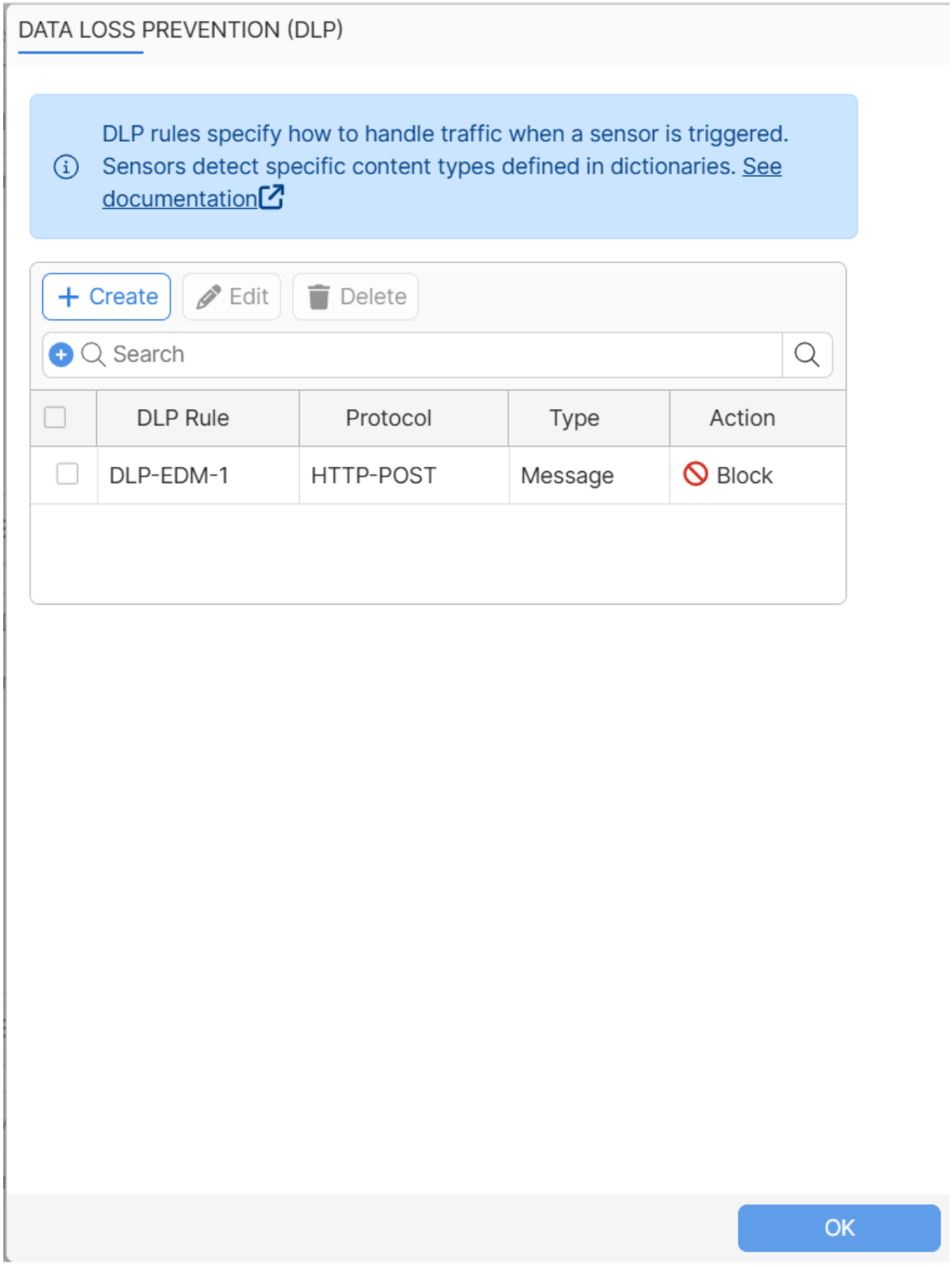
i. Click *OK* to create the new DLP template.

ii. Click *OK* to create the new sensor entry.

iii. Click *OK* to create the new sensor. You will be prompted to select the newly created sensor.

iv. Click *OK* to create the new DLP rule.

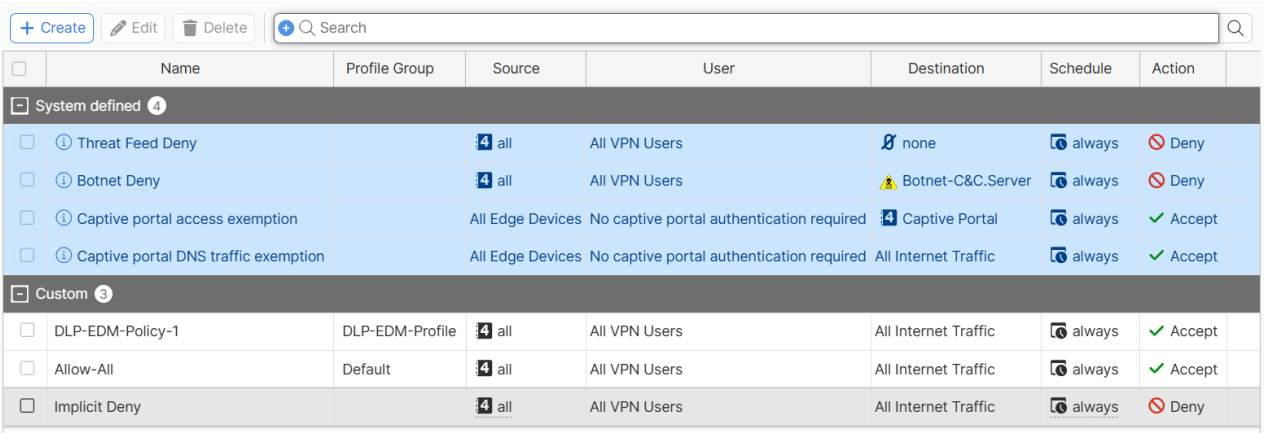
v. Click *OK* to complete DLP configuration customization.



5. Configure the updated profile group in a policy:
   a. Go to *Security* > *Traffic* > *Policies*.
   b. Create a new policy to apply the profile group to:

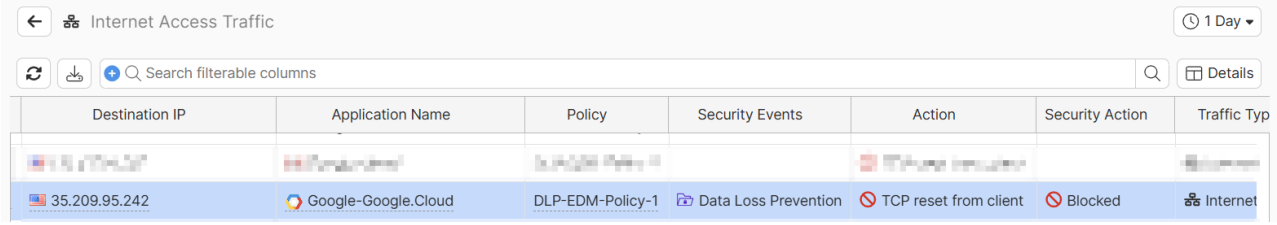
Field	Value
Name	DLP-EDM-Policy-1
Source Scope	*All*
Destination	*All Internet Traffic*
Service	*ALL*
Action	*Accept*
Profile Group	*Specify* Select *DLP-EDM-Profile*
Status	Enable
Log Allowed Traffic	Enable Select *All Sessions*

   c. Click *OK*.
6. Drag the DLP-EDM-Policy-1 policy to the top of the policy list. Ensure it is placed above Allow-All.



To verify blocking HTTPS upload traffic using an EDM template is working:

1. Ensure that your endpoint with FortiClient installed is registered with the FortiSASE Endpoint Management Service and that you have established a secure connection to FortiSASE.
2. On the connected endpoint, open the Chrome web browser in incognito mode.
3. In Chrome, go to https://dlptest.ai.
4. Under *Text upload to website*, enter *John 172-32-1176* and click *Submit Text*. FortiSASE blocks the upload traffic.
5. In FortiSASE, go to *Operations* > *Logs* > *Security* > *Data Loss Prevention (DLP)* and confirm that FortiSASE generated a DLP block log entry that corresponds to your agent and visiting https://dlptest.ai.
6. Go to *Operations* > *Logs* > *Traffic* > *Internet Access Traffic* and confirm that FortiSASE generated a DLP block log entry that corresponds to your agent and visiting https://dlptest.ai.



Prerequisites and considerations

- When using commonly used SSL-encrypted protocols such as HTTPS, SMTPS, POP3S, IMAPS, and FTPS, you must set SSL inspection to deep inspection. See Certificate and deep inspection modes on page 315.
- In this example, an EDM template named DLP-EDM-T-1 is created. During this process, a CSV file (customer_data.csv) is uploaded to FortiSASE.
- Create the following sample CSV file saved as customer_data.csv on your computer:

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 `ssn-us` data type.
  - Column index 3 and 9 contain patterns for the `edm-keyword` data type.
  - The patterns from column index 1 must match for FortiSASE to take an action.
  - The pattern from either column index 3 or 9 must match for FortiSASE 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.

Blocking HTTPS upload traffic using IDM with DLP fingerprinting example

Indexed document matching (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.

The file that the DLP profile filters is uploaded to a server and FortiSASE generates and stores a checksum fingerprint. FortiSASE generates a fingerprint for all the files that are detected in network traffic, and compares all the checksums stored in its fingerprint database. If FortiSASE finds a match, it takes the configured action.

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.

This configuration blocks HTTPS upload traffic that matches the fingerprints that are stored in the DLP fingerprint database.

Prerequisites and considerations

- When utilizing commonly-used SSL-encrypted protocols such as HTTPS, SMTPS, POP3S, IMAPS, and FTPS, SSL inspection must be set to Deep Inspection. See Certificate and deep inspection modes on page 315.
- A file server is required for the user to upload files. Each uploaded file will have a fingerprint generated by FortiSASE and will be stored locally as a checksum. Currently, only servers that are using the Samba (SMB) protocol are compatible.
- When creating or editing a DLP fingerprint database, the server scan and fingerprint database generation may take a few minutes to complete and may take longer if the network has high latency or if the database is large.
- The Samba file server can be an external server or an internal server behind a FortiGate SPA hub. Currently, only SPA hubs configured with the BGP per overlay design are supported.
- Currently, only the Server IP address can be used to specify the location of the Samba file server.
- In this example:
  - 10.100.99.103 is the IP address of the Samba file server behind the FortiGate SPA hub configured with BGP per overlay and FortiSASE has been configured with SPA accordingly.
  - Files of DOCX and TXT file types have been uploaded to the file server. These same files are uploaded via HTTP POST to trigger the DLP fingerprint detection and action.

To configure blocking HTTPS upload traffic matching fingerprints in the DLP fingerprint database:

1. Create a profile group
   a. Go to *Security > Traffic > Security profiles*.
   b. For *Profile Group*, select an existing profile group to edit or create a new profile group using *+* in the *Profile Group* dropdown list.
   c. In the *Create Profile Group* slide-in, in the *Name* field, enter DLP-FP-Profile.
   d. For *Initial Configuration*, select *Basic*. Click *OK*.
2. Disable all enabled security features (AntiVirus, Web Filter with Inline-CASB, DNS Filter) using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
3. In the *SSL inspection* section at the top of the page, ensure deep inspection is enabled:
   a. For *SSL inspection*, click *Configure SSL*.
   b. For *Inspection mode*, select *Deep inspection* and configure using Fortinet_CA_SSL as the CA certificate.
   c. Click *OK*.
4. Create a DLP fingerprint database:
   a. Click the *Profile resources* tab.
   b. Click the *DLP fingerprint databases* subtab.
   c. Click *Create*.

d. In the *Create DLP Fingerprint Database* slide-in, configure the following:

Field	Value
Name	DLP-FP-DB-1
Sensitivity level	*Critical*
Server settings	
Server IP/FQDN	10.100.99.103
Username	kiki
Password	< Password >
Server directory	private/
Include sub-directories	Enabled
File pattern	* (wildcard to select all files on server)
Synchronization settings	
Synchronization interval	*Daily*
Synchronize during specified time	12:00 AM
Remove fingerprints of deleted files	Enabled
Keep fingerprints of older file versions	Disabled
Scan on file creation	Enabled

e. Click *OK*.

5. Click the *Profiles* tab. The *DLP-FP-Profile* profile should still be selected.

6. Configure DLP:

a. Create a DLP rule:

i. In the *Data Loss Prevention (DLP)* widget, click the toggle button to enable this feature, and then click *Customize*.

ii. In the *Data Loss Prevention (DLP)* slide-in, click *Create* to create a new DLP rule.

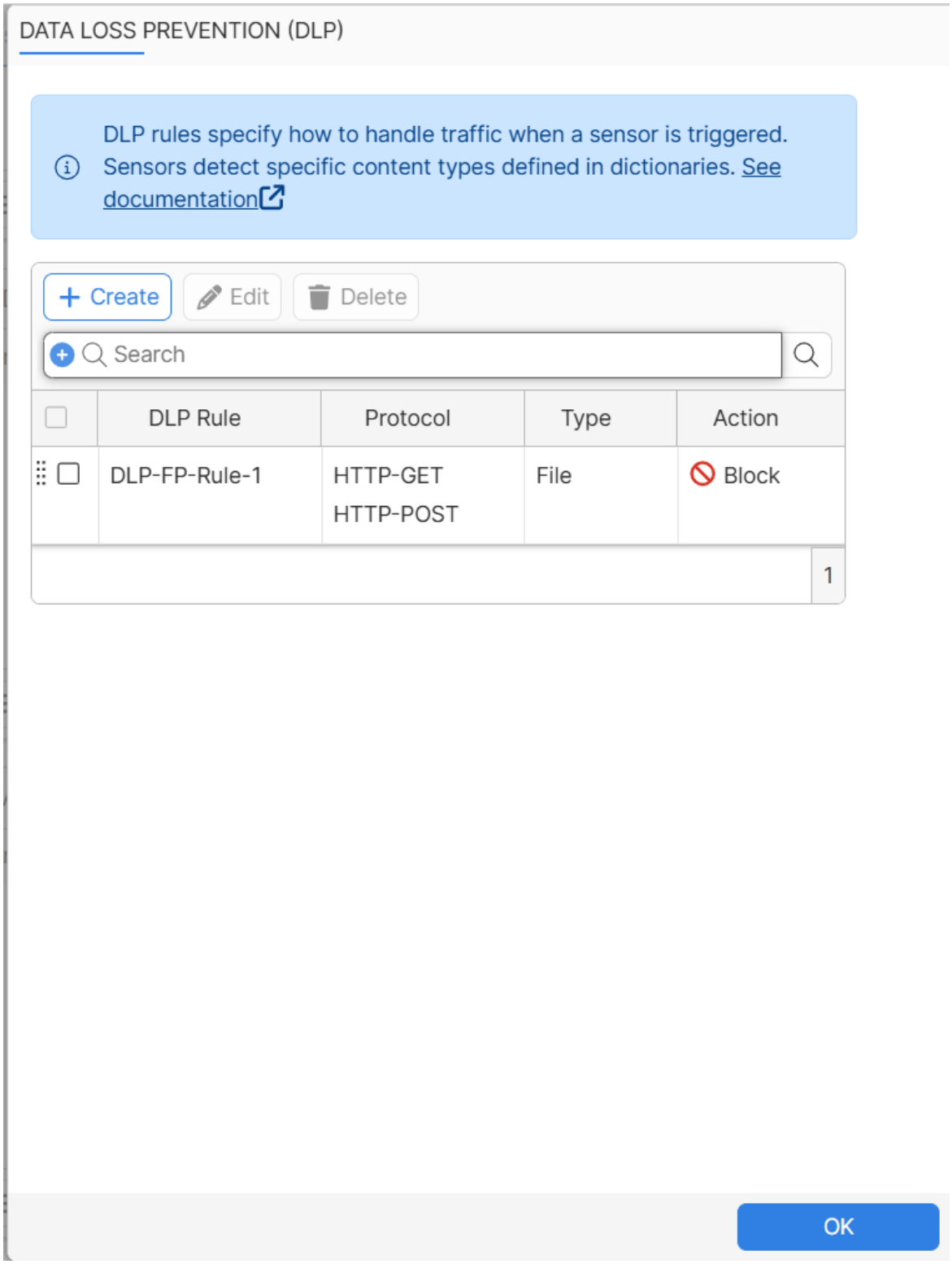
iii. In the *New Rule* slide-in, configure these settings:

Field	Description
Name	DLP-FP-Rule-1
Data Source Type	*Fingerprint*
Severity	*Critical*
Sensitivity Levels	*Critical*
Action	*Block*
File Type	*All*
Protocol	*HTTP-GET* *HTTP-POST*

b. Click OK a couple times to complete the configuration:

i. Click *OK* to create the new DLP rule.

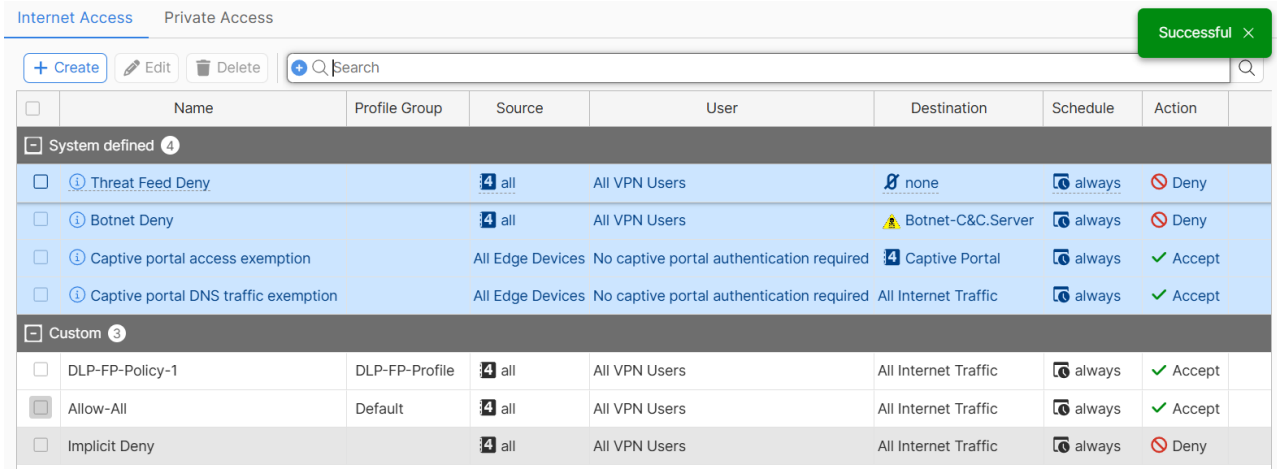
ii. Click *OK* to complete DLP configuration customization.



7. Configure the updated profile group in a policy:
   a. Go to *Security > Traffic > Policies*.
   b. Create a new policy to apply the profile group to:

Field	Value
Name	DLP-FP-Policy-1
Source Scope	*All*
Destination	*All Internet Traffic*
Service	*ALL*
Action	*Accept*
Profile Group	*Specify* Select *DLP-FP-Profile*
Status	Enable
Log Allowed Traffic	Enable Select *All Sessions*

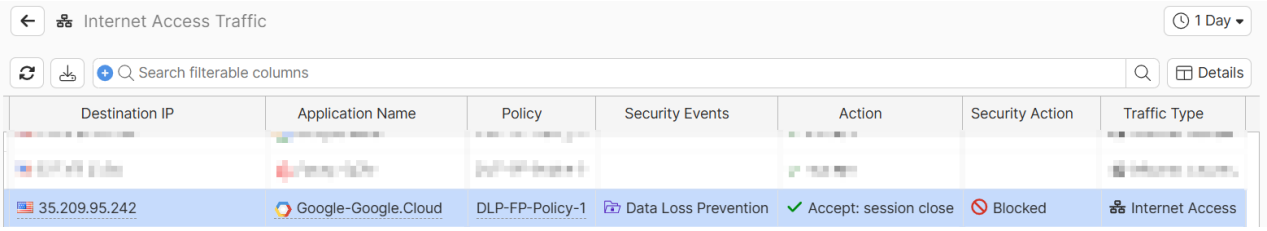
   c. Click *OK*.
8. Drag the DLP-FP-Policy-1 policy to the top of the policy list. Ensure it is placed above Allow-All.



To verify blocking HTTPS upload traffic using IDM is working:

1. Ensure that your endpoint with FortiClient installed is registered with FortiSASE Endpoint Management Service and that you have established a secure connection to FortiSASE.
2. On the connected endpoint, open the Chrome web browser in incognito mode.
3. In the web browser, go to https://dlptest.ai.
4. In *File Upload*, click on the area and select one of the DOCX or TXT files that were stored on the Samba file server.
5. Observe that FortiSASE has blocked the upload traffic based on the replacement message output given.
6. In FortiSASE, go to *Operations > Logs > Security > Data Loss Prevention (DLP)* and confirm that FortiSASE generated a DLP block log entry that corresponds to your agent and visiting https://dlptest.ai.

7. Go to *Operations* > *Logs* > *Security* > *Internet Access Traffic* and confirm that FortiSASE generated a DLP block log entry that corresponds to your agent and visiting https://dlptest.ai.



Web Filter

Web filter restricts or controls user access to web resources. In FortiSASE, Web Filter consists of the following components:

Component	Description
URL category	Provides categories from the FortiGuard Web Filter service that you can use to filter web traffic.
URL filter	Uses specific URLs with patterns containing text and regular expressions so FortiSASE can process the traffic based on the filter action (exempt, block, allow, monitor) and webpages that match the criteria.
Content filter	Blocks or exempts webpages containing words or patterns that you specify. Additionally, in HTTPS connections, since the HTTP payload is encrypted, the default certificate inspection cannot inspect the traffic. To apply content filter on HTTPS traffic, you must use SSL deep inspection. See Certificate and deep inspection modes on page 315.

These components interact with each other to provide maximum control over what users on your network can view and protect your network from many internet content threats.

FortiSASE applies web filters in the following order:

1. URL filter
2. URL category
3. Content filter

In FortiSASE, by default, there is one global Web Filter configuration that applies to all users using a default security profile group applied to a default allow agent or proxy policy. Administrators can customize configuration for Web Filter and other security features by creating a custom security profile group, customizing settings for the new profile group, creating a new agent or proxy policy with selected users or user groups specified, and then applying the profile group to the policy.

FortiSASE supports these Web Filter options:

Option	Description
Block Invalid URLs	Block websites when their SSL certificate CN field does not contain a valid domain name.

Option	Description
	This option also blocks URLs that contains spaces. If there is a space in the URL, you must write it as %20 in the URL path.
Allow websites when a rating error occurs	Allow access to websites that return a rating error from the FortiGuard Web Filter service.
Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex	This setting applies to popular search sites and prevents explicit websites and images from appearing in search results. The supported search sites are Google, Yahoo, Bing, and Yandex. To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 315.
Log all search keywords	Use this setting to log all search phrases from search sites including Google, Yahoo, Bing, Baidu, Vimeo, and Twitter. When this feature is enabled, in the *Web Filter with Inline-CASB* security logs, the *Key Word* column appears with search phrases from supported search sites.

Restricting web usage using FortiGuard URL categories and URL filter

To restrict web usage using FortiGuard URL categories and URL filter:

1. Go to *Security > Traffic > Security profiles*.
2. In the *Web Filter With Inline-CASB* widget, click *Customize*.
3. Enable *FortiGuard Category Based Filter*.
4. By default, FortiSASE allows access to FortiGuard categories when you enable the FortiGuard category-based filter. To change the category action to *Monitor* or *Block*, select the desired category, then select *Monitor* or *Block*. The following provides descriptions of the actions:

Type	Description
Allow	Passes the traffic to the remaining web filters, antivirus inspection engine, and DLP inspection engine. If the URL does not appear in the URL list, FortiSASE allows the traffic.
Monitor	Processes the traffic the same way as the Allow action. For the Monitor action, FortiSASE generates a log message each time it establishes a matching traffic pattern.
Block	Denies or blocks attempts to access any URL that belongs to the category. A replacement message displays.
Warning	Displays a message to the user allowing them to continue if they choose. You can customize this message in HTML templates on page 589.

Type	Description
	When you configure the action as *Warning*, you can also configure a warning interval. When the user first attempts to access a site that belongs to this category, the configured warning displays. After the configured warning interval, the warning displays again and the user must reacknowledge it to continue.
Disable	Remove the category from the from the web filter profile. This option is only available for custom categories.

5. Under *URL Filter*, click *Create*.
6. Configure the URL filter:
   a. In the *URL* field, enter the desired URL.
   b. For *Type*, select one of the following:

Type	Description
Simple	Tries to strictly match the full context. For example, if you enter www.facebook.com in the *URL* field, it only matches traffic with www.facebook.com. It does not match facebook.com or message.facebook.com. When FortiSASE finds a match, it performs the selected URL action.
Wildcard	Tries to match the pattern based on the rules of wildcards. For example, if you enter *fa* in the *URL* field, it matches all the content that has fa such as www.facebook.com, message.facebook.com, fast.com, and so on. When FortiSASE finds a match, it performs the selected URL action.
RegExp	Tries to match the pattern based on the rules of regular expressions. When FortiSASE finds a match, it performs the selected URL action.

   c. For *Action*, select one of the following:

Type	Description
Allow	Passes the traffic to the remaining web filters, antivirus inspection engine, and data loss prevention (DLP) inspection engine. If the URL does not appear in the URL list, FortiSASE allows the traffic.
Block	Denies or blocks attempts to access any URL that matches the URL pattern. A replacement message displays.
Exempt	Allows the traffic to pass through, bypassing other web filters, AV inspection engine, and DLP inspection engine.
Monitor	Processes the traffic the same way as *Allow*. FortiSASE generates a log message each time it establishes a matching traffic pattern.

   d. Configure the status as desired.
7. URL filter entries are evaluated in top-down order. To reorder a URL filter entry, hover over the left side of an entry and drag-and-drop it above or below other entries as desired.

8. Click *OK*.

Restricting web usage using content filter

Restricting web usage using content filter for HTTPS pages requires enabling SSL deep inspection. See Certificate and deep inspection modes on page 315.

To restrict web usage using content filter:

1. Go to *Security > Traffic > Security profiles*.
2. In the *Web Filter With Inline-CASB* widget, click *Customize*.
3. Under *Content Filter*, click *Create*.
4. For *Pattern Type*, select one of the following:

Type	Description
Wildcard	Blocks or exempts one word or text strings of up to 80 characters. You can also use wildcard symbols such as ? or * to represent one or more characters. For example, a wildcard expression forti*.com matches fortinet.com and fortiguard.com. The * represents any character appearing any number of times.
RegExp	Blocks or exempts patterns of regular expressions that use some of the same symbols as wildcard expressions, but for different purposes. In regular expressions, * represents the character before the symbol. For example, forti*.com matches fortiii.com but not fortinet.com or fortiice.com. In this case, the symbol * represents i appearing any number of times.

5. In the *Pattern* field, enter the desired pattern.
6. From the *Language* dropdown list, select the desired language.
7. For *Action*, select one of the following:

Type	Description
Exempt	Allows the traffic to pass through, bypassing other content filters, antivirus inspection engine, and DLP inspection engine.
Block	Denies or blocks attempts to access any URL that matches the URL pattern. A replacement message displays.

8. Configure the status as desired.
9. Click *OK*.

Web rating override using custom categories

Web rating overrides allow you to add specific URLs to custom web ratings categories.

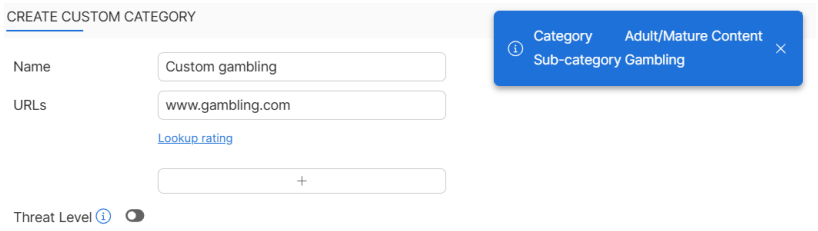
In a web filter profile, you can configure the action for each category. See Restricting web usage using FortiGuard URL categories and URL filter on page 356 for details. If a URL is in multiple categories, custom categories take precedence over FortiGuard categories.

For example, consider that you add www.gambling.com is added to a custom category and set the custom category action to Block. The default action for the FortiGuard Gambling category is Monitor. When a user browses to www.gambling.com, the custom category action takes precedence over the FortiGuard category, so access to www.gambling.com is blocked.

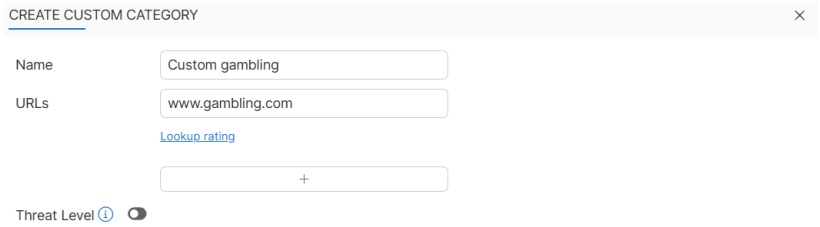
To configure web rating override using a custom category:

1. Go to *Security* > *Traffic* > *Security profiles* > *Profile resources* > *Custom Web Filter categories*.
2. Create a custom category:
   a. Click *Create Custom Category*.
   b. In the *URLs* field, enter the desired URL. In this example, it is www.gambling.com.
   c. (Optional) Click *Lookup rating* to observe the current category and subcategory from the FortiGuard Web Filter service assigned to the URL.

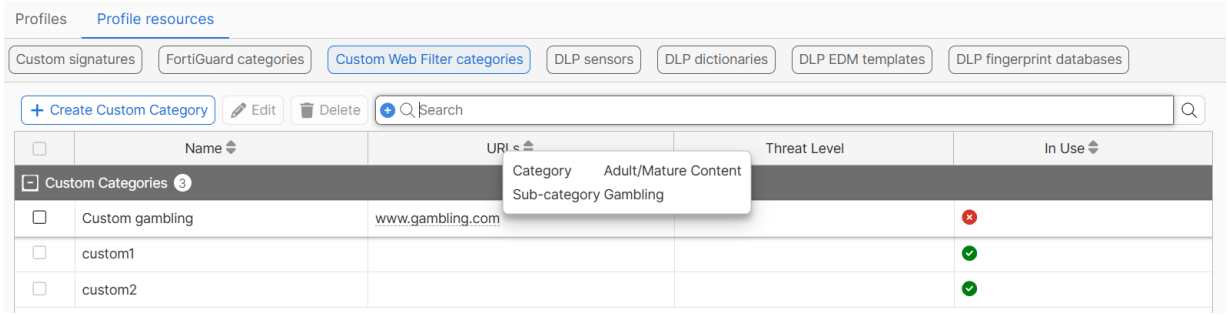
      In this example, www.gambling.com is assigned to:
      - Category: Adult/Mature Content
      - Subcategory: Gambling



   d. Configure other fields as desired.
   e. Click *OK*.



3. (Optional) In *Security* > *Traffic* > *Security profiles* > *Profile resources* > *Custom Web Filter categories*, you can also view the current category and subcategory from the FortiGuard Web Filter service assigned to a URL by hovering over it.



4. Go to *Profiles*.
5. In the *Web Filter With Inline-CASB* widget, click *Customize*.
6. Under *FortiGuard Category Based Filter > Custom Categories*, select the newly created category, then select the desired action. In this example, it is *Block*.
7. Click *OK*.

Enforcing safe search in web filter

To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 315.

To enforce safe search in web filter:

1. Go to *Security > Traffic > Security profiles*.
2. Create a new profile group by clicking on the dropdown next to *Profile Group* and clicking the plus sign (+) or select an existing profile group.
3. Enable *Web Filter With Inline-CASB*.
4. Under *Web Filter With Inline-CASB*, click *Customize*.
5. Under the *Settings* tab, scroll down to the *Options* section and enable *Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex*.
6. Click *OK*.

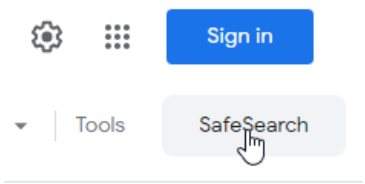
For individual search engine safe search specifications, refer to the documentation for Google, Yahoo, Bing, and Yandex.

To validate safe search after enforcing it in web filter:

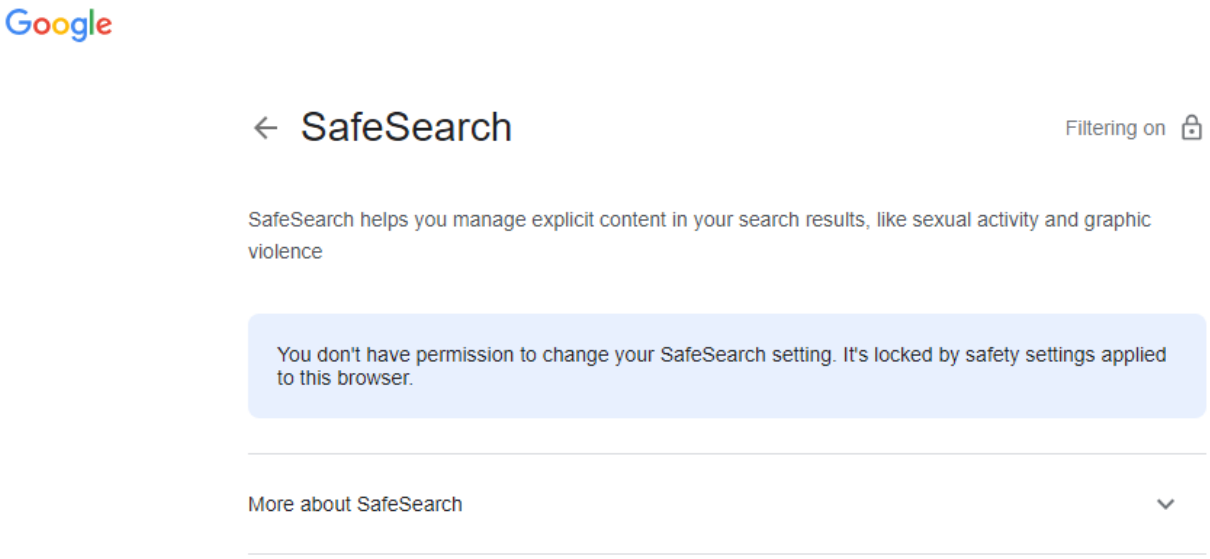
Safe search is still enforced from FortiSASE even if the individual search engine allows you to disable safe search from their search engine interface.

In the examples below, safe search was disabled for each of the individual search engines (except for Google which does not allow any modification).

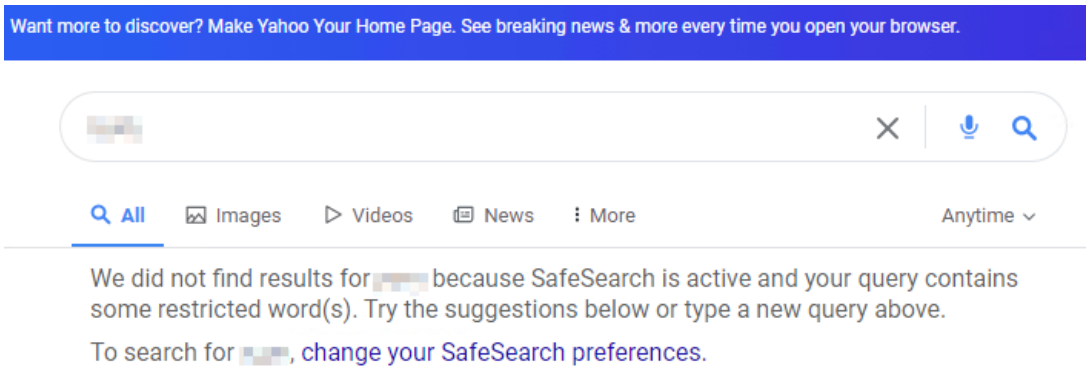
1. Go to a web browser, browse to Google and perform a search:
   a. Observe in the top-right corner that SafeSearch is enabled and cannot be modified.



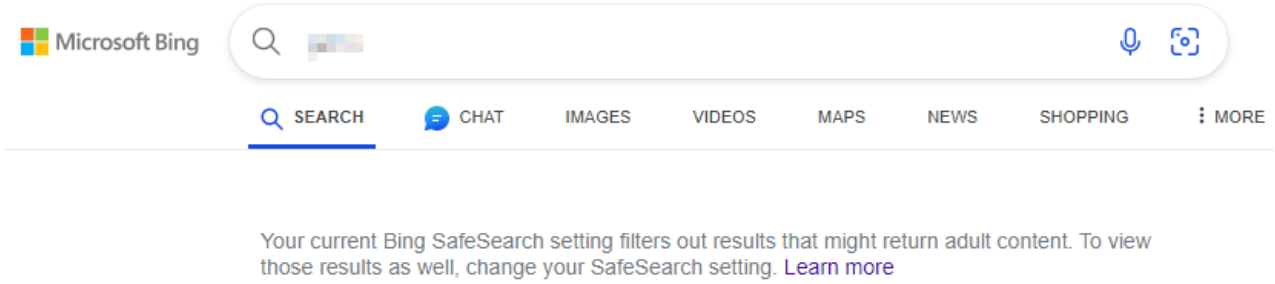
b. If you click on SafeSearch, then you will see the following message:



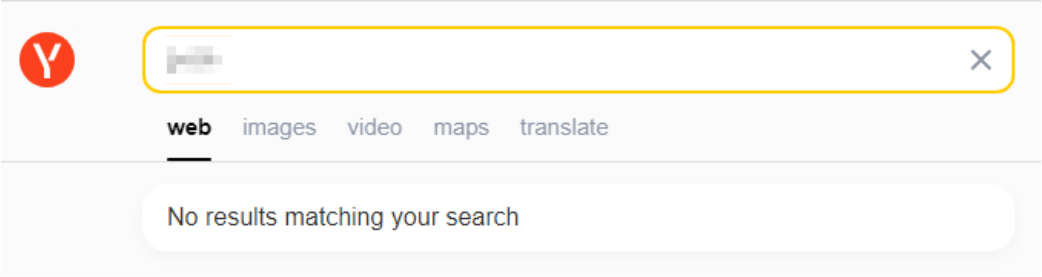
2. Go to a web browser, browse to Yahoo, perform a search, and observe that search results matching safe search criteria are blocked:



3. Go to a web browser, browse to Bing, perform a search, and observe that search results matching safe search criteria are blocked:



4. Go to a web browser, browse to Yandex, perform a search, and observe that search results matching safe search criteria are blocked:



Customizing inline-CASB headers

The FortiSASE Web Filter with Inline-CASB security component can be used to customize headers when agentless proxy or agent-based (FortiClient) remote users are accessing SaaS applications. When configured, FortiSASE intercepts HTTP headers and can modify them for outgoing traffic as follows:

- Add to request
- Add to response
- Remove from request
- Remove from response

The process of intercepting and customizing HTTP headers is also commonly known as HTTP header insertion.

By customizing HTTP headers for FortiSASE outgoing traffic destined for SaaS applications, the Web Filter with Inline-CASB can control SaaS application behaviour. Typically, customizing headers, namely, adding to request headers for access requests to SaaS applications is used to implement restricting tenants' access.

Prerequisites

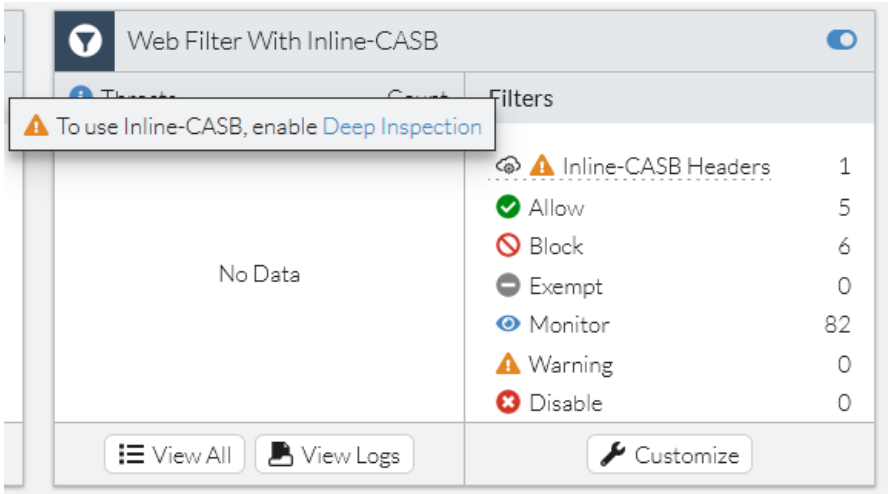
SSL deep inspection

Customizing HTTP headers using the Web Filter with Inline-CASB requires SSL deep inspection to be enabled on FortiSASE so that FortiSASE can intercept HTTP headers and add and remove them to header requests and responses as the SaaS application requires.

- To confirm SSL deep inspection is enabled, go to *Security* > *Traffic* > *Security profiles* and under the *SSL Inspection* widget, ensure that *Deep Inspection* displays.
- To enable SSL deep inspection, go to *Security* > *Traffic* > *Security profiles* and in the *SSL Inspection* widget, click *Customize*, and in the *SSL Inspection* slide-in, select *Deep Inspection* and click *OK*.

If you do not enable deep inspection, you see the following warnings:

- Under *Security* > *Traffic* > *Security profiles* in the *Web Filter With Inline-CASB* widget, you see a caution icon and when hovering over the tooltip, you see a warning message with a link to the *Deep Inspection* page.



- When clicking on *Customize* in the *Web Filter With Inline-CASB* widget and selecting the *Inline-CASB Headers* tab, you see a warning message with a link to the *Deep Inspection* page.

See Certificate and deep inspection modes on page 315.

SaaS vendor-specific headers

You must know the format and content of vendor-specific headers supported by a SaaS application to use with the Web Filter with Inline-CASB.

For more information on the specific headers used for restricted SaaS access, see SaaS vendor-specific documentation:

Vendor	Documentation link
Office 365	Restrict access to a tenant
Google Workspace	Block access to consumer accounts
Slack	Approve Slack workspaces for your network

Currently, all configured headers are added to outgoing FortiSASE traffic for agentless proxy remote users. Therefore, for this scenario, ensure you configure headers carefully considering their global scope to ensure they do not overlap or result in duplicate behaviour.

Customizing inline-CASB headers for restricted SaaS access

Large organizations may want to restrict SaaS access to resources like Microsoft Office 365, Google Workspace, and Slack by tenants 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 are only allowed to log in as the company's tenant and access the organization's applications.

Typically, access requests from clients pass through a security device or service, in this case FortiSASE, which inserts headers to notify the SaaS service to apply tenant restrictions with the permitted tenant list. Users are redirected to the SaaS service login page and can only log in if they belong to the permitted tenant list.

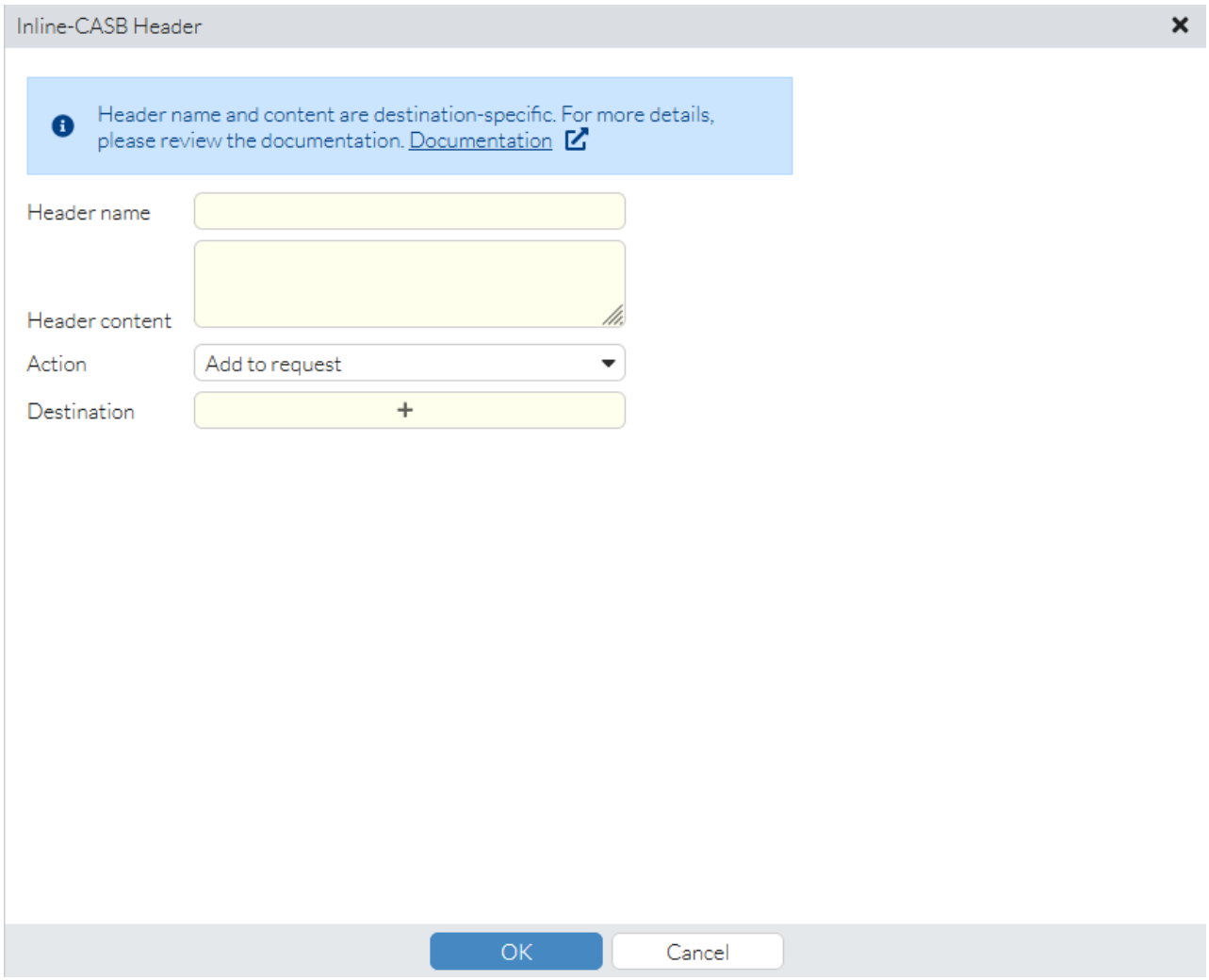
To customize headers for Office 365 tenant restriction, Google Workspace account access control, and Slack-approved workspaces for current network:

Ensure that you have reviewed Prerequisites on page 362 and have them in place before proceeding to customize headers to ensure proper functionality.

1. Go to *Security* > *Traffic* > *Security profiles* and select the desired *Profile Group*.
2. In the *Web Filter With Inline-CASB* widget, click *Customize*.
3. In the *Web Filter With Inline-CASB* slide-in, click the *Inline-CASB Headers* tab, then click *Create* to create a new inline-CASB header.
4. In the *Inline-CASB Header* slide-in, configure an inline-CASB header according to the vendors' specifications:
   a. Set the *Header name*. The service provider defines this.
   b. Set the *Header content* or HTTP header content to be inserted into the traffic. Your settings define this.
   c. Set the *Action* to one of the following:

Action when HTTP header is forwarded	Description
Add to request (default)	Add the HTTP header to request.
Add to response	Add the HTTP header to response.
Remove from request	Remove the HTTP header from request.
Remove from response	Remove the HTTP header from response.

   d. Set the *Destination*. This is an address object or address group containing domains that the service provider specifies.



5. Click *OK* to save the configured inline-CASB header.
6. Configure the applicable policy to use the security profile group with the Web Filter With Inline-CASB containing the newly configured Inline-CASB header:
   - For FortiClient agent-based remote users, go to *Security* > *Traffic* > *Policies* and do one of the following:
     - Create a new policy and select the security profile group.
     - Edit an existing policy and select the security profile group.
   - For agentless proxy remote users, go to *Security* > *Traffic* > *Proxy policies* and do one of the following:
     - Create a new proxy policy and select the security profile group.
     - Edit an existing proxy policy and select the security profile group.

For details on security profile groups and configuring them in policies, see Security profile groups on page 313.

The following tables list the vendor-specific headers that you must configure in the inline-CASB headers page:

Microsoft Office 365

Header name	Header content	Example header content	Action	Destination
`Restrict-Access-To-Tenants`	Domains and tenant ID	`azure.domain.com, domain.com, d0cf12c3-456c-7e89-0d1e-03e456de78f9`	Add to request	Use the built-in *Microsoft Office* 365 address group.
`Restrict-Access-Context`	Directory ID	`d1cf23c4-567c-8e90-1d2e-03e456de78f9`		
`sec-Restrict-Tenant-Access-Policy`	`restrict-msa`	`restrict-msa`		Create a new custom address object for login.live.com

The built-in Microsoft Office 365 address group includes:

- login.microsoftonline.com
- login.microsoft.com
- login.windows.net

For proper functioning of Microsoft Office 365 tenant restrictions, you must include the tenant ID in addition to the domains in a comma-separated list configured for `Restrict-Access-To-Tenants`.

Google Workspace

Header name	Header content	Example header content	Action	Destination
`X-GoogApps-Allowed-Domains`	Domain	`mydomain1.com, mydomain2.com`	Add to request	Use the built-in G Suite address group.

The built-in G Suite address group includes:

- gmail.com
- wildcard.google.com (*.google.com)

Slack

Header name	Header content	Example header content	Action	Destination
`X-Slack-Allowed-Workspaces-Requester`	Workspace or organization ID representing your Business+ or Enterprise Grid account	`xxxxxx`	Add to request	Create a new address object called wildcard.slack.com containing an FQDN of *.slack.com

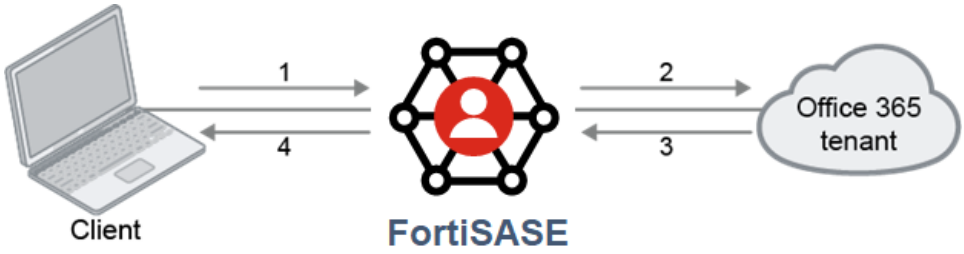
Header name	Header content	Example header content	Action	Destination
`X-Slack-Allowed-Workspaces`	Organization IDs or workspace ID	yyyyyy		

You must manually create a new address object called wildcard.slack.com containing the FQDN of *.slack.com via the *Create* button when in the *Select Entries* slide-in resulting from clicking the *Destination* in the *Inline-CASB Header* slide-in.

Due to vendors' changing requirements, these settings may no longer comply with the vendors' official guidelines. See the vendor documentation in SaaS vendor-specific headers on page 363.

Configuring inline-CASB header for Office 365 example

This example creates inline-CASB headers in FortiSASE to control permissions for Microsoft Office 365 to allow corporate domains and deny personal accounts, such as Hotmail and Outlook, that a user accesses through login.live.com.



- When a user attempts to access login.microsoftonline.com, login.microsoft.com, or login.windows.net:
  - For a FortiClient agent-based remote user, the traffic will match a policy
  - For an agentless proxy remote user, the traffic will match a proxy policy.
    If this is the first time the user has attempted to access the internet, then the user must enter valid credentials for the SSO authentication prompt.
- The Web Filter with Inline-CASB adds new headers to the customer tenant, indicating the allowed domain and restricted access for personal accounts. Next, FortiSASE starts a new connection with the Microsoft Office 365 domain controller including the new headers.
- The Microsoft Office 365 domain controller assesses this data and will allow or deny this access, then sends a reply to FortiSASE.
- FortiSASE sends a reply to the client.

FortiSASE Web Filter with Inline-CASB 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.

Inline-CASB headers configuration example

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.

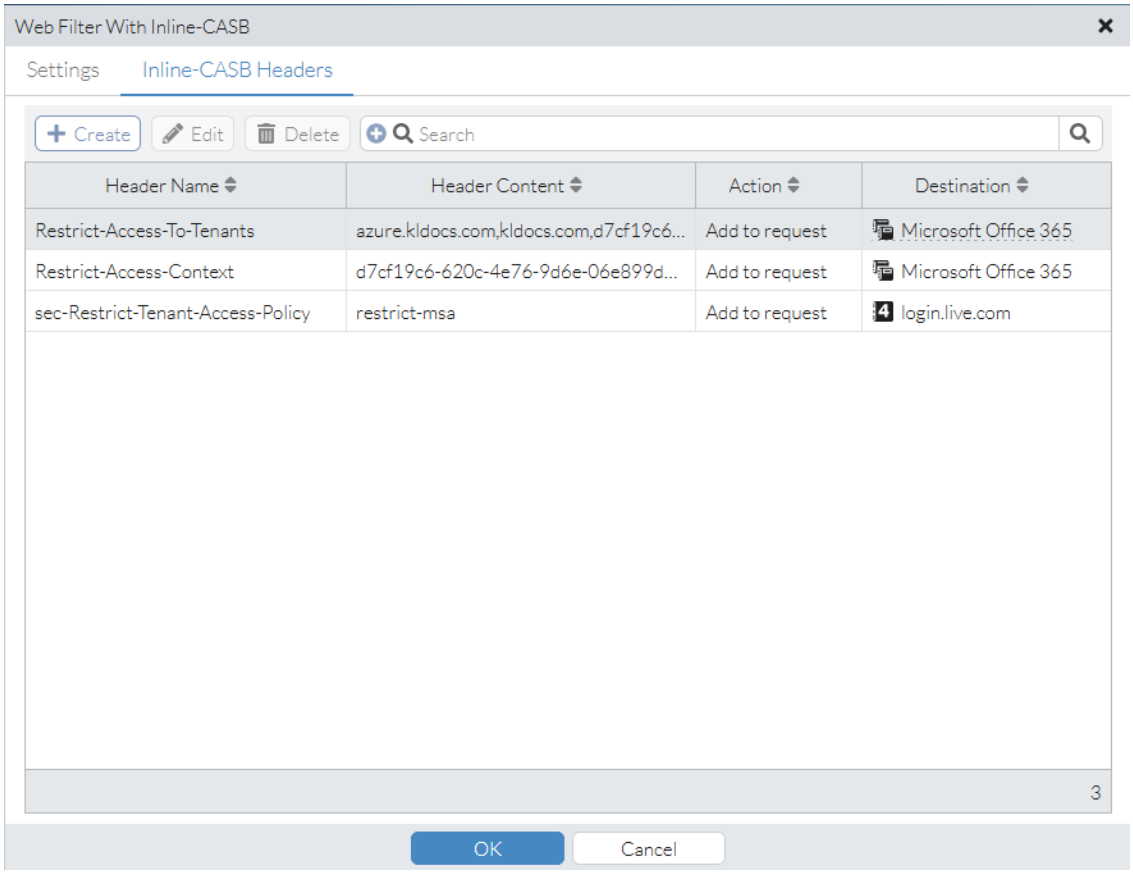
To restrict access to personal accounts using the login.live.com domain, the `sec-Restrict-Tenant-Access-Policy` header is inserted and uses `restrict-msa` as the header content.

Before configuring FortiSASE, collect the information related to the company domain in the Office 365 contract:

Header	Company domain-specific information
`Restrict-Access-To-Tenants`	• <domain.com> • Tenant ID
`Restrict-Access-Context`	Directory ID
`sec-Restrict-Tenant-Access-Policy`	`restrict-msa`

For proper functioning of Microsoft Office 365 tenant restrictions, you must include the tenant ID in addition to the domains in a comma-separated list configured for `Restrict-Access-To-Tenants`.

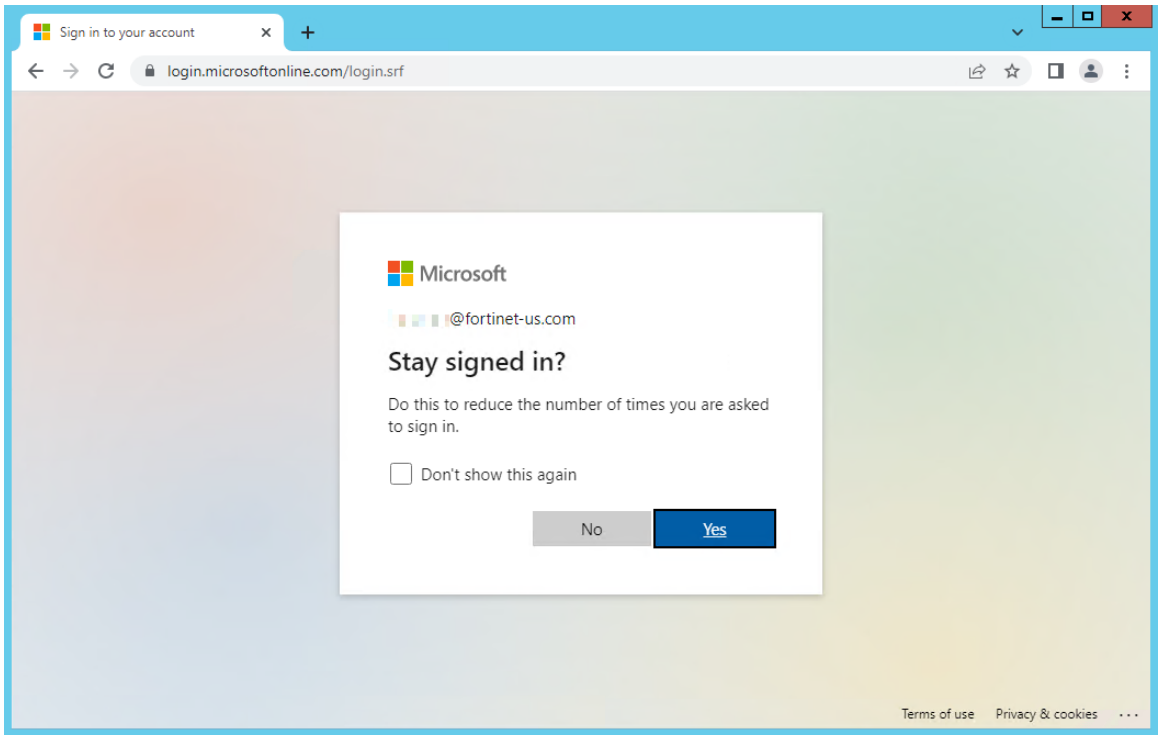
Following is an example of completed configuration in the *Inline-CASB Headers* tab within the *Web Filter with Inline-CASB* slide-in:



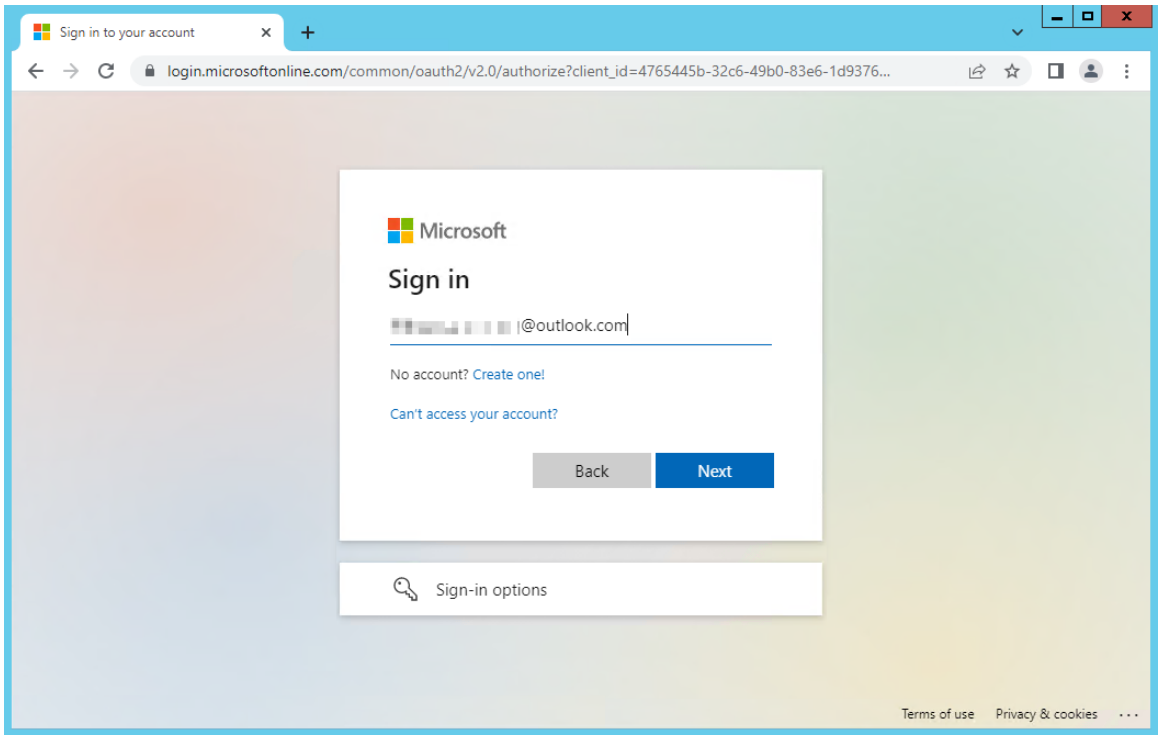
To test the access to corporate domains and personal accounts:

This section outlines the steps for testing the access with a client using an agentless proxy remote user. The steps are similar with a client using a FortiClient agent-based remote user.

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



2. The client can 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 by the cross-tenant access policy restricts it.

5. Try to log in using another corporate email with Microsoft 365 access that is from a domain not allowed on this tenant and observe the message about external access being blocked by policy.

To verify customized inline-CASB headers in security logs:

1. In FortiSASE, go to *Operations* > *Logs* > *Security* > *Web Filter With Inline-CASB* to view the corresponding logs.
2. Right-click a table heading and add *Change Headers* to make HTTP headers visible.
3. Drag and drop the *Change Headers* heading to the left to make it easy to see without scrolling.
4. Click a log entry of interest and click *Details* to drill down to see details.

DNS Filter

You can apply DNS category filtering to control user access to web resources. DNS filtering has the following features:

Feature	Description
FortiGuard filtering	Filters the DNS request based on the FortiGuard domain rating. This makes use of FortiGuard's continuously updated domain rating database for more reliable protection.
Botnet C&C domain blocking	Blocks the DNS request for the known botnet C&C domains. FortiGuard 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.
Domain filter	Allows you to define your own domain list to block or allow. In a DNS filter profile, the local domain filter has a higher priority than FortiGuard category-based domain filter. DNS queries are scanned and matched first with the local domain filter. If an entry matches and the local filter action is set to block, then that DNS query is blocked and redirected.

Feature		Description
		If the local domain filter list has no match, then the FortiGuard category-based domain filter is used. If a DNS query domain name rating belongs to the block category, the query is blocked and redirected. If the FortiGuard category-based filter has no match, then the original resolved IP address is returned to the client DNS resolver. If the local domain filter action is set to allow and an entry matches, it will skip the FortiGuard category-based domain filter and directly return to the client DNS resolver. If the local domain filter action is set to monitor and an entry matches, it will go to the FortiGuard category-based domain filter for scanning and matching.
DNS translation		Maps the resolved result to another IP address that you have defined. 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.
Options	Redirect botnet C&C requests to Block Portal	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.
	Log all DNS queries and responses	Enable to log all domains visited (detailed DNS logging).
	Edge device captive portal support	This option is mandatory for captive portal SSO authentication to work with edge devices. It will alter DNS resolution behavior for the captive portal FQDN.

Feature		Description
	Allow DNS requests when a rating error occurs	Enable to allow all domains when FortiGuard DNS servers fail, or they are unreachable from FortiSASE. When this happens, a log message is recorded in the DNS logs by default.
	Enforce 'Safe Search' on Google, Bing, YouTube	Enable to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines. To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 315.

To configure a DNS Filter profile:

1. Go to *Security > Traffic > Security profiles*.
2. Enable *DNS Filter*.
3. Click *Customize*.
4. To configure FortiGuard filtering, do the following:
   a. Enable *FortiGuard Category Based Filter*.
   b. Select the desired category, then select the desired action: *Allow*, *Monitor*, or *Redirect Block Portal*.
   c. If desired, click *Manage Categories*. Select the desired category, then click *Edit*. You can enable and configure the *Threat Level* for the category. You must configure a threat level for this category to appear in FortiView Threats after the DNS filter blocks it.
5. To configure domain filter, do the following:
   a. Click *Create* under *Domain Filter*.
   b. Enter a domain, and select a *Type* and *Action*.
   c. Click *OK*. The example has configured three domain filters:

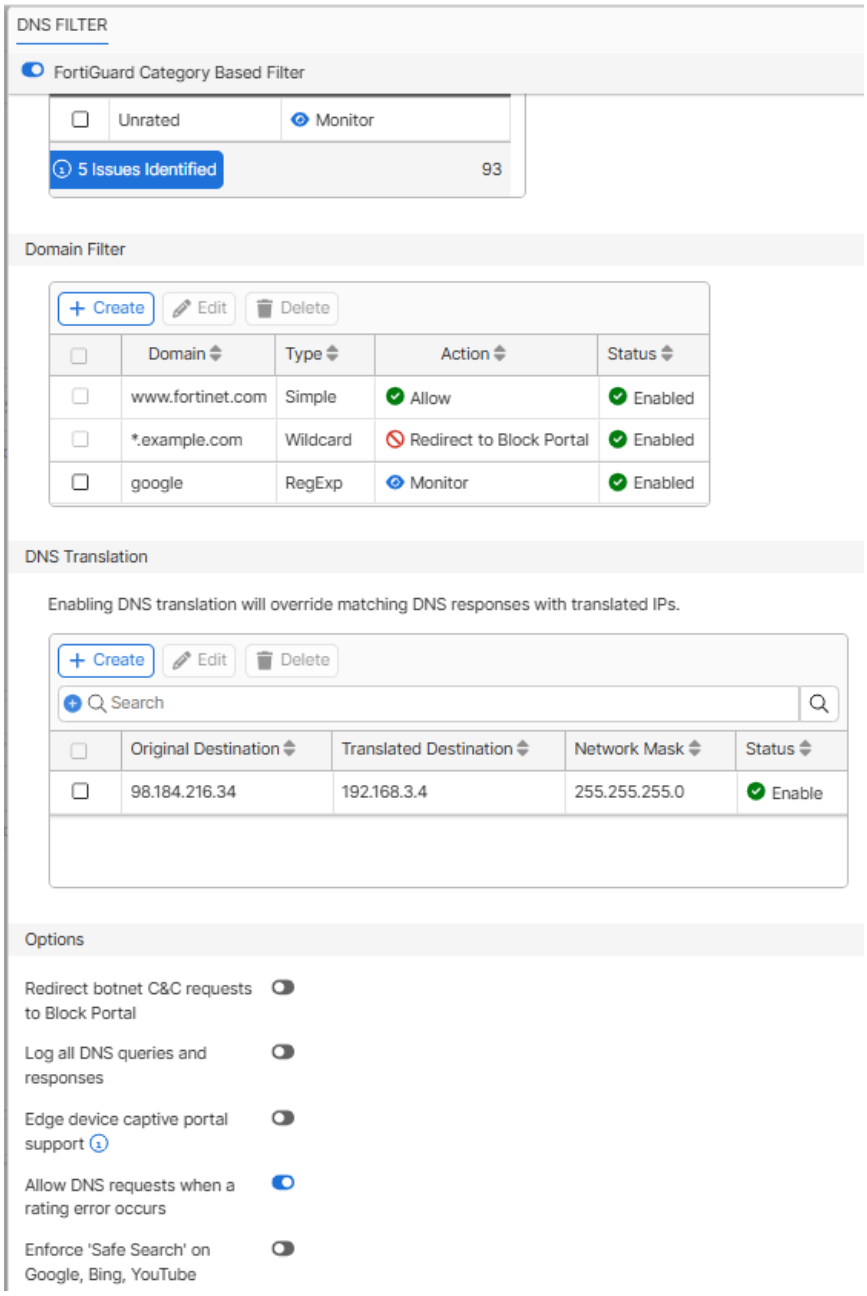
Domain	Type	Action
www.fortinet.com	Simple	Allow
*.example.com	Wildcard	Redirect to Block Portal
google	Regular expression	Monitor

6. To configure DNS translation, do the following:
   a. Under *DNS Translation*, click *Create*.
   b. In the *Original Destination* field, enter the domain's original IP address. For example, if you want the DNS filter profile to translate 93.184.216.34 (www.example.com) to 192.168.3.4, you would configure the original destination as 93.184.216.34.
   c. In the *Translated Destination* field, enter the translated destination IP address. For the example, you would enter 192.168.3.4 as the translated destination.
   d. In the *Network Mask* field, enter the desired network mask.

e. Click *OK*. With this configuration, when an internal network user performs a DNS query for www.example.com, they do not get the original www.example.com IP address of 93.184.216.34. Instead, the DNS filter replaces it with 192.168.3.4.

7. To configure *Options*, do the following:
   a. To enable botnet C&C domain blocking, enable *Redirect botnet C&C requests to Block Portal*. If desired, you can click the botnet package link to view the latest list of botnet C&C domain definitions.
   b. If desired, enable *Log all DNS queries and responses*. You can view these logs in *Operations > Logs > Security > DNS Filter*.
   c. For captive portal SSO authentication to work for edge devices, you must enable *Edge device captive portal support*. This option will alter DNS resolution behaviour for the captive portal FQDN.
   d. If desired, enable *Allow DNS requests when a rating error occurs*. When FortiGuard DNS servers fail, or they are unreachable from FortiSASE, allow DNS requests from all domains and record a log message in *Operations > Logs > Security > DNS Filter*.
   e. If desired, enable *Enforce 'Safe Search' on Google, Bing, YouTube* to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines. To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 315.

8. Click *OK*.



Considerations

- For individual search engine safe search specifications, refer to the documentation for Google, Bing, and YouTube.
- DNS filter not supported for proxy.
- For edge devices, additional configuration is required to support DNS redirection rules and DNS filter functionality:

a. Go to *Security* > *Traffic* > *Policies*.
b. In the *Custom* section, edit the *Captive portal DNS traffic exemption (captive-dns-exempt)* policy.
c. For *Profile Group*, select *Default* or select *Specify* and select a profile group with the DNS filter enabled.
d. Click *OK* to save the policy changes.

- For captive portal SSO authentication to work for edge devices, you must enable *Edge device captive portal support*. This option will alter DNS resolution behavior for the captive portal FQDN.

Enforcing safe search in DNS filter

To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 315.

To enforce safe search in DNS filter:

1. Go to *Security* > *Traffic* > *Security profiles*.
2. Create a new profile group by clicking on the dropdown next to *Profile Group* and clicking the plus sign (+) or select an existing profile group.
3. Enable *DNS Filter*.
4. Under *DNS Filter*, click *Customize*.
5. Scroll down to the *Options* section and enable *Enforce 'Safe Search' on Google, Bing, YouTube*.
6. Click *OK*.

For individual search engine safe search specifications, refer to the documentation for Google, Bing, and YouTube.

To validate safe search after enforcing it in DNS filter:

You can use a tool such as dig or nslookup to demonstrate that the domain lookup for a search site has been replaced by its safe search equivalent site.

1. On a Windows endpoint in the Windows Command Prompt, run nslookup for Google and observe the following output:

```
nslookup google.com
...
Non-authoritative answer:
Name:    forcesafesearch.google.com
Addresses:  2001:4860:4802:32::78
216.239.38.120
Aliases:  google.com
```

2. On a Windows endpoint in the Windows Command Prompt, run nslookup for Bing and observe the following output:

```
nslookup bing.ca
...
```

```
Non-authoritative answer:
Name:    strict.bing.com
Address:  204.79.197.220
Aliases:  bing.ca
```

3. On a Windows endpoint in the Windows Command Prompt, run nslookup for YouTube and observe the following output:

```
nslookup youtube.com
...
Non-authoritative answer:
Name:    restrict.youtube.com
Addresses:  2001:4860:4802:32::78
216.239.38.120
Aliases:  youtube.com
```

Application Control With Inline-CASB

FortiSASE can recognize network traffic that a large number of applications generate. Application Control With Inline-cloud access security broker (Inline-CASB) uses Intrusion Prevention System (IPS) protocol decoders that can analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols. Application Control With Inline-CASB supports traffic detection using the HTTP protocol (versions 1.0, 1.1, and 2.0).

FortiSASE uses Application Control and SSL deep inspection to act as an Inline-CASB by providing access control to software-as-a-service (SaaS) cloud application traffic. A CASB sits between users and their cloud service to enforce security policies as they access cloud-based resources.

Application Control With Inline-CASB features are not guaranteed to work when other security features are disabled. Enabling one of the following security features is recommended: antivirus (AV), file filter, data loss prevention (DLP), web filter, or DNS filter.

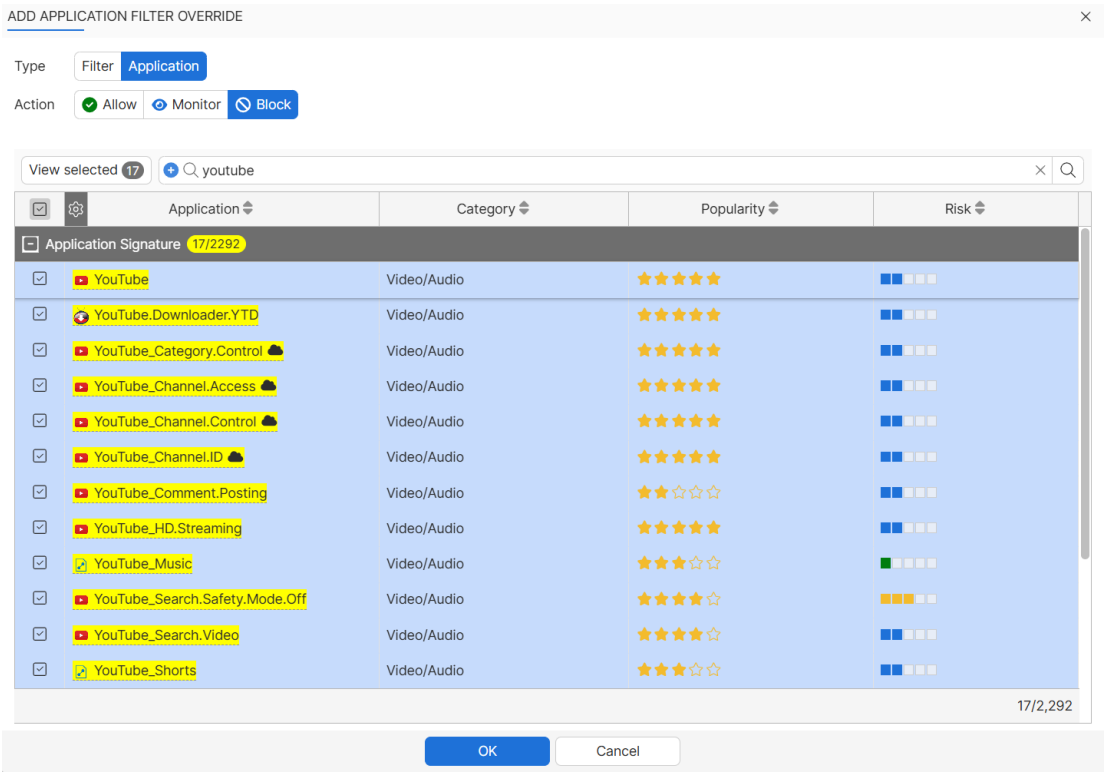
To configure Application Control With Inline-CASB:

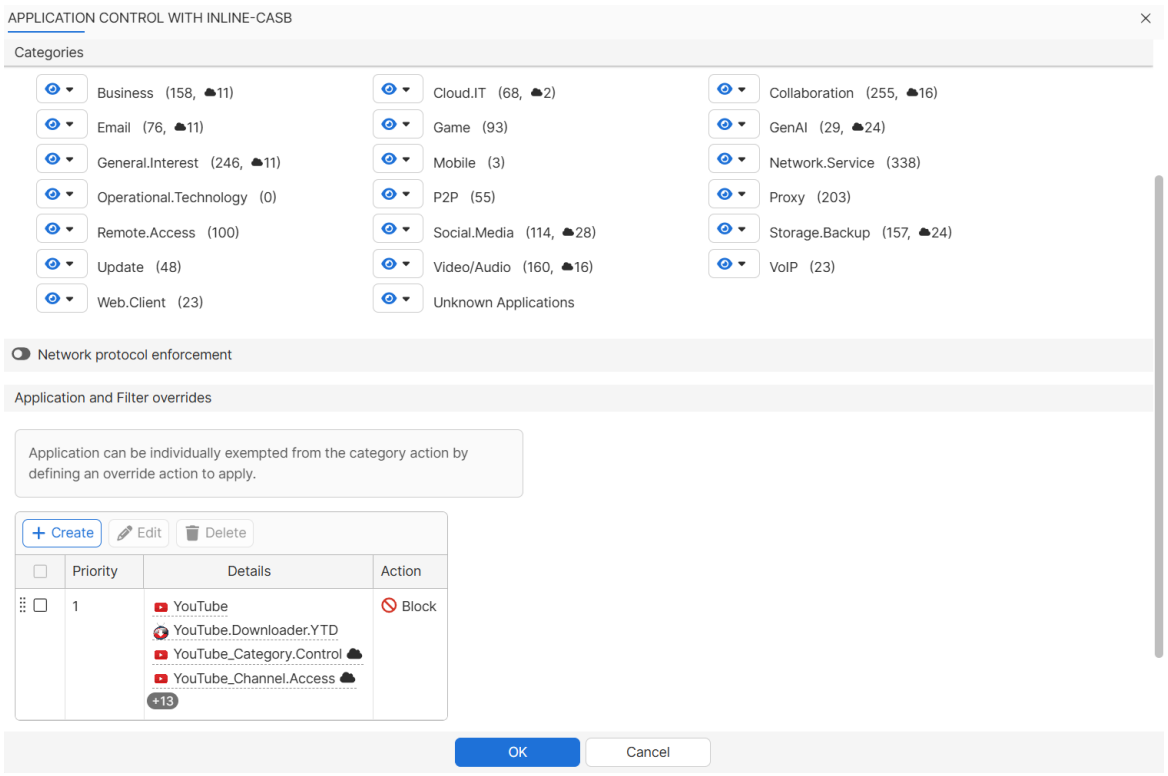
1. Go to *Security > Traffic > Security profiles*.
2. Enable *Application Control With Inline-CASB*.
3. In the *Application Control With Inline-CASB* widget, click *Customize*.
4. The *Application Control With Inline-CASB* pane displays the application categories. You can configure one of the following actions for each category:

Type	Description
Allow	Passes the traffic to the web filters, AV inspection engine, and DLP inspection engine.

Type	Description
Monitor	Processes the traffic the same way as the Allow action. For the Monitor action, FortiSASE generates a log message each time it establishes a matching traffic pattern.
Block	Denies or blocks attempts to access any application that belongs to the category.

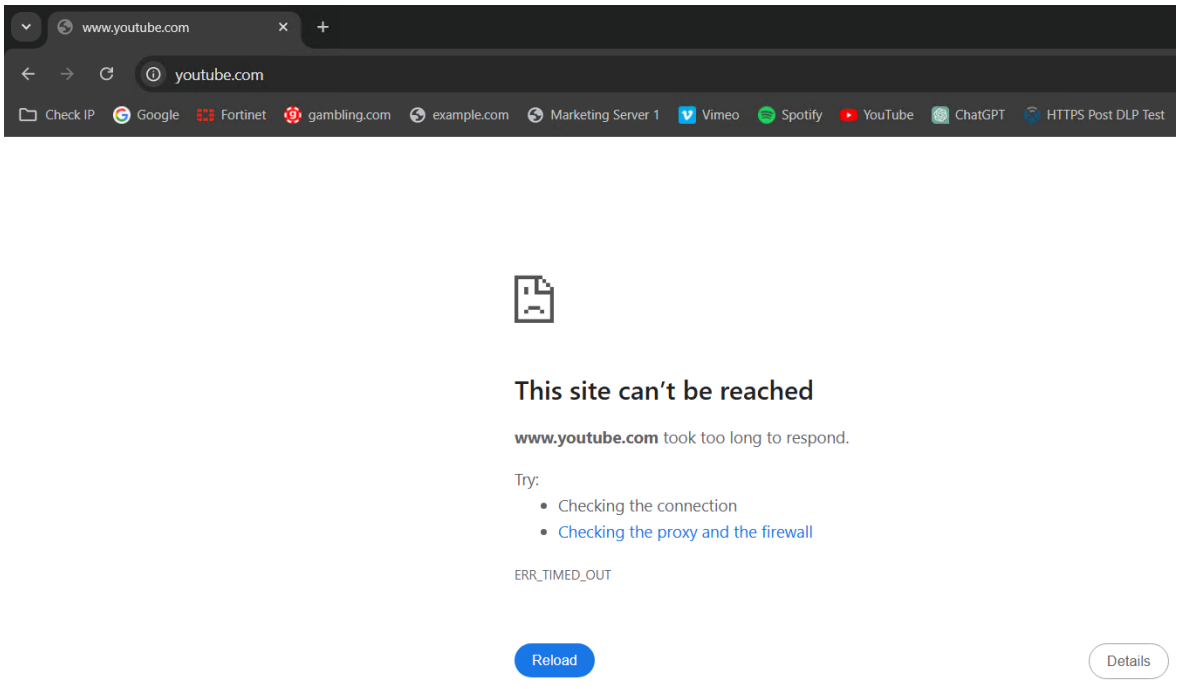
5. In *Application and Filter Overrides*, you can configure actions for individual applications, overriding the action configured for their category, or configure actions for filters based on multiple criteria including application category behavior, popularity, protocol, rish, technology, and vendor.
   You can also configure actions for custom application signatures in either application or filter overrides.
   - To configure actions for individual applications:
     i. Click *Create*.
     ii. Select *Type* as *Application*.
     iii. Select the desired action.
     iv. Select the desired applications by clicking the checkboxes next to the applications.
     v. Click *OK*.
     vi. You can search for the desired applications, and filter the list to show only cloud applications. The *Application and Filter Overrides* pane denotes cloud applications with a cloud icon, such as for the YouTube_Category.Control application in the following screenshot.
     The following example allows the Video/Audio category, and blocks YouTube.





vii. Click *OK*.

When the user attempts to access YouTube under these settings, the browser times out.

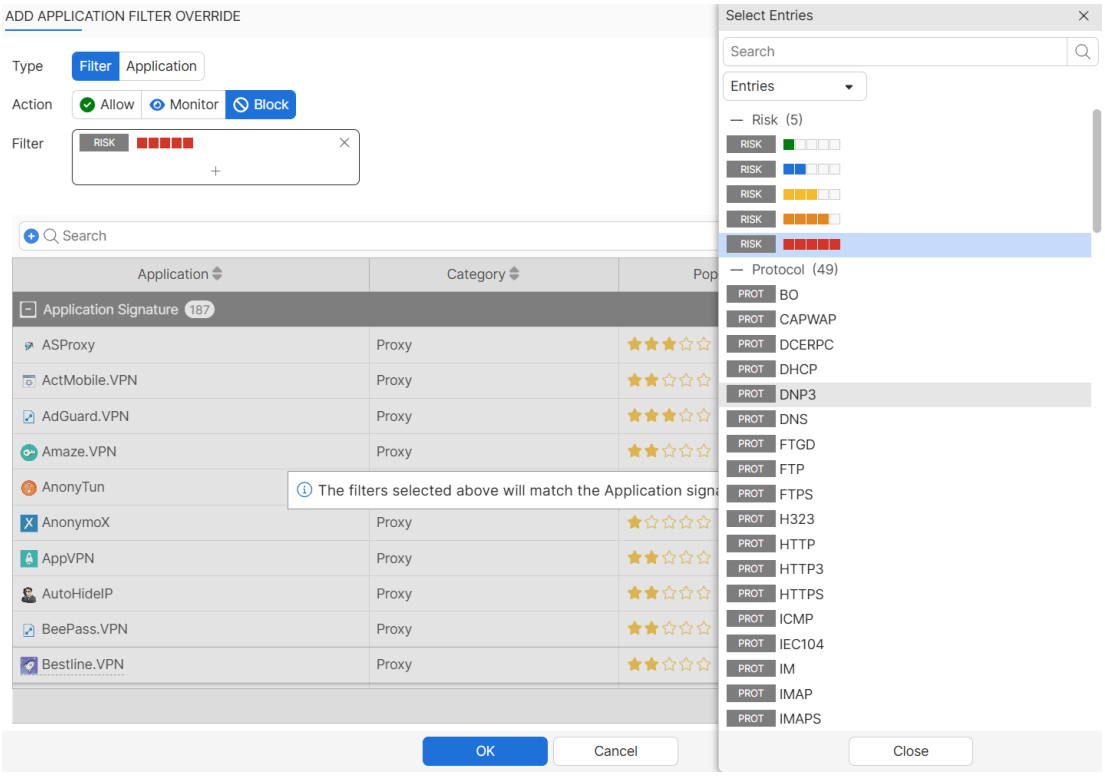


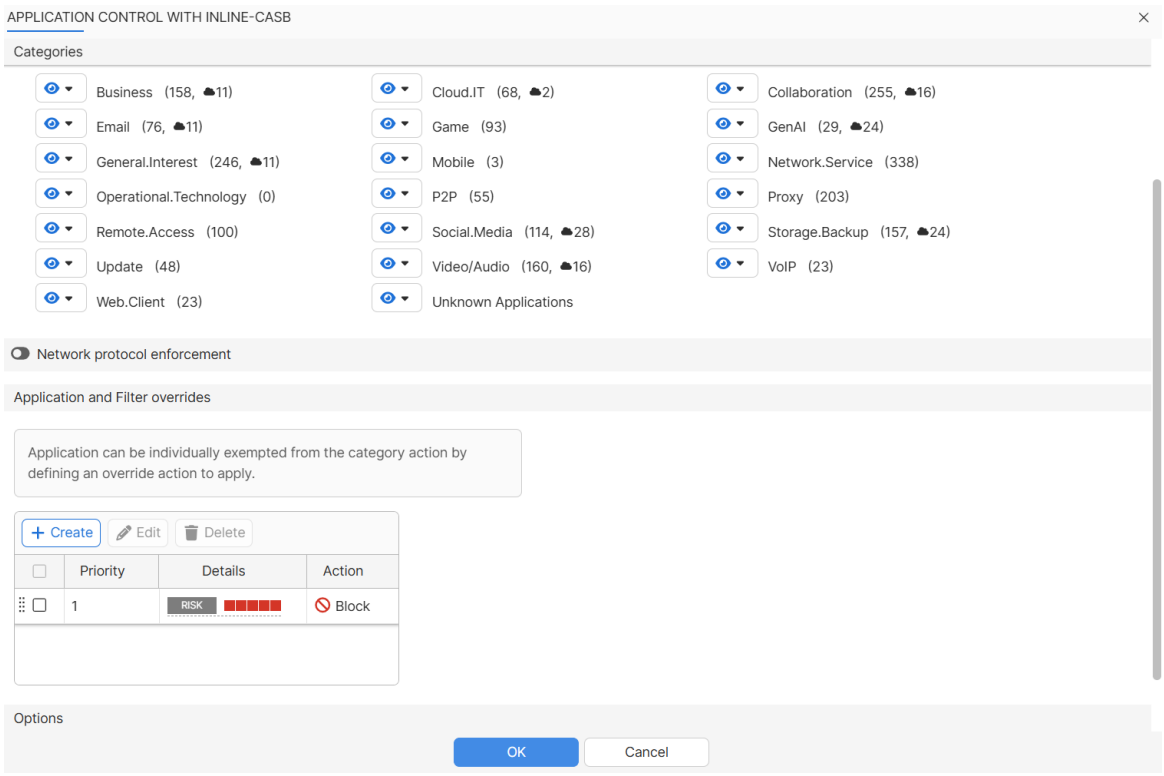
You can view data for cloud application access attempts in *Dashboards > FortiView Cloud Applications*.

- To configure actions using filters:

i. Click *Create*.
ii. Select *Type* as *Filter*.
iii. Select the desired action.
iv. In the *Filter* field, click *+*.
v. In the Select Entries pane, select the desired filter entries used to filter desired applications.

The following example filters critical risk applications (Risk with five red bars) as determined by the FortiGuard Application Control Service.





vi. Click *OK*.

vii. Click *OK*. When the user attempts to access any application considered as critical risk under these settings, the browser times out.

To create, edit, and delete a custom Application Control signature:

1. Go to *Security* > *Traffic* > *Security profiles*.
2. Select the *Profile resources* tab from the toolbar.
3. Select *Custom IPS signatures* to see all custom IPS signatures created across different security profile groups.
4. Do one of the following:
   - To create an Application Control signature, click *Create* > *Application Control*. In the slide-in, specify *Tag*, *Comments*, and *Signature* using Creating IPS and application control signatures. Click *OK*. The newly created IPS signature is available to use in the *Application Control* widget across different security profiles.
   - To edit an Application Control signature, select the desired Application Control signature and click *Edit*. After making the required edits, click *OK*.
   - To delete, select the desired Application Control signature available in the *Custom IPS signatures* list and click *Delete*. On the *Confirm delete* prompt, click *OK*.

Network protocol enforcement

Protocol enforcement allows you to enforce known protocols (e.g. FTP, HTTP, HTTPS) on known ports (e.g. 21, 80, 443). If the port of incoming traffic does not match the allowed protocol(s), or is not allowlisted, then the

Intrusion Prevention System (IPS) engine applies the configured violation action, such as blocking or monitoring the traffic.

You can use this feature in the following scenarios:

- When an IPS protocol decoder identifies a network traffic service, it checks whether the service port aligns with the enforced protocol(s). If the decoder finds a match, that is, the traffic is allowlisted, then the traffic proceeds without restriction. If there is no match, the traffic is classified as a violation and the specified action, monitoring or blocking, is applied.
- When there is no confirmed service for the network traffic, the traffic is classified as a violation if IPS protocol decoders 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 ports for network services are defined by FortiGuard. See Application Control Service.

In the following example, an application sensor is configured to enforce HTTPS on port 443 (block).

To configure network protocol enforcement:

1. Go to *Security > Traffic > Security profiles*.
2. Select an existing *Profile Group* from the dropdown or create a new one by clicking the dropdown and clicking *+*.
3. Enable *Application Control With Inline-CASB*.
4. In the *Application Control With Inline-CASB* widget, click *Customize*.
5. Enable *Network protocol enforcement*.
6. Click *Create*.
   a. Configure a new network service with these settings:

Field	Value
Port	Port number for the network service. For example, enter *443*.
Enforce protocols	Select one or more protocols to enforce from a list of common network protocols. For example, select *HTTPS*.
Violation action	Action to take for protocols which are not allowed under the selected port. For example, select *Block*.

   b. Click *OK*.
   The entries are displayed in a table.
7. Click *OK*.
   After applying the above application control settings, FortiSASE allows traffic on port 443 exclusively for HTTPS services while blocking traffic on port 443 for HTTP services.

Blocking applications detected on non-default ports

Most networking applications run on specific ports. For example, SSH runs on port 22, and Facebook runs on ports 80 and 443.

If the default network service is enabled in the application control profile, the IPS engine performs a check at the application profile level, and any detected application signatures running on the non-standard TCP/IP port are blocked. This means that each allowed application runs on its default port.

Default ports for network services are defined by FortiGuard. See Application Control Service.

In the following example, an application sensor is configured to enforce HTTP on port 443.

To configure blocking applications detected on non-default ports:

1. Go to *Security* > *Traffic* > *Security profiles*.
2. Select an existing *Profile Group* from the dropdown or create a new one by clicking the dropdown and clicking *+*.
3. Enable *Application Control With Inline-CASB*.
4. In the *Application Control With Inline-CASB* widget, click *Customize*.
5. In *Options*, enable *Block applications detected on non-default ports*.
6. In *Application Overrides*, you can configure actions for individual applications, overriding the action configured for their category.
   a. Click *Create*.
   b. Select the desired action from the dropdown list in the upper left corner. For example, select *Allow*.

      When an application is configured with an action of *Monitor* or *Allow*, when its traffic is detected on non-standard ports then the application will be blocked. An application configured with an action of *Block* will have its traffic blocked regardless of the port its traffic is detected on.

   c. Select the desired applications. For example, select *HTTP.BROWSER*.
   d. Click *OK*.
      The entries are displayed in a table.
7. Click *OK*.
   After applying the above application control settings, FortiSASE allows HTTP traffic with the standard port (port 80) while blocking HTTP traffic detected on a non-standard port (port 8080).

Video Filter

The video filter feature allows you to allow, monitor, or block YouTube videos based on FortiGuard categories. It also provides the flexibility to override the actions configured for a FortiGuard category on a per-channel basis using their channel IDs.

Video filter requires enabling SSL deep inspection inside the profile group. See Certificate and deep inspection modes on page 315. It also requires a Google API key to access the YouTube Data API. To generate an API key, see YouTube Data API Overview.

To configure a video filter:

1. Go to *Security* > *Traffic* > *Security profiles* and select the desired *Profile Group*.
2. In the *Video Filter* widget, enable the toggle and click *Customize*.

3. Select the required *Default* action:

Action	Description
Allow	Allows the traffic
Monitor	Allows and logs the traffic
Block	Blocks access and presents a Video Block page. To customize the Video Block page, see HTML templates on page 589.

4. Enter the *API key*. To generate API keys, see YouTube Data API Overview.
5. Select FortiGuard categories and set their action to *Allow*, *Monitor*, or *Block* as desired. This overrides the *Default* action configured earlier for the selected FortiGuard categories.
6. (Optional) To override a particular YouTube channel from the configured action of FortiGuard categories, do the following:
   a. Under *Channels*, click *Create*.
   b. Enter the *Channel name*.
   c. Enter the *Channel ID* for the desired YouTube channel.
   d. Set *Action* to *Allow*, *Monitor*, or *Block* as desired.
7. Click *OK*.
8. Click *OK*.

FortiSASE evaluates the configured channel overrides before the FortiGuard categories.

Profile resources

The *Profile resources* tab is available on the toolbar under *Security > Traffic > Security profiles*. It consists of options to configure the following settings that are shared and available across different security profile groups:

- Custom IPS and Application Control signatures
- FortiGuard categories
- Custom Web Filter categories
- DLP sensors: Create custom sensors or view predefined sensors managed by the FortiGuard DLP service
- DLP dictionaries: Create custom dictionaries or view predefined dictionaries managed by the FortiGuard DLP service
- DLP EDM templates
- DLP fingerprint databases

To create, edit, and delete a custom IPS signature:

1. Go to *Security > Traffic > Security profiles*.
2. Select the *Profile resources* tab from the toolbar.
3. Select *Custom IPS signatures* to see all custom IPS signatures created across different security profile groups.

4. Do one of the following:
   - To create an IPS signature, click *Create > IPS Signature*. In the slide-in, specify *Tag*, *Comments*, and *Signature* using Creating IPS and application control signatures. Click *OK*. The newly created IPS signature is available to use in the *Intrusion Prevention* widget across different security profiles. These custom IPS signatures can be viewed in the *Custom IPS Signature* section of the *IPS signatures* table when the *Custom* profile is selected, when *IPS Signatures and Filters > Create* or *Edit* are selected, and when *Type* is selected as *Signature*.
   - To edit an IPS signature, select the desired IPS signature and click *Edit*. After making the required edits, click *OK*.
   - To delete, select the desired IPS signature available in the *Custom IPS signatures* list and click *Delete*. On the *Confirm delete* prompt, click *OK*.

To create, edit, and delete a custom Application Control signature:

1. Go to *Security > Traffic > Security profiles*.
2. Select the *Profile resources* tab from the toolbar.
3. Select *Custom IPS signatures* to see all custom IPS signatures created across different security profile groups.
4. Do one of the following:
   - To create an Application Control signature, click *Create > Application Control*. In the slide-in, specify *Tag*, *Comments*, and *Signature* using Creating IPS and application control signatures. Click *OK*. The newly created IPS signature is available to use in the *Application Control* widget across different security profiles.
   - To edit an Application Control signature, select the desired Application Control signature and click *Edit*. After making the required edits, click *OK*.
   - To delete, select the desired Application Control signature available in the *Custom IPS signatures* list and click *Delete*. On the *Confirm delete* prompt, click *OK*.

To edit FortiGuard category threat levels:

1. Go to *Security > Traffic > Security profiles*.
2. On the *Profile resources* tab, select *FortiGuard categories*.
3. Click desired FortiGuard category from the list and click *Edit*.
4. Enable the *Threat level* toggle and select the appropriate level as per your requirement.
5. Click *OK*.

To create Custom Web Filter Category from Profile resources:

1. Go to *Security > Traffic > Security profiles*.
2. On the *Profile resources* tab, select *Custom Web Filter categories*. Two default custom categories, custom1 and custom2, are available to use across different security profile groups.
3. To edit a default custom category, do the following:
   a. Select *custom1* or *custom2* and click *Edit*.
   b. Specify the desired URLs and configure the threat level for the default custom category. Click *OK*.
4. To create a new category, do the following:
   a. Click *Create Custom Category*.
   b. Specify the desired *Name*, *URLs*, and *Threat Level* for the custom category.

c. Click *OK*. These custom categories are available to use in Web Filter settings across different security profile groups.

To create a custom DLP dictionary from Profile resources:

1. Go to *Security > Traffic > Security profiles*.
2. On the *Profile resources* tab, select *DLP dictionaries*.
3. Click *+Create*.
4. In the *New DLP Dictionary* pane, configure these settings:

Field	Description
Name	Dictionary name.
Entries to evaluate	Logic used to apply to dictionary entry matches to trigger sensor: • *All*: logical AND condition on matching entries • *Any*: logical OR condition on matching entries
Table of dictionary entries	Create one or more dictionary entries.

5. Create a new dictionary entry by clicking *+*. In the *New Entry* pane, configure these settings:

Field	Description
Type	Select a predefined *DLP Data Type* from the dropdown list.
Repeat	Enable or disable repeat matching of the selected *DLP Data Type*.
Status	Select whether the dictionary entry is *Enabled* or *Disabled*.

6. Click *OK* to create the new dictionary entry.
7. Click *OK* to create the DLP dictionary.

To create a custom DLP sensor from Profile resources:

1. Go to *Security > Traffic > Security profiles*.
2. On the *Profile resources* tab, select *DLP sensors*.
3. Click *+Create*.
4. In the *New DLP Sensor* pane, configure these settings:

Field	Description
Name	Sensor name.
Entry matches needed to trigger sensor	Logic used to apply to sensor entry matches to trigger sensor: • *All*: logical AND condition on matching entries • *Any*: logical OR condition on matching entries
Table of entries	Create one or more entries.

5. Create a sensor entry by clicking *Create*. In the *New Entry* pane, configure these settings:

Field	Description
ID	Numerical ID for the sensor entry
Dictionary	Select the dictionary for this sensor entry. You can create a new dictionary and then select it or select a predefined dictionary managed by the FortiGuard DLP service.
Dictionary matches needed to consider traffic DLP risk	Number of dictionary matches to trigger sensor entry.
Status	Select whether the sensor entry is enabled or disabled.

6. Click *OK* to create the new sensor entry.
7. Click *OK* to create the new sensor.

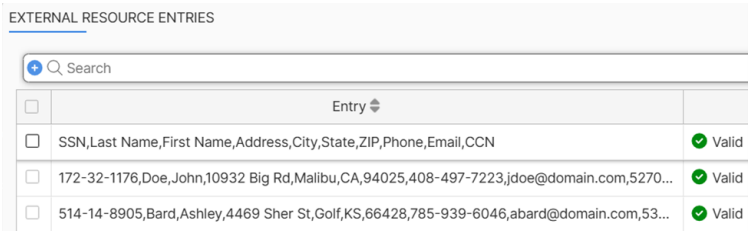
To create a DLP EDM template from Profile resources:

1. Go to *Security > Traffic > Security profiles*.
2. On the *Profile resources* tab, select *DLP EDM templates*.
3. Click *+Create*.
4. In the *New DLP EDM template* pane, configure these settings:

Field	Description
Name	EDM template name.
Resource settings	
Resource type	Select one of two options: • *External feed*: Device will periodically fetch entries from URL using HTTP(s). • *File upload*: Entries are provided from a local file
External feed URL	If *External feed* is selected, the link to an external resource file. The file must be a CSV, with each column representing a data type. For example: 213321,john,doe 201111,karen,smith 322122,rick,wong
Upload file	If *File upload* is selected, upload a local CSV file by clicking to select the file or dropping the file into area provided. The file must be a CSV, with each column representing a data type. For example: 213321,john,doe 201111,karen,smith 322122,rick,wong
HTTP basic authentication	If *External feed* is selected, enable to use HTTP basic authentication with the server hosting the external resource file.
Refresh rate	If *External feed* is selected, the time interval to refresh external resource (1-43200 minutes, default = 5 minutes).

Field	Description
Match criteria	
+All of these fields	Configure a logical AND for the fields as match criteria, where each field consists of a column index and its mapping to a DLP data type. Click *+* to add more fields.
+Any of these fields	Configure a logical OR for the fields as match criteria, where each field consists of a column index and its mapping to a DLP data type. Click *+* to add more fields.

5. Click *View Entries* to view the data entries imported from the CSV file.



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.

6. Click *OK* to create the new DLP template.
   For an example, see Blocking HTTPS upload traffic using EDM template example on page 345.

To create a DLP fingerprint database from Profile resources:

1. Go to *Security* > *Traffic* > *Security profiles*.
2. On the *Profile resources* tab, select *DLP fingerprint databases*.
3. Click *+Create*.
4. In the *New DLP fingerprint database* pane, configure these settings:

Field	Description
Name	Name of the DLP fingerprint database.
Sensitivity level	Select a sensitivity or threat level for matches with this fingerprint database. Select either *Warning*, *Private*, or *Critical*.
Server settings	
Server IP/FQDN	IP/FQDN of the server. Currently, only the Server IP address can be used to specify the location of the Samba file server.
Username	User name required to log into the file server.
Password	Password required to log into the file server.

Field	Description
Server directory	Directory/path on the server to the fingerprint files
Include sub-directories	Enable/disable scanning subdirectories to find files to create fingerprints from.
File pattern	Files matching this pattern on the server are fingerprinted. Optionally use the * and ? wildcards.
Synchronization settings	
Synchronization interval	Frequency for which the server is checked for new or changed files. Select *Daily*, *Weekly*, or *Monthly*.
Synchronize during specified time	Specified time in GMT on which to scan the server.
Remove fingerprints of deleted files	Enable to keep the fingerprint database up to date when a file is deleted from the server. • *Enabled*: Keep the fingerprint database up to date when a file is deleted from the server. • *Disabled*: Do not check for deleted files on the server. Saves system resources.
Keep fingerprints of older file versions	Enable so that when a file is changed on the server FortiSASE keeps the old fingerprint and adds a new fingerprint to the database. • *Enabled*: Keep the old fingerprint and add a new fingerprint when a file is changed on the server. • *Disabled*: Replace the old fingerprint with the new fingerprint when a file is changed on the server.
Scan on file creation	Enable to initiate an immediate update of the fingerprint database after creating it. • *Enabled*: Immediately scan the file server after creating the fingerprint database. • *Disabled*: Disable immediate scan of the file server. Files will be scanned at the scheduled interval.

5. Click *OK*.
   For an example, see Blocking HTTPS upload traffic using IDM with DLP fingerprinting example on page 350.

ZTNA

Agent-based ZTNA

Zero trust network access (ZTNA) application gateways and applications are key components in the FortiSASE ZTNA solution for agent-based remote users. A ZTNA application gateway serves as a secure entry point that mediates the connection between remote users and internal ZTNA applications. A ZTNA application represents

the actual application or service that remote users attempt to access. A ZTNA application can be any internal web or enterprise application, cloud service, or on-premise resource. A ZTNA application gateway acts as a reverse proxy, ensuring that only authorized and compliant users can access ZTNA applications based on security policies that the organization defines. You can configure a FortiGate to serve as the ZTNA application gateway. See Zero Trust Network Access.

FortiSASE enables administrators to configure and manage ZTNA application gateways and ZTNA application configurations for agent-based remote users in *Security > Traffic > ZTNA > Agent-based*.

Once you configure ZTNA application gateways and applications, you can reference and use them in individual endpoint profiles on the *ZTNA* tab. See ZTNA on page 464.

To configure ZTNA application gateway on FortiSASE:

1. Go to *Security > Traffic > ZTNA > Agent-based*.
2. Select the *Gateways* tab.
3. Click *Create* and enter the following details for the ZTNA application gateway:

Field	Value
Name	Enter a unique name for your application gateway.
Address	Specify either IP or FQDN of FortiGate that is configured to act as the ZTNA application gateway.
Port	Specify port number on FortiGate that is designated for ZTNA access.

To configure ZTNA application gateway on FortiSASE:

1. Go to *Security > Traffic > ZTNA > Agent-based*.
2. Select *Private applications* tab.
3. Click *Create* to configure new ZTNA application, and enter the following details:

Field	Value
Name	Enter unique name for your application.
Type	Select either from IP, FQDN or Wildcard FQDN
IP/FQDN	Based on Type selected, specify either IP address or FQDN of the ZTNA application.
Port	Select Any or click Specify to enter a specific port number.
Application gateway	Click + to select Application gateway configured in earlier steps.

4. Click *OK*.

Syncing ZTNA tags between FortiSASE and the ZTNA application gateway for RBAC

FortiSASE can be share configured ZTNA tags with the ZTNA application gateway (i.e. FortiGate) to enforce role-based access control (RBAC) for ZTNA applications. To enable this integration, the FortiGate must be connected to FortiClient Cloud. See Configuring FortiClient EMS.

Once the FortiGate is connected to FortiClient Cloud, you can deny or authorize the ZTNA application gateway. Only authorized FortiGates can synchronize endpoint and tagging data from FortiSASE for access control enforcement.

To authorize or disconnect the ZTNA application gateway on FortiSASE:

1. Go to *Security > Traffic > ZTNA > Agent-based*.
2. On the *Connectors* tab, select the serial number of the FortiGate to authorize or disconnect.
3. Click *Authorize* or *Disconnect*. The FortiGate status changes.

Considerations

- Endpoint features do not apply for proxy mode users. See Proxy agentless mode on page 15.
- For demonstrations of various configuration options for implementing FortiSASE endpoint management features, such as custom endpoint profiles, tunnel autoconnect, split tunnel, vulnerability scan, ZTNA, and more, see the FortiSASE Endpoint Management Deployment Guide.
- FortiSASE and the FortiGate must be registered under the same FortiCloud account for FortiSASE to discover the FortiGate.
- If a FortiGate ZTNA application gateway is running FortiOS 7.4.4 or later, then FortiSASE automatically learns TCP forwarding and non-Web ZTNA applications previously configured on the FortiGate.

FortiClient endpoint sharing

FortiSASE supports sharing the resolved IP and MAC addresses (host tags) of a FortiClient endpoint with zero trust network access (ZTNA) application gateways (i.e. FortiGate devices) when the endpoint has a ZTNA tag applied.

For a selected FortiGate gateway, FortiSASE supports the following modes:

Mode	Description
Directly connected endpoints	Only share host tags for endpoints directly connected to this FortiGate gateway (recommended for better performance)
All	Share host tags for all endpoints regardless of whether the endpoints are connected to this FortiGate gateway
Endpoints connected to selected FortiGate(s)	Share host tags for endpoints connected to the selected FortiGate gateway and connected to up to four additional specified gateways

To edit FortiClient endpoint sharing in FortiSASE:

1. Go to *Security > Traffic > ZTNA > Agent-based*.
2. On the *Connectors* tab, select the serial number of the FortiGate.
3. Click *Edit FortiClient endpoint sharing*.
4. Select an option from the *FortiClient endpoint sharing from* dropdown. If *Endpoints connected to selected FortiGate(s)* is selected, you can select up to four FortiGates in *Filter tag IP/MAC addresses from specific FortiGate(s)*.
5. Click *OK*.

To verify FortiClient endpoint sharing with a FortiGate gateway:

1. In FortiSASE, configure a ZTNA tag and a ZTNA tagging rule. See Security posture tags and tagging rules on page 486.
   a. For example, create a tag called Windows10 and create a tagging rule set for OS version of Windows 10.
   b. Ensure the test endpoint is tagged as desired.
2. On the FortiGate, go to *Policy & Objects > ZTNA* and switch to the *ZTNA Tags* tab.
   a. Verify that the ZTNA tag created in FortiSASE has been synchronized to the FortiGate using the *FortiClient EMS Cloud* fabric connector. See Configuring FortiClient EMS.
   b. Hover over the ZTNA IP tag or the ZTNA MAC tag, and select *View Resolved Addresses*.
   c. Observe the IP address or MAC address of your test endpoint that was tagged with the ZTNA tag. This confirms that FortiSASE has shared the host tags for your endpoint with this FortiGate gateway.

Prerequisites and considerations

Prerequisites

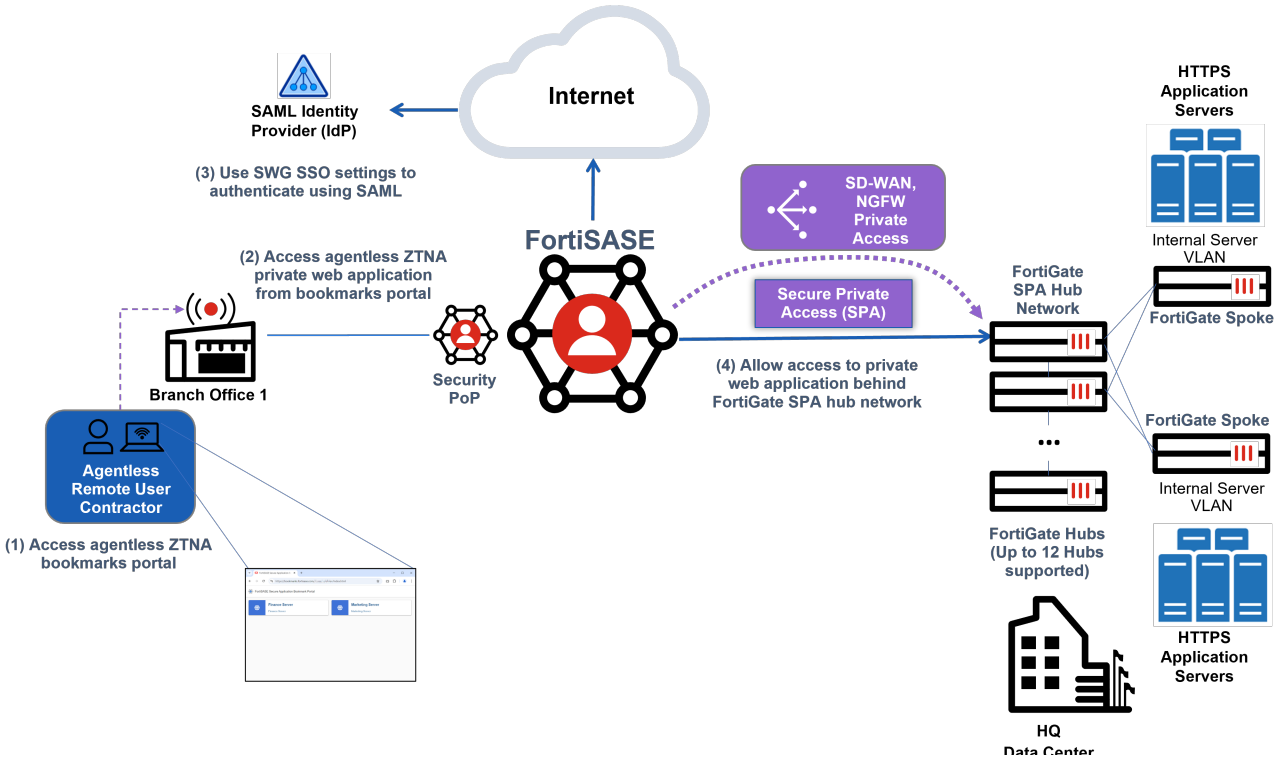
This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

Considerations

- Changing sharing settings triggers a resync of FortiClient tag information to the selected FortiGate. Multiple changes in a short time may temporarily degrade performance.
- Using *Directly connected endpoints* mode is recommended for better performance.

Agentless ZTNA

FortiSASE supports agentless zero trust network access (ZTNA), which allows contractors or temporary workers to access a private web-based application behind an already configured secure private access (SPA) service connection with proxy single sign on user authentication simply by using a web browser without requiring an agent.



FortiSASE provides an agentless ZTNA bookmark portal that you can share with contractors or temporary workers to make it convenient for them to access private applications using agentless ZTNA.

Each web-based application is assigned to a custom domain name associated with the FortiSASE instance so that you do not have to maintain a separate set of domain names dedicated to private web applications.

FortiSASE becomes a ZTNA application gateway for HTTPS traffic and functions as a reverse proxy on behalf of the private web-based applications it is protecting. Before granting access to the protected application, FortiSASE verifies:

- User identity by enforcing user authentication to a SAML identity provider from within the remote user's web browser
- Remote user geolocation by using geofencing

Based on the application policy configured, FortiSASE grants access. As a ZTNA application gateway, FortiSASE uses SPA to access the private application.

Prerequisites and considerations

See Prerequisites and considerations on page 392.

Prerequisites and considerations

Prerequisites

Using agentless zero trust network access (ZTNA) requires the following:

- FortiSASE has the Advanced or Comprehensive remote users subscription applied.
- The following FortiSASE features are configured:
  - Proxy
  - Proxy user single sign on (SSO)
  - Secure private access (SPA) for BGP per overlay or BGP on loopback with the FortiGate device. See SPA on page 101.
- The private web-based application to be accessed using agentless ZTNA fulfills the following:
  - Reside on the local network behind a FortiGate device
  - Support HTTPS
- SPA is licensed for the FortiGate device which will be the SPA hub. See SPA Service Connection subscription and SPA FortiCloud account prerequisites.

Considerations

- Although you must configure proxy and proxy SSO to configure agentless ZTNA, you do not need to configure the remote user endpoints for proxy. In other words, you do not need to configure remote user endpoints with a proxy autoconfiguration file or with a CA certificate for SSL deep inspection. Agentless ZTNA simply uses configuration from proxy and proxy SSO for remote user authentication.
- Proxy and agent users cannot access private application bookmarks configured for agentless ZTNA.
- For Agentless ZTNA to work with SPA hubs configured with either BGP routing design (BGP per overlay or BGP on loopback) and private web-based applications configured with the *Server Type* set to *FQDN*, the corresponding DNS rule must be set with *Access Type* to *Private*. See DNS redirection rules on page 265.
- Although agentless ZTNA is designed for accessing private applications, it is still possible to configure a public IP or FQDN for an application server. In this case, even for dedicated IP instances, the agentless ZTNA user traffic originates from the shared public IP address associated with the Security PoP. This shared public IP address must be used when restricting access to agentless ZTNA users on the FortiGate SPA hub or spoke device (depending on your network topology). See Restricting access to agentless ZTNA users on page 405.

Configuration workflow



Ensure that you are aware of agentless zero trust network access (ZTNA) Prerequisites and considerations on page 392.

Reviewing the prerequisites and considerations is necessary before following the configuration workflow that follows.

The workflow for configuring agentless ZTNA is as follows:

1. Enable proxy from *Network* > *Proxy configuration*. See Proxy configuration on page 285.
2. Enable SSO authentication for proxy users. For a configuration example, see Configuring FortiSASE with Entra ID SSO in proxy agentless mode on page 526.
3. Configure user groups for proxy users. See Users and groups on page 502.
4. Configure a Private Access security profile group. See Security profile groups on page 313.
5. Configure SPA for the FortiGate device acting as an SPA hub. See SPA on page 101.

6. Configure access control based on the geolocation of the remote user, also known as geofencing, from the *Network > Geofencing* page. Geofencing applies not only to agentless ZTNA but all incoming remote user access such as remote user and edge device connectivity. See Geofencing on page 269.
7. Configure a private application from the *Security > Traffic > ZTNA > Agentless > Private applications* tab. See Configuring a private application on page 394.
   - A private application is assigned to a custom FortiSASE domain name and added as a bookmark entry to the agentless ZTNA bookmark portal.
   - Alternatively, when you enable *Use custom domain name* you can specify a custom domain that you own and a certificate for the custom domain that can be used to access a ZTNA private application. Using your DNS domain/host tools, you must configure the custom domain DNS CNAME record with the FortiSASE private application domain for the private application.
8. Configure an application policy using a user group, security profile group, and private application which were all configured in previous steps. See Configuring an application policy on page 396.
9. Initialize the bookmark portal and configure a bookmark policy. See Configuring the bookmark portal on page 397.
10. Access the bookmark portal to see all configured private applications. Remote users can only access the bookmark portal after successfully authenticating with the configured proxy SSO provider. See Accessing the bookmark portal on page 399.
11. Verify agentless ZTNA access to the desired private web-based application. See Verifying agentless ZTNA functionality on page 401.
12. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs from which agentless ZTNA users are originating traffic are allowed to access the SPA hub. See Restricting access to agentless ZTNA users on page 405.
13. When done accessing private applications using agentless ZTNA, a remote user can log out of the bookmark portal using the *Sign out* link from the top-right of the page. This performs SAML single sign-out for the previously logged in remote user.

Configuring a private application



Ensure that you are aware of agentless zero trust network access (ZTNA) Prerequisites and considerations on page 392.

This topic describes one of many steps in the Configuration workflow on page 393.

For agentless ZTNA, you must configure one or more private applications to be accessed by remote users.

For each private application, you must specify these parameters for the web-based application:

- Private IP address or FQDN
- Port
- Sub-domain name used for setting the unique custom domain name
- Name and description for the application to be used in the bookmark portal

Optionally, you can also configure the private application to use your custom domain name if you meet these prerequisites prior to configuring the private application using steps below:

- Custom domain name that you own and administer. You must have access to the DNS domain/host tools to create a CNAME record where the custom domain name becomes an alias for the FortiSASE private application domain.

- Certificate issued for the custom domain name. The certificate must have been previously issued through a public certificate authority (CA) and must be uploaded to FortiSASE as a local certificate in either PKCS#12 format or PEM format with private key supplied.

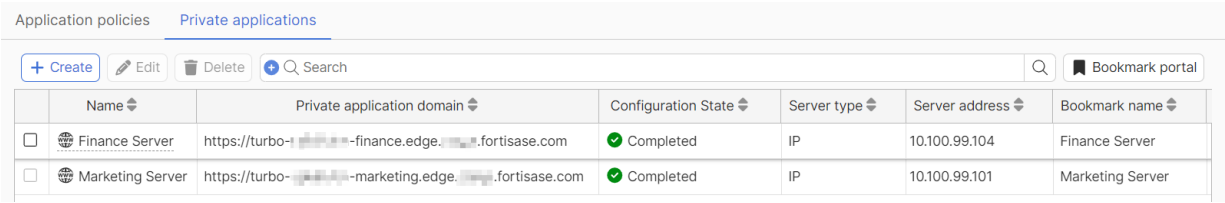
To configure a private application:

1. Go to *Security > Traffic > ZTNA > Agentless*.
2. Click the *Private applications* tab.
3. Click *Create*.
4. Configure these fields:

Field	Value	Example Value
Name	Name of the web-based application. This name will be used to identify the private application within agentless ZTNA configuration settings and will be displayed as the name of the private application bookmark card in the bookmark portal.	Finance Server
Private application domain	The sub-domain name is specified here. It will be used with the FortiSASE root domain to create a custom domain name for this application	finance This sub-domain results in the following domain: turbo-abcxyz-finance.edge.prod.fortisase.com
Use custom domain name	Enable to specify a custom domain that you already own and a certificate for the custom domain that can be used to access a ZTNA private application. Using your DNS domain/host tools, you must configure the custom domain DNS CNAME record with the FortiSASE private application domain for the private application. Once the custom domain is configured, the private application is no longer accessible using the FortiSASE private application domain.	myapp.com Using your DNS domain/host tools, you must configure the DNS record for myapp.com with a CNAME of *turbo-abcxyz-finance.edge.prod.fortisase.com*
Client Certificate	When *Use custom domain name* is configured, select the customer's certificate used for the private server application. This certificate must first be uploaded using *System > Certificates* and *Import > Local Certificate* before it is visible in this dropdown.	Certificate in the FortiSASE *Local Certificate* category created for the custom domain previously specified.
Server type	The address type used to reach the application server: • *IP*: IP address is used to reach the application • *FQDN*: Fully qualified domain name (FQDN) is used to reach the application	IP

Field	Value	Example Value
Server address	IP address or FQDN corresponding to the application server. This address type must match the Server type specified previously.	10.100.99.104
Port	Port used by the private application. Default: 443 (HTTPS)	443
Description	This description will be used to describe the private application within agentless ZTNA configuration settings and will be displayed as the description of the private application bookmark card in the bookmark portal.	Finance Server

5. Click *OK*. The *Configuration State* will display *Creating* followed by *Completed*. The private applications configured are displayed in a table.



Configuring an application policy

Ensure that you are aware of agentless zero trust network access (ZTNA) Prerequisites and considerations on page 392.

This topic describes one of many steps in the Configuration workflow on page 393.

After configuring a private application, you must configure an application policy, or agentless ZTNA policy, to enforce user-based authentication for remote users attempting to access the private application.

In other words, agentless ZTNA policies control the traffic that is proxied through FortiSASE from end users to designated private applications.

In addition to user-based authentication, you can configure access control based on the geolocation of the remote user, or geofencing, from the *Network > Geofencing* page. It applies not only to agentless ZTNA but all incoming remote user access such as remote user and edge device connectivity. See Geofencing on page 269.

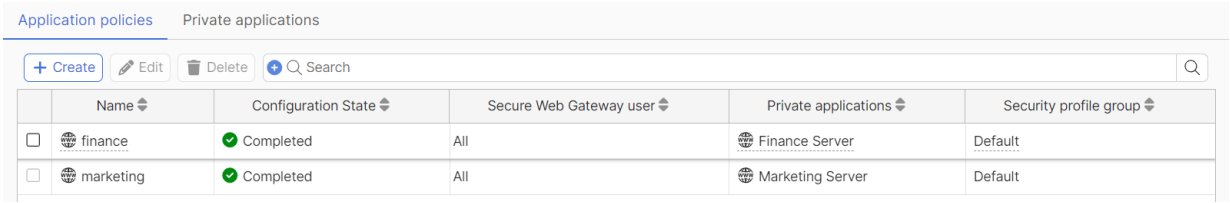
To configure an application policy:

1. Go to *Security > Traffic > ZTNA > Agentless*.
2. Click the *Application policies* tab. This is the default tab.
3. Click *Create*.

4. Configure these fields:

Field	Value	Example Value
Name	Name of application policy.	finance
Proxy user	The users that are allowed access to the private application. • *All*: All SSO-authenticated agentless ZTNA users can access this application. • *Specify*: Only SSO-authenticated agentless ZTNA users in the specified users groups can access this application.	All
Private applications	The private applications that this policy applies to. One or more previously configured private applications can be added to this field.	Finance Server
Security profile group	The security profile group applied to this policy. • *Default*: The default security profile group will be applied. • *Specify*: The selected security profile group will be applied.	Default

5. Click *OK*. The *Configuration State* will display *Creating* followed by *Completed*. The application policies configured are displayed in a table.



Configuring the bookmark portal

Ensure that you are aware of agentless zero trust network access (ZTNA) Prerequisites and considerations on page 392.

This topic describes one of many steps in the Configuration workflow on page 393.

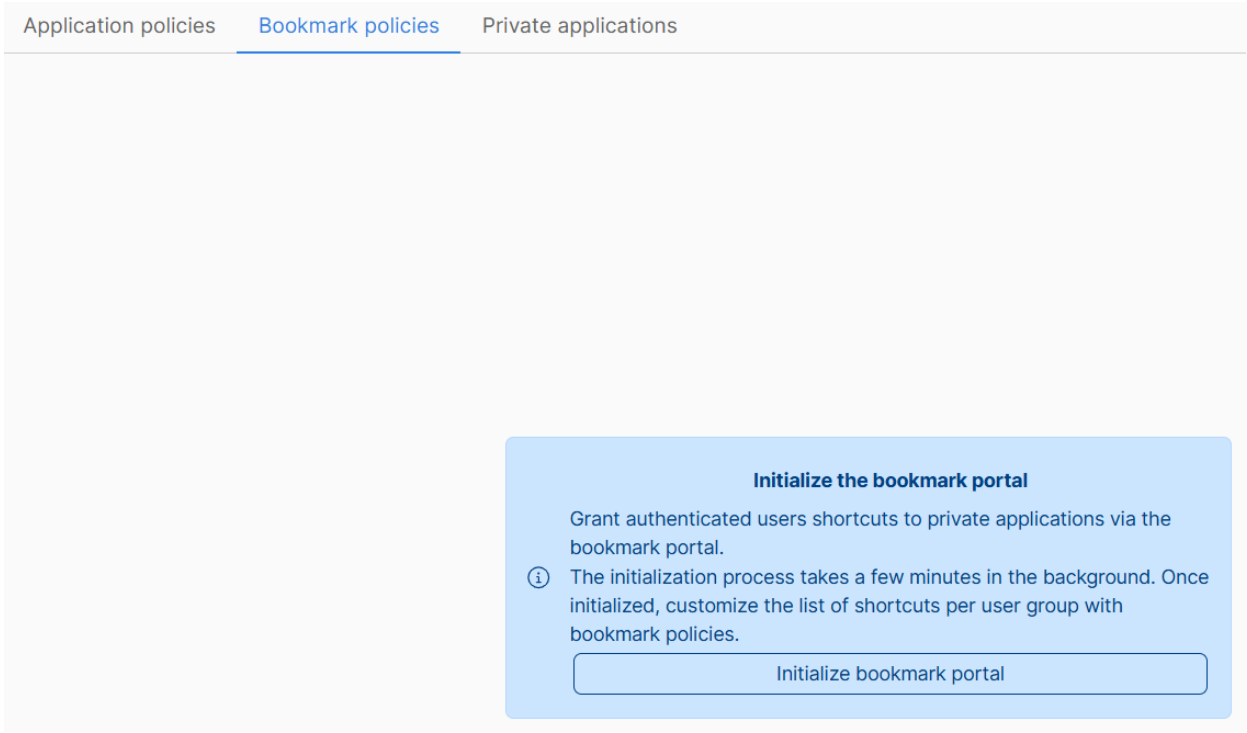
The bookmark portal enforces user access permissions using bookmark policies to allow only specified users and groups to access specified private applications and show only those applications in the bookmark portal.

- The bookmark portal provides authenticated users with shortcuts to private applications. You must initialize it before use.
- A bookmark policy determines which private application bookmarks are visible in the bookmark portal after a configured user or group is authenticated.
- The bookmark portal supports a maximum of 200 private applications since a single bookmark policy supports this as the maximum.

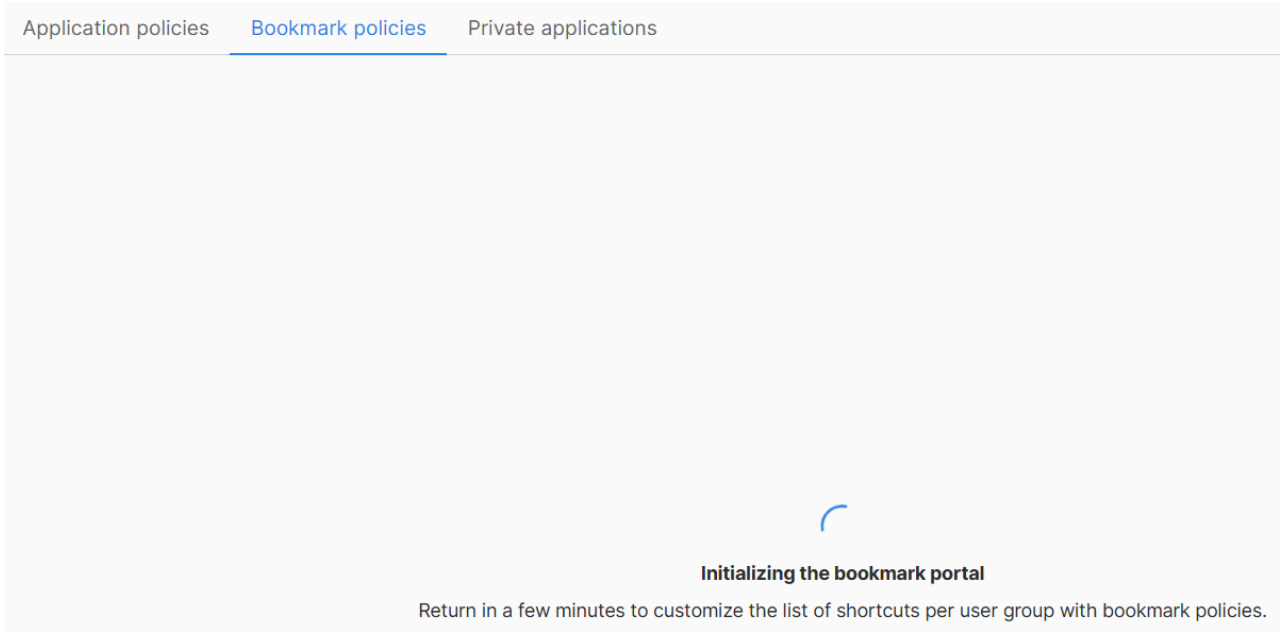
To initialize the bookmark portal:

1. Go to *Security* > *Traffic* > *ZTNA* > *Agentless*.
2. Click *Bookmark portal*.

3. Observe a prompt to initialize the bookmark portal. Click *Initialize bookmark portal* to begin the initialization process.



4. Observe a message indicating the bookmark portal is initializing.



After some time, observe *Successfully generated bookmark portal URL* in the top-right corner.

To configure a bookmark policy:

1. Go to *Security* > *Traffic* > *ZTNA* > *Agentless*.
2. Click the *Bookmark portal* tab.
3. Click *Create*.
4. Configure these fields:

Field	Value	Example Value
Name	Name of bookmark policy.	Finance-Bookmark-Policy-1
Source	The source hosts or host groups of endpoints that are allowed access to the bookmark portal • *All*: All endpoints can access the bookmark portal. • *Specify*: Specific endpoints with specific source hosts or host groups can access the bookmark portal.	*All*
Users	The users that are allowed access to the private application. • *All*: All SSO-authenticated agentless ZTNA users can access this application. • *Specify*: Only SSO-authenticated agentless ZTNA users in the specified users groups can access this application.	Finance
Private applications	The private applications that are added and visible in the bookmark portal. All, one or more previously configured private applications can be added to this field. • *All*: All private applications are added. • *Specify*: Specified private applications are added.	Finance Server
Action	The action applied in this policy: • *Accept*: All private applications are added. • *Deny*: Specified private applications are added.	*Accept*
Status	The status of the policy either Enabled or Disabled	*Enabled*

5. Click *OK*.

Accessing the bookmark portal

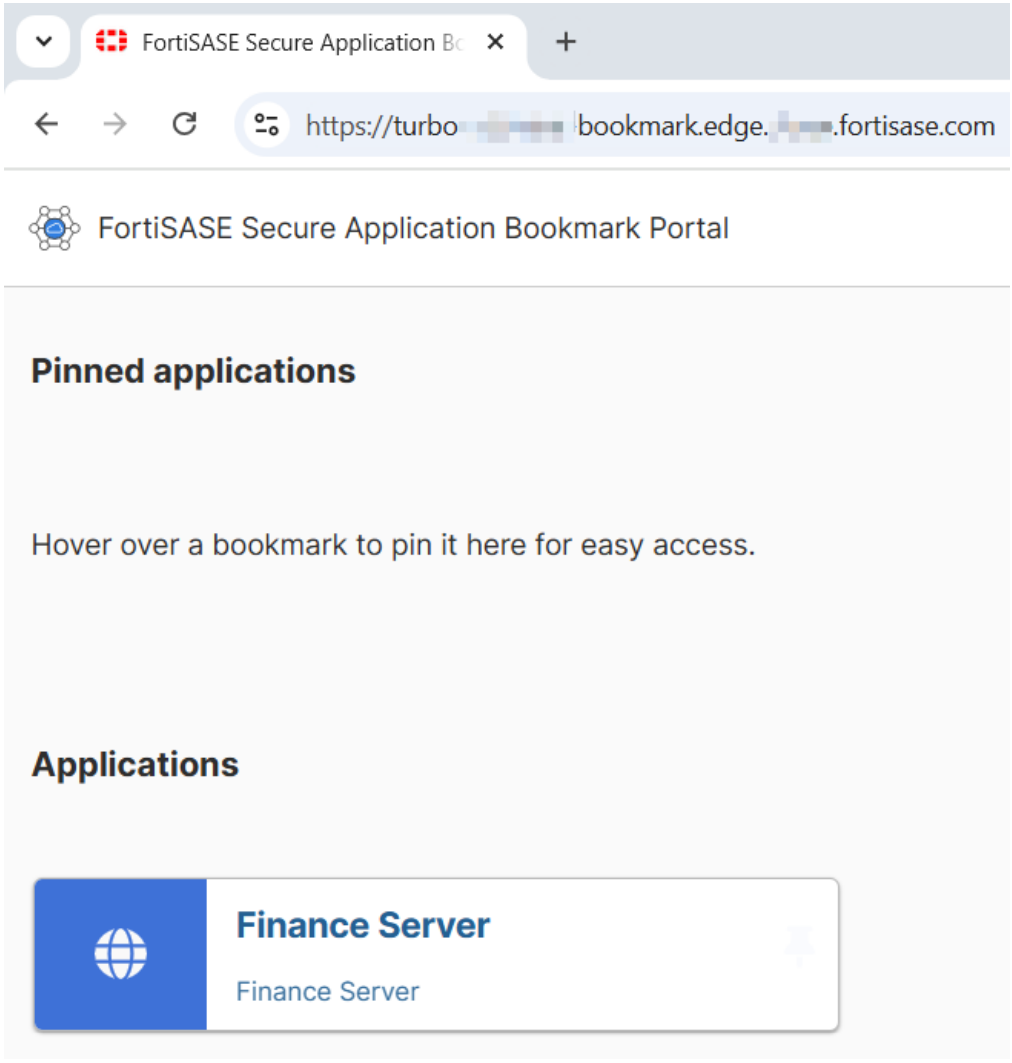
Ensure that you are aware of agentless zero trust network access (ZTNA) Prerequisites and considerations on page 392.

This topic describes one of many steps in the Configuration workflow on page 393.

All successfully configured agentless ZTNA applications are also accessible via the FortiSASE Secure Application Bookmark Portal, which remote users can access only after successfully authenticating with the configured proxy SSO provider.

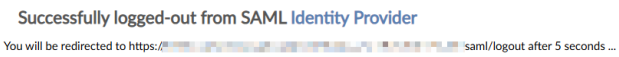
To access the bookmark portal:

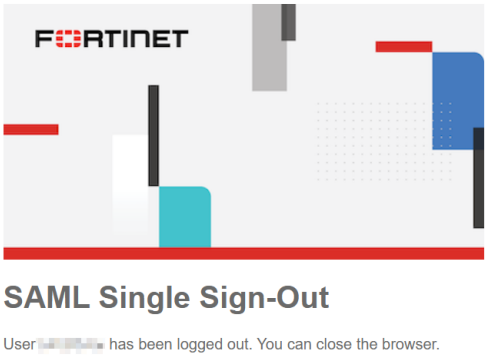
1. Go to *Security* > *Traffic* > *ZTNA* > *Agentless*.
2. Click the *Bookmark portal* tab.
3. On the top-right corner of the page, hover over the information icon and in the tooltip, click *Copy portal URL*.
4. Paste the link to a web browser and observe the bookmark portal load. You will be prompted to authenticate by the proxy SSO provider. Upon successful authentication, remote users can access private applications through this portal.



5. When done accessing private applications using agentless ZTNA, a remote user can log out of the bookmark portal using the *Sign out* link from the top-right of the page. This performs SAML single sign-out for the previously logged in remote user.

   Upon sign out, FortiSASE provides a logged-out notification.





Also, upon sign-out, observe the IdP provide a SAML single sign-out notification.

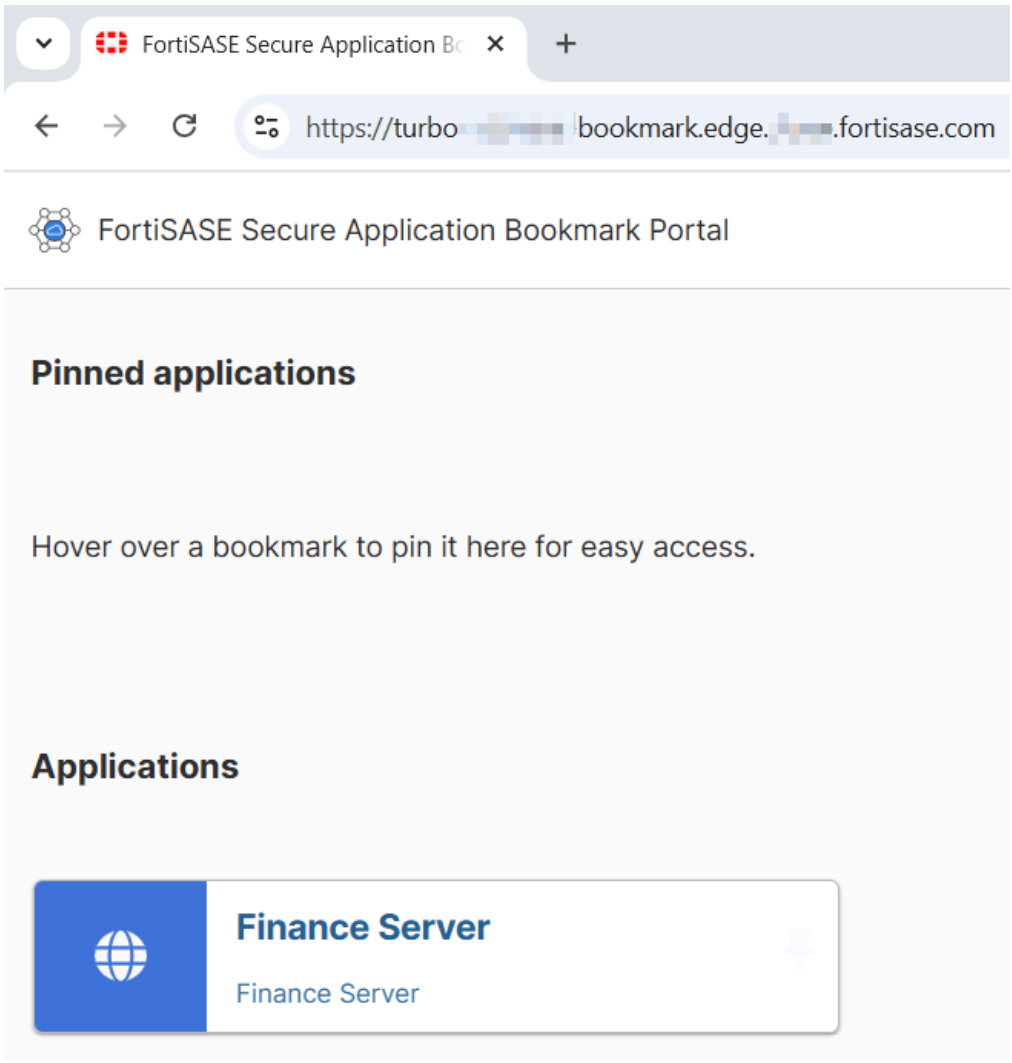
- The notification will be different for each IdP.
- The above notification is an example of the single sign-out notification from FortiAuthenticator as the IdP.

Verifying agentless ZTNA functionality

After following all the steps in Configuration workflow on page 393, you can proceed with verifying agentless ZTNA functionality.

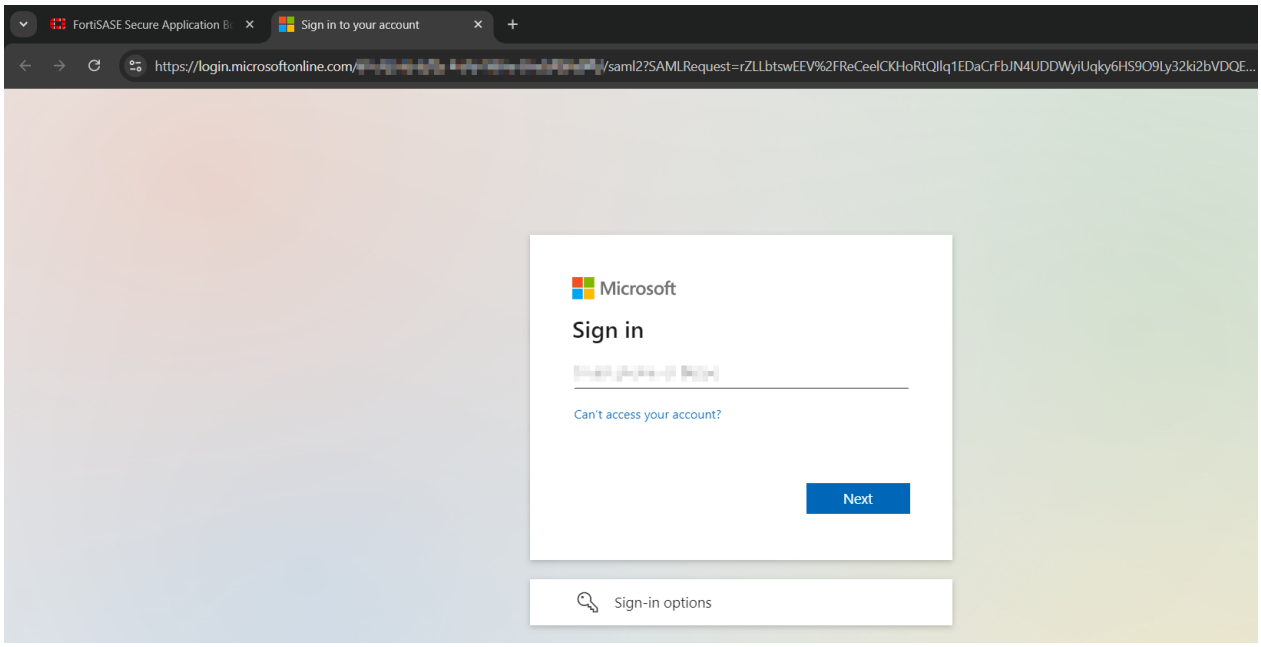
To verify agentless ZTNA functionality:

1. Using a web browser, obtain the bookmark portal link and access it. See Accessing the bookmark portal on page 399.

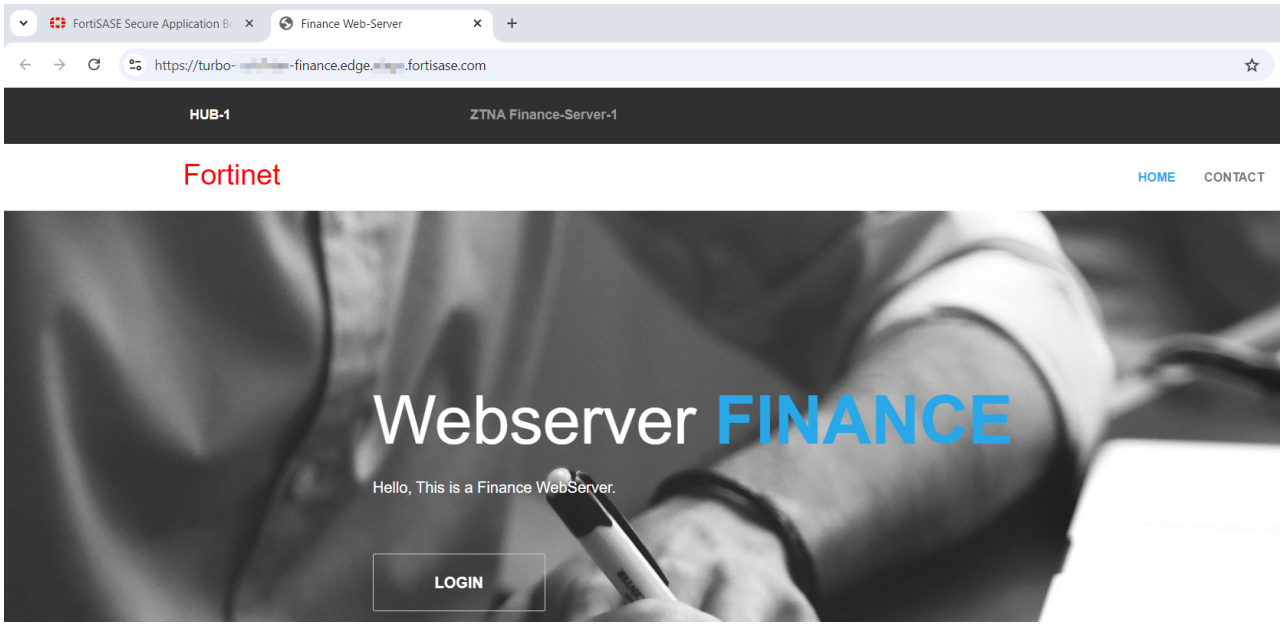


If geofencing has been configured, ensure the endpoint has a source IP address located in an allowed country/region.

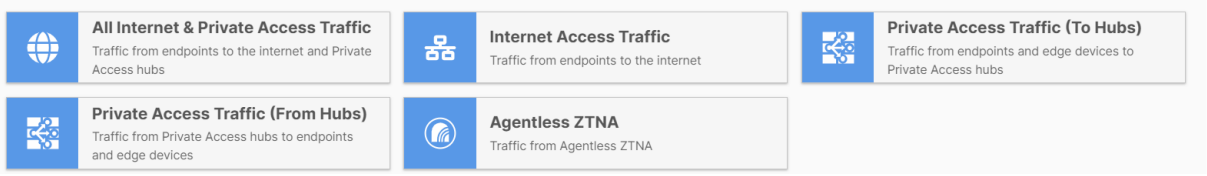
2. Click on one of the bookmarks. For example, click on *Finance Server*.
3. A new tab is opened in the web browser. The configured SAML IdP will prompt for user authentication. Sign in using valid SSO user credentials.



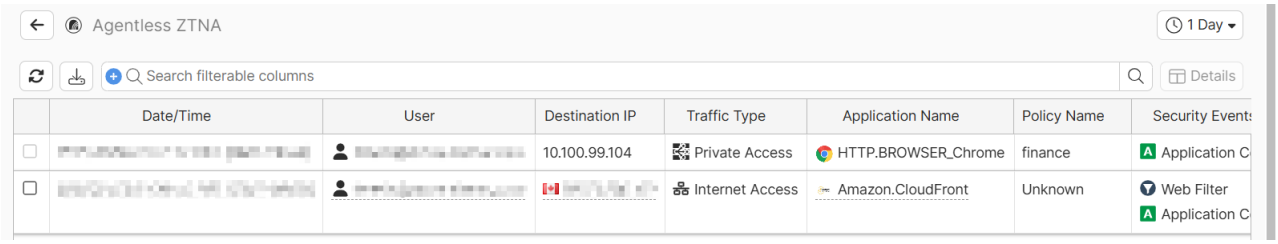
4. Upon successful user authentication, the private application loads as desired.



5. Go to *Operations* > *Logs* > *Traffic* and click *Agentless ZTNA* to view agentless ZTNA traffic logs.



6. Observe the agentless ZTNA traffic to the Finance Server private application as seen through the *Destination IP* value.



7. Click a traffic log entry to see details, namely, to confirm the expected hostname or URL used to access the Finance Server private application.



8. When done accessing private applications using agentless ZTNA, a remote user can log out of the bookmark portal using the *Sign out* link from the top-right of the page. This performs SAML single sign-out for the previously logged in remote user.

Restricting access to agentless ZTNA users

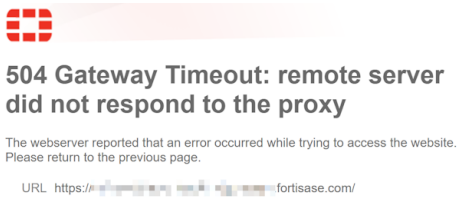
As part of the Prerequisites on page 362 for using agentless zero trust network access (ZTNA), you previously licensed and configured a FortiGate secure private access (SPA) hub device for use with FortiSASE SPA on page 101.

Depending on your network topology, the private HTTPS server you are providing access to using agentless ZTNA may either be connected to the FortiGate SPA hub device directly or to a FortiGate spoke device that is connected to the hub device using an IPsec overlay, specifically, ADVPN. For reference, see diagram in Agentless ZTNA on page 391.

If you have previously configured SPA, then you are already using a firewall policy on either your FortiGate SPA hub device or FortiGate spoke device (if applicable to your network topology) to the LAN interface that your private HTTPS server is connected to. As a best practice, you may have restricted access to your private HTTPS server from agents only by specifying the IPAM subnet as a source address. See IPAM on page 278.

You can update this firewall policy to restrict access to your private HTTPS server from agentless ZTNA users by adding the SPA BGP spoke IP range as a source address. This spoke IP range determines the private IP addresses that the SPA hub assigns after Security PoPs establish IPsec VPN connections with it. This spoke IP range is configured on the FortiGate SPA hub as part of the IPsec VPN Phase 1 configuration in the IKEv2 mode configuration address range settings.

If you do not update this firewall policy, then agentless ZTNA users may encounter the following 504 gateway timeout error when trying to access a private server:



For more details on updating this firewall policy on the FortiGate SPA hub, see Restricting access using a FortiGate SPA hub/spoke policy on page 146.

Considerations

- Although agentless ZTNA is designed for accessing private applications, it is still possible to configure a public IP or FQDN for an application server. In this case, even for dedicated IP instances, the agentless ZTNA user traffic originates from the shared public IP address associated with the Security PoP. This shared public IP address must be used when restricting access to agentless ZTNA users on the FortiGate SPA hub or spoke device (depending on your network topology).

Hosts

Hosts define sources and destinations of network traffic. You can use hosts to define the *Source* and *Destination* fields in a policy based on its selected *Location*.

When creating a host, there are several host types that you can specify. Which one you choose depends on which method most easily yet accurately describes the hosts that you are trying to include with as few entries as possible based on the information that you have. For instance, if you are trying to describe the hosts of a specific company's web server but do not know how extensive their web server farm is, you would be more likely to use a fully qualified domain name (FQDN) rather than a specific IP address range. On the other hand, some computers do not have FQDNs, so configuring a specific IP address range is preferable.

If you have several hosts that will commonly be treated the same or require the same security policies, you can put them into host groups, rather than entering multiple individual hosts in each policy that refers to them.

When you configure a host group with no members in a policy, the policy does not match any traffic and just matches the implicit deny policy.

To configure a host:

1. Go to *Security* > *Hosts*.
2. Click *Create* > *Host*.
3. For *Location*, select the appropriate traffic direction for the host object based on its intended usage:

Host type	Description
Ingress	Host object is available for usage in *Source* field of Internet Access and Private Access policies.
Internet	Host object is available for usage in *Destination* field of Internet Access policies.
Private Access Hub	Host object is available for usage in *Destination* field of Private Access policies.
Unspecified	When selected, you can use the address object in the *Source* and *Destination* fields of Internet Access and Private Access policies.

4. For *Name*, enter the desired name for this host.
5. From the *Type* dropdown list, select the desired host type. The configured *Location* affects which host types are available:

Host type	Description
Subnet	The subnet host type is expressed using a host address and a subnet mask. This is the most flexible host type because the host can refer to as little as one individual address (x.x.x.x/32) or as many as all of the available addresses (0.0.0.0/0). In the *IP/Netmask* field, enter the desired subnet. For example, you could enter 192.168.1.0/24.
IP range	You can use the IP range type to define a continuous set of IP addresses between one specific IP address and another (inclusive). It is a flexible way to describe a continuous set of addresses while being specific and granular without needing to fall within the boundaries of standard subnets.

Host type	Description
	In the *IP Range* field, enter the desired IP address range. For example, you could enter 192.168.1.0-192.168.1.252.
FQDN	The FQDN address type accepts an address string and resolves it to one or more IP addresses. It relies on DNS to keep up with address changes without having to manually change the IP addresses on FortiSASE. In the *FQDN* field, configure the desired FQDN. For example, you could enter www.example.com. You can also specify an FQDN as a wildcard address, such as *.example.com.
Geography	Geography addresses are those determined by the country or region of origin. The IP addresses for the country or region are automatically determined from the Geography IP database. From the *Country/Region* dropdown list, select the desired country or region.

6. Click *OK*.

To configure a host group:

1. Go to *Security* > *Hosts*.
2. Click *Create* > *Host Group*.
3. For *Name*, enter the desired name for this host group.
4. In *Members*, click *+*. In the *Select Entries* pane, select the desired hosts and host groups to include in this host group.
5. Click *OK*.

You can configure the host or host group as a source or destination in a policy. See Adding policies to perform granular firewall actions and inspection on page 297 .

Schedules

Schedules define recurring and one-time time-based settings that can be applied to policies and proxy policies. You can use schedules to define the Schedule field in a policy or proxy policy which can restrict the specific dates and times when the policy or proxy policy is applied to matching traffic.

You can configure the following schedule types:

Schedule type	Description
Recurring	Schedule that can be defined for repeated day(s) of the week and time. The day of the week and time are based on GMT timezone.
One-time	Schedule that can be defined for one-time use with a start and end timestamp (date and time combined). When the one-time schedule has expired, it is highlighted in *One-time schedules* page.

Multiple schedules can be combined into a schedule group. A schedule group must have at least one schedule selected as a member.

To configure a recurring schedule:

1. Go to *Security* > *Resources* > *Schedules* > *Recurring schedules*.
2. Click *+Create*.
3. For *Name*, enter the desired name for this recurring schedule.
4. For *Days*, select one or more days of the week.
5. For *Time*, select *All day* or *Specify* with *Start* and *End* times specified.
   - If the end time is set earlier than the start time, the end time will be during the next day.
   - For recurring schedules, the day of the week and time are based on GMT timezone.
6. Click *OK*.

To configure a one-time schedule:

1. Go to *Security* > *Resources* > *Schedules* > *One-time schedules*.
2. Click *+Create*.
3. For *Name*, enter the desired name for this one-time schedule.
4. For *Start time* and *End time* enter the start and end timestamps (dates and times combined), respectively, when the one-time schedule will apply.
   - You can use the date picker by clicking on the calendar icon to the right of each field.
   - The current local time zone is also listed on the right of each field.
5. Click *OK*.

To configure a schedule group:

1. Go to *Security* > *Resources* > *Schedules* > *Schedule groups*.
2. Click *+Create*.
3. For *Name*, enter the desired name for this schedule group.
4. Click *+*. In the *Select Entries* pane, select the desired schedule to include in this schedule group, or click *+* to create a new schedule.
5. Click *OK*.

You can configure the schedule or schedule group as a schedule in a policy or proxy policy. See Adding policies to perform granular firewall actions and inspection on page 297 and Configuring a proxy policy on page 303.

External feeds

You can configure external feeds on FortiSASE to dynamically import an external list from an HTTP/HTTPS server hosted in the form of a plain text file. The imported list is then available as an external feed and you can use it to enforce special security requirements, such as long-term policies to always allow or block access to certain websites or short-term requirements to block access to known compromised locations. The external

feeds are dynamically synchronized and updated periodically at the configured refresh rate so that any changes in entries of external list are immediately imported to FortiSASE.

FortiSASE supports the following external feed types:

External feed type	File description	Example format
External hosts	One IP address, IP address range, or subnet address per line. An address can be IPv4 or IPv6. You do not need to enter an IPv6 address in [ ] format.	192.168.2.100 172.200.1.4/16 172.16.1.2/24 172.16.8.1-172.16.8.100 2001:0db8::eade:27ff:fe04:9a01/120 2001:0db8::eade:27ff:fe04:aa01-2001:0db8::eade:27ff:fe04:ab01
DNS filter domains	One domain per line. Supports simple wildcards and international domain names.	mail.*.example.com *-special.example.com www.*example.com example.com
Web filter FQDNs	One URL per line.	http://example/com.url https://example.com/url http://example.com:8080/url

Consider the following file format requirements for an external resources files:

- In plain text format with each URL list, IP address, and domain name occupying one line.
- Limited to 10 MB or 128 × 1024 (131072) entries, whichever limit is hit first.
- There is no duplicated entry validation for the external resources file (entry inside each file or inside different files).
- If the number of entries exceeds the limit, FortiSASE does not load additional entries beyond the threshold.

You can set the external resources update period by configuring *Refresh rate*.

FortiClient blocks IPv6 traffic and it does not traverse through the FortiSASE tunnel. External feeds only support listing IPv6 addresses for external feed interoperability with different devices, but FortiSASE does not support IPv6 traffic traversal.

Considerations

- External feeds do not work when hosted on a private server behind a secure private access (SPA) hub configured with BGP on loopback routing design.

Configuring an external feed

You can configure a maximum of 20 external feeds of the same or different types. Depending on their type, you can use external feeds to configure traffic or proxy policies, DNS filter, or Web Filter to allow or deny access to network resources that the information retrieved from the external feed specifies.

To configure a feed:

1. Go to *Security* > *External feeds*. Click *Create*.
2. In the *New External Feed* page, configure the following:

Field	Value
Name	Enter a unique name.
Comments	(Optional) Add a comment.
Status	Enable or disable the feed.
Refresh rate	Enter a value from 1 to 43200 in minutes as per your requirement.
Feed type	Select feed type from the following: • External hosts • DNS filter domains • Web filter FQDNs
URI	Select a protocol for FortiSASE to use to access the external feed: • http:// • https://
HTTP basic authentication	(Optional) Enable or disable basic HTTP authentication. When enabled, enter the username and password in the requisite fields.
Block in Threat Feed Deny policy	Available for external hosts feed. When you enable this option, FortiSASE automatically adds this feed in the *Destination* field for the default Threat Feed Deny policy blocking access for secure internet access traffic. **To view the feed in Threat Feed Deny policy:** • For agent-based endpoints, go to *Security* > *Traffic* > *Policies* > *Threat Feed Deny*. View the *Destination* field. • For agentless endpoints, go to *Security* > *Traffic* > *Proxy policies* > *Threat Feed Deny*. View the *Destination* field.
Block in default internet access profile group	Available for DNS filter domains and Web filter FQDNs feed. When you enable this option, FortiSASE automatically adds this feed with an *Action* of *Block* in the default internet access profile group. **To view the block action for the feed:** 1. Go to *Security* and select the Default profile group. 2. Do one of the following:

Field	Value
	• For a DNS filter domains feed, under *DNS Filter*, click *Customize*. Under *FortiGuard Category Based Filter*, view the *Domain feeds* category. • For a web filter FQDNs feed, under *Web Filter With Inline-CASB*, click *Customize*. Under *FortiGuard Category Based Filter*, view *FQDN feeds*.

3. Click *OK*. The feed is visible under *Security > External feeds*.

Considerations

- External feeds do not work when hosted on a private server behind a secure private access (SPA) hub configured with BGP on loopback routing design.

Applying an external feed

To apply an external host feed:

You can use an external host feed as the source or destination for a traffic or proxy policy for secure internet access (SIA) and secure private access traffic (SPA).

1. Do one of the following:
   - Go to *Security > Traffic > Policies*.
   - Go to *Security > Traffic > Proxy policies*.
2. Select the desired policy, then click *Edit*.
3. In the *Source/Destination* field, click *Specify*.
4. From the *Select Entries* slide in, select the required external feed under *External threat feeds*. Click *Close*.
5. Specify the policy action as *Accept* or *Deny* as per your need.
6. Click *OK*.

To apply a DNS filter domain feed:

You can use a DNS filter domain feed as a domain feed category in *DNS Filter*.

1. Go to *Security > Traffic > Security profiles*. Select the appropriate *Profile Group* from the dropdown in the top right corner.
2. Go to *DNS Filter* and click *Customize*.
3. In the slide in, a *Domain feeds* category appears under *FortiGuard Category Based Filter*, which shows all the configured DNS filter domain feeds. Click the required DNS filter domain feed and select the appropriate action:

Action	The DNS request is...	Security log generated under *Operations > Logs > Security > DNS Filter*?
Allow	Allowed to pass	No
Monitor	Allowed to pass	Yes
Redirect to Block Portal	Blocked. Returns a FortiGuard block page	Yes

4. Click *OK*.
5. Do one of the following under *Internet Access* (SIA) or *Private Access* (SPA):
   - For agent-based users, go to *Security > Traffic > Policies*.
   - For agentless users, go to *Security > Traffic > Proxy policies*.
6. Select the required policy and click *Edit*.
7. In the *Profile Group* field, select the profile group that has *DNS filter domain feed* configured
8. Click *OK*.

To apply a web filter FQDN feed:

You can use a web filter FQDN feed as a web filter FQDN feed category.

1. Go to *Security > Traffic > Security profiles*. Select the appropriate *Profile Group* from the dropdown in the top right corner.
2. Go to *Web Filter With Inline-CASB* and click *Customize*.
3. In the slide in, a *FQDN feeds* category appears under *FortiGuard Category Based Filter*, which shows all the configured Web filter FQDN feeds. Click the required FQDN feed and select the appropriate action:

Action	Description
Allow	Permit access to websites in the .
Monitor	Permit and log access to websites in the category.
Block	Prevent access to websites in the category. Users trying to access a blocked site see a replacement message indicating that FortiSASE blocks the site.
Warning	Display a message to the user allowing them to continue if they choose.
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.

4. Click *OK*.
5. Do one of the following under *Internet Access* (SIA) or *Private Access* (SPA):
   - For agent-based users, go to *Security > Traffic > Policies*.
   - For agentless users, go to *Security > Traffic > Proxy policies*.
6. Select the required policy and click *Edit*.
7. In the *Profile Group* field, select the profile group that has *Web filter FQDN feed* configured.

8. Click *OK*.

Considerations

- External feeds do not work when hosted on a private server behind a secure private access (SPA) hub configured with BGP on loopback routing design.

Applications

The API-based CASB feature supports onboarding these cloud applications:

- AWS S3
- Google Cloud Storage
- Office 365

The *Security > API-based CASB > Applications* page provides *Connect*, *Disconnect*, *Configure*, and *Monitor* options for supported cloud applications.

Connect

You can perform onboarding of supported cloud applications on the *Security > API-based CASB > Applications* page.

To onboard supported cloud applications:

1. Click on a card for the cloud application and select *Connect*.
2. You must perform configuration steps within the cloud application first before configuring the API-based CASB feature within FortiSASE. You can view cloud application-specific step-by-step tutorials.
   The API-based CASB feature supports onboarding these cloud applications:
   - AWS S3
   - Google Cloud Storage
   - Office 365

   Ensure these cloud application steps are performed before moving on to entering details in FortiSASE.
3. Complete the cloud application-specific details within FortiSASE.

Disconnect

To remove a cloud application from being monitored by the API-based CASB feature, click on a card for a previously onboarded cloud application and select *Disconnect*.

Configure

For some cloud applications, after onboarding the application you can configure API-based CASB settings for it, specifically, to configure policies for *Predefined threats*, *Customized threats*, and *Compliance*.

- Threat protection policies track suspicious user behavior.
- Compliance policies monitor cloud accounts in compliance with various compliance standards (SOX-COBIT, PCI, HIPAA, etc.).

Threat protection and *Compliance* are available for specific cloud applications only.

See Policy and Policy Configuration.

Monitor

You can click on the card for any previously onboarded cloud application and select *Monitor* to drill down further with *Alerts* and *Files* tabs on analytics focused on the specific cloud application. You can drill down further by clicking within elements on each tab.

Data Protection

The API-based CASB supports data protection, specifically, data loss prevention (DLP) that scans files using *FortiGuard patterns*, *Custom patterns*, and *Data policies*. These are configurable from the *Security > API-based CASB > Data Protection* page.

Feature	Description
FortiGuard patterns	Default DLP patterns classifying private and confidential data that should be regulated in accordance to regulatory compliance requirements. Additional data patterns are added with the support through FortiGuard under three pattern categories: • *Financial information* • *Malware* • *Personal Identity Information*
Custom patterns	User-defined DLP patterns that can be applied to data like FortiGuard patterns. The following fields can be configured to create a custom pattern: • *Category* • *Max uncompressed file size (MB)* • *Max compressed file size (MB)* • *Matching threshold* • *Regex (PCRE)*
Data policies	Defines which DLP data patterns should be monitoring what type of files under which cloud applications, and what activities would trigger an alert. In addition, when a data security alert is triggered, what action should be taken to mitigate.

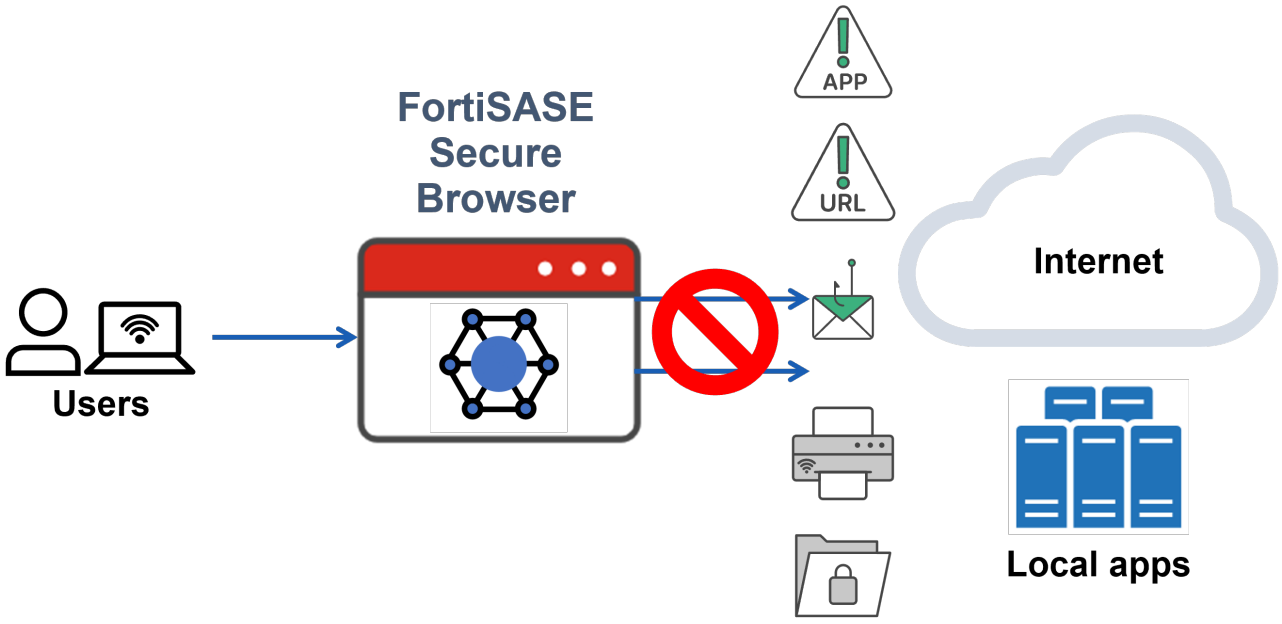
Feature	Description
	• *Use default rule*: Use predefined default data policy where all files under all onboarded cloud application accounts are monitored for all types of file activities basic predefined data patterns. • *Use custom rule*: Use the predefined default data policy with customized alert options including *File types*, *OCR scan for image files*, *Access permissions*, and *File activity triggers*

Secure Browser

FortiSASE supports integrated management of the FortiSASE Secure Browser extension used with unmanaged and contractor devices or deployed on top of existing agent (FortiClient) and agentless (Proxy) deployments. With the deployment of the FortiSASE Secure Browser extension, administrators can gain full visibility into browser activity without deep inspection, can monitor and block web-based threats, and can prevent data exfiltration.

The web browser is the most common application used on endpoints for accessing internet and local applications. This makes it the most common vector for highly evasive attacks such as phishing, malware and other malicious content and files. In addition, the browser is also a source of data loss of sensitive information through copy-and-paste of content to file formats, physical printing, or by unintentionally screen sharing during remote meetings.

FortiSASE Secure Browser through a browser extension for supported web browsers including Google Chrome and Microsoft Edge can mitigate client-side threats on endpoints themselves and complement the protection already provided by steering web traffic to FortiSASE using agent and agentless solutions.



Prerequisites

See Secure Browser.

Considerations

- Currently, the *Display watermark* website display option is not applied when saving a local copy of a website.
- Currently, the *Pasting text copied from specified websites* option for URL domain group overrides is not applied for websites including AI applications containing code blocks with an inline copy button.
- In private browsing mode, browser extensions are disabled by default and must be enabled by the end user. For most deployments, it is highly recommended to disable private browsing mode (Incognito mode in Google Chrome and InPrivate mode in Microsoft Edge) in web browsers on all devices.
- IdP attribute mapping is important for user assignment rules, used to match the contents of attributes to assign secure browser profiles to specific users or groups of users. *Email* is a required attribute for Secure Browser user assignment rules.

Enable FortiSASE Secure Browser

To enable FortiSASE Secure Browser:

1. Go to *Security > Browser > Secure Browser Profiles*.
2. Click *Enable FortiSASE Secure Browser*. You will be prompted to configure Secure Browser SSO settings.

Configure Secure Browser SSO settings

SAML SSO users must be integrated with FortiSASE Secure Browser before the feature can be configured and deployed. Therefore, this feature requires access to a SAML SSO IdP such as Entra ID.

On the SAML SSO IdP side, you must create a new application to integrate SSO with the FortiSASE Secure Browser:

- This is because the Secure Browser SSO settings on the FortiSASE as SAML SSO SP provides unique Entity ID and ACS URL values.
- For Entra ID this means a new Enterprise Application must be created and used only with FortiSASE Secure Browser feature.

To configure Secure Browser SSO settings:

1. After enabling Secure Browser, click *Secure Browser SSO settings*. Alternatively, go to *Access & Authentication > Authentication Sources > SSO* and select the *Secure Browser* tab.
2. In the *Configure identity provider* page, add FortiSASE as a Service Provider using the information on this page:

- Base URL
- Entity ID
- Assertion Consumer Service (ACS) URL

3. In the *Configure service provider* page, populate the fields with configuration from your Identity Provider:
   - IdP entity ID
   - IdP single sign-on URL
   - IdP single log-out URL
   - IdP certificate
4. Click *Next*.
5. (Required for user assignment rules) In Entra ID, follow these steps to obtain the Attribute and SAML claim values:
   a. Log into the Azure portal. You should already have an enterprise application created in Entra ID.
   b. Under *Azure Services*, click E*nterprise applications*. Select the enterprise application created for Secure Browser.
   c. Click *Manage* > *Single sign-on*.
   d. In the *Attributes & Claims* box, click *Edit*.
      i. In the *Attributes & Claims* page, in *Additional claims*, look for the claim with the desired parameter in the *Value* column.

         Common claims include *user.userprincipalname*, *user.mail*, and *user.groups*.

         For example, click on the claim for *user.userprincipalname*.
      ii. In the *Manage claim* page, observe the fields and how they map to FortiSASE settings:

Entra ID field in *Manage claim* page	Setting in FortiSASE *Attribute Mapping* page
Name	SAML claim specified as *<Namespace> / <Name>*
Namespace	
Source attribute	Attribute including the *user.* string

   e. In the *Attribute mapping* page, click *Create* to add Attribute and SAML claim pairs corresponding to the IdP attribute mapping and *OK* to add the mapping.

      IdP attribute mapping is important for user assignment rules, used to match the contents of attributes to assign secure browser profiles to specific users or groups of users. *Email* is a required attribute for Secure Browser user assignment rules.
      - Attribute corresponds to the fixed attribute name on the IdP.
      - SAML claim corresponds to the full configurable SAML claim value on the IdP mapped for the attribute including the namespace. Therefore, you will need to confirm the full SAML claim value in the format of *<Namespace>/<Name>*.

        For example:

Attribute	SAML claim
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
user.userprincipalname	username

Attribute	SAML claim
user.group	group

- By default, *User Attributes & Claims* in Entra ID include the default namespace *http://schemas.microsoft.com/ws/2008/06/identity/claims/*. When combined with the *Name*, the full claim name is *http://schemas.microsoft.com/ws/2008/06/identity/claims/<Name>*.
- However, it is possible to add a new claim and remove the default namespace as was done for user.userprincipalname and user.groups in the example above. Observe that *Email* uses the default namespace in its SAML claim.

6. Click *Create* to add multiple attribute mappings.
7. Click *Next*.
8. Review the configured settings and click *Submit*.

Considerations

- User *Attributes & Claims* in Entra ID allows only one single group claim. You must delete the existing group claim and then add a new claim or you can edit the existing group claim. With this approach, the end result is to change *user.groups* to *All groups* with a custom *Claim Name* of *group*.

  Alternatively, you can keep the existing group claim with default settings of *user.groups* set to *Security Groups* with *Claim Name* of *http://schemas.microsoft.com/ws/2008/06/identity/claims/groups*. This is a valid approach using the official claim name that Microsoft specifies.

  Regardless of the approach chosen, you must ensure that in the FortiSASE SAML SSO user settings, the *SAML Claims Mapping > Group Name* field matches the *Claim Name* specified in the *User Attributes & Claims* section in the Entra ID SAML settings for the FortiSASE enterprise application.
- Configuring group matching using a user assignment rule depends on the *Source attribute* of the SAML group claim configured in Entra ID. By default, Entra ID returns the *user.groups* attribute with a *Source attribute* as Group ID, that is, using the Object ID of the group that the user is a member of. By default, the user assignment rule should be configured with either:
  - *Value* as a substring of the Group ID when using *Relationship* as *Contains*, or
  - *Value* as the exact Group ID string when using *Relationship* as *Equals*.
- If there are multiple user assignment rules, then the order of the rules is significant. When a user signs-in to the Secure Browser Extension, the first user assignment rule that is matched is applied to the user.
- If the user has already signed into the IdP in the browser profile and the organization has not enforced re-authentication via UEM, the user is authenticated into the Secure Browser extension automatically.

Secure Browser profiles

Secure Browser profiles are used to define the behavior of the FortiSASE Secure Browser extension and can be assigned to different set of users based on specific access requirements.

The following settings can be defined in a Secure Browser profile in a new or existing profile within *Security > Browser > Secure Browser* profiles:

Option	Description
Dynamic page inspection	*Block when accessing malicious websites*: • Block access to malicious websites (enabled by default). • Secure Browser relies on its own detection engines to perform real-time, dynamic page inspection of active content for zero-hour phishing detection. • This feature operates independently of the FortiGuard category-based website rules.
FortiGuard category-based website rules	Apply various secure browser features to groups of websites categorized using FortiGuard categories. This feature relies on real-time category lookups of websites based on categories maintained by FortiGuard. Categories in the *Security Risk* main category are blocked by default.
URL domain group overrides	Configure actions for individual websites, overriding the features configured for their category. You can define groups of URL domains, or URL domain groups, which the overrides can be applied to.

These FortiSASE Secure Browser settings are defined in each FortiGuard category-based website rule:

Option	Description
User actions	
Inputting sensitive data	Configure the action taken when inputting sensitive data into a website: • *Allow (default)*: Allow sensitive data to be entered into a website. • *Warn*: Warn the end user when FortiSASE Secure Browser detects sensitive data being entered into a website and log the event.
File downloads	Configure the action taken when file downloads from a website occur: • *Allow (default)*: Allow all file downloads from a website. • *Block all*: Block all file downloads from a website. • *Block specific extensions*: Block downloads of files with specified extensions.
File uploads	Configure the action taken when file uploads to a website occur: • *Allow (default)*: Allow file uploads to a website. • *Block*: Block all file uploads to a website.
Printing	Configure the action taken when the user initiates printing: • *Allow (default)*: Allow printing from websites. • *Block*: Block printing from websites.
Website access	Configure the action taken when the user access a website. • *Allow*: Allow website access. • *Warn*: Displays a warning message when a user tries to access a website. • *Block*: Block access to the website.

Option	Description
	There is no default action for this setting since it depends on the category default defined by FortiGuard.
Website display options	
Display watermark	• *Enable*: Display a watermark in the browser's user interface when visiting a website. • *Disable (default)*: Do not display a watermark. This option is not applied when saving a local copy of a website.
Blur when not in focus	• *Enable*: Blur websites when they are not in focus. This helps to limit information leakage to nearby people who should not have access to information in these websites. • *Disable*: Do not blur websites.
Change summary	A table indicates *No change* or the setting state change recently made by the administrator.

These FortiSASE Secure Browser settings are defined in each URL domain group override entry:

Option	Description
Name	Provide a name for the URL domain group override .
Comments	Provide optional comments about the URL domain group override .
URL domain group	Select the URL domain group that this override applies to. You can use the + to create a new URL domain group from the dropdown list.
User actions	
Inputting sensitive data	Configure the action taken when inputting sensitive data into a website: • *Allow (default)*: Allow sensitive data to be entered into a website. • *Warn*: Warn the end user when FortiSASE Secure Browser detects sensitive data being entered into a website and log the event.
File downloads	Configure the action taken when file downloads from a website occur: • *Allow (default)*: Allow all file downloads from a website. • *Block all*: Block all file downloads from a website. • *Block specific extensions*: Block downloads of files with specified extensions.
File uploads	Configure the action taken when file uploads to a website occur: • *Allow*: Allow file uploads to a website. • *Block (default)*: Block all file uploads to a website.
Pasting text copied from specified websites	This feature is only supported with URL domain group overrides. Prevents users from copying text from a website and pasting it elsewhere. • *Allow*: Allow copying-and-pasting text from specified websites.

Option	Description
	• *Block*: Block copying-and-pasting text from specified websites. • Block paste attempts are not logged. • Currently, the *Pasting text copied from specified websites* option for URL domain group overrides is not applied for websites including AI applications containing code blocks with an inline copy button.
Printing	Configure the action taken when the user initiates printing: • *Allow*: Allow printing from websites. • *Block (default)*: Block printing from websites.
Website access	Configure the action taken when the user access a website. : • *Allow (default)*: Allow website access. • *Warn*: Displays a warning message when a user tries to access a website. • *Block*: Block access to the website. All other options are only available if *Website access* is set to *Allow* or *Warn*.
Website display options	
Display watermark	*Enable*: Display a watermark in the browser's user interface when visiting a website. *Disable (default)*: Do not display a watermark. This option is not applied when saving a local copy of a website.
Blur when not in focus	• *Enable*: Blur websites when they are not in focus. This helps to limit information leakage to nearby people who should not have access to information in these websites. • *Disable*: Do not blur websites.

URL domain groups

A URL domain group is a group of URL domains that are individually defined by the administrator. URL domain groups are used mainly with URL domain group overrides.

Option	Description
Name	Provide a name for the URL domain group.
Comments	Provide optional comments about the URL domain group.
Domains	Define at least one URL domain for this group. Click + to add more URL domains.

User assignment rules and users

User assignment rules allow specific secure browser settings to be assigned to specific users or sets of users based on the contents of their attributes. Therefore, user assignment rules rely heavily on attribute mappings configured in the *Secure Browser* SSO settings.

User assignment rules

You can configure the following settings when creating a user assignment rule:

Option	Description
Name	Provide a name for user assignment rule.
Comments	Provide optional comments about the user assignment rule.
SAML IdP attribute mapping	
Attribute	Select from the dropdown list of attributes assigned in the *Secure Browser* SSO settings.
Relationship	Define the relationship between the attribute and the specified value: • *Contains*: The attribute contains the value. • *Equals*: The attribute matches the value exactly.
Value	The specified value used for matching with the attribute.
Assignment when condition has been met	
Profile	The profile to assign when the condition defined has been met. You can use the + to create a new secure browser profile from the dropdown list.

Considerations

- If there are multiple user assignment rules, then the order of the rules is significant. When a user signs-in to the Secure Browser Extension, the first user assignment rule that is matched is applied to the user.
- Configuring group matching using a user assignment rule depends on the *Source attribute* of the SAML group claim configured in Entra ID. By default, Entra ID returns the *user.groups* attribute with a *Source attribute* as Group ID, that is, using the Object ID of the group that the user is a member of. By default, the user assignment rule should be configured with either:
  - *Value* as a substring of the Group ID when using *Relationship* as *Contains*, or
  - *Value* as the exact Group ID string when using *Relationship* as *Equals*.

Users

In *Security > Browser > User assignment rules*, in the *Users* tab, an administrator can view details about logged on users including their username, last activity, and the secure browser profile assigned to users.

Onboard users

The FortiSASE Secure Browser extension must be onboarded or deployed on endpoints, either directly for unmanaged endpoints or using a user endpoint management (UEM) tool such as ManageEngine Endpoint Central for managed endpoints.

Before onboarding user endpoints, an administrator must enable the Secure Browser feature from within FortiSASE and configure Secure Browser SSO settings. See Enable FortiSASE Secure Browser on page 416 and Configure Secure Browser SSO settings on page 416.

This topic covers the following:

- Onboard unmanaged Windows endpoints directly on page 423
- Onboard managed Windows endpoints with UEM on page 424

Onboard unmanaged Windows endpoints directly

To onboard the secure browser extension for unmanaged Windows endpoints:

1. Ensure the user account has already been created on the SSO IdP server that is configured with Secure Browser. If not, first add the user account to the SSO IdP server.
2. Go to *Security > Browser > User assignment rules > Onboard users*.
3. In the section *Step 1: Install the extension onto endpoints*, download and install the secure browser extension on your browsers:
   - To deploy in the Chrome browser:
     i. Click the *Chrome Web Store* link.
     ii. Click *Add to Chrome* to install the secure browser extension.
   - To deploy in the Edge browser:
     i. Click the *Edge Add-ons* link.
     ii. Click *Get* to install the secure browser extension.
4. While still in *Security > Browser > User assignment rules > Onboard users*, in the section *Step 2: Connect extension to FortiSASE*, download the Windows PowerShell script.
5. To open PowerShell in Admin mode, open *Windows PowerShell* using *Run as Administrator* or open *Terminal (Admin)*.
   a. Run the following command to modify permissions and enter `Y` when prompted:

      ```
      Set-ExecutionPolicy Unrestricted -Scope CurrentUser
      ```

   b. Run the downloaded script.

   > Steps 4 and 5 above to install the PowerShell script are only required when a user authenticates with the SSO IdP provider using the FortiSASE Secure Browser extension for the first time on an endpoint.
   >
   > These steps can be omitted if the same user installs the FortiSASE Secure Browser extension on to additional browsers on the same endpoint.

6. Close and re-open the web browser.

7. (Recommended) To increase visibility of the *Fortinet Browser Security* browser extension, pin the extension in the browser toolbar by:
   a. Clicking *Pin* in Google Chrome.
   b. Clicking *Pin to toolbar* in Microsoft Edge.
8. A login prompt from the SSO provider should appear. If not, click on the extension and log in manually. Log in with user credentials.
9. After login is successful, the FortiSASE Secure Browser extension should change from red to blue indicating a successful connection and login.
10. In FortiSASE confirm the user login by going to *Security > Browser > User Assignment Rules > Users*.

In some cases, you may need to uninstall the secure browser extension for troubleshooting on an endpoint or for decommissioning of an endpoint.

To uninstall the secure browser extension for unmanaged Windows endpoints:

1. Open the web browser.
2. Click on the secure browser extension menu and uninstall the browser extension:
   - In Google Chrome:
     i. Right-click the browser extension in the browser toolbar and select *Remove from Chrome*.
     ii. Click *Remove*.
   - In Microsoft Edge:
     i. Right-click the browser extension in the browser toolbar and select *Remove from Microsoft Edge*.
     ii. Click *Remove*.

Onboard managed Windows endpoints with UEM

This example demonstrates how to onboard a Windows endpoint managed with user endpoint management (UEM) software, specifically, using ManageEngine Endpoint Central. This example builds upon an existing deployment where endpoints already have the UEM agent downloaded and installed.

Before onboarding with the UEM, you must first obtain the extension ID and download the deployment script from FortiSASE.

To obtain extension ID and deployment script from FortiSASE needed for UEM deployment:

1. Go to *Security > Browser > User assignment rules > Onboard users*.
2. Copy the extension IDs corresponding to the browsers you want to use, such as Chrome or Edge.
3. Download the script corresponding to your endpoint platform (Windows or Mac) that is used to connect the extension to FortiSASE. This script will be used for onboarding and deploying the secure browser extension using UEM software. This script is unique to each FortiSASE instance.

To onboard the secure browser extension for managed endpoints using ManageEngine Endpoint Central UEM software:

1. Go to *Browsers > Manage > Groups & Computers > Groups* and click *+Create Group*. You may need to click the ellipsis (...) on the top menu to display the *Browsers* menu item.

   a. Create a new group. such as the *Secure Browser* group.
      i. Add devices as members by dragging and dropping them from *Available Computers* to *Added Computers*.
      ii. Click *Create Group*.
2. Deploy the *Fortinet Browser Security* browser extension for Chrome:
   a. Go to *Browsers > Manage > Extension Repository*.
      i. Go to *Add Extensions > Google Chrome*.
      ii. For *Enter Extension Identifier*, enter the *Extension ID* copied for Chrome in FortiSASE and then click *Add*.
      iii. Click *Add*.
   b. For the Chrome extension, under *Action*, click the ellipsis (...) and then *Distribute to Group(s)*.
      i. Select the *Secure Browser* group.
      ii. Click *Deploy*.
   c. Confirm the deployment by clicking on *Fortinet Browser Security* for Google Chrome and clicking on the *Distributed Computers* tab. You should observe the *Status* of *Policy Deployed Successfully*.
3. Deploy the *Fortinet Browser Security* browser extension for Edge:
   a. Go to *Browsers > Manage > Extension Repository*.
      i. Go to *Add Extensions > Microsoft Edge*.
      ii. For *Enter Extension Identifier*, use the *Extension ID* copied for Edge in FortiSASE and then click *Add*.
      iii. Click *Add*.
   b. For the Edge extension, under *Action*, click the ellipsis (...) and then *Distribute to Group(s)*.
      i. Select the *Secure Browser* group.
      ii. Click *Deploy*.
   c. Confirm the deployment by clicking on *Fortinet Browser Security* for Microsoft Edge and clicking on the *Distributed Computers* tab. You should observe the *Status* of *Policy Deployed Successfully*.
4. (Recommended) To increase visibility of the *Fortinet Browser Security* browser extension, create an Add-on Management policy to pin the extension to the browser's toolbar.
   a. Go to *Browsers > Policies > Add-on Management* and click *Manage Extensions*.
   b. Create a new policy and rename it in the text field.
      i. In the Google Chrome tab, in *Pin Extensions* select *Fortinet Browser Security* and click *Save*.
      ii. In the Microsoft Edge tab, in *Pin Extensions* select *Fortinet Browser Security* and click *Save*.
      iii. Click *Publish*.
   c. Go to *Browsers > Manage > Groups & Computers*, select the computers to be updated, and click *Associate Policy*.
   d. In the *Deploy Policies* window, select the newly created *Add-on Management* policy and click *Deploy*. You should observe the *Status* of *Policy Deployed Successfully*.
   e. Confirm this change by going to a computer that the policy was deployed on and confirming that the *Fortinet Browser Security* browser extension is pinned to the browser toolbar.
5. Import the PowerShell script after deploying the browser extension to the devices. The script configures the secure browser extension to connect to your specific FortiSASE instance.

a. Go to *Software Deployment* > *Settings* > *Script Repository* and click *+Add Script*.
   i. Configure the following settings:

Field	Value
Script Name	Click *Browse*. Select *windows-powershell-full.ps1* that was downloaded to your machine from FortiSASE.
Platform	Windows that is automatically detected upon uploading the script.

   ii. Click *Add*.

6. Create a single deployment policy for Chrome and Edge and specify Windows PowerShell script:
   a. Go to *Admin* > *Configuration Settings* > *Deployment Policies* and click *+Create Policy*.
      i. For *Deployment Schedule*, configure the following settings:

Field	Value
Week(s) & Day(s) for deployment	Click *Select All (All selected)*. Click *Select All (All selected)*.
Deployment Time Period	01:00 to 22:59
Month(s) for deployment	Leave all selected

      ii. Click *Save & Continue*.
      iii. For *Pre-deployment Activities*, click *Save & Continue*.
      iv. For *Pre-deployment user notification* > *User Notification*, click *Save & Continue*.
      v. For *Post-deployment Activities*:
         i. Drag-and-drop *Custom Script* to the white text box on the left. After doing this, *Custom Script* will have a green checkmark, and you should also see *Custom Script* in the white text box.
         ii. Click *Custom Script*.
         iii. For *Script Name*, select *windows-powershell-full.ps1* which was imported in the previous step.
         iv. Click *Save & Continue*.
      vi. Click the pencil icon at the top-left corner and enter the *Template Name* as *SecureBrowser-Windows*.
      vii. Click *Save & Continue*.
7. Create a package for Chrome from a template.
   a. Go to *Software Deployment* > *Package creation* > *Templates*.
      i. Use search tool on the top-right to enter `Chrome`.
      ii. Locate the Windows package for Google Chrome, such as *Google Chrome (x64)...*, select it, and click *Create Package*.
      iii. Select *Automatically update Google Chrome to latest version when available*.
      iv. For *Assign Policy*, select *Default Auto Update Policy* (default).
      v. Click *Create Package*.
   b. Confirm the package has been created in *Software Deployment* > *Package creation* > *Packages*.
8. Create a package for Edge from a template.

a. Go to *Software Deployment > Package creation > Templates*.
   i. Use search tool on the top-right to enter Edge.
   ii. Locate the Windows package for Microsoft Edge, such as *Microsoft Edge for chromium business (...) (x64)*, select it, and click *Create Package*.
   iii. Select *Automatically update Microsoft Edge for Business to latest version when available*.
   iv. For *Assign Policy*, select *Default Auto Update Policy* (default).
   v. Click *Create Package*.
b. Confirm the package has been created in *Software Deployment > Package creation > Packages*.

9. Deploy a new computer configuration to group with both selected packages.
   a. Go to *Software Deployment > Deployment > Install/Uninstall Software > Windows > Computer Configuration*.
   b. Configure the settings, selecting the Chrome package:

Field	Value
Name	SecureBrowser-Windows-Chrome
Package Settings	
Operation Type	Install
Package Name	Google Chrome (x64)...

   c. To add a second package, click *Add More Packages*.
      i. The previous package will appear in a table and a blank dropdown list will appear.
      ii. Select the Edge package in the dropdown list and configure the following settings:

Field	Value
Package Settings	
Operation Type	Install
Package Name	Microsoft Edge for chromium business (...) (x64)

      iii. Click *Add More Packages* to add the package to the table.
   d. Configure the remaining settings:

Field	Value
Deployment Settings	
Apply Deployment Policy	SecureBrowser-Windows
Define Target	
Domain	<Select domain>
Filter Computers based on	Custom Group Secure Browser

   e. Click *Deploy Immediately*.

10. When opening the web browser on managed endpoints, a login prompt from the SSO provider should appear. If not, click on the extension and log in manually. Log in with user credentials.

11. After login is successful, the FortiSASE Secure Browser extension should change from red to blue indicating a successful connection and login.
12. In FortiSASE, confirm the user login by going to *Security > Browser > User Assignment Rules > Users*.

In some cases, you may need to uninstall the secure browser extension for troubleshooting on an endpoint or for decommissioning of an endpoint.

To uninstall the secure browser extension for managed endpoints using ManageEngine Endpoint Central UEM software:

1. Go to *Browsers > Manage > Groups & Computers > Computers*, find the computer that has had the secure browser extension distributed to it and under the *Computer Name* column, click on its hyperlinked computer name.
   a. In the computer-specific page, in the *Extensions* tab, find the entry with the *Fortinet Browser Security* extension.
   b. Under *Action* click the ellipsis (...) and then *Remove*.
   c. In the prompt notifying you to confirm that the extension will be removed from this computer, click *Yes*.
   The *Status* should change from *Policy Deployed Successfully* to *Policy Revoke InProgress*.
2. Go back to *Browsers > Manage > Groups & Computers > Computers* and find the computer that you instructed to remove the secure browser extension from. Observe that the *Extension Distributed* number should be reduced by 1.
3. After some time when the computer synchronizes with the UEM software, confirm in the browser that the browser extension has been uninstalled.

Supported event logs

The following FortiSASE Secure Browser features generate log events in *Operations > Logs > Secure Browser*:

Secure Browser Feature	Conditions when log events generated
Inputting sensitive data	When feature is configured to *Warn* and sensitive data is detected.
Block when accessing malicious websites	When feature is *Enabled* and access to malicious website is blocked.
File downloads	When feature is configured to either: • *Block all* and a file is downloaded. • *Block specific extensions* and a file with the specified extension is downloaded.
File uploads	When feature is configured to *Block* and a file is uploaded.
Pasting text copied from specified websites	When feature is configured to *Block* and text copied from specified websites is attempted to be pasted.
Printing	When feature is configured to *Block* and user attempts to print from a website matched by FortiGuard category or URL domain override.
Website access	When feature is configured to *Warn* or *Block* and user accesses a website matched by FortiGuard category or URL domain override.

Example: Configuring a custom Secure Browser profile and custom user assignment rule

You can configure FortiSASE to enable the Secure Browser extension and apply its features to selected websites:

1. Enable Secure Browser on FortiSASE. See Enable FortiSASE Secure Browser on page 416.
2. Configure Secure Browser SSO settings with attribute mappings. See Configure Secure Browser SSO settings on page 416.
3. Onboard selected computers with the *FortiSASE Browser Security* browser extension and deployment script. See Onboard users on page 423.
4. Configure a custom *Secure Browser* profile.
5. Configure a custom user assignment rule based on attribute matching and specify the custom profile.
6. Verify Secure Browser functionality.

Building upon an existing deployment where Steps 1 through 3 have already been performed, this example demonstrates Steps 4 through 6 with the following conditions:

- The *FortiSASE Browser Security* browser extension was deployed on a Windows test computer running Google Chrome.
- A new or existing enterprise application in Entra ID has been configured for dedicated integration with Secure Browser with the following settings:
  - Entra ID has been configured to return the *user.groups* attribute using the group ID (object ID of group) current group name by configuring the following settings in the existing group claim:
    - *Which groups associated with the user should be returned in the claim as All Groups, Security Groups, or Groups assigned to the application.*
    - *Source attribute as Group ID*
  - Entra ID claim names for Email and user.groups were customized to emailaddress and group, respectively, for simplicity.
- The SAML SSO settings were configured for Entra ID.
- The following attribute mapping was configured:

Attribute	SAML claim
Email	emailaddress
user.groups	group

To configure a custom Secure Browser profile:

1. Go to *Security > Browser > Secure Browser profiles*.
2. Select the *Default Profile* and click *Edit > Clone*.
3. Enter the Name as Custom Profile 1 and click OK.
4. Observe *Dynamic page inspection* is configured to *Block when accessing malicious websites* by default. Keep this setting.
5. Select *Custom Profile 1* and click *Edit*.
6. In URL domain group overrides click *+Create*.

7. Configure the following settings:

Option	Value
Name	Custom Override 1
Comments	<Empty>

URL domain group	1. Use the + to create a new URL domain group from the dropdown list with the following settings:
	• *Name*: Custom domain group 1
	• *Domains*:
	  • example.com
	  • ipinfo.io
	2. Click *OK*.
	3. Click *OK* when asked to confirm selecting the new entry.

User actions	
Website access	Block

8. Click *OK*.

To configure a custom user assignment rule:

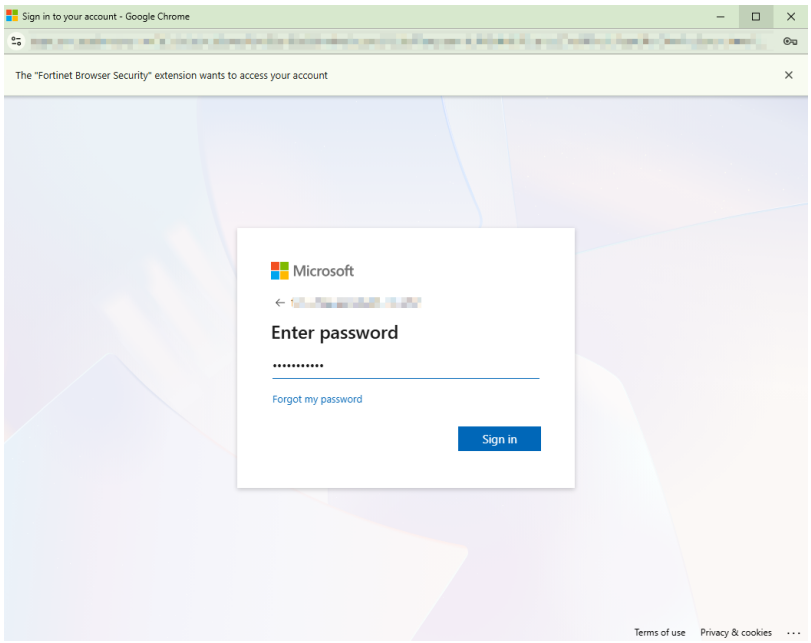
1. Go to *Security > Browser > User assignment rules*.
2. Click *+Create*.
3. Configure the following settings:

Option	Value
Name	Custom Rule 1
Comments	<Empty>
SAML IdP attribute mapping	
Attribute	Select *user.groups*
Relationship	Equals
Value	<Group ID>
Assignment when condition has been met	
Profile	Custom Profile 1

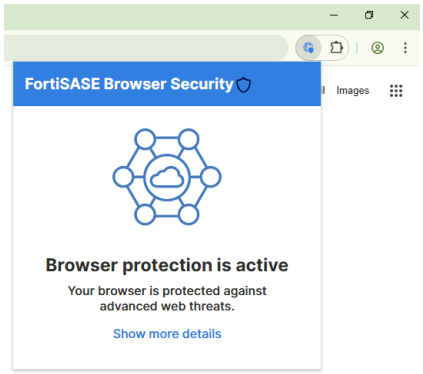
4. Click *OK*.

To verify Secure Browser functionality:

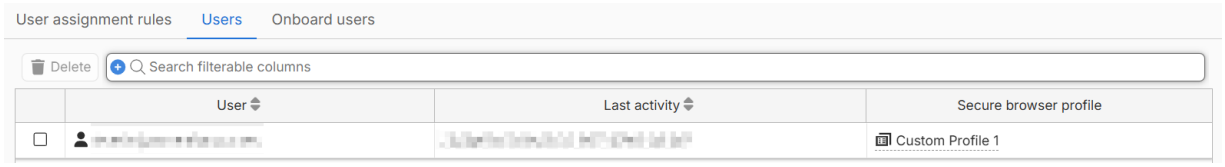
1. Sign into SSO authentication from the Google Chrome browser extension using the username specified in the user assignment rule.



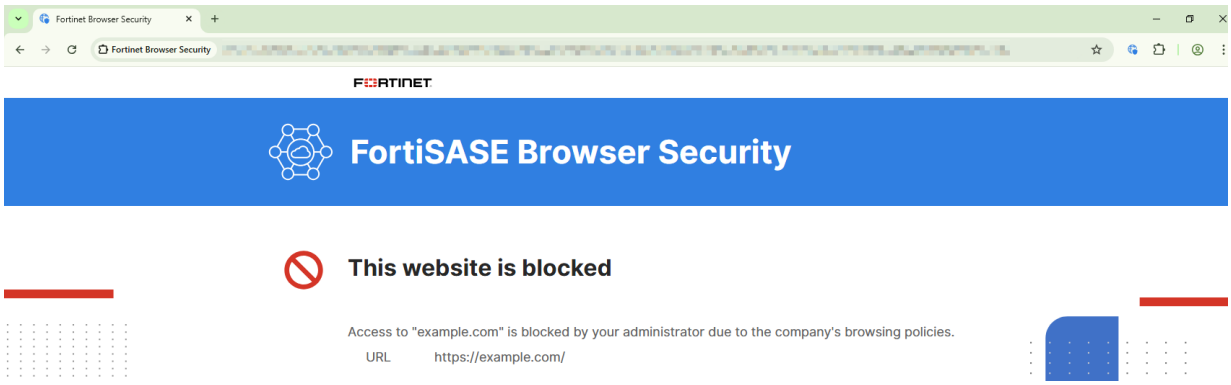
Upon successful log in, the *FortiSASE Browser Security* extension displays that it is actively protecting the endpoint.



2. Confirm from the custom profile is assigned to the user from the *Security* > *Secure Browser* > *User assignment rules* page in the *Users* tab.

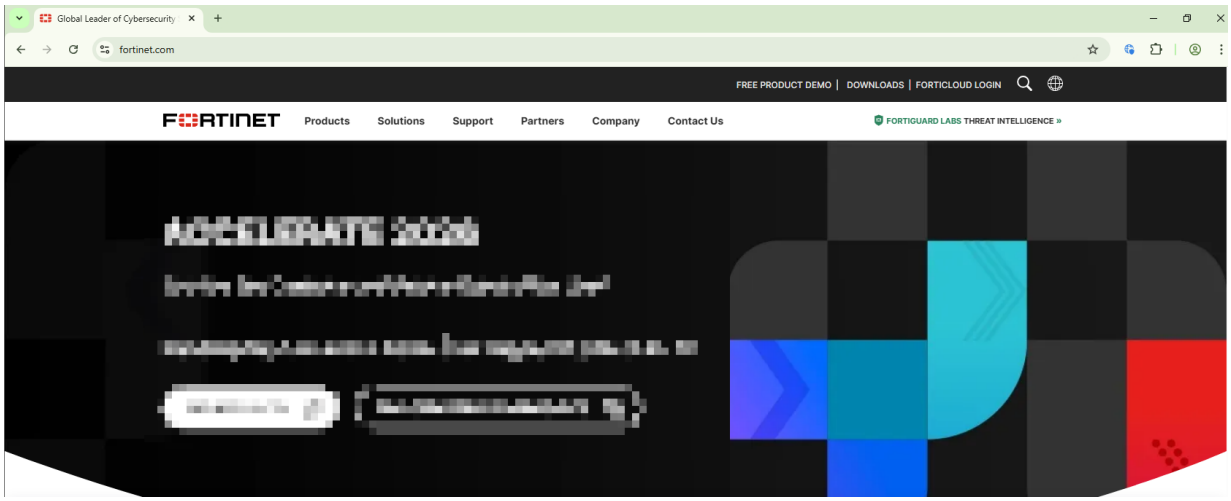


3. Perform some actions that are expected using the custom profile:
   a. Notice that the following websites are blocked:
      - example.com
      - ipinfo.io
      - gambling.com

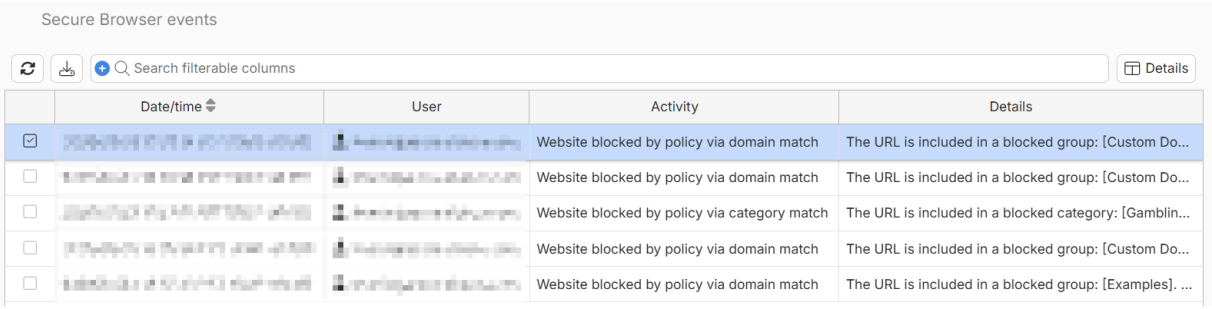


b. Notice the following websites are not blocked:

- fortinet.com
- google.com



4. Observe the blocked events in the log in *Operations* > *Logs* > *Secure Browser*.



Best practices for common use cases

FortiSASE Secure Browser can mitigate client-side threats on endpoints themselves and complement the protection already provided by steering web traffic to FortiSASE using agent and agentless solutions.

This topic covers best practices for deploying common Secure Browser use cases when Secure Browser is used together with agent and agentless solutions, respectively. Secure Browser controls are configured

independently from common FortiSASE security controls. Therefore, this topic introduces strategies to ensure streamlined operation of Secure Browser and steering method features.

Understanding Secure Browser use cases

Below is detailed comparison of security controls for the Secure Browser use cases:

Security Control Type	Security Control	Agent (FortiClient) with Secure Browser	Agentless (Proxy) with Secure Browser
Common FortiSASE security controls	Deep packet inspection	Yes	Yes
	FortiGuard-powered security features	Yes	Yes
Agent-specific controls	Full access to private applications with security posture checks	Yes	HTTP and HTTPS only No security posture checks
	IPsec agent tunnel support	Yes	No
	Agent-based digital experience monitoring (DEM)	Yes	No
	Full endpoint protection and security posture tagging	Yes	No
Proxy-specific controls	Agentless ZTNA support	No	Yes
Secure Browser controls	Essential DLP	Yes	Yes
	Dynamic page detection	Yes	Yes

Understanding Secure Browser controls

Essential DLP and dynamic page detection are key security controls offered by Secure Browser to mitigate client-side threats on web browsers themselves through a Secure Browser extension.

Secure Browser supports essential DLP (data loss prevention) security controls focused on preventing data exfiltration, namely, by blocking the following actions:

- *Website access*
- *Inputting sensitive data*
- *File downloads*
- *File uploads*
- *Printing*
- *Pasting text copied from specified websites (URL domain group overrides only)*

Essential DLP includes support for display features to deter data exfiltration:

- *Display watermark*: Adds the current user's email address as a watermark to the page to associate the page access with the current user.
- *Blur when not in focus*: Prevents data exfiltration from individuals with nearby physical access to the current user's screen.

Secure Browser supports dynamic page detection by relying on its own detection engines to perform real-time, dynamic page inspection of active content for zero-hour phishing detection. This feature operates independently of the FortiGuard category-based website rules and does not require deep packet inspection. Dynamic page scans are performed behind the scenes, without changing the user's browser experience, so that users can stay productive and safe.

Deployment best practices

When deploying Agent with Secure Browser or Proxy with Secure Browser, the following best practices are recommended. Depending on the customer deployment, the following best practices may either be managed by the administrator using a UEM or managed by the administrator directly using per-endpoint configuration.

Pin the extension to the browser toolbar

To increase browser extension visibility, administrators are strongly recommended to pin the Secure Browser extension to the toolbar of their organization's supported browsers.

Enhance essential DLP controls

To enhance essential DLP controls, administrators should consider deploying these browser settings:

- Block user from launching browsers with flags
- Block Chrome Incognito mode or Edge InPrivate mode
- Block third party extensions
- Disable or auto-close browser developer tools

In addition, administrators should consider restricting native browser features that may be misused for data exfiltration, such as restricting these right-click options:

- Search
- Ask AI chatbot
- Translate
- Edge Visual search or Chrome Search with Google Lens

Configure agent tunnel policies and FortiSASE security profiles with Secure Browser controls

To ensure the administrator does not inadvertently block Secure Browser traffic affecting Secure Browser functionality:

- Avoid configuring any agent tunnel policies that deny all traffic
- Avoid blocking the Search engines and portals FortiGuard category in the FortiSASE web filter. Secure Browser traffic is categorized by FortiGuard Web Filtering Service as Search engines and portals.

If any security feature within a FortiSASE security profile group is configured to block and present a block or replacement page, then it is expected that the Secure Browser control will operate on the block page. For example, if a Secure Browser profile has enabled blurring of web pages when not in focus, then it is expected that the FortiSASE security block page will be blurred when not in focus.

This combination of Secure Browser controls and FortiSASE security controls may lead to end user confusion and is strongly not recommended:

- Secure Browser profile is configured with *Website access* set to *Warn* to display a warning page, and
- If any security feature within a FortiSASE security profile group is configured to block and present a block or replacement page.

Endpoint management

In *Endpoint management*, you can configure the following:

- Endpoint profiles on page 436
- Security posture tags and tagging rules on page 486
- Endpoint management settings on page 496
- Endpoint upgrade on page 497

Endpoint profiles

FortiSASE supports multiple endpoint profiles to provide granular behavior for different user types that belong to an Active Directory (AD) group or a non-AD group, such as:

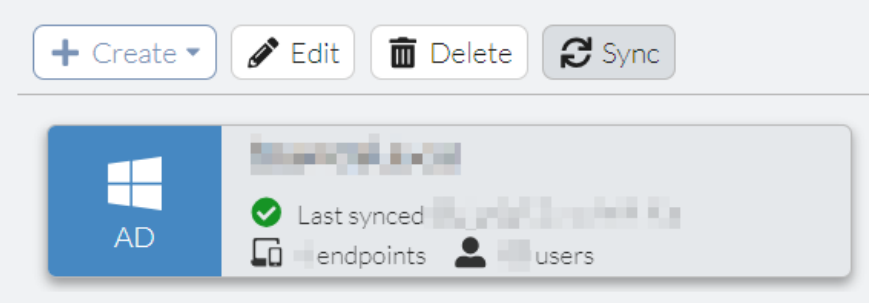
- IT can disconnect from always-on tunnels.
- Marketing can use removable media and authenticates using LDAP.
- All other users cannot disconnect from always-on tunnels or use removable media, and authenticate using single sign on (SSO).

Endpoint management > *Endpoint profiles* presents a table of profiles, with the *Default* profile assigned to all other users if you have not defined custom profiles. You cannot delete the *Default* profile. For accounts that have a Standard or Not-for-Resale remote users FortiSASE subscription, an endpoint profile named *DEM trial* is present, used for activating free 90-days DEM trials on endpoints. See Digital Experience Monitoring on page 71.

You can prioritize and assign endpoint profiles to on-net endpoints based on matching AD domain users and groups or you can assign endpoint profiles based on endpoints assigned to different non-AD groups.

Viewing users and groups from an AD server requires an AD connection in *Access & authentication* > *Authentication Sources* > *Domains*. LDAP user and group information is shared with the FortiSASE Endpoint Management service, which assigns profiles to endpoints that are locally connected to the LDAP domain whenever domain users are logged in by matching selected users or groups.

In *Access & authentication* > *Authentication Sources* > *Domains*, click an AD domain card and click *Sync* to synchronize the AD connection with any updates from the AD server, if necessary:



When creating a new endpoint profile, you can use the *Groups & AD Users* tab to select which AD users/groups or non-AD groups you will apply the profile to, and you can use an option in the *Connection* tab to enable/disable SSO authentication per profile. To assign endpoints to different non-AD groups, see Groups & AD Users on page 469.

To configure Profiles options:

1. Go to *Endpoint management* > *Endpoint profiles*.
2. Do one of the following:
   - Click *Create* to create a new endpoint profile. In the *Name* field, enter the desired name of the endpoint profile.
   - To modify an existing endpoint profile, select the profile, then click *Edit*.
3. Configure the options on each tab as the following topics describe:
   - Connection on page 443
   - Protection on page 459
   - Sandbox on page 462
   - ZTNA on page 464
   - FSSO on page 468
   - Groups & AD Users on page 469
   - FortiClient GUI Settings on page 470
4. Click *OK* to save the endpoint profile.
5. (Optional) Once you have configured an endpoint profile, you can clone it to quickly create additional endpoint profiles. This feature is useful when setting up multiple profiles with slight variations while maintaining a consistent baseline configuration. To clone an existing endpoint profile, do the following:
   a. Select an existing endpoint profile and click *Edit* > *Clone*.
   b. In the *Name* field, enter the desired name.
   c. Click *OK*.



For demonstrations of various configuration options for implementing FortiSASE endpoint management features, such as custom endpoint profiles, autoconnect tunnels, split tunnel, vulnerability scan, zero trust network access (ZTNA), and more, see the FortiSASE Endpoint Management Deployment Guide.

Considerations

- This feature does not apply for proxy mode users. See Proxy agentless mode on page 15.
- FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with any BGP routing design.

  Implicit and split DNS rules for tunnel traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

  Ensure that your FortiSASE remote users have access to the LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 47.

- The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.
- For a FortiSASE instance expecting heavy SMB traffic patterns with its agent remote users, to ensure optimal performance, for endpoint profiles with *Sandbox mode* set to *FortiSASE* (FortiSASE Sandbox is enabled), in *Profile Configuration > Sandbox* ensure the *File submission options > All files executed from mapped network drives* option is disabled.

Global connection settings

Global connection settings are common settings that apply to all endpoint profiles, including the Default endpoint profile. Therefore, any changes you make to these settings apply to all endpoints across different endpoint profiles.

To access these common connection settings, go to *Endpoint management > Endpoint profiles* and from the toolbar, select *Global connection settings*.

FortiSASE Cloud Security tunnel advanced settings

Authentication setting	Description	Minimum value (seconds)	Maximum value (seconds)
Authentication timeout	Duration, in seconds, after which remote users must reauthenticate to connect to the FortiSASE Cloud Security tunnel, regardless of whether the user session is active or idle.	0	259200 (72 hours)
Idle timeout	Duration, in seconds, after which remote users are signed out of their session if no traffic is detected. Connecting to the FortiSASE Cloud Security tunnel requires reauthentication.		

Authentication setting	Description	Minimum value (seconds)	Maximum value (seconds)
Session resumption timeout	The tunnel is maintained in idle state for specified timeout, which allows for uninterrupted usage even after a client resumes from sleep or when connectivity is restored after a disruption and reduces the need to re-authenticate when reconnecting. The session resumption timeout must be shorter than the authentication timeout.	120	172800 (48 hours)
Dead peer detection	For instances with IPsec agent support, dead peer detection settings configurable on Security PoPs. See IPsec dead peer detection customization on page 471.		
	DPD retry count (number of retries, default 3)	0	10
	DPD retry interval (default 60 seconds)	0	3600
Pre-shared key	It is strongly recommended to schedule a maintenance window before changing the pre-shared key for IPsec instances. Currently connected endpoints will be disconnected from FortiSASE for a few minutes while the change is applied. See Considerations on page 441 for details.	Not applicable	Not applicable

Authentication setting	Description	Minimum value (seconds)	Maximum value (seconds)
	To update the pre-shared key: 1. Click *Update*. 2. In the pane: a. Enter a new pre-shared key or click *Generate* to randomly generate a new pre-shared key. b. Click the eyeball icon to view the pre-shared key. c. Click the copy button to copy the pre-shared key and save it to a secure location. This is an important step since the pre-shared key is not visible after clicking *OK*. 3. Click *OK*. 4. Click *Apply*. For IPsec, the pre-shared key must be configured the same for the FortiSASE Cloud Security tunnel and these on-premise FortiGate gateways to support these corresponding features: • Gateway used for regional compliance • Gateway used for failover sequence		
FortiSASE Cloud Security Tunnel encapsulation	Encapsulation used for FortiSASE Cloud Security tunnel:	Not applicable	Not applicable

Authentication setting	Description	Minimum value (seconds)	Maximum value (seconds)

	• *Auto*: Attempts UDP encapsulation and fails back to TCP encapsulation.
	  • When standard IPsec ports 500 and 4500 over UDP are blocked by networks, use IPsec over TCP with TCP port 443.
	  • When IPsec over TCP is used, SSO SAML authentication also uses TCP port 443.
	• *UDP* (default): IKE and ESP packets are sent via UDP encapsulation.		

Considerations

- IPsec VPN instances only have the *Authentication timeout* and *Pre-shared key* options available.
  - For new IPsec VPN instances with Windows or Mac endpoints and FortiClient 7.4.5 or later, the *FortiSASE Cloud Security Tunnel encapsulation* is also supported. For existing instances where the SSL to IPsec migration has been completed, *FortiSASE Cloud Security Tunnel encapsulation* and *Session resumption timeout* are only available after fully migrating to IPsec and disabling SSL tunnels.
- It is strongly recommended to schedule a maintenance window before changing the pre-shared key for IPsec instances.
  - Currently connected endpoints will be disconnected from FortiSASE for a few minutes while the change is applied.
- Before changing the *Pre-shared key* setting, consider the following effects depending on the specific combination of configuration settings:

Endpoint profile setting for *Endpoint connects to FortiSASE Cloud Security*	User has selected *Save Password* in endpoint local configuration	Effect of changing *Pre-shared key* setting on endpoints
Automatically	Yes	Currently connected endpoints will be disconnected from FortiSASEfor a few minutes

Endpoint profile setting for *Endpoint connects to FortiSASE Cloud Security*	User has selected *Save Password* in endpoint local configuration	Effect of changing *Pre-shared key* setting on endpoints
		while the change is applied.
Automatically	No	Users will be prompted to re-authenticate before reconnecting to FortiSASE.
Manually	Yes or No	Users will remain disconnected until they manually reconnect to FortiSASE. Any disconnect in this mode requires manual intervention by users.

Endpoint profile setting for *Endpoint connects to FortiSASE Cloud Security*	Use Case	Effect of changing *Pre-shared key* setting on endpoints
Automatically	• SSO is configured • User has selected to stay signed in when prompted by the IdP (Entra ID, Okta, etc.)	Currently connected endpoints will be disconnected from FortiSASE for a few minutes while the change is applied.
Automatically	• Endpoint is domain-joined and off-net • Endpoint profile option to *Exempt endpoint from FortiSASE auto-connect when endpoint is on-net* is enabled.	

FortiPAM integration

Enabling FortiPAM integration allows you to leverage the FortiClient privileged access management (PAM) module for secure and controlled privileged access on endpoint devices. This integration generates a new FortiClient installer preconfigured with the FortiPAM agent and activates the FortiPAM agent on FortiClient endpoints. Thus, enabling FortiPAM integration requires reinstalling FortiClient on all targeted endpoints using the updated installer to enable PAM functionality.

Once the FortiPAM agent is active, it automatically installs the necessary browser extensions for supported browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge to ensure seamless interaction with privileged web sessions.

The default port that FortiPAM agent listens to is 9191. This port should also match with the port number that is configured on the FortiPAM server under *System > Settings > Client port* for successful agent to server communication.

Only Windows endpoints support FortiPAM integration. Ensure to use a supported FortiClient version. See Product integration and support.

To enable FortiPAM integration on FortiClient endpoints via FortiSASE:

1. Go to the *Settings* tab and enable *FortiPAM integration*.
2. Set *Port* as 9191 (default port).
3. (Optional) If you specify a custom port, ensure to specify the same port on the FortiPAM server under *System > Settings > Client port*.
4. Click *Apply*.
5. FortiSASE generates a new FortiClient installer with a built-in FortiPAM agent. Uninstall the current FortiClient from endpoints and install the new version using the provided installer. See Client onboarding on page 730 for installation instructions.
6. Ensure the newly installed FortiClient is connected to FortiSASE Management Service.

To verify FortiPAM agent installation and status:

1. Open FortiClient on the endpoint and go to *Settings > Advanced*.
2. Under *Enable Privileged Access Management*, you should see the updated port number in the *Local Server Port* field.
3. (Optional) On a Windows endpoint, use Task Manager to check that the following processes are running:
   - fortivrs.exe
   - fortiTcs.exe
4. (Optional) On a Windows endpoint, use Command Prompt to check if the agent is listening on the correct port. For example, run the following command for port 9191:

```
netstat -an | findstr :9191
```

For more information on troubleshooting FortiPAM issues on FortiClient, see FortiClient troubleshooting tips.

Pre-logon authentication settings for Windows and macOS endpoints

See Pre-logon tunnel on page 472.

Connection

To configure the Connection tab:

1. Create a new profile or edit an existing one:
   a. Go to *Endpoint management > Endpoint profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. If creating a new profile, in the *Name* field, enter the desired name of the endpoint profile.

2. On the *Connection* tab, do one of the following:
   - To enable autoconnect to the FortiSASE Cloud Security tunnel, under *FortiSASE Cloud Security tunnel settings*, set *Endpoint connects to FortiSASE Cloud Security* to *Automatically*. Disable the toggle for *Show option to disconnect from security PoP* to prevent endpoints from being able to disconnect from the FortiSASE Cloud Security tunnel or enable it to allow endpoints to disconnect using a *Disconnect* button on FortiClient.
   - To disable autoconnect and let endpoint users manually connect to the *FortiSASE Cloud Security tunnel* or *Custom tunnel*, select *Endpoint connects to FortiSASE Cloud Security* to *Manually*.
3. Configure the remaining options as the following topics describe:
   - Pre-connection posture checks on page 444
   - Advanced settings on page 445
   - On/off-net Settings on page 447
   - Network lockdown on page 450
   - Steering bypass destinations on page 453
   - Custom tunnels on page 455
   - Tunnel Settings on page 457
4. You must configure some more important FortiClient settings on the *FortiClient GUI Settings* tab. See FortiClient GUI Settings on page 470.
5. Click *OK* to save endpoint profile.

Pre-connection posture checks

FortiSASE can enforce pre-connection posture checks on FortiClient endpoints attempting to establish a connection to either the *FortiSASE Cloud Security tunnel* or a *Custom tunnel* of type *IPsec*, by leveraging security posture tags assigned to the endpoints.

In this workflow, FortiClient performs the actual posture check by evaluating whether the connecting endpoint has the specified security posture tag, defined in its associated endpoint profile. FortiClient can either allow or deny the endpoint to connect to *FortiSASE Cloud Security tunnel* or a *Custom tunnel* of type *IPsec*, based on the action configured in FortiSASE when specified security posture tag is detected.

FortiSASE also allows configuring customized denial message that FortiClient displays to users when access is denied. Thus, pre-connection posture checks help validate endpoint compliance and ensure that only compliant endpoints are allowed to connect.

This feature is only available for FortiSASE instances enabled with IPsec remote agent support. See IPsec remote agent support on page 54.

To configure pre-connection security posture checks for FortiSASE Cloud Security tunnel:

1. In the desired endpoint profile, navigate to *Connection* tab. Under *FortiSASE Cloud Security tunnel* settings, enable the option *Run posture check before initiating FortiSASE Cloud Security tunnel*.
2. In the *Posture tag* dropdown, select an existing tag or click *+* to configure a new posture tag. See Security posture tags and tagging rules on page 486.
3. For *Action if endpoint is tagged*, choose from desired action:
   - *Allow*: Permit endpoints to establish a connection to *FortiSASE Cloud Security tunnel* if endpoint has a specified security posture tag.

- *Deny*: Block endpoints to establish a connection to *FortiSASE Cloud Security tunnel* if endpoint has the specified security posture tag.

4. To display a message to endpoints that are denied from connecting to *FortiSASE Cloud Security tunnel*, enable *Customize message shown to endpoint when access denied* and specify the message in message box.
5. Configure the remaining options on the *Connection* tab. See Connection on page 443.

To configure pre-connection security posture checks for Custom tunnel of type IPsec:

1. In the desired endpoint profile, navigate to *Connection* tab. Under *FortiSASE Cloud Security tunnel settings*, set *Endpoint connects to FortiSASE Cloud Security* to *Manually*. This disables autoconnect to let endpoint users manually connect to the *FortiSASE Cloud Security tunnel* or *Custom tunnels*.
2. Under *Custom tunnels*, select the desired tunnel of type *IPsec* and click *Edit*. To configure a new *Custom tunnel*, see Custom tunnels on page 455.
3. Enable the option *Run posture check before initiating FortiSASE Cloud Security tunnel*.
4. In the *Posture tag* dropdown, select an existing tag or click *+* to configure a new posture tag. See Security posture tags and tagging rules on page 486.
5. For *Action if endpoint is tagged*, choose from desired action:
   - *Allow*: Permit endpoints to establish a connection to selected custom tunnel of type IPsec if endpoint has a specified security posture tag.
   - *Deny*: Block endpoints to establish a connection to selected custom tunnel of type IPsec if endpoint has the specified security posture tag.
6. To display a message to endpoints that are blocked from connecting to *Custom tunnel* of type *IPsec*, enable *Customize message shown to endpoint when access denied* and specify the message in message box.
7. Click *OK* to save the custom IPsec tunnel setting.
8. Configure the remaining options on the *Connection* tab. See Connection on page 443.

Advanced settings

The advanced settings discussed below apply to *FortiSASE Cloud Security tunnel* and to any on-premise gateways configured under *Failover sequence*.

1. Enable *Pre-logon authentication* to enable the pre-logon tunnel feature. This option is only configurable if *Pre-logon authentication settings for Windows and macOS endpoints* is enabled in *Global connection settings*. See Pre-logon tunnel on page 472.
2. Disable *Disable internet check* to start agent tunnel auto-connect only after internet connectivity is confirmed (default setting). Otherwise, when the internet check is disabled, agent tunnel auto-connect starts without verifying connectivity.
3. Enable *Authenticate with SSO* to enable using SAML Single sign on for user authentication to connect to *FortiSASE Cloud Security tunnel* or on-premise gateways. If SSO is already configured as user authentication method on FortiSASE, the setting *Authenticate with SSO* is enabled by default. To configure SSO on FortiSASE, see SSO on page 515.
4. Enable *Use FortiClient built-in browser for SAML authentication* to allow FortiClient to use the embedded browser built into FortiClient for SAML-based single sign-on (SSO), instead of the endpoint's default system browser.
5. Enable *Allow FIDO authentication* to support FIDO2 passkey or passwordless authentication for agent tunnels using FortiClient for Windows or MacOS.

- This feature is only available when *Authenticate with SSO* and *Use FortiClient built-in browser for SAML authentication* are enabled.
- This feature requires Entra ID to have already been configured for FIDO2 authentication. See Enable passkeys (FIDO2) for your organization.
- Currently, the *Allow FIDO authentication setting* only restricts this authentication method for FortiClient MacOS endpoints. For FortiClient Windows endpoints, in addition to enabling this setting, the FIDO2 authentication method must also be configured in the Entra ID Enterprise Application for which SAML-based SSO is configured for in FortiSASE.

6. Enable *Failover sequence* setting to allow FortiClient endpoints to fail over between *FortiCloud Cloud Security tunnel* and one or more on-premise gateways and to define a priority list for failover sequence.
   - Once enabled, by default, the *FortiSASE Cloud Security tunnel* appears as the first entry in the failover sequence. This is the primary tunnel used for Secure Internet Access (SIA).
   - To add an on-premise gateway, click the + icon and enter the gateway's IPv4 address or fully qualified domain name (FQDN). You can add multiple on-premise gateways.
   - Use the drag-and-drop utility to reorder the list and define the connection priority. FortiClient attempts to connect to the tunnels in the defined order. If the first tunnel fails, it tries the next one in sequence and so on in a round-robin fashion based on the specified priority order. The priority order list of tunnels are visible on FortiClient endpoints belonging to respective endpoint profile under *Remote Access*.
   - FortiSASE only manages the *FortiSASE Cloud Security tunnel*. Any on-premise tunnels added to the failover sequence must be independently configured on the corresponding VPN gateways. Ensure that these on-premise tunnels use the same tunnel settings as those used by the *FortiSASE Cloud Security tunnel* as FortiSASE Endpoint Management server applies these settings uniformly. To view the specific tunnel settings used by FortiSASE, see FortiClient on page 56.
   - If the endpoint reboots or shuts down, FortiClient restarts the tunnel connection process from the top of the failover list upon startup. It does not resume from the last connected or attempted tunnel. Additionally, if a user manually disconnects from a connected tunnel, FortiClient does not automatically switch to the next available tunnel even if a higher priority tunnel becomes reachable. Manual reconnection is required.
   - (Windows only) If Pre-logon VPN is enabled and the endpoint connects to it during system startup, FortiClient will attempt to reconnect using the Failover Sequence after the Pre-logon VPN tunnel is terminated. Thus once the user logs in and the Pre-logon VPN is disconnected, FortiClient begins a new connection attempt starting from the top of the defined tunnel list in Failover sequence.

   This setting is configurable on a per endpoint profile basis and is available on FortiSASE instances with either SSL VPN or IPsec remote agent support enabled. For IPsec, the pre-shared key must be configured the same for the FortiSASE Cloud Security tunnel and for the on-premise FortiGate failover gateway.

   To apply a similar connection prioritization mechanism across all endpoint profiles, based on the geographic location of the endpoint, see Geofencing on page 269.
7. Enable *Dead peer detection* to reestablish IPsec agent tunnels on idle connections and clean up dead IKE peers, if required, and configure DPD retry count and DPD retry interval accordingly. See IPsec dead peer detection customization on page 471.
   - *DPD retry count*: Set to the number of DPD retry attempts. Default: 3
   - *DPD retry interval*: Set the length of the DPD retry interval. Default: 5 seconds
8. If required, in the *DNS suffix* option, configure a DNS suffix and click *+* to configure additional DNS suffixes. This feature requires Windows endpoints running FortiClient 7.4.5 or later.

- DNS suffixes are used for resolving short hostnames and are appended to subdomains.
- DNS resolutions of endpoints apply the DNS suffixes in the order they are configured. To modify the order of DNS suffixes, hover the cursor to the left of the configured DNS suffix then click and drag it to the desired order.
- Whenever a DNS suffix is configured or modified, users must reconnect the agent tunnel for changes to take effect.

On/off-net Settings

On-net rule sets determine if FortiSASE considers endpoints trusted or on-net, meaning they are in a corporate network that has some level of on-premise security and do not need to automatically connect to FortiSASE tunnel for security inspection. This also helps to optimize FortiSASE bandwidth usage.

For example, by configuring an on-net rule set that uses your corporate network's public IP address, any endpoints behind this corporate network do not autoconnect to the FortiSASE Cloud Security tunnel. Instead, endpoints only autoconnect when their public IP addresses do not match the configured public IP address in the on-net rule, indicating they are untrusted or off-net and enforcing security inspection via FortiSASE SIA.

FortiSASE supports on-net rule sets with the following detection types to determine if an endpoint is connecting from a trusted location:

Detection type	Description
Receives a successful HTTP(S) 200 OK response from a known server	**To use an internal HTTP server:** 1. In the *HTTP(S) server IP addresses* field, specify the IPv4 or IPv6 IP address of the HTTP server. FortiSASE considers the endpoint as satisfying the rule if FortiClient user manually sends an HTTP GET request to specified internal IP address and receive a 200 OK in response. **To use an internal HTTPS server:** 1. In the *HTTP(S) server IP addresses* field, specify the IPv4 or IPv6 IP address of the HTTPS server. 2. Enable *Use HTTPS* and specify *CN/SNI* of the HTTPS server certificate. 3. FortiSASE considers the endpoint to satisfy the rule if the FortiClient user manually sends an HTTPS GET request to the specified internal IP address and receives a server certificate with the specified Server Name Indication (SNI) or Common Name (CN). If you configure multiple HTTP(S) servers, FortiSASE considers the endpoint as satisfying the rule if a successfully query is completed to any configured server.
Connects with a known public IP	In the *Known public (WAN) IP addresses* field, enter the desired IP address. You can configure multiple addresses using the + button. FortiSASE supports configuration of single IP addresses and IP subnets. FortiSASE considers the endpoint as satisfying the rule if its public (WAN) IP address matches the one specified.

Detection type	Description
Is connected to a known DNS server	In the *Known server IP addresses* field, configure at least one IP address for the desired DNS server. You can configure multiple IP addresses using the *+* button. FortiSASE considers the endpoint as satisfying the rule if it is connected to a DNS server that matches the specified configuration.
Make a successful query to a known DNS server	In the *DNS query* field, enter the IP address of the DNS server and hostname to query. FortiSASE considers the endpoint to satisfy the rule if it sends a DNS query to specified DNS server and successfully resolves the hostname to an IP address. To ensure DNS queries are sent, configure the endpoint's DNS server to match the IP address of DNS server specified in *DNS query* field. If multiple DNS servers are configured, FortiSASE considers the rule satisfied if any of the configured DNS servers successfully respond to a query.
Is connected to a known DHCP server	If you enable *Identify servers by IP/MAC addresses*, configure the IP and/or MAC address for the desired DHCP server in the *Known server IP addresses* and *Known MAC addresses* fields, respectively. If configuring *Identify servers by IP/MAC addresses*, the *MAC Address* field is optional. If you enable *Identify servers by DHCP option 224*, configure the DHCP code for the desired DHCP server. If the DHCP server is a FortiGate, you can use the FortiGate serial number as the DHCP code, if desired. Otherwise, the DHCP code can be any string configured in the DHCP server as option 224. You can configure *Identify servers by IP/MAC addresses*, *Identify servers by DHCP option 224*, or both. You can configure multiple IP and MAC addresses and DHCP codes using the *+* button on each tab. FortiSASE considers the endpoint as satisfying the rule if it is connected to a DHCP server that matches the specified configuration.
Connects from a known local subnet	In the *Known subnets* field, enter an IP address range. In the *Known gateway MAC addresses* field, optionally enter the default gateway MAC address. You can configure multiple addresses using *+*. FortiSASE considers the endpoint as satisfying the rule if its Ethernet or wireless IP address is within the range specified and if its default gateway MAC address matches the one specified, if it is configured.
Can ping a known server	In the *Known server IP addresses* field, enter the server IP address. You can configure multiple addresses using *+*. FortiSASE considers the endpoint as satisfying the rule if it can access the server at the specified IP address.

Logic used for multiple rules within a rule set:

- If you configure rules of multiple detection types for a rule set, the endpoint must satisfy all configured rules (AND logic condition) to satisfy the entire rule set.

Logic used for multiple conditions within a rule:

- For most rules, if you configure multiple conditions, then the endpoint needs to satisfy only one of them (OR logic condition) to satisfy the rule.

  An exception to this is when *Connects from a known local subnet* is enabled where both *Known subnets* and *Known gateway MAC addresses* are specified. In this case, only one of the multiple known subnets specified (OR logic condition) and one of the known gateway MAC addresses (AND logic condition) is required is satisfy the rule.

To configure on/off-net settings:

1. In the desired profile, on the *Connection* tab, under *On/off-net Settings*, set *On/off-net detection* to *Enable*. To configure an on-net rule set to prevent autoconnect to the FortiSASE Cloud Security tunnel when endpoints are on-net, do the following:
   a. Set *On/off-net detection* to *Enable*.
   b. From the *On-net rule set* dropdown list, click + to create a new on-net rule set.
   c. In the *Create new rule set* slide-in, select one or more detection types by toggling them.
   d. Configure the required fields as described for each detection type.
   e. Click *OK* to save the on-net rule set.
   f. Click *OK* on the confirm prompt to select the newly created on-net rule set.
   g. Enable *Exempt endpoint from FortiSASE auto-connect when endpoint is on-net*.

   On-net rule sets can also be created, edited, and deleted in *Endpoint management* > *Endpoint profiles* from the *On-net rule sets* tab. From this tab, you can also view which profiles each rule set is used in.
2. Enable *Allow local LAN access* to allow remote users to access their network resources (e.g. printers, file shares etc.) connected in their LAN subnet while staying connected to the FortiSASE Cloud Security tunnel. When enabled, traffic destined for local LAN resources is routed through the endpoint's physical adapter instead of the FortiSASE Cloud Security tunnel. This option can be enabled per endpoint profile and based on endpoint's on-net and off-net status. This feature is available only on FortiSASE instances that are enabled with IPsec remote agent support. See IPsec remote agent support on page 54.

   For FortiClient version 7.2.8 and below, the *Allow local LAN access* option requires at least one *Steering bypass destination* of type *Subnet* to take effect. As a workaround, you can specify a dummy subnet with an unused IP address to fulfill this requirement.

   To enable local LAN access based on endpoint's on-net status, do the following:
   a. Set *On/off-net detection* to *Enable*, and select the desired on-net rule set.
   b. To enable local LAN access for on-net endpoints, enable toggle for *Allow local LAN access when endpoint is on-net*.
   c. To enable local LAN access for off-net endpoints, enable toggle for *Allow local LAN access when endpoint is off-net*.

   Behavior when local LAN subnet conflicts with Steering bypass destinations subnet

   If the endpoint's local LAN subnet matches with a subnet configured under *Steering bypass destinations*, the traffic flow is determined by whether *Allow local LAN access* is enabled or disabled.

Allow local LAN access	Outcome
Disabled	Traffic to LAN resource exits via endpoints physical LAN adapter and does not use the FortiSASE Cloud Security tunnel.
Enabled	LAN resources are not accessible unless you modify the conflicting subnet in *Steering bypass destination*.

Behavior when local LAN subnet conflicts with SPA subnet

If endpoint's local LAN subnet matches a subnet reachable via FortiSASE secure private access (SPA) and *Allow local LAN access* is enabled, the traffic flow depends on the IP address of the resource that endpoint is trying to reach. See the following table:

Condition	Outcome
Resource IP address is not assigned to any device in the endpoint's local LAN network	The endpoints traffic to the resource flows via SPA.
Resource IP address is already assigned to a device in the endpoint's local LAN network	The endpoint's traffic flows to the local LAN device instead of SPA. As a result, the endpoint cannot access the remote resource available via SPA.
Resource has a unique IP address on both the local LAN and SPA network	The endpoint can access the resource via both local LAN and SPA, using their respective unique IP address.

Once option *Allow local LAN access* is enabled, this setting appears on FortiClient endpoints as *Allow local LAN* under Phase 1 configuration of SIA remote access profile.

Considerations

Exempt endpoint from FortiSASE auto-connect when endpoint is on-net is designed to prevent FortiSASE from automatically establishing a secure connection (SIA) when the endpoint is already within the trusted and secured corporate network (i.e. on-net). This is useful for reducing unnecessary SIA bandwidth usage and ensuring traffic is routed directly through corporate firewall when the endpoint is already behind one. However, the exemption mechanism is event-driven and only takes effect after specific system-level or network events occur on the endpoint that include: system login/logout, system power on/off, system restart, network reset, or change in network status.

Thus, if an off-net endpoint that is already connected to FortiSASE via the FortiSASE Cloud Security tunnel transitions to an on-net status without triggering any of the aforementioned events, the autoconnect exemption is not immediately applied. In such cases, the endpoint continues to stay connected to FortiSASE even though it is on-net.

Network lockdown

You can initiate a network lockdown for Windows or macOS endpoints that are off-net. For example, you can initiate a network lockdown for Windows or macOS endpoints that do not satisfy on-net rule sets in the endpoint profile.

Network lockdown feature is available exclusively for FortiSASE instances with IPsec remote agent support enabled. See IPsec remote agent support on page 54.

The settings to configure Network lockdown are visible on FortiSASE portal only if endpoints are running FortiClient version 7.2.5 or later.

The feature is supported only for Windows and macOS endpoints. See Product integration and support.

Network lockdown requires enabling FortiClient 7.2 support to be visible on the FortiSASE portal. Network lockdown exclusively applies to Windows endpoints running a supported FortiClient 7.2 version.

When network lockdown is configured, and FortiSASE determines an endpoint to be off-net based on on-net detection rule sets used in endpoint profile, a timer starts for configurable grace period during which off-net endpoints can access their network without any restrictions. The grace period provides some time for users to attempt connecting to the FortiSASE Cloud Security tunnel or an alternate or personal tunnel to regain its on-net status. Any tunnel connection attempts made during grace period resets grace period for respective endpoint. During grace period, users can retry authenticating to the tunnel, up to a configurable maximum tunnel authentication limit, beyond which, endpoints must be rebooted to refresh its tunnel authentication attempts limits.

If grace period expires and endpoint remains off-net, FortiClient initiates network lockdown and notifies the user via FortiClient system tray icon. In network lockdown, endpoints are restricted from accessing their network except for the following:

- Tunnel access: To allow users connect to the FortiSASE Cloud Security tunnel or alternate or personal tunnel to regain its on-net status.
- Destinations configured under *Exempt destinations*.

FortiClient exits from network lockdown, when the endpoints are determined to be on-net again.

Network lockdown activates only when an endpoint is off-net. Administrators should carefully configure on-net rule sets to avoid unintended behavior. These rules must be designed to allow endpoints to switch from off-net to on-net by connecting to the FortiSASE Cloud Security tunnel or a custom or personal tunnel, enabling them to exit network lockdown.

To configure network lockdown:

1. In the desired profile, on the *Connection* tab, enable *On/off-net detection* and apply a suitable rule set under *On-net rule set*.
2. Enable *Lockdown endpoint when off-net*.
3. For *Grace period*, configure a suitable time period to let endpoints have unrestricted network access for configured duration. The recommended grace period is 120 seconds.
4. If your network has a captive portal that requires user authentication, enable *Exempt captive portals* to allow FortiClient to access the captive portal during a network lockdown. When a captive portal is detected by using network probes after a network change such as connecting to Wi-Fi, FortiClient automatically displays the captive portal using its embedded browser. If SAML authentication is enabled on the captive portal, there is no need to manually specify identity provider (IdP) URLs in the *Exempt Destination* configuration, even during network lockdown, as FortiClient handles this automatically.
5. To have FortiClient handle the captive portal on endpoints, enable the option *Disable native Windows captive portal prompt*. The default setting for this option is disabled, which means that Windows handles

the captive portal on endpoints. This ensures that when network lockdown is enabled, WiFi does not disconnect after agent tunnel disconnects.

6. Under *Exempt destinations*, specify certain trusted destinations that endpoints can access during network lockdown:
   a. To exempt certain IP address destinations, do the following:
      i. Set *Type* as *IP*.
      ii. For the *IP address or subnet* field, specify desired IP or subnet.
      iii. (Optional) Specify destination port under *Exclude by port*.
      iv. (Optional) Specify protocol type under *Protocol*.
      v. Click *OK*.
   b. To exempt certain FQDN destinations, do the following:
      i. Set *Type* as *Domain*.
      ii. In *Domain* field, specify desired FQDN/domain.
      iii. Click *OK*.
7. Specify suitable *Maximum tunnel authentication attempts* limit. To understand the different use cases and implications of configuring various grace period values for network lockdown, see Use cases on page 452.
8. Configure the remaining options on the *Connection* tab as Connection on page 443 describes.

Use cases

Network lockdown can be tailored to meet various customer requirements. Below are common use cases and the recommended settings to achieve the desired outcome.

Use Case	Description	Recommended Configuration
Strict Lockdown	High-security environments requiring remote users to have no internet access until tunnel connection is established.	1. Set *Grace period* to 0. 2. (Optional) Enable *Exempt captive portals* if required. 3. (Optional) Specify critical IPs, subnets, or FQDNs for access during lockdown under *Exempt destinations*.
Traveling Nomads	Users who travel frequently and need extra time for network onboarding tasks (e.g., booting up, connecting to guest Wi-Fi, passing through captive portals, and tunnel authentication).	1. Set *Grace period* to ≥120 seconds. Grace period starts as soon as the device starts boot up, so account for device's boot time. 2. (Optional) Enable *Exempt captive portals* if required. 3. (Optional) Specify critical IPs, subnets, or FQDNs for access during lockdown under *Exempt destinations*.
General Users	General users who do not require strict lockdown but need sufficient time for network connectivity.	1. Set *Grace period* to 120 seconds. 2. (Optional) Enable *Exempt*

Use Case	Description	Recommended Configuration
		captive portals if required. 3. (Optional) Specify critical IPs, subnets, or FQDNs for access during lockdown under *Exempt destinations*.

Considerations

- When FortiSASE configures the grace period on FortiClient endpoints, the countdown timer begins as soon as the device starts its boot-up process, if it was previously powered off. If the device was not shut down, the grace period timer starts immediately upon receiving the grace period configuration from FortiSASE. It is important to select an appropriate time window for the grace period as per your environment.
- If SAML SSO is enabled for endpoints connecting to the FortiSASE Cloud Security tunnel, Alternative tunnel, or Personal tunnel, FortiClient uses its embedded browser for SAML login, eliminating the need to specify IdP URLs under Exempt destinations. However, if *Use external browser as user-agent for SAML login* is enabled, IdP URLs must be manually specified under *Exempt destinations*. To simplify configuration, it is recommended to disable this setting and use FortiClient's embedded browser instead.

Steering bypass destinations

You can configure split tunneling destinations to optimize FortiSASE bandwidth by excluding trusted traffic from flowing through the FortiSASE Cloud Security tunnel. Such traffic is redirected to the endpoint's physical interface, bypassing FortiSASE. For example, you can add high-bandwidth applications like Microsoft Teams or Zoom as split tunneling destinations.

To configure steering bypass destinations:

1. Go to *Endpoint management* > *Endpoint profiles*.
2. In the desired profile, on the *Connection* tab, under *Steering bypass destinations*, click *Create*.
3. Configure the following fields:

Option	Description
Type	Select *Infrastructure*, *FQDN*, *Local Application*, or *Subnet*.
Match	• If you selected *Infrastructure*, select the desired application from the dropdown list. • If you selected *FQDN*, enter or select the desired fully qualified domain name (FQDN). The FQDN resolved IP address is dynamically added to the route table when in use and removed after disconnection. For example, to exclude YouTube from the tunnel, enter youtube.com. When endpoint users use any popular browser such as Chrome, Edge, or Firefox to access youtube.com, this traffic does not go through the tunnel. • If you selected *Local Application*, specify an application using its process name, full path, or the directory where it is installed. When entering the directory, you must end the value with \. You can enter file and directory paths using environment variables, such as %LOCALAPPDATA%, %programfiles%, and %appdata%. Do not use spaces in the tail or head, or add double quotes to full paths with spaces. You can add multiple

Option	Description
	entries by separating them with a semicolon. For example, to exclude Microsoft Teams and Firefox from the tunnel, enter any of the following combinations: • *Application Name*: teams.exe;firefox.exe • *Full Path*: C:\Users\<username>appData\Local\Microsoft\Teams\current\Teams.exe;C:\Program Files\Mozilla Firefox\firefox.exe • *Directory*: C:\Users\<username>appData\Local\Microsoft\Teams\current\;C:\Program Files\Mozilla Firefox\ To find a running application's full path, on the *Details* tab in Task Manager, add the *Image path name* column. • If you selected *Subnet*, enter the desired subnet. The subnet is dynamically added to the route table when in use and removed after disconnection. You can select host groups when using the *Subnet* match type. You must create host groups in *Security* > *Hosts* before they become visible in the *Create Destination* dialog. • For FortiSASE instances with SSL remote agent connectivity: • You can select host groups when using the *Subnet* match type. You must create host groups in *Security* > *Hosts* before they become visible in the *Create Destination* dialog. • You can only configure a *Subnet* or *IP range* steering bypass destination for the Default endpoint profile. All custom endpoint profiles inherit and apply the subnet destinations defined in the Default profile. • For FortiSASE with IPsec remote agent connectivity: • You can only configure the subnet using the input field in the *Create Destination* dialog. • You can configure unique *Subnet* steering bypass destinations for custom profiles and the Default profile.
Apply condition	To apply split tunneling destinations based on an endpoint's on-net or off-net status, enable *On-net Detection* and select an appropriate rule set for FortiSASE to determine the endpoint's status. Then select from: • *On-net*: applies split tunneling destination only to endpoints identified as on-net. • *Off-net*: applies split tunneling destinations only to endpoints identified as off-net. • *Both*: applies split tunneling destinations to endpoints identified as on- or off-net.

4. Click *OK*.
5. Configure the remaining options on the *Connection* tab as Connection on page 443 describes.

Considerations

- Windows FortiClient endpoints support application-based split tunneling or full tunneling with FortiSASE. FortiClient endpoints on other platforms support full tunneling. See Supported FortiClient features.

- FortiSASE does not support wildcard FQDNs when configuring an FQDN split tunneling destination.
- For subnet-based destinations, the *Apply condition* option is only available on FortiSASE instances with IPsec remote agent connectivity.
- Destinations using the *Infrastructure*, *FQDN*, or *Local Application* types can have the *Apply condition* specified on both FortiSASE instances with IPsec or SSL remote agent connectivity.

Custom tunnels

You can modify limited settings for the default FortiSASE Cloud Security tunnel. Additionally, you can configure custom IPsec or SSL tunnel settings, allowing FortiClient users to connect to a custom or alternative gateway. Once configured, the custom tunnel settings appear in *Remote Access* on FortiClient. The custom tunnel settings configured on FortiSASE must be consistent with tunnel settings configured on the gateway to ensure that the tunnel connection establishes successfully between FortiClient and the gateway. Under *FortiSASE Cloud Security tunnel setting* set *Endpoint connects to FortiSASE Cloud Security* to *Manually* to view the options to configure *Custom tunnels* on FortiSASE portal.

In FortiSASE 24.1.c and older versions, *Authenticate with SSO* was previously located in the *Settings* tab.

In FortiSASE 24.2.a and later, you can find *Authenticate with SSO* in the *Connection* tab, in *Custom tunnels*, and by collapsing *Advanced Settings*. Also, in FortiSASE 24.2.a and later, you can edit the default SSL FortiSASE Cloud Security tunnel configuration.

To configure Custom tunnels:

1. In the desired profile, on the *Connection* tab, under *FortiSASE Custom Security tunnel*, set *Endpoint connects to FortiSASE Cloud Security* to *Manually*.
2. Under *Custom tunnels*, click *Create*, and select *SSL tunnel* or *IPsec tunnel* as per your requirement.
3. Enter the *Name* of the tunnel.
4. Do one of the following:

- For an IPsec tunnel, configure the following settings:

Field	Value
Remote gateway	Remote gateway FQDN or IP address.
Authentication method	Select preshared key, smart card certificate, or system store certificate to connect to the IPsec gateway.
Pre-shared key	Pre-shared key for custom IPsec tunnel.
Prompt for username	Display a prompt for the end user to enter their username and password for user authentication.
Run posture check before initiating	Enable this to configure pre-connection posture checks. See Pre-connection posture checks on page 444.
Advanced settings	Enable the toggle for required options to be visible on FortiClient. When you enable *Authenticate with SSO*, FortiClient is enabled with single sign on (SSO) as an authentication option and uses its built-in browser agent by enabling *Use FortiClient built-in browser for SAML* by default. For IPsec instances, you can also customize the *SAML port* using the field provided, which defaults to 443. You can enable *Allow FIDO authentication* if you have configured Entra ID for FIDO2 authentication. See Enable passkeys (FIDO2) for your organization. Enable *Dead peer detection* to reestablish IPsec agent tunnels on idle connections and clean up dead IKE peers, if required, and configure DPD retry count and DPD retry interval accordingly. See IPsec dead peer detection customization on page 471. • *DPD retry count*: Set to the number of DPD retry attempts. Default: 3 • *DPD retry interval*: Set the length of the DPD retry interval. Default: 5 seconds

  Ensure that settings configured on custom or alternative gateways match with the tunnel settings that the FortiSASE Endpoint Management Service applies to FortiClient. See Tunnel Settings on page 457.
- For an SSL tunnel, configure the following settings:

Field	Value
Remote gateway	Remote gateway FQDN or IP address.
Port	SSL tunnel port number.
Require certificate	Enable to use certificate-based user authentication.
Prompt for username	Display a prompt for the end user to enter their username and password for user authentication.

Field	Value
Advanced settings	Enable the toggle for required options to be visible on FortiClient. When you enable *Authenticate with SSO*, FortiClient is enabled with SSO as an authentication option and uses its built-in browser agent by enabling *Use FortiClient built-in browser for SAML* by default. To use an external browser, disable *Use FortiClient built-in browser for SAML*. On FortiClient (macOS), if the *Non-Secure site connections > Warn before connecting to a website over HTTP* option is enabled in Safari and using an external browser for SAML authentication is configured in FortiSASE, tunnel connection may fail. You can enable Allow FIDO authentication if you have configured Entra ID for FIDO2 authentication. See Enable passkeys (FIDO2) for your organization.

5. Configure the remaining options on the *Connection* tab as Connection on page 443 describes.

Considerations

- Currently, the *Allow FIDO authentication* setting only restricts this authentication method for FortiClient MacOS endpoints. For FortiClient Windows endpoints, in addition to enabling this setting, the FIDO2 authentication method must also be configured in the Entra ID Enterprise Application for which SAML-based SSO is configured for in FortiSASE.
- It is strongly recommended to schedule a maintenance window before changing dead peer detection settings.
  - Currently connected endpoints will be disconnected from FortiSASE for a few minutes while the change is applied.

Tunnel Settings

To configure Tunnel settings:

1. In the desired profile, go to the *Connection* tab and navigate to *Tunnel Settings* to configure options based on your specific use case.
2. Enabling a hidden option, *Allow custom tunnel configurations*, grants individual FortiClient users ability to configure, edit, and delete their own personal tunnels directly within FortiClient. Each FortiClient user manages these user-defined tunnels independently, giving users full control over their configurations. This flexibility allows organizations to support both centrally managed tunnel settings such as alternative or custom gateway via FortiSASE, while also enabling individual FortiClient users to configure their own custom tunnel configurations. This option is disabled by default and can be enabled on per endpoint profile basis. Note that the default and custom gateway settings available under *Tunnels available to users*, cannot be deleted by FortiClient users. To view this hidden option in FortiSASE, at least one of following conditions must be met:
   - Set *Endpoint connects to security PoP* to *Manually*.
   - Set *Endpoint connects to security PoP* to *Automatically* and enable toggle for *Show option to disconnect from security PoP*.

- Set *Endpoint connects to security PoP* to *Automatically*, enable *On/off-net detection* to use appropriate *On-net rule set*. Additionally, enable *Exempt endpoint from FortiSASE auto-connect when endpoint is on-net*.

After enabling the option on FortiSASE, remote users can configure personal tunnels on FortiClient under *Remote Access* tab by using the hamburger button to select *Add a new connection*.

Since personal tunnel settings configured through this option are managed solely by FortiClient users and are not controlled by FortiSASE, it is strongly recommended to enable this setting only on endpoint profiles designated for FortiClient endpoints used by administrators. This ensures that only trusted users with administrative privileges can configure personal tunnel connections on FortiClient, reducing the risk of unauthorized tunnel access.

FortiSASE supports authentication using multiple SSO providers using FortiAuthenticator Cloud. See Configuring FortiSASE with FortiAuthenticator Cloud as SAML IdP proxy for Entra ID SSO on page 538.

3. These settings only apply to *Custom tunnels* of type SSL.
   - Enable the option *Accept invalid server certificate* to prevent connection errors on FortiClient due to invalid SSL certificates installed on the on-premise gateway.
   - Additionally, enable *Preferred DTLS Tunnel* for FortiClient to prioritize DTLS (Datagram Transport Layer Security) that uses UDP, over TLS that uses TCP, when establishing an SSL tunnel.
4. The option *Use advanced SAML engine for FortiClient built-in browser* controls how FortiClient handles user authentication when re-connecting to its SSL or IPsec tunnel using SAML SSO-based login. A dropdown menu presents these options:
   - *Web browser*
   - *Electron*
   - *WebView2 and Web browser*
   - *WebView2 and Electron*

   Each of the options have the following dependencies:

Browser type	Dependents
Web browser	• Support pre-logon tunnel
WebView2	• Required to allow for dynamic scaling of customer environments, as needed • Required for FIDO authentication for IPsec tunnel
Electron	• Required for FIDO authentication for SSL tunnel • Will force disabling save password for SSL tunnel • Allows bypassing the credential prompt for SSL users that are Entra ID domain joined • Supports pre-logon tunnel

5. You can configure a custom MTU for an IPsec tunnel. Across varying network environments such as DS-Lite, mobile networks, or those with specific MTU constraints configuring a custom MTU value for IPsec tunnels maybe necessary to ensure optimal performance. By default for a newly created endpoint profile, when an endpoint connects to the IPsec-based FortiSASE Cloud Security tunnel, or an alternative IPsec tunnel, or to the pre-logon tunnel, the default MTU value on the endpoint's virtual tunnel adapter is set to 1280 bytes. To override this default, go to the *IPsec tunnel MTU size* configuration, select *Specify*, and enter a custom value between 576 and 1500 bytes, depending on your network requirements.

   The following FortiClient versions also support this feature:

- Windows endpoints running FortiClient version 7.2.9 or later
- macOS endpoints running FortiClient version 7.2.10 or later

See Product integration and support.

For endpoints belonging to existing endpoint profiles, the default MTU value of 1280 bytes is not applied automatically. Instead, the MTU defaults to the value defined by the endpoint's operating system.

To enforce a consistent MTU configuration across these endpoints:

- Navigate to the corresponding endpoint profile under *Endpoint management* > *Endpoint profiles*.
- Go to the *Connection* tab.
- Under *Tunnel Settings*, locate the *IPsec Tunnel MTU size* setting.
- Select *Specify*, enter 1280, and click *OK* to save the profile.

Configure the remaining options on the *Connection* tab as Connection on page 443 describes.

To enable autoconnect on FortiClient for *Custom tunnels*, set *Endpoint connects to FortiSASE Cloud Security* to *Manually* and under required Custom tunnels, enable *Show 'Auto Connect'* under *Advanced settings* for individual alternative tunnel configurations. If the tunnel connections fails, FortiClient does not automatically connect to the backup FortiSASE Cloud Security tunnel. Endpoint users must then manually connect to the FortiSASE Cloud Security tunnel.

When *Endpoint connects to FortiSASE Cloud Security* is set to *Manually*, you can configure FortiSASE to provide an option to the end user to save their tunnel login password with or without SAML configured under *Custom tunnels* > *<Tunnel>* > *Advanced settings*. When using SAML authentication, feature of saving password relies on persistent sessions being enabled in the identity provider (IdP), discussed as follows:

- Azure
- Okta

If the IdP does not support persistent sessions, FortiClient cannot save the SAML password. The end user must provide the password to the IdP for each tunnel connection attempt.

Protection

To configure the Protection tab:

1. Create a new profile or edit an existing one:
   a. Go to *Endpoint management* > *Endpoint profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *Protection* tab, in *Malware*, configure the following:
   a. Enable *Next Generation AntiVirus*. This feature includes real-time protection against viruses, as well as cloud-based malware detection. Cloud-based malware protection protects endpoints from high risk file

types from external sources such as the internet or network drives by querying FortiGuard to determine whether files are malicious. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient.

i. Enable *Scheduled scanning* and select these settings:
   - For *Schedule type*, select *Monthly* (default), *Weekly*, or *Daily*.
   - For *Scan on*, select *Sunday* (default), or specify a day from *Monday* through *Saturday* when *Weekly* or *1st* (default) through *31st* when *Weekly*.
   - For *Start at*, specify the desired time to start the scan, 7:30 PM (default)
   - For *Scan type*:
     - *Quick*: Runs the rootkit detection engine to detect and remove rootkits. The quick scan only scans executable files, DLLs, and drivers that are currently running for threats.
     - *Full* (default): Runs the rootkit detection engine to detect and remove rootkits, then performs a full system scan of all files, executable files, DLLs, and drivers.

b. Enable *Anti-Ransomware*. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient. Antiransomware protects all content in the selected folders against unauthorized changes. You can click *Create* to add a custom directory. To remove a folder, select it then click the *Delete* button.

3. FortiClient includes a vulnerability scan component to check endpoints for known vulnerabilities and the ability to automatically patch vulnerabilities with the configured minimum severity level. You can view a summary of endpoint vulnerability information on the Dashboard.

On the *Protection* tab, in *Scan for Vulnerabilities*:

a. Enable *Scheduled scanning* and select these settings:

i. For *Schedule type*, select *Weekly* (default), *Daily*, or *Monthly*.

ii. For *Scan on*, select *Sunday* (default), or specify a day from *Monday* through *Saturday* or *1st* through *31st*.

iii. For *Start at*, specify the desired time to start the scan.

b. Enable *Event-based scanning*. This feature automatically scans for vulnerabilities when the following occur:
- Endpoint connects to FortiSASE.
- Endpoint OS is updated.
- Vulnerability signatures are updated.

c. Enable *Trigger vulnerability scan on software change*. This feature automatically scans for vulnerabilities when the following occur:
- New software is installed and detected.
- Existing software is updated.
- New Potentially Unwanted Applications (PUA) are detected.

d. Enable *Automatically patch vulnerabilities*. When enabled, patches are installed automatically when vulnerabilities are detected after vulnerability scans.
- Vulnerabilities requiring endpoint users to manually patch are excluded.
- Endpoints may need to be rebooted to complete the automatic vulnerability patching process.

When this feature is enabled, you must select the Minimum severity level of detected vulnerabilities to automatically patch.
- With *Low* configured, FortiSASE will automatically patch vulnerabilities classified with severity levels from Low to Critical (all vulnerabilities).
- With *Critical* configured, only critical vulnerabilities will be automatically patched.

Automatically patch vulnerabilities when configured with the *Minimum severity level* in an endpoint profile should be sufficient to automatically patch vulnerabilities after performing vulnerability scans.

You can also schedule automatically patching selected individual vulnerabilities on-demand from the *Vulnerability Summary* widget in *Dashboard > Security*. See Drilling down on vulnerabilities on page 60.

4. To exclude specific folders, files or file extensions from Next Generation Antivirus scans (i.e. real time AV protection and on-demand AV scanning), click *Create* under *Exclude specific folders, files and extensions*. Configure the following:

Option	Description
Type	Select *File*, *Folder*, or *Extension*.
Path	Enter the file or folder name or provide its fully qualified path along with file or folder name to exclude from Next Generation Antivirus scans. Wildcards (e.g., *filename or *folder*) can be used to define exclusions. For Windows endpoints leading-only and trailing only wildcards are not supported. E.g., *eicar or, eicar* For macOS endpoints, ensure that you specify full-qualified path down to the innermost folder. E.g., To exclude all files named eicar within a folder, specify its complete path using wildcard: /Users/tamigerber/Documents/test/folder/f1/*eicar* File extensions can also be excluded using the *File* type and using leading-only wildcard. For example, to exclude all .zip files from antivirus scanning, you can set *Type* to *File* and *Path* to *.zip
Value	Specify file extension (e.g., zip, txt) to be excluded.

5. On the *Protection* tab, in *Removable Media Access Control*, configure the following:
   a. For *Default Removable Media Access Control*, select *Allow* (default), *Block*, or *Monitor*. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient.
   b. Enable *Notify Endpoint of Blocks* to display a bubble notification when FortiClient takes action with a removable media device.
   c. In *Access Control Rules*, click *Create* to create a removal media access rule. Configure the following fields. For the class, manufacturer, vendor ID, product ID, and revision, you can find the desired values for the device in one of the following ways:
      - Microsoft Windows Device Manager: select the device and view its properties.
      - USBDeview

Option	Description
Type	Select *Simple* or *Regex* for the rule type. When *Simple* is selected, FortiClient performs case-insensitive matching against classes, manufacturers, vendor IDs, product IDs, and revisions.

Option	Description
	When *Regex* is selected, FortiClient uses Perl Compatible Regular Expressions (PCRE) to perform matching against classes, manufacturers, vendor IDs, product IDs, and revisions.
Action	Configure the action to take with removable media devices connected to the endpoint that match this rule. Available options are: • *Allow*: Allow access to removable media devices connected to the endpoint that match this rule. • *Block*: Block access to removable media devices connected to the endpoint that match this rule.
Class	Enter the device class.
Manufacturer	Enter the device manufacturer.
Vendor ID	Enter the device vendor ID.
Product ID	Enter the device product ID.
Revision	Enter the device revision number.

d. Click *OK*.

Sandbox

To configure the Sandbox tab:

1. Create a new profile or edit an existing one:
   a. Go to *Endpoint management* > *Endpoint profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *Sandbox* tab, configure the following. This feature only works for endpoints where Sandbox Detection was enabled when installing FortiClient. Configure the following options:

Options	Description
Sandbox mode	Select *FortiSASE* to configure connection to FortiSASE Sandbox or *Standalone FortiSandbox* to configure connection to an on-premise standalone FortiSandbox.
IP address/Hostname	For a standalone FortiSandbox, enter the FortiSandbox IP address, FQDN, or hostname.
Authentication	Optional. Enable to configure credentials to communicate with a standalone FortiSandbox.
Username	Optional. Enter the FortiSandbox username. This option is only available for a standalone FortiSandbox.

Options	Description
Password	Optional. Enter the FortiSandbox password. This option is only available for a standalone FortiSandbox.
Region	FortiSASE Sandbox region.
Time Offset	FortiSASE Sandbox time offset.
Wait for FortiSandbox results before allowing file access	Have the endpoint user wait for FortiSandbox scanning results before being allowed access to files. Set the timeout in seconds.
File submission options	
All files executed from removable media	Submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis.
All files executed from mapped network drives	Submit all files executed from mapped network drives.
All web downloads	Submit all web downloads.
All email downloads	Submit all email downloads.
Notification type	Choose one of the following notification levels: • *Lite*: Displays notification balloon only when FortiSandbox detects malware in a submitted file. • *Full*: Displays a popup for every file submission sent to FortiSandbox regardless of the result.
Remediation Actions	
Action	Choose *Quarantine* or *Alert & Notify* for infected files. Whether FortiClient quarantines the file depends on if FortiSandbox reports the file as malicious and the *Sandbox Detection Verdict Level* setting.
Sandbox Detection Verdict Level	Select the desired detection verdict level. For FortiClient to apply the action selected in the *Action* field to an infected file, FortiSandbox must detect the file as this level or higher. For example, if *Action* is configured as *Quarantine* and *FortiSandbox Detection Verdict Level* is configured as *Medium*, FortiClient quarantines all infected files that FortiSandbox detects as Medium or a higher level (High or Malicious). FortiClient does not quarantine files for which FortiSandbox returns a verdict below this level (Low Risk or Clean).
Exceptions	
Exclude Files from Trusted Sources	Exclude files signed by trusted sources from FortiSandbox submission. Following is a list of sources that FortiSandbox trusts: • Microsoft • Fortinet • Mozilla

Options	Description
	• Windows • Google • Skype • Apple • Yahoo! • Intel
Exclude Specified Folders/Files	Click *Create* to exclude specified files/folders from FortiSandbox submission. You can use wildcards to specify file/folder exclusions.

Considerations

- When enabling Sandbox in an endpoint profile, and when using a FortiSASE-managed endpoint running FortiClient (macOS) and Microsoft Defender, you must enable passive mode on Microsoft Defender.
- FortiSASE Sandbox uses the FortiClient Cloud Sandbox service. See the FortiClient Cloud Sandbox (FortiSandbox SaaS) Service Description in the Fortinet Support portal.
  - For each endpoint, FortiClient can send a maximum of 300 files daily to FortiClient Cloud Sandbox (SaaS).
  - If multiple files are submitted around the same time, FortiClient sends one file to FortiClient Cloud Sandbox (SaaS), waits until it receives the verdict for that file, then sends the next file to FortiClient Cloud Sandbox (SaaS).
  - The file size limit is 100 MB.
  - When the daily limit is reached, FortiClient Cloud Sandbox (SaaS) sends a signal to the FortiClient endpoint to stop file submission to save resources on both sides.
- For a FortiSASE instance expecting heavy SMB traffic patterns with its agent remote users, to ensure optimal performance, for endpoint profiles with *Sandbox mode* set to *FortiSASE* (FortiSASE Sandbox is enabled), in *Profile Configuration > Sandbox* ensure the *File submission options > All files executed from mapped network drives* option is disabled.
- FortiSASE Sandbox only checks the following file types:

  7z, arj, bz2, cpl, dll, doc, docm, docx, dot, dotm, dotx, exe, fla, flv, gz, jsfl, mht, mhtml, msi, ocx, odp, odt, pdf, pot, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, ps1, rar, rtf, swc, swf, swz, tar, thmx, xfl, xl, xlam, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, xps, xz, z, zip

ZTNA

Zero trust network access (ZTNA) application gateways and applications are key components in the FortiSASE ZTNA solution for agent-based remote users. A ZTNA application gateway serves as a secure entry point that mediates the connection between remote users and internal ZTNA applications. A ZTNA application represents the actual application or service that remote users attempt to access. A ZTNA application can be any internal web or enterprise application, cloud service, or on-premise resource. A ZTNA application gateway acts as a reverse proxy, ensuring that only authorized and compliant users can access ZTNA applications based on security policies that the organization defines. You can configure a FortiGate to serve as the ZTNA application gateway. See Zero Trust Network Access.

FortiSASE enables administrators to configure and manage ZTNA application gateways and ZTNA application configurations for agent-based remote users in *Security > Traffic > ZTNA > Agent-based*.

Once you configure ZTNA application gateways and applications, you can reference and use them in individual endpoint profiles.

For Windows Entra ID domain-joined endpoints, new instances of FortiSASE support ZTNA automatic login using OAuth configurable in the Microsoft Entra ID Options section.

- This configuration allows Windows users signed in to their workstations, joined to a Microsoft Entra ID domain, to be automatically allowed access to ZTNA-protected TCP resources by using the same login information.
- For instructions for locating the domain name and application ID on the Entra ID portal and end-to-end deployment details for configuring remote Windows endpoints with the FortiClient agent for Windows to automatically login to ZTNA using Entra ID credentials, see ZTNA single sign-on with Entra ID.
- This configuration requires FortiClient 7.4.5 or later.

To configure ZTNA application gateway on FortiSASE:

1. Go to *Security > Traffic > ZTNA > Agent-based*.
2. Select the *Gateways* tab.
3. Click *Create* and enter following details for the ZTNA application gateway:

Field	Value
Name	Enter a unique name for your application gateway
Address	Specify the IP address or FQDN of the FortiGate that is configured to act as the ZTNA application gateway.
Port	Specify the port number on the FortiGate that is designated for ZTNA.

To configure a ZTNA application on FortiSASE:

1. Go to *Security > Traffic > ZTNA > Agent-based*.
2. Select the *Private applications* tab.
3. Click *Create* to configure a new ZTNA application and enter the following details:

Field	Value
Name	Enter unique name for your application.
Type	Select *IP*, *FQDN*, or *Wildcard FQDN*. Additionally, for instances with supported FortiClient versions, select *IP range* or *CIDR*.
IP/FQDN/IP range/CIDR	Based on the *Type* selected, specify the IP address or FQDN of the ZTNA application. Additionally, for instances with supported FortiClient versions, specify the *IP range*, such as *192.168.1.1-192.168.1.100*, or the *CIDR*, such as *192.168.1.0/24*.

Field	Value
Port	Select *Any* or click *Specify* to enter a specific port number. Additionally, for instances with supported FortiClient versions, specify *Port list* to enter a list such as *80*, *443*, *8080* or *Port range* to enter a range such as *1000-2000*.
Application gateway	Click *+* to select the application gateway configured in earlier steps.

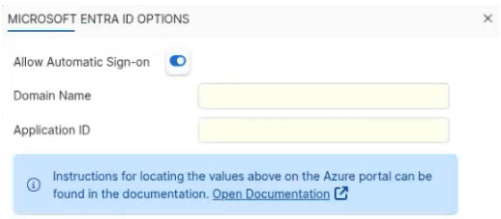
4. Click *OK*.

To use ZTNA application gateway and ZTNA application in endpoint profiles:

1. Create a new profile or edit an existing one:
   a. Go to *Endpoint management > Endpoint profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. Select the *ZTNA* tab.
   a. For *Status*, click *Enable*.
   b. Under *Connection Rules*, click *Create*.
   c. Use the *Agent-based ZTNA application* dropdown to select the ZTNA application.
   d. Enable or disable *Encryption*. By default, encryption is disabled. When encryption is enabled, traffic between FortiClient and ZTNA application gateway (i.e. FortiGate) is always encrypted, even if the original traffic has already been encrypted. When encryption is disabled, traffic between FortiClient and the ZTNA application gateway (i.e. FortiGate) is not encrypted.
   e. The *Browser for SAML authentication* setting allows you to specify how FortiClient performs SAML-based authentication when the endpoint tries to access the ZTNA application. You can configure the setting per ZTNA application and also per ZTNA gateway within each ZTNA application. The two options provided are:
      - *Use FortiClient built-in browser*: endpoint leverages the inbuilt and embedded browser within FortiClient for a seamless in-app authentication experience. This is the default setting.
      - *Use external browser*: redirects the SAML authentication to an external browser, such as Chrome, Firefox, or Edge, installed on the endpoint.
   f. Under *Browser for SAML authentication*, select a gateway and select *Use FortiClient built-in browser* or *Use external browser*.
   g. Click *OK*.

To configure Microsoft Entra ID Options for ZTNA automatic login using OAuth:

1. In the *Microsoft Entra ID Options* section, click *Configure*.
2. In the *Microsoft Entra ID Options* pane, select *Allow Automatic Sign-on* and enter the domain name and application ID.



3. Click *OK*.

   This configuration allows Windows users signed in to their workstations, joined to a Microsoft Entra ID domain, to be automatically allowed access to ZTNA-protected TCP resources by using the same login information.

   For instructions for locating the domain name and application ID on the Entra ID portal and end-to-end deployment details for configuring remote Windows endpoints with the FortiClient agent for Windows to automatically login to ZTNA using Entra ID credentials, see ZTNA single sign-on with Entra ID.

Prerequisites and considerations

Prerequisites

- For ZTNA applications, *IP range* and *CIDR* types, and *Port list* and *Port range* fields are visible in FortiSASE and supported for these versions of FortiClient:
  - FortiClient for Windows 7.2.8 or later
- For Windows Entra ID domain-joined endpoints, FortiSASE supports ZTNA automatic login using OAuth configurable in the Microsoft Entra ID Options section.
  - This section is visible in FortiSASE and supported for these versions of FortiClient:
    - FortiClient for Windows 7.4.5 or later.
    - FortiGate devices acting as ZTNA application gateways must be running FortiOS 7.6.1 or later.
    - This feature requires valid supporting Entra ID configuration.
    - For instructions for locating the domain name and application ID on the Entra ID portal and end-to-end deployment details for configuring remote Windows endpoints with the FortiClient agent for Windows to automatically login to ZTNA using Entra ID credentials, see ZTNA single sign-on with Entra ID.

Considerations

- Endpoint management functionalities, including endpoint profile configuration and some zero trust network access (ZTNA) functionality, may be intermittently inaccessible while the rolling software upgrade for a FortiSASE instance is occurring during the scheduled monthly maintenance window. See Appendix E - Monthly maintenance on page 815.
- FortiSASE supports a maximum of 32000 ZTNA connection rules.
- If the ZTNA application gateway uses SAML for user authentication, FortiClient by default uses system's default browser as an external user agent for SAML authentication FortiClient.
- In some cases, agent-based ZTNA functionality, also known as *ZTNA destination* on FortiClient, can conflict with other applications on managed endpoints. To resolve this conflict on an endpoint profile that has previously had agent-based ZTNA functionality enabled, you can set *Status* to *Disable* in the *ZTNA* tab.

FSSO

FortiSASE supports the FortiClient Single Sign On (SSO) Mobility Agent for FortiClient endpoints. The agent sends up to date authentication information, including IP changes, to FortiAuthenticator. Fortinet Single Sign On (FSSO) is an authentication protocol allowing users to transparently authenticate across Fortinet Fabric devices.

In *Endpoint management > Endpoint profiles* in the *FSSO* tab in an endpoint profile, settings can be configured with the IP address or hostname, port, and pre-shared key fields of FortiAuthenticator.

To configure the FSSO tab:

1. Create a new profile or edit an existing one:
   a. Go to *Endpoint management > Endpoint profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *FSSO* tab, configure the following. This feature only works for Windows and MacOS endpoints where the Single Sign-On Mobility Agent feature was enabled when installing FortiClient. Configure the following options:

Option	Description
FortiClient SSO mobility agent	Select *Enable* to enable the FortiClient SSO mobility agent feature. Default setting is *Disable*.
FortiAuthenticator address or hostname	For a FortiAuthenticator, enter its IP address, FQDN, or hostname. The configured FortiAuthenticator needs to be accessible by the endpoints for this feature to work. Best practices are to have the FortiAuthenticator behind an SPA hub, or to have it accessible through a public IP address.
Port	Enter the FortiAuthenticator TCP port used for listening to FSSO Mobility Agents. Default setting is 8001.
Pre-shared key	Optional. If *Enable Authentication* is configured with a *Secret key* specified on FortiAuthenticator in *Fortinet SSO Methods > General > Fortinet Single Sign-On (FSSO)*, then enter the matching key in this field.

Prerequisites and considerations

Prerequisites

- The FortiClient single sign on mobility agent (FSSOMA) is only supported on Windows and MacOS FortiClient. See Supported FortiClient features.
- The configured FortiAuthenticator needs to be accessible by the endpoints for this feature to work. Best practices are to have the FortiAuthenticator behind an SPA hub, or to have it accessible through a public IP address.

Considerations

FortiAuthenticator SSO Mobility Agent (SSOMA) for Entra ID is only supported for FortiClient 7.2. For details regarding FortiAuthenticator SSOMA for Entra ID see FortiAuthenticator SSOMA for native Microsoft Entra ID joined workstation.

Groups & AD Users

To configure the Groups & AD Users tab:

1. Create a new profile or edit an existing one:
   a. Go to *Endpoint management > Endpoint profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *Groups & AD Users* tab, you can select Active Directory (AD) users, non-AD groups, or AD groups to assign the endpoint profile to.
3. Click *Add* and select *AD Users* or *Groups* as per your requirements:
   - When selecting *AD Users*, a slide-in appears, which allows you to view the domains corresponding to configured AD servers. You can collapse the LDAP domain and select AD users from the list of AD users.
   - When selecting *Groups*, do one of the following:

Group type	Description
AD groups	A slide-in appears that allows you to view the domains corresponding to configured AD servers and select AD groups. To select AD user groups, you can collapse the LDAP domain using the + button and select the required AD groups from a tree view of groups using the toggle.
Non-AD groups	A slide-in appears that allows you to create nested non-AD user groups under *Non-AD Groups* and assign endpoints to the group. To configure a non-AD user group and add endpoints to the newly created non-AD group, do the following: 1. Collapse *Non-AD Groups* using the + button. 2. Select the group under that you want to create a group under and click *Create sub-group*. 3. Enter the *Name* of the group as desired. 4. Select the available non-AD endpoints to add to the group. Click *Add selected*. 5. Click *OK*. 6. Only enable the toggle of the specific group to assign the profile to. 7. Click *OK*.

4. Click *OK*.
5. Repeat step 3 to add more groups and AD users. If you add more groups to the list, the endpoint user must be a part of at least one group for FortiSASE to assign the profile to the endpoint.

6. Click *OK* to save the endpoint profile.
7. To view the endpoints that are assigned to a profile, click the profile and select *View Endpoints* from the toolbar.

Prerequisites and considerations

Prerequisites

Viewing users and groups from an AD server requires configuring an AD connection in *Access & authentication* > *Authentication Sources* > *Domainss*. See Domains on page 580.

Considerations

- The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the AD subdomains if you have already imported the LDAP AD parent domain previously into it.
- When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.
- FortiSASE only supports *Create sub-group* for non-AD groups and local AD groups. FortiSASE does not support this operation for Entra ID groups.
- FortiSASE cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE as well.

FortiClient GUI Settings

To configure the FortiClient GUI Settings tab:

1. Create a new profile or edit an existing one:
   a. Go to *Endpoint management* > *Endpoint profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *FortiClient GUI Settings* tab, configure the following:
   a. Enable or disable *Show option to backup configuration*. This setting is enabled by default. When enabled, users can back up their FortiClient configuration directly from the endpoint from *Settings* > *System* > *Restore a configuration* on FortiClient.
   b. Enable or disable *Allow debug log generation*. This setting is disabled by default which sets the FortiClient *Log Level* to *Info* for associated endpoints. When enabled, the FortiClient *Log Level* is set to *Debug*.
   c. Enable or disable *Show security posture tags*. When enabled, the end user can view the tags applied on their endpoint.

d. Enable or disable *Show notifications for endpoint status, telemetry, and management*. When enabled, the endpoint displays notifications for device status, telemetry, and management events such as when policies are installed, action is taken with a removable media device, etc.
e. Enable or disable *Notify endpoint of tunnel connectivity issues*. When enabled, a notification displays to the end user when FortiClient cannot connect to FortiSASE tunnel.
f. Under *Debugging options*, when you enable *Show option to disconnect from endpoint management*, FortiClient's *Zero Trust Telemetry* tab shows a *Disconnect* option.
   Alternatively you can enable *Require disconnect password* and enter a password. When this option is configured, the endpoint user must enter the password on FortiClient to disconnect from the FortiSASE Management Service. You can use this option as an offline method of deregistering a FortiClient endpoint from the FortiSASE Management Service.
g. Under *Show features on FortiClient*, show only selected FortiClient tabs, including *Remote Access*, *ZTNA Destination*, *Malware Protection*, *Sandbox Detection*, and *Vulnerability Scan* can be toggled individually. Features disabled within an endpoint profile will also be disabled from being shown in FortiClient.
   Also, for the *Default tab* setting, you can change the default tab shown in FortiClient from the *Zero trust telemetry* tab (default selection, shown as a blank entry in the dropdown list) to one of the other enabled features in the dropdown list.

3. Click *OK*.

IPsec dead peer detection customization

For instances supporting IPsec, FortiSASE supports customizing dead peer detection settings applicable to IPsec agent tunnels. Dead peer detection reestablishes IPsec agent tunnels on idle connections and cleans up dead IKE peers if required.



It is strongly recommended to schedule a maintenance window before changing dead peer detection settings.

Currently connected endpoints will be disconnected from FortiSASE for a few minutes while the change is applied.

Security PoPs

For Security PoPs, dead peer detection settings are configurable in *Endpoint management* > *Endpoint profiles* > *Global connection settings*. The behaviors and ideal use cases for available dead peer detection options are provided as follows:

Option	Behavior	Ideal use case
Disable	FortiSASE does not actively generate any DPD messages; instead it will respond to any incoming DPD messages from the other peer of the IPsec tunnel (such as for FortiClient DPD messages).	For highly stable environments where DPD overhead is unwarranted.

Option	Behavior	Ideal use case
On-idle (default)	Trigger DPD when IPsec is idle. Balances connectivity assurance with resource utilization.	For networks with regular traffic intervals.
On-demand	IKE sends DPD messages only when outgoing messages have been transmitted but no incoming ones have been received during the DPD retry interval specified.	For environments where traffic patterns are unpredictable and an immediate response to connectivity issues is critical.

When *Dead peer detection* is enabled, you must specify a *DPD retry count* and a *DPD retry interval*. By default, FortiSASE will use 60-second intervals and wait for three missed attempts before declaring the peer dead and dropping the agent tunnel.

Endpoint profile for agent tunnels

Dead peer detection settings for agent tunnels are configurable through *Advanced settings* within an endpoint profile for the FortiSASE Cloud Security tunnel and any custom tunnels, respectively.

Considerations

- This is a select availability feature. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
- As a best practice, the endpoint profile dead peer detection settings are typically configured to match the corresponding settings configured for Security PoPs.

Pre-logon tunnel

Pre-logon tunnels are typically useful to onboard remote users who have never logged in to their Windows machines, where the user's Windows machines are domain-joined to their organizational Active Directory (AD) environment.

Initial user login to domain-joined Windows machines using user AD credentials requires real-time connectivity to the AD server. You can provide connectivity to the AD server via a tunnel. Using a pre-logon tunnel, upon bootup, Windows machines can self-authenticate and connect to a gateway using their machine certificates. Once Windows machines connect over a tunnel, they can access the AD server. Users can then log in to the Windows machine using their AD credentials. After login to the Windows machine, the pre-logon tunnel connection disconnects. Users then can connect to the FortiSASE Cloud Security tunnel automatically or manually depending on FortiSASE configuration. For subsequent user logins to Windows machines, users can then use their locally cached Windows AD credentials.

For pre-logon tunnel to work, it is assumed that Windows administrators have already prestaged the domain-joined Windows machines with a preconfigured FortiClient installer with the proper supported FortiClient version, along with machine certificates before shipping devices to users.

- There are several options for generating and managing certificates. For an example of creating a CA certificate and Client certificate that can be used client-based authentication for pre-logon tunnels, see Creating certificates with XCA.

> Configuring pre-logon tunnels is available in FortiClient 7.2.0 and later for FortiSASE instances enabled with IPsec or SSL remote agent support. This feature is exclusive to Windows endpoints.
>
> By default, the option to configure a pre-logon tunnel is visible for both existing and new FortiSASE instances enabled with IPsec remote agent support. See IPsec remote agent support on page 54.
>
> However, for existing FortiSASE instances enabled with SSL remote agent support, the option is hidden by default. To enable its visibility on FortiSASE, submit a ticket through FortiCare Support.

Prior to 25.4.b, FortiSASE supported configuring the legacy method of using a customer-managed FortiGate gateway for SSL or IPsec certificate-based authentication. In FortiSASE Feature 25.4.b, this feature is still supported for instances that have an existing pre-logon tunnel configuration prior to this version. After disabling the last endpoint profile with the legacy pre-logon authentication method, the instance will only allow configuration using the new pre-logon authentication method introduced in FortiSASE Feature 25.4.b.

Starting in FortiSASE Feature 25.4.b, a newly configured pre-logon tunnel on an endpoint connects directly to the FortiSASE infrastructure and the configuration workflow has changed. In *Global connection settings*, you can enable *Pre-logon authentication settings for Windows and macOS endpoints*, configure the global pre-logon authentication settings, then enable the feature on individual endpoint profiles.

- The IPsec tunnel settings configured on the endpoint profile will also apply to the pre-logon tunnel.
- You can click *View endpoint profiles with pre-logon authentication enabled* to display a slide-in with the corresponding list of endpoint profiles.

To configure global pre-logon authentication settings on FortiSASE Feature 25.4.b and later:

1. Configure these settings:

Setting	Value
Server certificate	Select the server certificate that FortiSASE presents to endpoint machines. By default, the *FortiSASE Default Certificate* is selected.
CA certificate	Select the CA certificate that issued the endpoint machine certificate. This CA certificate has either been already imported via *System > Certificates > Import > Remote Certificate* (select *Remote CA certificate* type) or can be imported from the dropdown by clicking *+* in the *Import Remote CA Certificate* pane.
Endpoint machine certificate *Common name* and *Issuer* have a logical AND relationship for matching.	
Common name	Select common name matching criteria: • *Any*: Match any common name. • *Plain text*: Match using plain text match patterns, where you can utilize * character as a wildcard. • *Regex*: Match using regex patterns.
Issuer	Select common name matching criteria: • *Any*: Match any common name. • *Plain text*: Match using plain text match patterns, where you can utilize * character as a wildcard. • *Regex*: Match using regex patterns.
Allowed destinations	
+Create Edit Delete	Manage allowed destinations by clicking on *+Create*, *Edit* or *Delete*. When creating new allowed destinations (domains or subnets), you can specify either FQDN or subnet types. You must configure at least one destination, otherwise the following error message appears: *No destinations specified. Traffic will not be able to access any addresses through the Pre-logon tunnel.*

2. Click *Apply*.

To enable pre-logon authentication for an endpoint profile on FortiSASE Feature 25.4.b and later:

1. Go to *Endpoint management > Endpoint profiles*. Select the respective profile and click *Edit*.
2. On the *Connection* tab, configure one of the following:

Endpoint connects to security PoP setting	FortiClient behavior after the user logs in to Windows
Manually	Disconnects from pre-logon gateway. The user can manually log in to the desired tunnel connection from the configured list of tunnels shown

Endpoint connects to security PoP setting	FortiClient behavior after the user logs in to Windows
	under *Tunnels available to users*.
Automatically	Disconnects from pre-logon gateway and uses autoconnect to connect to the FortiSASE Cloud Security tunnel automatically. Switching the setting to *Automatically* will delete any prior configured custom tunnels show under the option *Tunnels available to users*.

3. In *Connection* > *Advanced settings*, enable *Pre-logon Authentication*.
4. Click *OK*.

To configure pre-logon tunnel on FortiSASE Feature 25.4.b or earlier (legacy authentication method):

1. Go to *Endpoint management* > *Endpoint profiles*. Select the respective profile and click *Edit*.
2. On the *Connection* tab, configure one of the following:

Endpoint connects to security PoP setting	FortiClient behavior after the user logs in to Windows
Manually	Disconnects from pre-logon gateway. The user can manually log in to the desired tunnel connection from the configured list of tunnels shown under *Tunnels available to users*.
Automatically	Disconnects from pre-logon gateway and uses autoconnect to connect to the FortiSASE Cloud Security tunnel automatically. Switching the setting to *Automatically* will delete any prior configured custom tunnels show under the option *Tunnels available to users*.

3. Enable toggle *Authenticate endpoint before user logon* to see pre-logon tunnel configuration options.

> If you are in FortiSASE Feature 25.4.b or later and disable *Authenticate endpoint before user logon* for all endpoint profiles, when disabling it for the last profile which had it previously enabled, then you will be prompted to confirm the following by clicking *OK* to proceed or *Cancel* to exit:
>
> *You are turning off the legacy pre-logon authentication method. When you next enable pre-logon authentication on any endpoint profile, the feature will be updated. Do you wish to continue?*

4. Select the *Pre-logon tunnel type* from either *SSL* or *IPsec*.
5. Enter desired FQDN or IP address for *Remote gateway*.
6. The *Port* option allows configuring custom SSL port number for gateway (The option is thus available only if pre-logon tunnel type is set as *SSL*). Default port is 443.
7. The *Endpoint machine certificate* configuration consists of *Common name* and *Issuer* field, used by FortiClient to select proper machine certificate to authenticate itself to gateway. *Common name* and *Issuer* field have a logical AND operation.
8. Enter *Common name*, and *Issuer* using either *Any*, *Plain text* or *Regex* option such that FortiClient is able to select correct Windows machine certificates to authenticate itself to gateway.

9. Click *OK*.

You can configure the FortiGate as a gateway for SSL or IPsec to perform certificate-based authentication. See SSL VPN with certificate authentication and Dialup IPsec with certificate authentication.

Default settings for pre-logon IPsec

If configuring a new pre-logon tunnel on a FortiSASE instance running 26.1.99 Feature, using *IPsec* for *Pre-logon tunnel type*, FortiSASE configures the following IPsec settings on FortiClient endpoint belonging to corresponding endpoint profile. This applies to FortiSASE instances running 25.2.a and later versions:

Tunnel settings	
IKE version	*Version 2*
Mode Config	Enabled
Phase 1	
IKE proposal	*Encryption: AES128, Authentication: SHA256* *Encryption: AES256, Authentication: SHA256*
DH Group	15
Key Life	86400 seconds
Dead Peer Detection	Enabled
NAT Traversal	Enabled
Phase 2	
IKE proposal	*Encryption: AES128, Authentication: SHA256* *Encryption: AES256, Authentication: SHA256*
Key Life	43200 seconds
Replay Detection	Enabled
Perfect Forward Secrecy (PFS)	Enabled
DH Group	15

Thus, ensure to match the default IPsec tunnel settings with the remote gateway's configuration to establish the tunnel between FortiClient and remote gateway.

Legacy settings for pre-logon IPsec tunnel

If a pre-logon tunnel was configured on FortiSASE 25.1.c or earlier, FortiSASE retains the legacy IPsec settings unless one of the following actions occur, after which FortiSASE configures the following IPsec settings using the default IPsec configuration as Default settings for pre-logon IPsec on page 476 describes on FortiClient endpoints belonging to corresponding endpoint profile:

- Removing existing pre-logon tunnel configuration by disabling *Authenticate endpoint before user logon* and saving, then reconfiguring pre-logon tunnel

- Changing *Pre-logon tunnel type* originally configured as *SSL* to *IPsec*.
- Configuring pre-logon tunnel using *Pre-logon tunnel type* as *IPsec* for the first time

Tunnel settings	
IKE version	*Version 1*
Mode	*Aggressive*
Mode Config	Enabled
Phase 1	
IKE proposal	*Encryption: AES128, Authentication: SHA256* *Encryption: AES256, Authentication: SHA256*
DH Group	5
Key Life	86400 seconds
Dead Peer Detection	Enabled
NAT Traversal	Enabled
Phase 2	
IKE proposal	*Encryption: AES128, Authentication: SHA1* *Encryption: AES256, Authentication: SHA1*
Key Life	43200 seconds
Replay Detection	Enabled
Perfect Forward Secrecy (PFS)	Enabled
DH Group	5

To upgrade the legacy IPsec settings that FortiClient uses without removing the existing pre-logon tunnel, contact Fortinet Support to request a change through a new technical support ticket.

Endpoint groups

Endpoint groups are used for grouping endpoints based on your organizational requirements.

- Endpoints can be assigned to endpoint groups using the *Groups & AD Users* tab when creating or editing non-default endpoint profiles. See Groups & AD Users on page 469.
- Endpoints can also be assigned to endpoint groups using custom invitation codes. See Invitation codes on page 478.

To configure the Endpoint groups tab:

1. Go to *Endpoint management* > *Endpoint profiles*. By default, the *Profiles* tab is selected.
2. Click the *Endpoint groups* tab. By default, the *Group directory management* subtab is selected.
3. You can view non-AD groups, or AD groups that endpoints can be assigned to.
4. You can expand a non-AD group and create new sub-groups by clicking *Create sub-group*.

5. To view the endpoints that are already assigned to an endpoint group, hover over the group, and select *View endpoints* from the popup.

Prerequisites and considerations

Prerequisites

Viewing groups from an AD server requires configuring an AD connection in *Access & authentication* > *Authentication Sources* > *Domains*. See Domains on page 580.

Considerations

- The FortiSASE Endpoint Management Service does not support importing AD subdomains if you have already imported the AD parent domain previously into it.
- When the FortiSASE Endpoint Management Service uses AD servers with Endpoint groups, these servers must use public IP addresses or publicly accessible FQDNs when configuring the Server address in the AD connection and may require some configuration or topology changes.
- FortiSASE only supports Create sub-group for non-AD groups and local AD groups. FortiSASE does not support this operation for Entra ID groups.

Invitation codes

After downloading and launching the FortiClient installer, an invitation code must be input into FortiClient to allow managed users to be automatically provisioned to connect to FortiSASE.

FortiSASE supports a default invitation code for your instance. This invitation code is preconfigured in the preconfigured installer for Windows and macOS. With the default invitation code, endpoints are assigned to the default endpoint profile.

FortiSASE supports creating custom invitation codes, which you can use to onboard non-Active Directory (AD) joined endpoints to a designated endpoint group and associated endpoint profile. Once onboarded, endpoints can be manually reassigned.

To create a custom invitation code:

1. Go to *Endpoint management* > *Endpoint profiles* and click on the *Invitation codes* tab.
2. Click *Create*.
3. Configure these fields:

Field	Description	Example Value
Name	Name of the invitation code	UntrustedDevices
Expiring	Enable or disable the ability to configure an expiry date for the invitation code for temporary onboarding access	Enabled
Expiry date	If Expiring is enabled, configure the expiry date	07/31/2025

Field	Description	Example Value
Endpoint group	Onboard endpoints using this custom invitation code with the specified endpoint group and associated endpoint profile	UntrustedDevices

4. Click *OK*.
5. Select the newly created custom invitation code entry in the table. Click *Copy code* to copy the custom invitation code to the clipboard and save for future reference.

Prerequisites and considerations

Prerequisites

- Support for custom invitation codes is a select availability feature in FortiSASE that is not enabled by default on new instances and requires that the instance has been provisioned with Feature version support. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
- The preconfigured FortiClient installers for MacOS and Windows platforms are preconfigured with the *Default* invitation code.
- When using a custom invitation code, administrators must assign the invitation code using endpoint CLI commands and the `-r` or `--register` flag with enterprise mobility management or mobile device management software.
  - FortiClient (Windows) CLI commands
  - FortiClient (macOS) CLI commands

  For an example of assigning an invitation code for iOS endpoints using Intune, see Enterprise mobility management on page 752.

  Refer to the documentation for your enterprise mobility management or mobile device management software for details on running the above endpoint CLI commands in endpoint deployment scripts.

Considerations

- Endpoints onboarded without custom invitation codes are assigned to the *Default* endpoint profile.
- Non-AD endpoints can only belong to one non-AD group and a single endpoint profile at a time
- An Entra ID-joined endpoint is assigned to a non-AD group if the endpoint has been onboarded using a custom invitation code. In this case, the endpoint profile matching is based on the priority of endpoint profiles. However, this same behavior does not apply to AD-joined endpoints.
  - Instead, an AD-joined endpoint will either match a specified AD group in an endpoint profile and be assigned to that profile, or it will be assigned to the *Default* profile. See Groups & AD Users on page 469.

Example: Configuring a custom endpoint profile applied to an AD group

This example demonstrates how to configure a custom endpoint profile applied to an Active Directory (AD) group. It demonstrates how to configure an AD server that allows group matching, configure a custom endpoint

profile to use this AD server to select a specific AD group with which this profile will be applied, and test that the correct profile is applied to an AD user within the selected AD group.

This example makes the following assumptions:

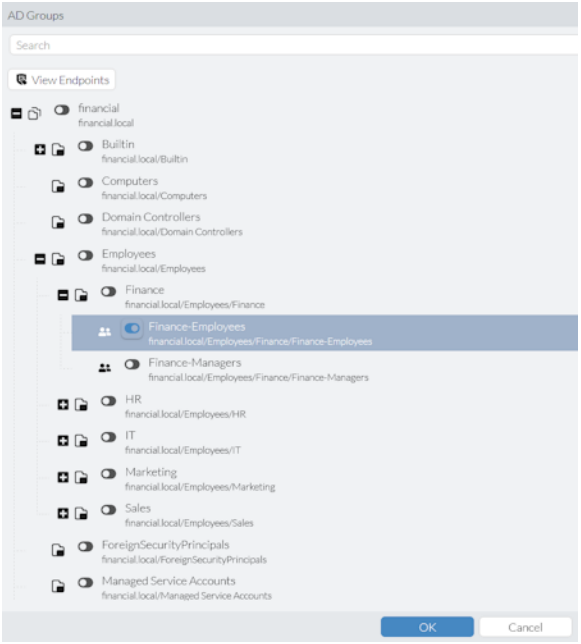
- The AD server has already been configured with AD services, AD users, and AD groups. The AD user johnlocus is a member of the Finance-Employees AD group.
- You have already configured SSO authentication on the SSO provider side and in FortiSASE.
- The endpoint used for testing the AD group matching is on-net, that is, locally on the same network as the AD server and joined to the AD domain.
- Default endpoint profile has been configured with *Authenticate with SSO* disabled to ensure that the configuration uses LDAP for agent authentication.
- You have already configured an AD connection. See To configure an AD connection: on page 580:

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

To configure a custom endpoint profile applied to an AD group:

1. Go to *Endpoint management > Endpoint profiles* and click *Create*. By default, the *Profiles* tab is selected.
2. Add a name to the profile. For this example, use FinanceEmployees.
3. Go to the *FortiClient GUI settings* tab and configure these settings:
   a. Enable *Show security posture tags*.
   b. Enable *Notify endpoint of tunnel connectivity issues*.
4. Go to the *Connection* tab and configure these settings:
   a. For *Endpoint connects to security PoP*, select *Manually*.
   b. Enable *Show option to disconnect from security PoP*.
   c. For *Tunnels available to users*, select *FortiSASE Cloud Security* and click *Edit*. In *Advanced settings*, enable *Authenticate with SSO*.

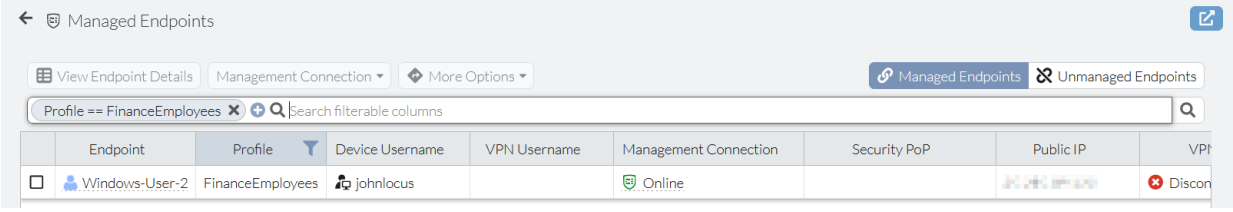
5. Go to the *Groups & AD Users* tab to configure the AD group that the custom endpoint profile will apply to:
   a. Click *Add* > *AD Groups*. The LDAP domain and non-AD groups will be visible in the slide in window.
   b. To select the AD group, collapse the LDAP domain and select the desired AD group.



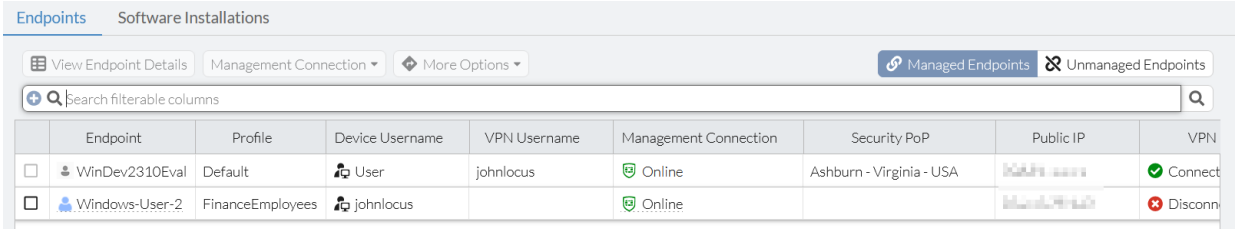
   c. Click *OK*.
   d. Review the selected AD group.
   e. Click *OK*.
   f. Observe that the newly created endpoint profile has an associated AD group and is enabled.

To test the custom endpoint profile is correctly assigned:

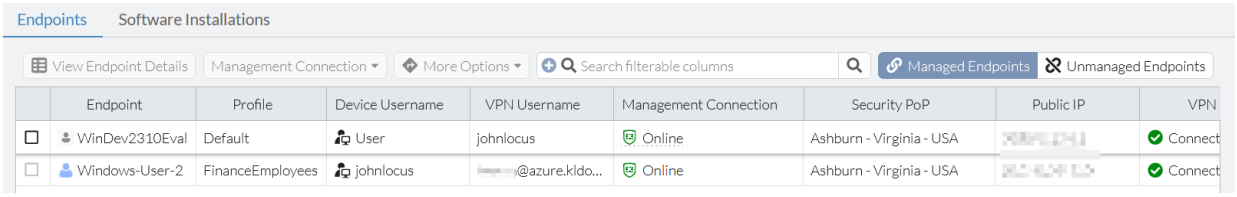
1. Log into the domain-joined endpoint using an AD user.
2. Go to *Endpoint management* > *Endpoint profiles*. By default, the *Profiles* tab is selected. Select the custom endpoint profile just created, and click *View Endpoints*. The *Managed Endpoints* view filtered with endpoints using the selected profile displays.



3. Alternatively, you can view all endpoints with different profiles using *Operations* > *Connectivity* > *Endpoints*.



4. Establish a tunnel connection on the test endpoint using SSO authentication.
5. Go to *Operations* > *Connectivity* > *Endpoints* and observe the test endpoint authenticated username indicates SSO authentication while another endpoint shows an authenticated username indicating LDAP authentication. This demonstrates that SSO authentication and LDAP authentication can be used for authentication of agents with different profiles.



Example: Configuring FSSOMA support with FortiAuthenticator behind SPA hub for Windows domain endpoint

This example demonstrates how to configure the FSSO Mobility Agent settings in an endpoint profile for the scenario when a FortiAuthenticator has a private IP address and is connected behind a FortiGate hub used for Secure Private Access (SPA), and for tracking logins from Windows endpoints joined to a Windows Active Directory domain. In this scenario:

- An on-net endpoint can send authentication information to the FortiAuthenticator directly through the local network.
- An off-net endpoint connected to its FortiSASE tunnel can send authentication information to FortiAuthenticator through SPA.

This example demonstrates how to configure FortiAuthenticator followed by how to configure FortiSASE. It also demonstrates how to verify configuration on a Windows FortiClient endpoint and how to verify proper operation using FortiAuthenticator.

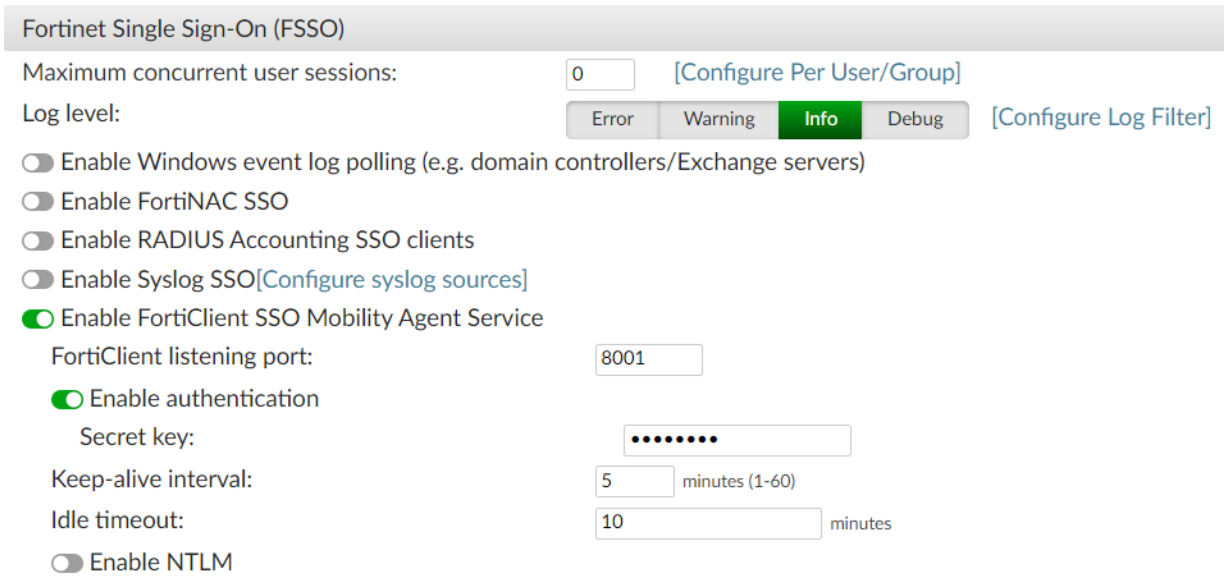
FortiAuthenticator 6.1.1 was used for this example. Refer to the FortiAuthenticator Admin Guide corresponding to your version for version-specific configuration details.

To configure FSSO Mobility Agent support in FortiAuthenticator:

1. To enable FSSO service:
   a. Go to *System* > *Network* > *Interfaces*, and double-click on the port that FortiClient endpoints will connect to, in this example, port1, to edit it.
   b. In *Access Rights*, in *Services*, enable *FortiClient FSSO*.
   c. Click *Save*.
2. To enable FortiClient SSO Mobility Agent Service:
   a. Go to *Fortinet SSO Methods* > *SSO* > *General*.
   b. In *Fortinet Single Sign-On (FSSO)*, click the toggle next to *Enable FortiClient SSO Mobility Agent Service* to enable it.

c. Configure these settings:

Option	Value
FortiClient listening port	8001 (default value)
Enable authentication	Enabled
Secret key	< Enter Pre-shared key value >
Keep-alive interval	5 minutes (default value)
Idle timeout	10 minutes (default value)
Enable NTLM	Disabled



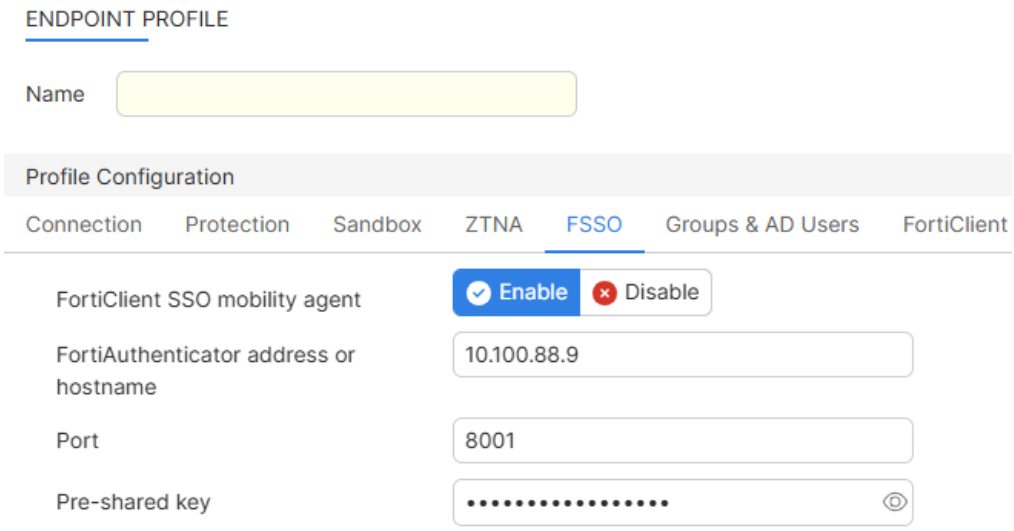
d. Click *OK*.

To configure FSSO Mobility Agent support in FortiSASE:

1. Go to *Endpoint management* > *Endpoint profiles*. By default, the *Profiles* tab is selected.
2. Depending on your requirements, either select the Default profile and click *Edit* or create a new custom profile by clicking *Create*. In this example, the Default profile is edited.
3. Configure settings in the *Connection*, *Protection*, *Sandbox*, *ZTNA*, and *FortiClient GUI settings* tabs based on your requirements.
4. On the *FSSO* tab, configure the following options:

Option	Value
FortiClient SSO mobility agent	*Enable*
FortiAuthenticator address or hostname	For a FortiAuthenticator, enter the FortiSandbox's private IP address. For example, 10.100.88.9
Port	8001

Option	Value
Pre-shared key	Click *Change* and enter the < Pre-shared key value > configured on the FortiAuthenticator.

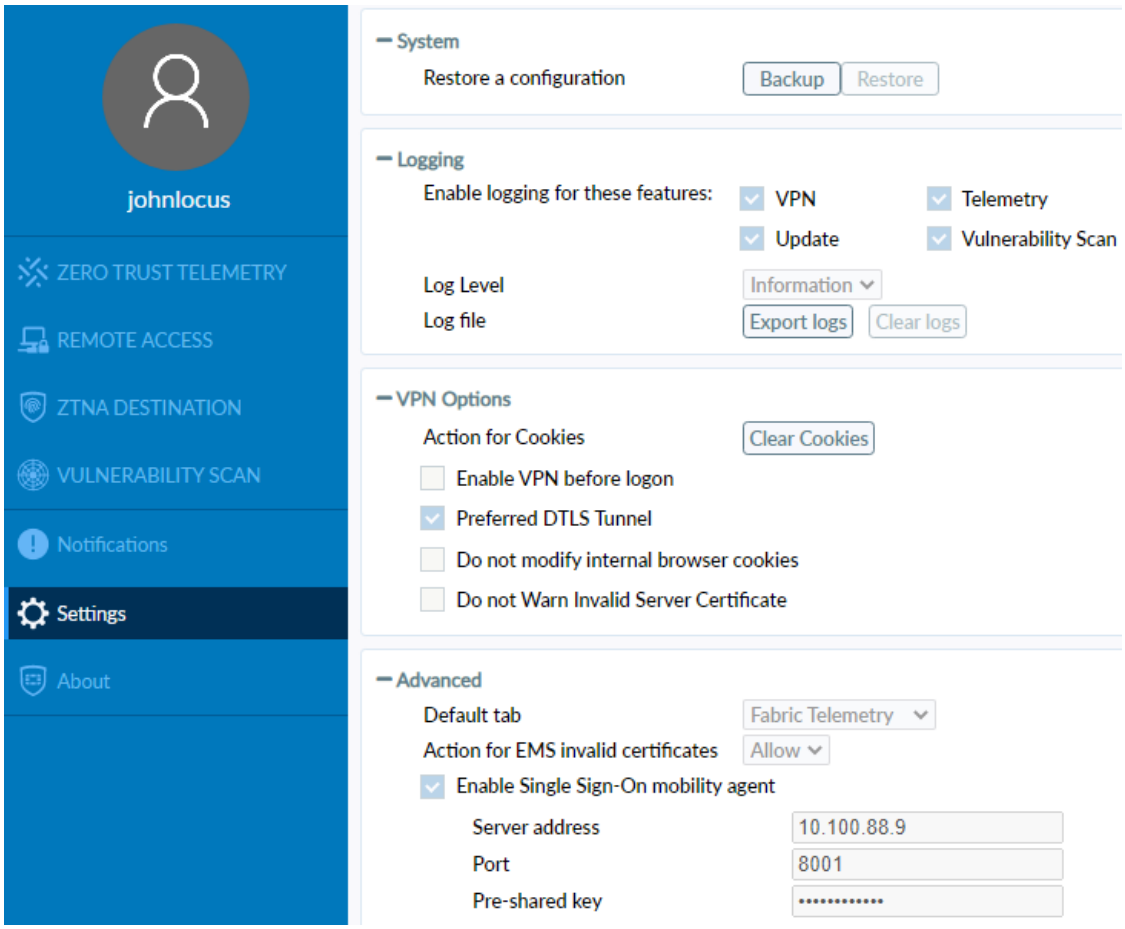


5. Click *OK*.

To verify FSSO Mobility Agent has been configured in a FortiClient endpoint:

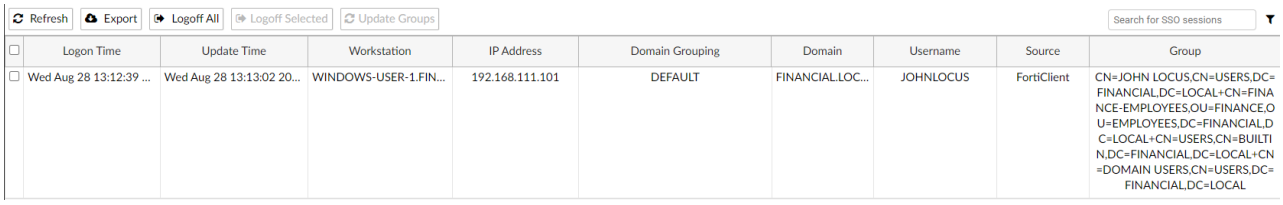
1. Ensure that the FortiClient endpoint has been registered to FortiSASE with a valid invitation code. If the endpoint is not registered, then go to *Zero Trust Telemetry*, in *Register with Zero Trust Fabric*, in the *Enter Server address or Invitation code* field, copy and paste the FortiSASE invitation code.
2. Observe the following notification from the FortiClient system tray: *Configuration update was received from Endpoint Management Server (EMS)*.
3. Go to *Settings* and in the *Advanced* section, observe these settings have been configured:

Option	Value
Enable Single Sign-On mobility agent	*Enable*
Server address	10.100.88.9
Port	8001
Pre-shared key	< Pre-shared key value > (value hidden)



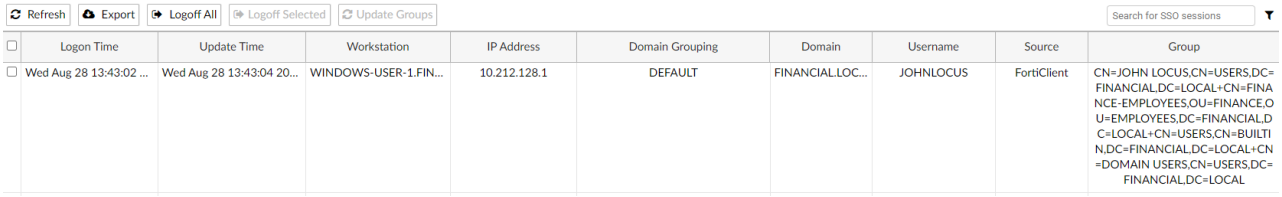
To verify log on events using an on-net FortiClient endpoint:

1. Ensure that the on-net endpoint has been joined to the local Windows Active Directory domain. See Join a Computer to a Domain.
2. Reboot the endpoint or log off and log back into the endpoint to generate a log in event.
3. In FortiAuthenticator, go to *Monitor* > *SSO* > *SSO Sessions* and observe the current SSO sessions. Observe the log on event for your endpoint is visible with the IP address of the endpoint's LAN connection.



To verify log on events using an off-net FortiClient endpoint:

1. Ensure that the off-net endpoint has been connected to the FortiSASE tunnel. This will allow the SSO Mobility Agent to communicate with the FortiAuthenticator via the SPA connection.
2. In FortiAuthenticator, go to *Monitor* > *SSO* > *SSO Sessions* and observe the current SSO sessions. Observe the log on event for your endpoint is visible with the IP address of the endpoint's tunnel connection.



Security posture tags and tagging rules

You can create security posture tags and tagging rules for Windows, macOS, iOS, and Android endpoints based on their OS versions, logged in domains, running processes, and other criteria. FortiSASE uses the security posture tagging rules to dynamically tag endpoints.

The following occurs when using tagging rules with FortiSASE and FortiClient:

1. FortiSASE sends tagging rules to endpoints.
2. FortiClient checks endpoints using the provided rules and sends the results to FortiSASE.
3. FortiSASE receives the results from FortiClient.
4. FortiSASE dynamically tags endpoints using the tag configured for each rule. You can view the dynamically tagged endpoints in *Endpoint management* > *Security posture tags*.

See Tagging rule types on page 489 for descriptions of all tagging rule types.

Configuring security posture tags and tagging rules

You can use tags to build dynamic policies that do not need to be manually reconfigured whenever endpoints statuses change. Security posture tag creation is dependent on the FortiClient version and FortiSASE instance. See Product integration and support for the FortiClient version recommended for your instance.

For information on configuring security posture tags and tagging rules, see the following use cases:

- Use case 1: Create security posture tags and tagging rules separately on page 486
- Use case 2: Create security posture tags and tagging rules simultaneously on page 487

Use case 1: Create security posture tags and tagging rules separately

In existing FortiSASE instances created before 25.4.c, the security posture tags must be manually created in the *Endpoint management* > *Security posture tags* > *Tags* tab or while configuring a tagging rule. The new tag can then be assigned to a security posture tagging rule in the *Endpoint management* > *Security posture tags* > *Tagging rules* tab.

To see endpoints with the security posture tags applied, in the *Endpoint management* > *Security posture tags* > *Tags* tab, select the desired tag and click *View tagged endpoints*.

To configure Security posture tags and tagging rules in existing FortiSASE instances:

1. Go to *Endpoint management* > *Security posture tags*.
2. To create new security posture tags, do the following:
   a. In the *Tags* tab, click *Create*.
   b. Enter a unique *Name* for the tag.
   c. Click *OK*.
3. To create new security posture tagging rules, do the following:
   a. In the *Tagging rules* tab, click *Create*.
   b. In the *Name* field, enter the desired rule set name.
   c. Toggle *Enabled* on or off to enable or disable the rule.
   d. (Optional) In the *Comments* field, enter any desired comments.
   e. Do one of the following:
      - Use the *Security Posture tag* dropdown to select a tag if already created.
      - Click *+* and in the slide in enter desired tag *Name*. The tag name can be same or different as that of rule name. Click *OK*.
   f. To apply the selected tag on endpoints running different OS, enable the toggle and specify security posture tagging rules for each applicable OS: Windows, macOS, iOS and Android.
   g. Configure a rule:
      i. Click *Create* to define a tagging rule type for the selected OS.
      ii. Specify suitable *Rule type*. See Tagging rule types on page 489.
      iii. After selecting a rule type and configuring its required options, click *OK* to save the rule type.
      iv. To add additional security posture tagging rules for the same OS, repeat steps i-iii.
      v. To define an expression in the *Logic* field, consider the following:
         - By default, FortiSASE applies either AND or OR logic based on security posture tagging rule type configured for each OS. For AND logic, the tag is assigned only when all tagging rules for the respective OS are satisfied. For OR logic, the tag is assigned when at least one of the configured rules is satisfied for respective OS.
         - You can override the default behavior by defining a custom logic expression using a combination of AND, OR, and parentheses ( ) operators to group conditions. This is achieved by referencing the corresponding Rule IDs along with desired logical operators in the *Logic* field. It is recommended to configure all required rule types for each operating system before modifying the default logic. Once all rule types are defined, then you may use their corresponding Rule IDs to specify your custom logic expression in the Logic field.
      vi. Click *OK* to save the security posture tag and tagging rule.

Use case 2: Create security posture tags and tagging rules simultaneously

For new FortiSASE instances created after 25.4.c, security posture tags and tagging rules must be created simultaneously in the *Endpoint management* > *Security posture tags* > *Tagging rules* tab. After configuring a security posture tagging rule, a matching security posture tag will be created and will appear on any endpoints matching the tagging rule.

To see endpoints with the security posture tags applied, in the *Endpoint management > Security posture tags > Tagging rules* tab, select the tagging rule with the same name as the desired tag and click *View tagged endpoints*.

The features described in this use case require FortiClient 7.4.5 or later.

To configure Security posture tags and tagging rules in new FortiSASE instances:

1. Go to *Endpoint management > Security posture tags*.
2. Create a new security posture tagging rule:
   a. In the *Tagging rules* tab, click *Create*.
   b. In the *Name* field, enter the desired rule set name.
   c. Toggle *Enabled* on or off to enable or disable the rule.
   d. (Optional) In the *Comments* field, enter any desired comments.
   e. In the *User notification message*, enter a message.
   f. To apply the selected tag on endpoints running different OS, enable the toggle and specify security posture tagging rules for each applicable OS: Windows, macOS, iOS and Android.
   g. Configure a rule:
      i. Click *Create* to define a tagging rule type for the selected OS.
      ii. Specify suitable *Rule type*. See Tagging rule types on page 489.
      iii. After selecting a rule type and configuring its required options, click *OK* to save the rule type.
      iv. To add additional security posture tagging rules for the same OS, repeat steps i-iii.
      v. To define an expression in the *Logic* field, consider the following:
         - By default, FortiSASE applies either AND or OR logic based on security posture tagging rule type configured for each OS. For AND logic, the tag is assigned only when all tagging rules for the respective OS are satisfied. For OR logic, the tag is assigned when at least one of the configured rules is satisfied for respective OS.
         - You can override the default behavior by defining a custom logic expression using a combination of AND, OR, and parentheses ( ) operators to group conditions. This is achieved by referencing the corresponding Rule IDs along with desired logical operators in the *Logic* field. It is recommended to configure all required rule types for each operating system before modifying the default logic. Once all rule types are defined, then you may use their corresponding Rule IDs to specify your custom logic expression in the Logic field.
      vi. Click *OK* to save the security posture tagging rule. A security posture tag with the same name will be created and applied to any endpoints matching the rule criteria.
3. Review that the security posture tag has been configured and applied:
   - In FortiClient EMS, go to *Security Posture Tags > Tags*.
   - On a matching endpoint, review the FortiClient *Security Posture Tags*.
   - In FortiOS, go to *Policy & Objects > ZTNA > Security Posture Tags*.

Rule logic example

The following provides an example to assign a specific tag to Windows endpoints when any of the following conditions are true:

- Windows Firewall is turned off (Rule ID 1)
- Antivirus (AV) is not running (Rule ID 2)
- AV signature definitions are not up to date (Rule ID 3)

In this case, you would create three individual tagging rule sets, each evaluating one condition. Then, in the *Logic* field, enter `1 or 2 or 3`.

This ensures the tag is applied if any one of the conditions is met.

For demonstrations of various configuration options for implementing FortiSASE endpoint management features, such as custom endpoint profiles, tunnel autoconnect, split tunnel, vulnerability scan, zero trust network access (ZTNA), and more, see the FortiSASE Endpoint Management Deployment Guide.

Considerations

- This feature does not apply for proxy mode users. See Proxy agentless mode on page 15.
- Using security posture tags only for private access policies is strongly recommended. See Configuring security posture tags in private access policies on page 131.
- Using security posture tags for Secure Internet Access policies is recommended to control granular application access based on security posture. With this usage, it is recommended that an allow-all policy remains in place to allow general internet traffic for all users.

Tagging rule types

The following table describes tagging rule types and the operating systems (OS) that they are available for. For all rule types, you can configure multiple conditions using the + button.

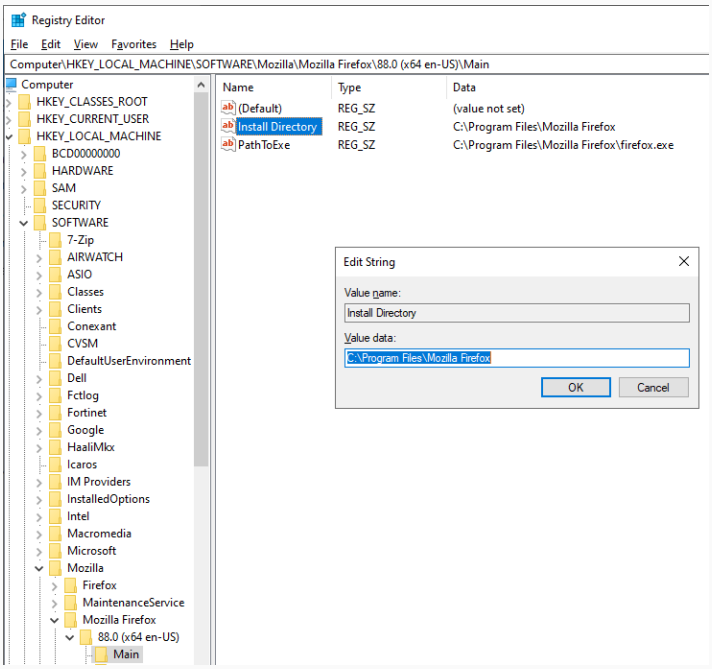
Rule type	OS	Description
User in AD Group	• Windows • macOS	From the *User in AD Group* dropdown list, select the desired Active Directory (AD) group that users should be members of. You can also use *Negate* for the rule to require that the user not be a part of the selected AD group. Viewing users and groups from an AD server requires an LDAP server configuration. The endpoint must satisfy all configured conditions to satisfy this rule. For information related to FortiClient (macOS), see Considerations on page 495.

Rule type	OS	Description
AntiVirus	• Windows • macOS	From the *AntiVirus* dropdown list, select the desired conditions. You can require that an endpoint have antivirus (AV) software installed and running and that the AV signature is up-to-date. You can also use the *Negate* option for the rule to require that the endpoint does not have AV software installed or running or that the AV signature is not up-to-date. This rule applies for FortiClient AV. For Windows endpoints, this rule type also applies for third-party AV software that registers to the Windows Security Center. The third-party software notifies the Windows Security Center of the status of its signatures. FortiClient queries the Windows Security Center to determine what third-party AV software is installed and if the software reports signatures as up-to-date. • For Windows, this feature supports third-party AV applications. • For Windows Server and macOS this feature can only check if FortiClient AV protection is enabled and does not recognize third-party AV applications. The endpoint must satisfy all configured conditions to satisfy this rule.
Certificate	• Windows • macOS	In the *Subject CN* and *Issuer CN* fields, enter the certificate subject and issuer. When using FortiClient 7.2, *Subject CN* supports simple, regular expression, and wildcard matching as selected in the *Subject Match* dropdown list. • *Simple*: perform case-insensitive matching against the *Subject* field. • *Regex*: use Perl Compatible Regular Expressions to perform matching against the *Subject* field. • *Wildcard*: use **?*** wildcards. **?** matches any character once. For example, the pattern **123???** matches **123abc** but not **123a** or **123abcdef**. * matches zero or more characters. For example, if the subject CN contains a username, user ID, and department: Subject CN: **David-200999.Marketing.fortiClient.fortinet.local** • David is the username. • 200999 is the user ID. • Marketing is the department. Then the regular expression to use for *Regex* subject matching is as follows:

Rule type	OS	Description
		\b\w+\b\-\d{6}\.\w+\.fortiClient\.fortinet\.local For example, if the subject CN contains the office location, device owner ID, and host asset number: Subject CN: **SEA-200998-Desktop1.fortinet.local** • SEA is the office location. • 200998 is the device owner ID. • Desktop1 is the host asset number. Then the regular expression to use for *Regex* subject matching is as follows: **SEA\-\d{6}\-Des\w{4}\d(\..+)+** *Issue CN* does not support case-insensitivity, regex, or wildcards. Therefore, you must enter the desired value exactly as on the installed certificate. You can use *Negate* to indicate that the rule requires that a certain certificate is not present for the endpoint. FortiClient checks certificates in the current user personal store and local computer personal store. It does not check in trusted root or other stores. The endpoint must satisfy all conditions to satisfy this rule. For example, if the rule is configured to require certificate A, certificate B, and not certificate C, then the endpoint must have both certificates A and B and not certificate C.
Common Vulnerabilities and exposures	• Windows • macOS	In the CVE- field, enter the common vulnerabilities and exposures (CVE) ID in the format CVE-YYYY-NNNN (or more N digits). For example, you could enter CVE-2020-26950. You can also use the *Negate* toggle to indicate that the rule requires that the specified CVE is not present on the endpoint. If multiple CVE is specified FortiSASE considers the endpoint as satisfying the rule if it satisfies even one of CVEs.
CrowdStrike ZTA score	• Windows	For new instances, the CrowdStrike Falcon sensor generates a CrowdStrike ZTA score that reflects the security posture of an endpoint. The CrowdStrike ZTA score rule type is supported with FortiClient 7.4.5 or later. Use the slider to specify a CrowdStrike ZTA score (default: 60). Select the desired condition relative to that ZTA score to check if the rule is satisfied. You can also use the Negate toggle to indicate the rule requires the inverse of the condition specified relative to the ZTA score. You can add an additional CrowdStrike ZTA score to allow a maximum of two scores with associated conditions to allow checking within a range of scores for the rule to be satisfied.
Domain	• Windows	In the *Domain* field, enter a domain name.

Rule type	OS	Description
	• macOS	You can use *Negate* for rules to require that endpoint must not belong to specified domain. Click + to specify additional domains. If you specify multiple domains, FortiSASE considers the endpoint as satisfying the rule if it belongs to any specified domain. For information related to FortiClient (macOS), see Considerations on page 495.
EMS Management	• Windows • macOS • iOS • Android	FortiSASE considers the endpoint as satisfying the rule if the endpoint has FortiClient installed and Telemetry is connected.
File	• Windows • macOS	In the *File* field, enter the file path. You can also use *Negate* to indicate that the rule requires that a certain file is not present on the endpoint. The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require file A, file B, and NOT file C, then the endpoint must have both files A and B and not file C.
FortiClient Version	• Windows • macOS • iOS • Android	In the *FortiClient Version* field, enter the desired FortiClient version. You can use comparators to configure the rule to apply to endpoints with a range of FortiClient versions. You can use *Negate* for rules to require that the endpoint must not have a specified FortiClient version installed. Click + to specify additional FortiClient versions. If you specify multiple FortiClient versions, FortiSASE considers the endpoint as satisfying the rule if it has at least one specified FortiClient version installed.
IP Range	• Windows • macOS • iOS • Android	In the *IP Range* field, enter the IP address, IP address range, or IP address with subnet. If multiple IP ranges and/or addresses are configured, FortiSASE considers the endpoint as satisfying the rule if its IP address matches one of the configured ranges or addresses.
On-Net status	• Windows • macOS • iOS • Android	You must enable *On-net detection* and specify an *On-net rule set* under respective endpoint profiles to tag the endpoint with On-Net status. See On/off-net Settings on page 447. You can also use the *Negate* option to indicate that the rule requires that the endpoint is Off-Net.
Operating System Version	• Windows • macOS • iOS • Android	From the *Operating System Version* field, select the OS version. If the rule is configured for multiple OS versions, FortiSASE considers the endpoint as satisfying the rule if it has one of the configured OS versions installed.

Rule type	OS	Description
		The following option is available for Windows: • *Enable latest update check*: FortiSASE checks if Windows OS updates were recently installed.
Security Status	• iOS • Android	Select out of the following options: • *Jail-broken / Rooted-device*: Devices where software restrictions that the manufacturer or operating system provider imposes on devices have been removed. • *Passcode Enabled*: Devices with screen lock enabled. • *Biometrics Protected*: Devices with touch or face ID enabled. You can also use the *Negate* option for rules to require that endpoints must not have a certain security status option enabled. Click *+* to specify additional security status options. If multiple security status options are specified, FortiSASE considers endpoint as satisfying the rule if it satisfies all of specified security status options.
Registry Key	• Windows	In the *Key* field, enter the registry path or value name. End the path with \ to indicate a registry path, or without \ to indicate a registry value name. You can also use the *Negate* option to indicate that the rule requires that a certain registry path or value name is not present on the endpoint. This rule does not support using the value data. For example, the following shows a system where Firefox is installed. In this example, the registry path is `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\88.0 (x64 en-US)\Main`. The value name is `Install Directory`, and the value data is `C:\Program Files\Mozilla Firefox`. You can configure a registry key rule to match `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\88.0 (x64 en-US)\Main` as the path or `Install Directory` as the registry value name, but you cannot configure a rule to match `C:\Program Files\Mozilla Firefox`. Do not use square brackets when configuring this rule type.

Rule type	OS	Description
		 The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require registry key A, registry key B, and NOT registry key C, then the endpoint must have both registry keys A and B and not registry key C.
Running Process	• Windows • macOS	In the *Process Name* field, enter the process name. You can also use the *Negate* option to indicate that the rule requires that a certain process is not running on the endpoint. The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require process A, process B, and NOT process C, then the endpoint must have both processes A and B running and process C not running.
Sandbox	• Windows • macOS	From the *Sandbox Detection* dropdown list, select the desired condition. You can require that Sandbox detected malware on the endpoint in the last seven days. You can also use the *Negate* option for the rule to require that Sandbox did not detect malware on the endpoint in the last seven days.
User Identity	• Windows • macOS • iOS • Android	Under *User Identity*, select the following: • *User Specified*: endpoint user manually entered their personal information in FortiClient. • *Social Network Login*: endpoint user provided their personal information by logging in to their Google, LinkedIn, or Salesforce account in FortiClient. You can further select one of the following: • *All Accounts*: all endpoints where the user logged in to the specified social network account type.

Rule type	OS	Description
		• *Specified*: enter a specific Google, LinkedIn, or Salesforce account. For example, you can enter joanexample@gmail.com to configure the rule to apply specifically to only that Google account. You can specify multiple social network accounts. FortiSASE considers the endpoint as satisfying the rule if it satisfies one of the conditions. You can also use *Negate* for the rule to require that the endpoint user has not manually entered user details or logged in to a social network account to allow FortiClient to obtain user details. FortiClient (iOS) does not support social network login with LinkedIn or Salesforce. FortiClient (Android) does not support social network login with Salesforce.
Vulnerable devices	• Windows • macOS	Specify the desired vulnerability severity range using one or more of the following levels: *Any*, *Medium*, *High*, or *Critical*. When you select multiple severity levels, FortiSASE considers the endpoint compliant if it has a vulnerability matching any of the selected levels or higher. You can refine the rule by using *With* or *Without*: • *With*: requires that the endpoint has at least one vulnerability of the specified severity or higher. • *Without*: ensures that the endpoint does not have any vulnerabilities of the specified severity or higher.
Windows Security	• Windows	From the *Windows Security* dropdown list, select the desired conditions. You can require that an endpoint have Windows Defender, BitLocker Disk Encryption, Exploit Guard, Application Guard, and/or Windows Firewall enabled. You can use *Negate* for the rule to require that the endpoint have Windows Defender, BitLocker Disk Encryption, Exploit Guard, Application Guard, and/or Windows firewall disabled. The endpoint must satisfy all configured conditions to satisfy this rule.

Considerations

- For certain posture tagging rule types such as the Running Process rule type all defined conditions within a single rule must be satisfied for the rule to evaluate as true. However, there may be cases where you want the same tag to be applied to endpoints that meet different conditions.
  - For Example, suppose you want to tag endpoints that are running either Process A or Process B with the tag "RP". There are two ways to achieve this:
    - Use OR logic under the *Logic* option: Create two separate rules, one that checks for Process A and another for Process B and then combine them using OR logic by referencing their Rule IDs (i.e., 1

OR 2) under Logic field. This ensures the "RP" tag is applied if either process is running.
    - Create two separate tagging rule sets: Define two independent tagging rules, one that applies the "RP" tag to endpoints running Process A, and another that applies the same "RP" tag to endpoints running Process B.
  - Both methods result in the "RP" tag being applied to any endpoint running either Process A or Process B. For more information, see Security posture tags and tagging rules on page 486.
- For FortiClient (macOS), the *User in AD group* and *Domain* rule types are only supported with an AD server on-premise domain.
- For the *User in AD group* and *Domain* rule types, FortiClient (macOS) 7.4.5 or later does not support native Entra ID integration with FortiSASE. For the integration to work, macOS endpoints must be managed by Intune or JAMF and enrolled to company portal using Entra ID.

Endpoint management settings

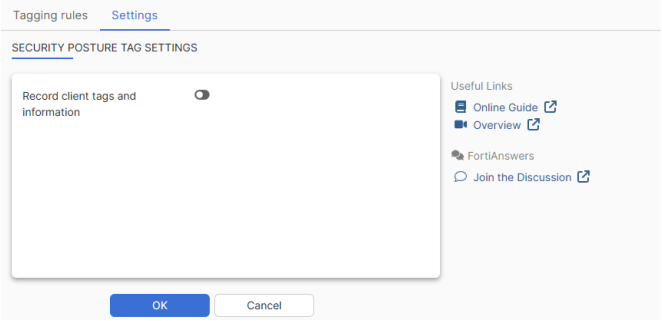
The *Endpoint Management > Security posture tags > Settings* tab allows you to configure features related to security posture tags in your endpoint management system.

In the event of FortiClient EMS becoming unreachable due to network issues or service failure, FortiSASE can learn security posture tags directly from FortiClient when using ZTNA application gateway tag sharing. This ensures a continuance of service and use of ZTNA-dependent policies.

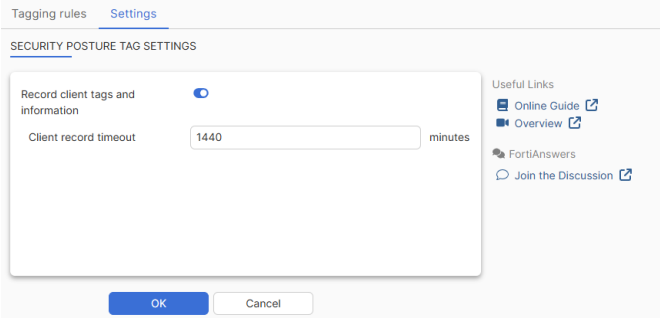
By enabling *Record client tags and information*, the security posture tag timeout value can be defined in FortiSASE. This will allow FortiSASE and FortiGates to learn ZTNA records directly from FortiClient.

To enable direct security posture tag access by the FortiGate:

1. Go to *Endpoint management > Security posture tags*.
2. Select the *Settings* tab.



3. Enable *Record client tags and information*.



4. Enter the *Client record timeout* value in minutes.
5. Click *OK*.
   Security posture tag information can be received directly from FortiClient.

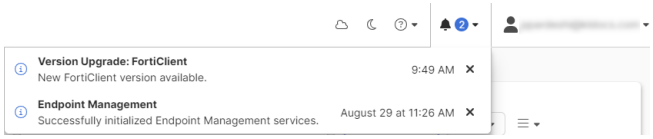
Prerequisites

- This feature is available for new FortiSASE instances created after 25.4.c. It requires FortiClient 7.4.6 and later.
- FortiGates must be on FortiOS 7.4.2 or later.
- This feature is available for FortiGate ZTNA proxy policies with security posture tags enabled. IPsec tunnel Phase 1 interface and firewall policies are not currently supported.

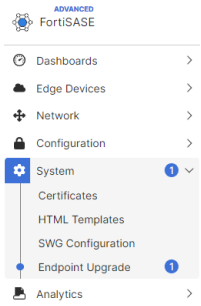
Endpoint upgrade

Endpoint upgrade rules allow you to immediately deploy or schedule rollout of the latest supported and recommended FortiClient version. This feature only supports deploying the most recent supported and recommended FortiClient version to endpoints. If you do not configure an endpoint upgrade rule, FortiClient versions are no longer automatically upgraded.

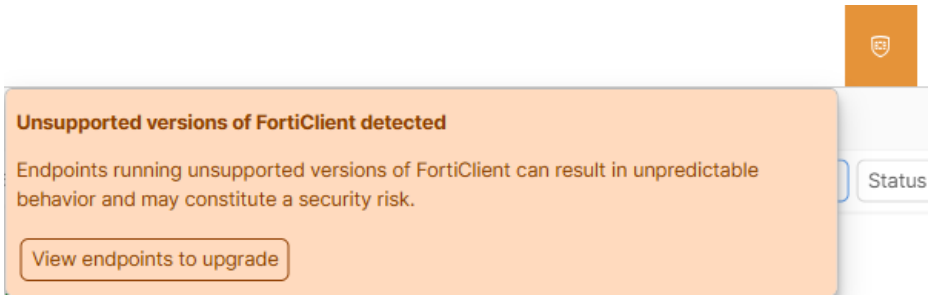
When a new and recommended FortiClient version becomes available, the FortiSASE portal displays a notification in the bell icon on the toolbar, indicating a new FortiClient version is available, with the message: *Version Upgrade: FortiClient, New FortiClient version available*.



Additionally, a numerical notification appears in the sidebar in *Endpoint management > Endpoint upgrade*.



FortiSASE automatically detects if any endpoints are running an older unsupported FortiClient version and displays following notification message via the FortiClient icon in the toolbar: *Unsupported version of FortiClient detected*. Click *View endpoints to upgrade* to see list of endpoints running unsupported FortiClient versions.



To view the current FortiClient version on all endpoints, go to *Operations* > *Connectivity* > *Managed Endpoints* and view the *FortiClient Version* column.



To schedule a FortiClient upgrade using an endpoint upgrade rule:

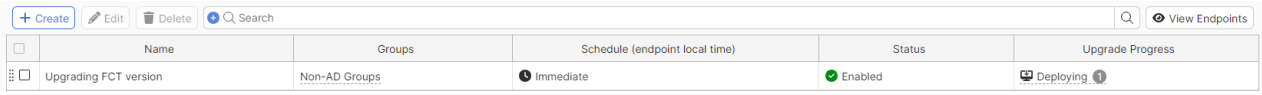
1. Go to *Endpoint management* > *Endpoint upgrade*.
2. Click *Create*.
3. Enter the desired *Name*.
4. For *Schedule time*, choose one of the following options:
   - *Immediate*: recommended and supported FortiClient version begins installing on endpoints immediately.
   - *Scheduled (endpoint local time)*: recommended and supported FortiClient version begins installation at the configured scheduled time.

     Use the clock icon to select a suitable time. The selected time is based on the endpoint local time zone. If the endpoint clock is past the selected time, the FortiClient installation begins the next day at the selected time.
5. Under *Groups*, click *Add* to specify the groups (Active Directory (AD) or non-AD groups) containing endpoints to which the upgrade rule applies. If you do not select a group, no endpoints are upgraded. FortiSASE can only assign an endpoint upgrade rule to a computer/device group or computer/device object. FortiSASE cannot apply an endpoint upgrade rule to a user group or user object.

6. Depending on your requirements, enable or disable *Allow automatic device reboot when users are not logged in*.

   This setting applies only to Windows endpoints.

7. Set *Status* to *Enable*.
8. Click *OK* to save the endpoint upgrade rule.
9. In *Endpoint management* > *Endpoint upgrade*, the *Upgrade Progress* column shows *Deploying* for immediate installations or *Scheduled* for scheduled installations.



10. Depending on the configured *Schedule time (Immediate or Schedule)*, the following actions occur on FortiClient endpoints in the order below:

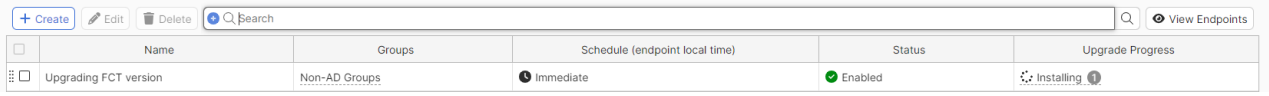
Immediate	Schedule (endpoint local time)
Begins installing recommended FortiClient version on endpoints immediately.	FortiClient's *setting utility* shows endpoint with a notification about new FortiClient version. Upon selecting the notification, it shows three options below to begin FortiClient download and installation: • *(default) Suggested install time*: Begins FortiClient installation at configured *Schedule time*. • *Select a time*: Users can postpone their FortiClient installation to begin at a different time. • *Install now*: Begins FortiClient installation immediately Users can also manually open FortiClient setting utility from their system tray to view the options above.
Post FortiClient installation, for endpoints running Windows OS, FortiClient settings utility prompts users to choose one of the following options to complete the installation: • *Reboot now* • *(default) Remind in 10 mins and reboot automatically in 15 mins* to complete installation. For endpoints running macOS, no prompt is presented and a reboot is not required to complete FortiClient installation.	

FortiClient deployment status

FortiClient deployment undergoes various stages such as *Scheduled*, *Deploying*, *Installing*, *Pending*, *Finished*, and so on. Monitoring these stages in real-time assists FortiSASE administrators to track the progress of their deployments.

To monitor real-time FortiClient deployment status:

1. Go to *Endpoint management* > *Endpoint upgrades*.
2. View the *Upgrade Progress* column to see current deployment stage of each endpoint upgrade rule.



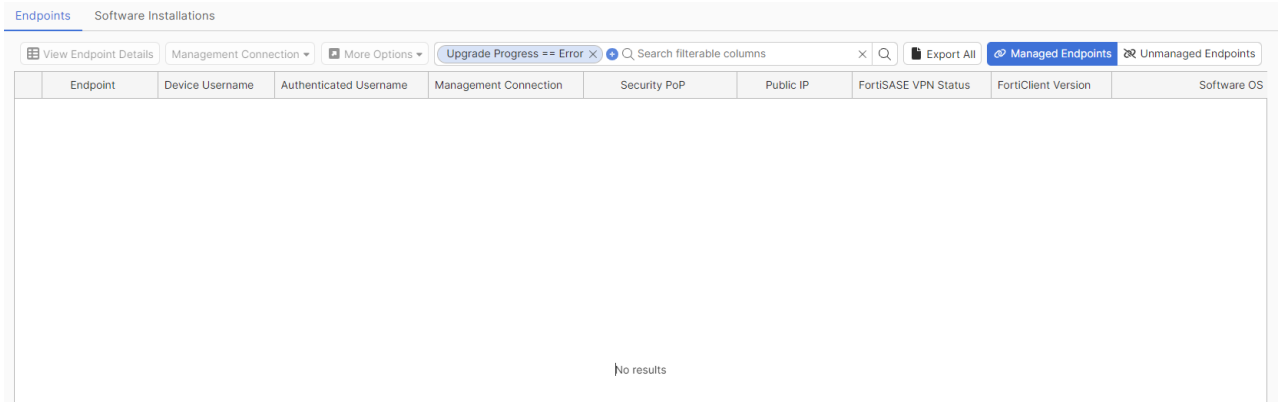
To reset a FortiClient deployment

Occasionally, an endpoint may encounter issues during FortiClient installation due to various reasons like their network, connectivity issue with FortiSASE or other system related errors. In such cases, the *Upgrade Progress* column under *Endpoint management* > *Endpoint upgrade* shows up *Error* for all affected endpoints.

FortiSASE admins can re-deploy FortiClient on such endpoint using *Reset endpoint upgrade* option.

To reset FortiClient upgrade for affected endpoint:

1. Go *Operations* > *Connectivity* > *Managed Endpoints*.
2. Set the column filter as *Upgrade Progress == Error* to view endpoints that have encountered an error.



3. Select respective endpoints, and from the *More Options* dropdown, select *Reset endpoint upgrade*.

Considerations

- Endpoint upgrade rules are prioritized in a top-to-bottom sequence. Thus, if the same computer/device group is used in different endpoint rules, the endpoint upgrade rule that is at top is evaluated first.
- If an ongoing FortiClient upgrade is scheduled or in progress and any new recommended FortiClient version becomes available, all endpoint upgrade rules are temporarily disabled and must be manually re-enabled. This ensures that FortiSASE administrators are aware of the new FortiClient version, allowing them to plan their FortiClient upgrade accordingly.
- Microsoft Entra ID domains are supported only on Windows endpoints running FortiClient 7.0.13 or later. These endpoints must be joined to the Entra ID domains and connected to the FortiSASE Endpoint Management Service. See Entra ID domains on page 581. As a result, the endpoint upgrade rule does not apply to Entra ID computer/device groups if the current FortiClient version on endpoints is 7.0.12 or earlier.
- Windows endpoints must reboot to complete FortiClient upgrades. Logged-in users will be notified when an upgrade is ready and have the option to defer the installation. Once the installation starts, the system will automatically reboot upon completion.

Access & authentication

In *Access & authentication*, you can control network access for different users and devices in your network. FortiSASE authentication controls system access by user group. By assigning individual users to the appropriate user groups, you can control each user's access to network resources. You can define local users and remote users in FortiSASE. You can also integrate user accounts on remote authentication servers and connect them to FortiSASE.

The following summarizes the provisioning process for different user types on FortiSASE:

User type	Provisioning process
LDAP	Configure remote users over LDAP to easily integrate FortiSASE with a Windows Active Directory (AD) server or another LDAP server. You can invite users in one of the following ways: • Define an individual user and send the invitation to them directly • Create a user group and send the invitation using the *Onboard Users* button See Configuring FortiSASE with an LDAP server for remote user authentication in FortiClient agent-based mode on page 504. See Configuring FortiSASE with an LDAP server for remote user authentication in proxy agentless mode on page 508.
RADIUS	Configure remote authentication with a RADIUS server. You can allow all users from the IdP or define a group in *Configuration* > *Users*. Send the invitation code to users using the *Onboard Users* button. See Configuring FortiSASE with a RADIUS server for remote user authentication on page 512.
Single sign on (SSO)	Configure an SSO connection with an authentication server such as Entra ID or Okta, where Entra ID or Okta is the identity provider (IdP) and FortiSASE is the service provider (SP). You can allow all users from the IdP or define a group in *Configuration* > *Users*. Send the invitation code to users using the *Onboard Users* button. See: • Configuring FortiSASE with Microsoft Entra ID SSO in FortiClient agent-based mode on page 517 • Configuring FortiSASE with Entra ID SSO in proxy agentless mode on page 526 • Configuring FortiSASE with Okta SSO on page 535
Local	Define user in *Configuration* > *Users* and send invitation to them directly. See Users and groups on page 502.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with any BGP routing design.

Implicit and split DNS rules for tunnel traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

Ensure that your FortiSASE remote users have access to the LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 47.

The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.

The *Onboard Users* button, which is available from the *Remote User Management* widget on the *Status* dashboard, allows you to send an email to users to invite them to FortiSASE. They can register their FortiClient to FortiClient Cloud by using the instructions in the invitation email. You must still provision users via one of the aforementioned methods to give them access to tunnels and other FortiSASE resources.

Users and groups

To create a local user:

1. Go to *Access & authentication > Access > Users and groups*.
2. Click *Create*.
3. Select *User*, then click *Next*.
4. In the *Email* field, enter the desired email address. FortiSASE sends instructions and an invitation code to this email address. The user uses this code to connect FortiClient to FortiSASE.
5. If desired, enable and configure *Temporary administrative password*. Users change their password during the activation process. You may want to configure a password if you anticipate that you need administrative access to this agent before the activation process.
6. Click *OK*.

To create a user group:

1. Go to *Access & authentication > Access > Users and groups*.
2. Click *Create > User Group*.
3. In the *Members* field, click +.
4. In the *Select Entries* pane, select the desired users to add to this user group.

5. In the *Remote Groups* field, select *Create*.
6. From the *Remote Server* dropdown list, select the desired server.
7. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK*.
8. Click *OK*.

To import users in bulk using a CSV file:

1. Go to *Access & authentication > Access > Users and groups*.
2. Click *Import/Export > Import Users*.
3. In the *Import Users* pane, click *Browse*.
4. Browse to and upload the CSV file that contains the desired email addresses. Click *Next*.
5. The *Import Users* pane displays the email addresses that it detected in the CSV file after removing those already associated with existing users. Review the email address list.
6. Click *Import*. The imported users display on the *Users and groups* page.

PKI

A public key infrastructure (PKI) user are users identified by a digital certificate.

PKI users are used to define peer users and are used with SPA Service Connections using IPsec when *Authentication Method* is configured as *Certificate*.

To create a PKI user:

1. Go to *Access & authentication > Access > PKI*.
2. Click *Create*.
3. In the *Name* field, enter the name of the PKI user.
4. (Optional) In the *Subject* field, enter the peer certificate name constraints. This is field can be empty, can contain only the CN value or can contain a substring of the certificate subject.

   For example, if the actual subject of the peer certificate is set to "C = CA, CN = dc1, L = VAN, O = MyCompany, OU = it, ST = BC, emailAddress = dc1@mycompany.com", you can configure then the *Subject* field with one of the following values:
   - Empty
   - "CN = dc1"
   - Substring of the whole subject:
     - "CN = dc1, L = VAN, O = MyCompany, OU = it, ST = BC, emailAddress = dc1@mycompany.com"

       OR
     - "C = CA, CN = dc1, L = VAN, O = MyCompany, OU = it, ST = BC"
5. For the *CA* dropdown list, specify which certificate FortiSASE uses to validate the peer's certificate. This can be any CA in the peer's certificate chain. You may need to upload a remote CA certificate to FortiSASE specifically to identify PKI peer users. See Certificates on page 592.
6. Click *OK*.

See Configuring a new service connection on page 113 for details on how to configure a defined PKI user.

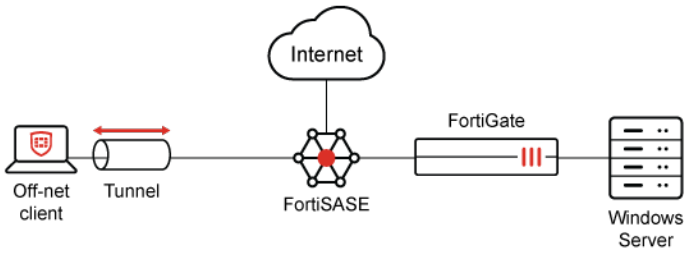
LDAP

Configuring FortiSASE with an LDAP server for remote user authentication in FortiClient agent-based mode

LDAP authentication is unavailable for remote agent users using IPsec.

FortiSASE can easily integrate with a Windows Active Directory (AD) server or another LDAP server for remote agent user authentication.

- This example has a Windows domain controller that has users defined in its AD.
- You want to allow certain agents access over FortiSASE. These users connect using their Windows domain credentials.



The Windows server is protected by a FortiGate that uses a virtual IP address (VIP) to port forward port 10636 to the Windows server. Communication over this VIP is allowed only for the FortiSASE IP address. The example domain is KLHOME.local.

Configuring the LDAP server in FortiSASE

To configure the LDAP server in FortiSASE:

1. Go to *Access & authentication* > *Authentication Sources* > *LDAP*.
2. Click *Create*.
3. Configure the following settings:

Field	Description
Name	Connection name.
Access Type	When set to *Private*, secure private access (SPA) is used for the LDAP server. Ensure the SPA network is configured with any BGP routing design. • Ensure that your FortiSASE remote users have access to the LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy

Field	Description
	on page 146.
Server IP/Name	LDAP server IP address or FQDN.
Server Port	By default, LDAP uses port 636 and a secure connection. If you are using a custom port, define it here. In this example, it is 10636.
Common Name Identifier	This is the attribute in which your LDAP server identifies the username. • In an AD, this is commonly the common name attribute, which is denoted `cn`. • Alternatively, you can use `sAMAccountName`. This is case-sensitive. • In other LDAP servers, it may be the user ID, which is denoted `uid`. • In an AD, for usernames in the username@domain format, use the user principal name (UPN) attribute, which is denoted `userPrincipalName`.
Distinguished Name	Used to look up user account entries on the LDAP server. It reflects the hierarchy of LDAP database object classes above the CN identifier in which you are doing the lookup. If you want to recursively look up all objects under the root domain in the example AD, specify `dc=KLHOME,dc=local`. If you want to look up users under a specific organization unit, specify `ou=Agents,dc=KLHOME,dc=local`.
Secure Connection	Enable to connect to server by LDAPS by default. Using LDAPS is recommended to ensure an encrypted connection. If disabled, communication occurs in clear text.
Password Renewal	Enable remote password renewal. When the LDAP user's password expires, the user can renew their password when authenticating with FortiSASE. This option is only available if using LDAPS.
Certificate	Select the CA certificate for your LDAPS connection. If this certificate is not signed by a known CA, you must export the certificate from your server and install this on FortiSASE. To import the certificate, do the following: **1.** Click *Certificate*, then *Create*. **2.** If you have the certificate file, select *File*. **3.** Click *Upload*. This creates a new remote CA certificate in the FortiSASE certificate store. You can also import and view the certificate in *System* > *Certificates*.
Server Identity Check	If enabled, the server certificate must include the server IP address/name defined in the *Server IP/Name* field.
Advanced Group Matching	Enable advanced group matching. Based on your LDAP server, you may need to configure additional properties to ensure that FortiSASE correctly matches LDAP groups.
Group Member Check	Determines which attributes FortiSASE uses for group matching: • Group object

Field	Description
	• POSIX group object • User attribute
Group Filter	Enter the filter to use for group matching. Required when *Group Member Check* is set to User attribute.
Group Search Base	Enter the search base to use for group searching. Required when *Group Member Check* is set to User attribute.
Member Attribute	Enter the name of the attribute from which FortiSASE retrieves the group membership information.

The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.

4. Configure the following *Authenticate* settings:

Field	Description
Bind Type	Select one of the following. Regular bind is recommended: • **Simple**: bind using simple password authentication using the client name. The LDAP server only looks up against the distinguished name (DN), but does not search on the subtree. • **Anonymous**: bind using anonymous user and search starting from the DN and recurse over the subtrees. Many LDAP servers do not allow this. • **Regular**: bind using username/password provided and search starting from the DN and recurse over the subtrees.
Username	If using regular bind, enter the username. In the example AD, this may be `KLHOME\administrator` or `administrator@KLHOME`.
Password	If using regular bind, enter the password.
Client Certificate	Enable client certificate for authentication with LDAPS server. Select the client certificate that you previously uploaded to FortiSASE.

5. Click *Test connection*. If the connection fails, return to the previous steps to reconfigure the LDAP server, or skip the test. If the connection succeeds, click *Next*.
6. Review the configuration, then click *Submit*.

Configuring remote users from the LDAP server

To configure remote users from the LDAP server:

1. Do one of the following:
   - To send invitations directly to individual users, do the following:
     i. Go to *Access & authentication* > *Access* > *Users and groups*.
     ii. Click *Create*.

iii. Select *LDAP User*, then click *Next*.
iv. From the *LDAP Server* dropdown list, select the server that you configured. Click *Next*.
v. FortiSASE displays the available remote users. It displays all users starting from the DN root to the subtrees. Select users as desired. Click *Next*.
vi. Provide the users' email addresses. FortiSASE sends invitation codes and connection instructions to these email addresses.
vii. Click *OK*.

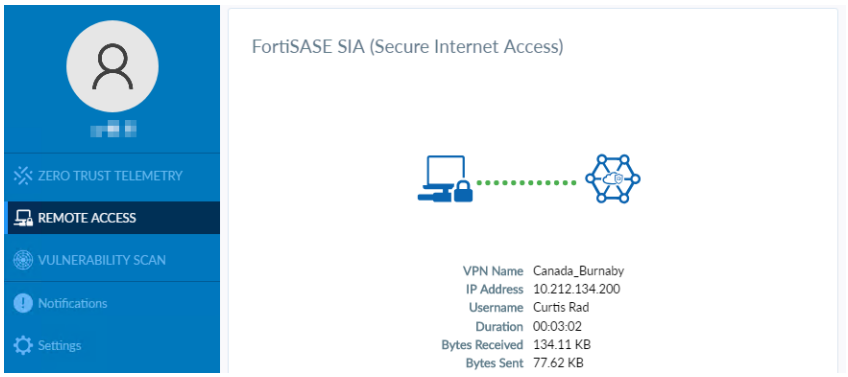
- To create and send invitations to a group of users, do the following:
  i. Go to *Access & authentication* > *Access* > *Users and groups*.
  ii. Click *Create* > *User Group*.
  iii. In the *Users* field, click +.
  iv. In the *Select Entries* pane, select the desired users to add to this user group.
  v. In the *Remote Groups* field, select *Create*.
  vi. From the *Remote Server* dropdown list, select the desired server.
  vii. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK* twice.
  viii. Go to *Monitoring* > *Dashboards* > *Status*. In the *Remote User Management* widget, click *Onboard Users*.
  ix. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Connecting to the tunnel from FortiClient

The end user follows these instructions to connect to the FortiSASE tunnel.

To connect to the tunnel from FortiClient:

1. Follow the instructions from the received email to install the compatible FortiClient version on to your device.
2. Once installed, open FortiClient.
3. On the *ZERO TRUST TELEMETRY* tab, in the *Join FortiClient Cloud* field, enter the invitation code from the received email.
4. FortiClient connects to and becomes provisioned by FortiClient Cloud. On the *REMOTE ACCESS* tab, connect to the preconfigured tunnel using your Windows username and password. If the administrator configured the CN identifier as `cn`, the username is likely the user's full name. Once connected, the *REMOTE ACCESS* tab displays the active tunnel connection and additional information.



Considerations

- FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with any BGP routing design.

  Implicit and split DNS rules for tunnel traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

  Ensure that your FortiSASE remote users have access to the LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.

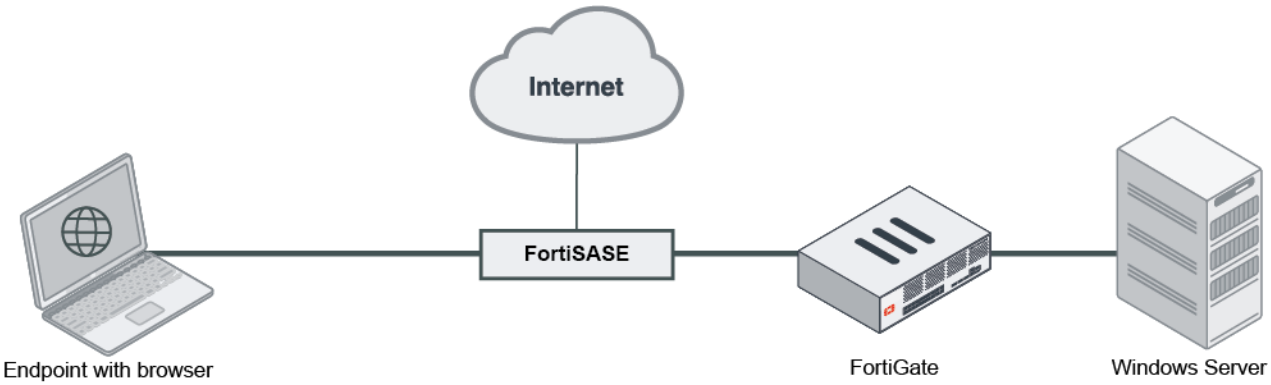
  When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

  See Network restrictions removed on page 47.
- The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.

Configuring FortiSASE with an LDAP server for remote user authentication in proxy agentless mode

> ⚠ FortiSASE performs proxy authentication via HTTP. Therefore, single sign on (SSO) authentication is strongly recommended for proxy users, see Configuring FortiSASE with Entra ID SSO in proxy agentless mode on page 526.

Configuring remote users over LDAP allows FortiSASE to easily integrate with a Windows Active Directory (AD) server or another LDAP server. This example has a Windows domain controller that has users defined in its AD. You want to allow certain users to configure FortiSASE as their proxy server. These users authenticate using their Windows domain credentials.



The Windows server is protected by a FortiGate that uses a virtual IP address (VIP) to port forward port 10636 to the Windows server. Communication over this VIP is allowed only for the FortiSASE IP address. The example domain is KLHOME.local.

Configuring the LDAP server in FortiSASE

To configure the LDAP server in FortiSASE:

1. Go to *Access & authentication* > *Authentication Sources* > *LDAP*.
2. Click *Create*.
3. Configure the following settings:

Field	Description
Name	Connection name.
Access Type	When set to *Private*, secure private access (SPA) is used for the LDAP server. Ensure the SPA network is configured with any BGP routing design. • Ensure that your FortiSASE remote users have access to the LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.
Server IP/Name	LDAP server IP address or FQDN.
Server Port	By default, LDAP uses port 636 and a secure connection. If you are using a custom port, define it here. In this example, it is 10636.
Common Name Identifier	This is the attribute in which your LDAP server identifies the username. • In an AD, this is commonly the common name attribute, which is denoted `cn`. • Alternatively, you can use `sAMAccountName`. This is case-sensitive. • In other LDAP servers, it may be the user ID, which is denoted `uid`. • In an AD, for usernames in the username@domain format, use the user principal name (UPN) attribute, which is denoted `userPrincipalName`.

Field	Description
Distinguished Name	Used to look up user account entries on the LDAP server. It reflects the hierarchy of LDAP database object classes above the CN identifier in which you are doing the lookup. If you want to recursively look up all objects under the root domain in the example AD, specify `dc=KLHOME,dc=local`. If you want to look up users under a specific organization unit, specify `ou=Agents,dc=KLHOME,dc=local`.
Secure Connection	Enable to connect to server by LDAPS by default. Using LDAPS is recommended to ensure an encrypted connection. If disabled, communication occurs in clear text.
Password Renewal	Enable remote password renewal. When the LDAP user's password expires, the user can renew their password when authenticating with FortiSASE. This option is only available if using LDAPS.
Certificate	Select the CA certificate for your LDAPS connection. If this certificate is not signed by a known CA, you must export the certificate from your server and install this on FortiSASE. To import the certificate, do the following: 1. Click *Certificate*, then *Create*. 2. If you have the certificate file, select *File*. 3. Click *Upload*. This creates a new remote CA certificate in the FortiSASE certificate store. You can also import and view the certificate in *System* > *Certificates*.
Server Identity Check	If enabled, the server certificate must include the server IP address/name defined in the *Server IP/Name* field.
Advanced Group Matching	Enable advanced group matching. Based on your LDAP server, you may need to configure additional properties to ensure that FortiSASE correctly matches LDAP groups.
Group Member Check	Determines which attributes FortiSASE uses for group matching: • Group object • POSIX group object • User attribute
Group Filter	Enter the filter to use for group matching. Required when *Group Member Check* is set to User attribute.
Group Search Base	Enter the search base to use for group searching. Required when *Group Member Check* is set to User attribute.
Member Attribute	Enter the name of the attribute from which FortiSASE retrieves the group membership information.

The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.

4. Configure the following *Authenticate* settings:

Field	Description
Bind Type	Select one of the following. Regular bind is recommended: • **Simple**: bind using simple password authentication using the client name. The LDAP server only looks up against the distinguished name (DN), but does not search on the subtree. • **Anonymous**: bind using anonymous user and search starting from the DN and recurse over the subtrees. Many LDAP servers do not allow this. • **Regular**: bind using username/password provided and search starting from the DN and recurse over the subtrees.
Username	If using regular bind, enter the username. In the example AD, this may be `KLHOME\administrator` or `administrator@KLHOME`.
Password	If using regular bind, enter the password.
Client Certificate	Enable client certificate for authentication with LDAPS server. Select the client certificate that you previously uploaded to FortiSASE.

5. Click *Test connection*. If the connection fails, return to the previous steps to reconfigure the LDAP server, or skip the test. If the connection succeeds, click *Next*.
6. Review the configuration, then click *Submit*.

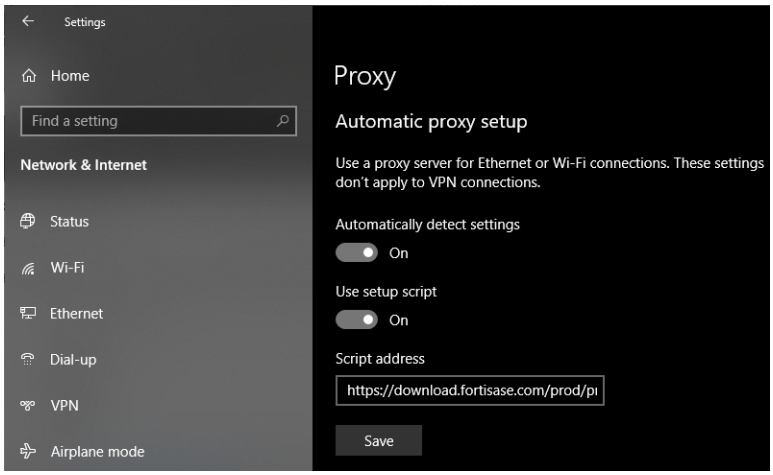
Configuring FortiSASE as a proxy server

The end user follows these instructions to configure proxy agentless mode on their machine. The end user can configure proxy settings at the OS level or in a browser. When proxy settings are configured at the OS level, they are applied to all installed browsers. The following gives instructions for configuring proxy settings at the OS level on a Windows 10 device.

To configure Windows 10 to use the FortiSASE proxy server:

1. In Windows, go to *Windows Settings* > *System* > *Proxy Settings*.
2. Enable *Use setup script*.

3. In the *Script address* field, enter the *Hosted PAC File* URL.



4. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their Windows domain credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

Considerations

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with any BGP routing design.

Implicit and split DNS rules for tunnel traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

Ensure that your FortiSASE remote users have access to the LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 47.

Configuring FortiSASE with a RADIUS server for remote user authentication

The RADIUS server must be reachable from the public internet or through private IP routable through a configured SPA hub.

To protect against the RADIUS vulnerability described in CVE-2024-3596, as a RADIUS client, FortiSASE will:

1. Force the validation of message-authenticator
2. Reject RADIUS responses with unrecognized proxy-state attribute.

Message-authenticator checking is made mandatory under UDP/TCP. It is not mandatory when using TLS.

Therefore, since FortiSASE uses UDP mode without RADSEC, the RADIUS server should be patched to ensure the message-authenticator attribute is used in its RADIUS messages.

To configure the RADIUS server in FortiSASE:

1. Go to *Access & authentication* > *Authentication Sources* > *RADIUS*.
2. Click *Create*.
3. Configure the following settings:

Field	Description
Name	Connection name.
Access Type	When set to *Private*, secure private access (SPA) is used for the RADIUS server. Ensure the SPA network is configured with any BGP routing design. Ensure that your FortiSASE remote users have access to the RADIUS server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.
Authentication Type	If you know the RADIUS server uses a specific authentication protocol, select *Specify* and select the desired protocol from the list. Otherwise, select *Default*.
Include All Users	Allow all users on the RADIUS server to authenticate with FortiSASE.

4. Configure the following *Configure Servers* settings. If the primary server does not respond, FortiSASE sends the access request to the secondary server if configured:

Field	Description
Primary Server	
IP/Name	Enter the domain name or IP address of the RADIUS server.
Secret	Enter the server secret key. This value must match the secret on the RADIUS primary server.
Secondary Server	
IP/Name	(Optional) Enter the domain name or IP address of the secondary RADIUS server.
Secret	(Optional) Enter the secondary server secret key. This value must match the secret on the RADIUS secondary server.

5. Click *Test connection*. If the connection fails, return to the previous steps to reconfigure the RADIUS server (s), or skip the test. If the connection succeeds, click *Next*.
6. Review the configuration, then click *Submit*.

To invite users using RADIUS authentication to FortiSASE:

The following procedure is not applicable for proxy agentless mode users. See Proxy agentless mode on page 15.

1. (Optional) If you want to define a group of users, create a user group:
   a. Go to *Access & authentication* > *Access* > *Users and groups*.
   b. Click *Create* > *User Group*.
   c. In the *Members* field, click +.
   d. In the *Select Entries* pane, select the desired users to add to this user group.
   e. In the *Remote Groups* field, select *Create*.
   f. From the *Remote Server* dropdown list, select the desired server.
   g. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK*.
   h. Click *OK*.
2. Go to *Monitoring* > *Dashboards* > *Status*.
3. In the *Remote User Management* widget, click *Onboard Users*.
4. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE.
5. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Prerequisites

- If the RADIUS server is behind a firewall, ensure that port 1812 for authentication is open and correctly forwarded. The RADIUS server requires a NAS IP address to be configured in its list of authorized NAS clients. For FortiSASE, this request is done using the public IP address, as listed in Appendix A - FortiSASE data centers on page 800.
- If the RADIUS server is behind a device that can take traffic captures, it is recommended to take a capture to see the RADIUS authentication exchange to see the NAS IP address that FortiSASE uses to make the request.
- If the RADIUS server is a FortiAuthenticator, you must configure the identified NAS IP address as a valid NAS client in the *RADIUS Service* section.

Considerations

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with any BGP routing design.

Implicit and split DNS rules for tunnel traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

Ensure that your FortiSASE remote users have access to the LDAP server. If access to the SPA hub is being restricted by a firewall policy, you must ensure security PoPs are allowed to access the SPA hub. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 47.

SSO

You can configure the following in SSO:

- Configuring FortiSASE with Microsoft Entra ID SSO: SAML configuration fields on page 515
- Configuring FortiSASE with Microsoft Entra ID SSO in FortiClient agent-based mode on page 517
- Configuring FortiSASE with Entra ID SSO in proxy agentless mode on page 526
- Configuring FortiSASE with AD FS SSO on page 528
- Configuring FortiSASE with Okta SSO on page 535
- Configuring FortiSASE with FortiAuthenticator as SAML IdP for SSO on page 545
- Searching user groups from SAML IdP on page 552
- Testing SSO configuration from FortiSASE on page 556
- Authenticated onboarding on page 562

Configuring FortiSASE with Microsoft Entra ID SSO: SAML configuration fields

Before you configure FortiSASE with Entra ID single sign on (SSO) for the FortiClient agent-based mode (agent SSO) or proxy mode (proxy user SSO), review the following tables to understand which Entra ID basic SAML configuration fields correspond to FortiSASE SAML fields.

For the *Configure Identity Provider* step, this table maps the FortiSASE SAML fields that you must copy from FortiSASE and configure in Entra ID:

FortiSASE SAML field	Entra ID Basic SAML configuration field
Entity ID	*Identifier (Entity ID)*
Assertion Consumer Service (ACS) URL	*Reply URL (Assertion Consumer Service URL)*
Single Logout Service (SLS) URL	*Logout Url (Optional)*
Portal (Sign On) URL	*Sign on URL*

User Attributes & Claims in Entra ID allows only one single group claim. You must delete the existing group claim and then add a new claim or you can edit the existing group claim. With this approach, the end result is to change *user.groups* to *All groups* with a custom *Claim Name* of *group*.

Alternatively, you can keep the existing group claim with default settings of *user.groups* set to *Security Groups* with *Claim Name* of *http://schemas.microsoft.com/ws/2008/06/identity/claims/groups*. This is a valid approach using the official claim name that Microsoft specifies.

Regardless of the approach chosen, you must ensure that in the FortiSASE SAML SSO user settings, the *SAML Claims Mapping > Group Name* field matches the *Claim Name* specified in the *User Attributes & Claims* section in the Entra ID SAML settings for the FortiSASE enterprise application.

For the *Configure Service Provider* step, this table maps the Entra ID SAML fields that you must copy from Entra ID and configure in FortiSASE:

FortiSASE SAML field	Entra ID Basic SAML configuration field
IdP Entity ID	Entra ID Identifier
IdP Single Sign-On URL	Login URL
IdP Single Log-Out URL	Logout URL
SAML Claims Mapping > Username	username
SAML Claims Mapping > Group Name	group
SAML Group Matching > Group ID	Object Id. See the following steps for identifying this field from a newly created group in Entra ID.
IdP Certificate	Base64 SAML certificate name. See the following steps for downloading this certificate from Entra ID. The certificate name must be alphanumeric and contain fewer than 30 characters.
Service Provider Certificate	You can use the built-in *FortiSASE Default Certificate* or your custom certificate from the dropdown list. To import the certificate, click + and import the certificate. See Certificates on page 592.
Digest Method	Use SHA-1 and SHA-256 depending on the hashing method that the identity provider (IdP) supports.

FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE that a well-known public CA signed and remains same across all of your points of presence.

FortiSASE Default Certificate periodically renews. Thus, if IdPs use *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with the new SP certificate. To avoid updating your IdP configuration frequently, uploading your own certificate is recommended.

While configuring *Service Provider Certificate*, the FortiSASE instances that have existing or old SSO configuration, are by default configured with the legacy default certificate (i.e. *Fortinet_Factory*) as its service provider (SP) certificate.

FortiSASE administrators can change the legacy default certificate (i.e. *Fortinet_Factory*) to use the new *FortiSASE Default Certificate*. Once FortiSASE is configured to use *FortiSASE Default Certificate*, FortiSASE administrators can no longer configure and use the legacy default certificate (i.e. *Fortinet_Factory*). Thus, ensure to update the SP certificate in your IdP configuration. Other FortiSASE instances with fresh SSO configuration have the direct option to use the *FortiSASE Default Certificate* in the *Service Provider Certificate* dropdown menu.

To find the Entra ID group ObjectID in Entra ID:

Enable and configure SAML group matching if you only want to allow Entra ID users of a certain group to authenticate. Otherwise, leave this setting disabled. You can define more granular groups when configuring user group settings.

1. In the left pane of the Azure portal (three horizontal lines), go to *Microsoft Entra ID > Manage > Groups*.
2. The default view shows all groups. Find the desired group and note the *Object Id*.

For details on creating a new security group, see Configure FortiGate SSL VPN for Single sign-on with Microsoft Entra ID.

You can find the full group claims list in Configure group claims for applications by using Microsoft Entra ID.

To download the IdP certificate from Azure:

1. In Entra ID, go to your Entra ID enterprise application, go to *Single sign-on > SAML Signing Certificate*.
2. For *Certificate (Base64)*, click *Download* to download the IdP certificate to your computer.

Configuring FortiSASE with Microsoft Entra ID SSO in FortiClient agent-based mode

You can configure a single sign on (SSO) connection with Entra ID via SAML where Entra ID is the identity provider (IdP) and FortiSASE is the service provider (SP). This allows end users to connect to the tunnel by logging in with their Entra ID credentials.

Before completing the following steps, see Configuring FortiSASE with Microsoft Entra ID SSO: SAML configuration fields on page 515 for how Entra ID SAML fields map to FortiSASE SAML fields.

Configuring FortiSASE with Entra ID SSO

To configure FortiSASE with Entra ID SSO:

1. In FortiSASE, go to *Access & authentication* > *Authentication Sources* > *SSO*. The SSO configuration wizard first step displays the entity ID, SSO URL, and single logout URL. You use these values to configure FortiSASE as an SP in Azure. Copy these values.
2. Create and configure your FortiSASE environment in Azure:
   a. In the Azure portal, go to *Microsoft Entra ID* > *Enterprise applications* > *New application*.
   b. Search for and select FortiSASE.
   c. Click *Create*.
   d. Assign Entra ID users and groups to FortiSASE.
   e. Go to *Set up single sign on*.
   f. For the SSO method, select *SAML*.
   g. In *Basic Configuration*, enter the values that you copied in step 1 in the *Identifier (Entity ID)*, *Reply URL*, *Sign on URL*, and *Logout URL* fields. Click *Save*.
3. Obtain the IdP information from Azure:
   a. The *SAML Signing Certificate* box contains links to download the SAML certificate. Download the certificate.
   b. The *Set up <FortiSASE instance name>* box lists the IdP information that you must provide to FortiSASE. Copy the values in the *Login URL*, *Entra ID Identifier*, and *Logout URL* fields.
4. Configure the IdP information in FortiSASE:
   a. In FortiSASE, click *Next* in the SSO wizard. In the *IdP Entity ID*, *IdP Single Sign-On URL*, *IdP Single Log-Out URL* fields, paste the values that you copied from the *Entra ID Identifier*, *Login URL*, and *Logout URL* fields, respectively.
   b. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
   c. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click *+* to add your own custom certificate.
   d. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Azure if *Certificate Verification* is enabled on Azure.
   e. For *Response and assertion signature validity*, select either:
      i. At least one (default): For one of the response or assertion from IdP to be signed and valid.
      ii. Both: For both response and assertion from IdP to be signed and valid.

      This security enforcement feature corresponds to the Entra ID configuration for the *Signing Option* setting when editing the *Single sign-on* > *SAML Certificates* > *Token signing certificate* settings.

   > *FortiSASE Default Certificate* is a built-in wildcard certificate on FortiSASE that a well-known public CA signed and remains same across all of your points of presence.
   >
   > *FortiSASE Default Certificate* periodically renews. Thus, if IdPs use *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with the new SP certificate. To avoid updating your IdP configuration frequently, uploading your own certificate is recommended.

5. Review the SAML configuration, then click *Submit*.

6. (Optional) For Entra ID to perform SP signature verification, download the *Service Provider Certificate* from FortiSASE from *System > Certificate*, select *FortiSASE Default Certificate* and click *Download*. On the Azure application, under *SAML Certificates*, upload the FortiSASE default certificate and select the digest method that matches what you configured on FortiSASE in step 4.d.
7. Invite Entra ID users to FortiSASE:
   a. (Optional) To define a group of users, create a user group:
      i. Go to *Access & authentication > Access > Users and groups*.
      ii. Click *Create*.
      iii. Select *User Group*, then click *Next*.
      iv. In the *Users* field, click *+*.
      v. In the *Select Entries* pane, select the desired users to add to this user group.
      vi. In the *Remote Groups* field, select *Create*.
      vii. From the *Remote Server* dropdown list, select the desired server.
      viii. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK*.
      ix. Click *OK*.
   b. In *Access & authentication > Authentication Sources > SSO*, click *Onboard Users*.
   c. For *FortiClient Installer*, select *Send link to users*.
   d. Under *Invite Users*, click *+* and enter the email addresses of the users to add to FortiSASE.
   e. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Verifying Entra ID SAML SSO configuration

To verify the Azure SAML SSO configuration:

1. In FortiClient on an endpoint, go to the *REMOTE ACCESS* tab. The tab displays a *SAML Login* button.
2. Click *SAML Login*.
3. In the dialog, sign in with your Entra ID credentials to connect to the tunnel.

Considerations

- A FortiSASE instance with IPsec remote users enabled does not support Microsoft Entra ID automatic login using OAuth. Only an SSL-enabled FortiSASE instance supports Entra ID automatic login using OAuth.
- FortiSASE supports configuring multifactor authentication (MFA) on Entra ID and prompts the user to enter the token code on FortiClient. You must enable and configure MFA on Entra ID for required users. See Enable per-user Microsoft Entra multifactor authentication to secure sign-in events.
- FortiSASE cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE as well.
- Currently, SSO authentication via SAML fails when the remote agent attempts to connect to the SAML IdP and there is any traffic load balancing involved such as remote agent traffic traversing a FortiGate SD-WAN or other SD-WAN device performing internet load balancing on the client end. All traffic from the agent to

the SAML IdP must be sent with a unique public IP and not change during the session with the SAML IdP.

Configuring API permissions and determining Entra ID SSO credentials

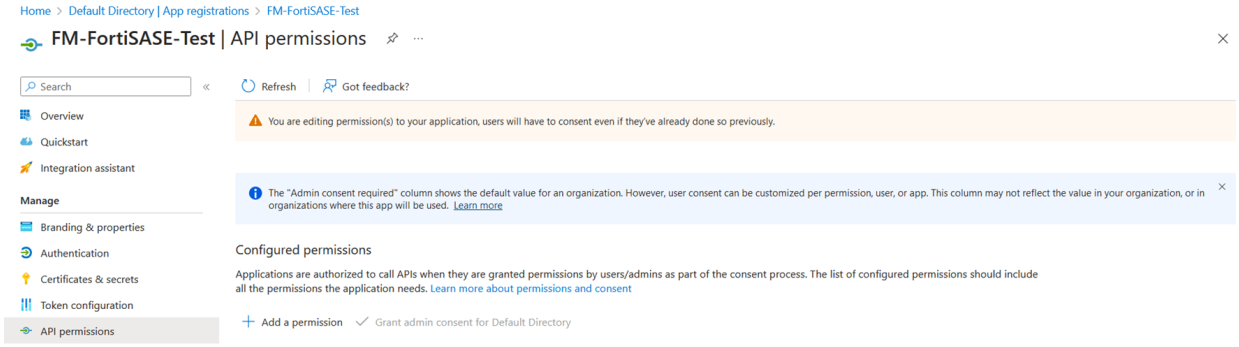
Before you can autoconnect to a tunnel using Microsoft Entra ID SSO and search user groups from Entra ID single sign on (SSO), you must configure API permissions for autoconnect and group searching, and then determine the SAML provider credentials from the Entra ID portal.

To access the Entra ID portal:

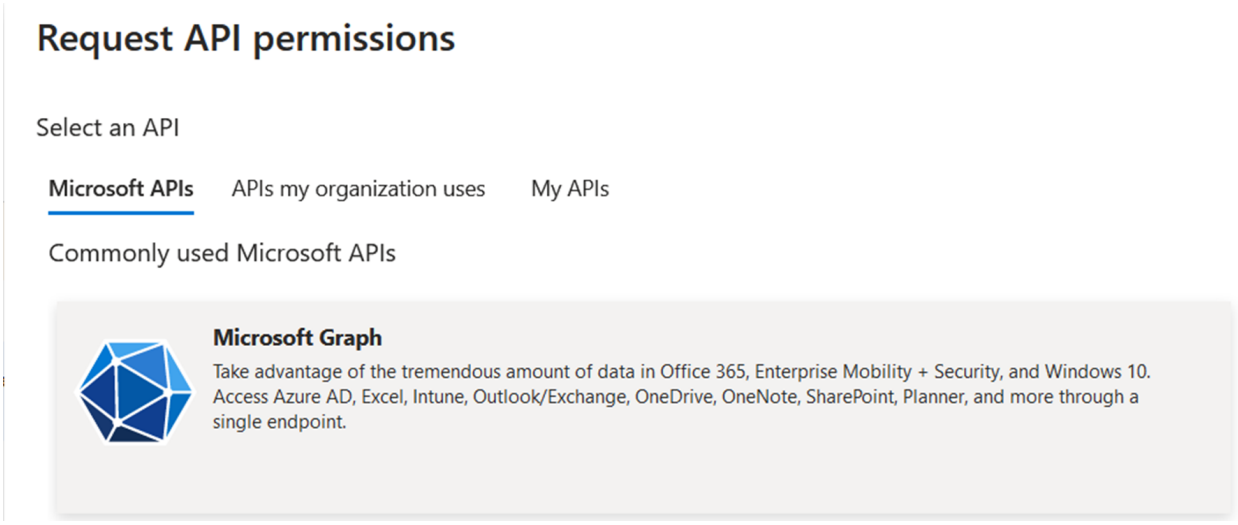
1. Log into the Azure portal. You should already have an enterprise application created in Entra ID. If this has not been created, see Creating an enterprise application using FortiSASE as a template from the gallery and collecting SAML IdP URL information.
2. On the homepage, do one of the following:
   - Under *Azure Services*, click *Microsoft Entra ID*.
   - Click the navigation menu and under *All Services*, click *Microsoft Entra ID*.

To add Microsoft Graph API application permissions required for autoconnect and searching user groups:

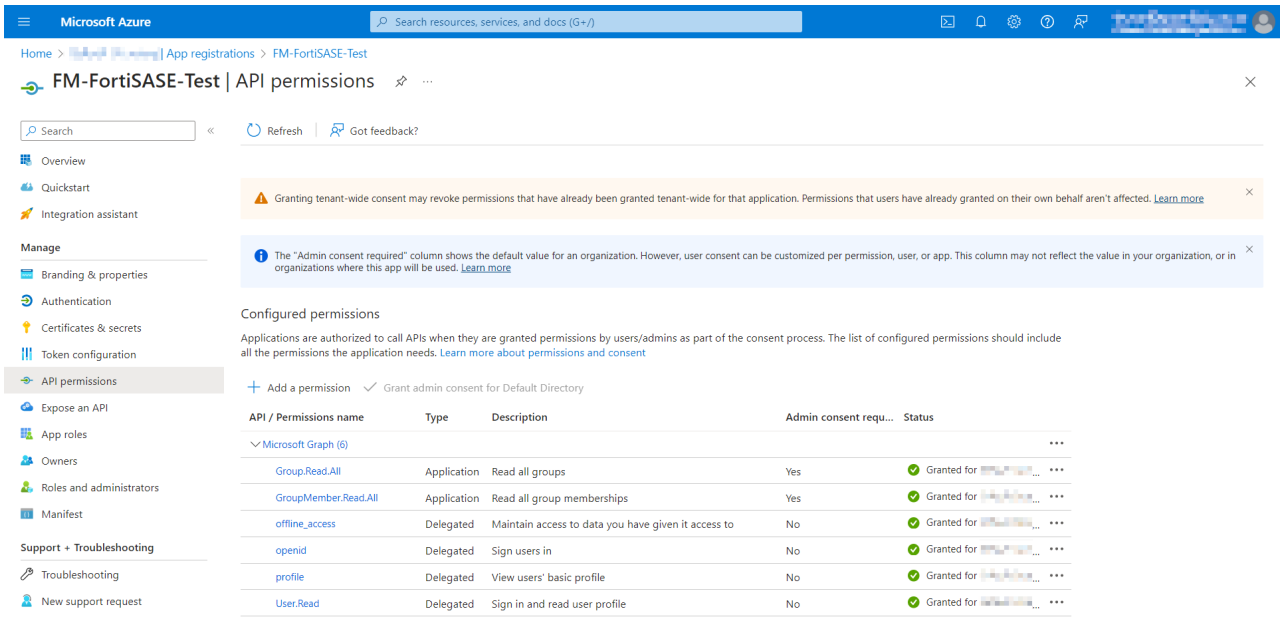
1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *API permissions*, and click *Add a permission*.



4. In the *Request API permissions* slide-in, click *Microsoft Graph*.



5. Add application permissions:
   a. Select *Application permissions*.
   b. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for group searching:
      - *Group > Group.Read.All – Read all groups*
      - *GroupMember > GroupMember.Read.All – Read all group memberships*\
   c. Click *Add permissions*.
6. Add delegated permissions:
   a. Repeat steps 1-4 to add a permission.
   b. Select *Delegated permissions*.
   c. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for autoconnect:
      - *Openid permissions > offline_access – Maintain access to data you have given it access*
      - *Openid permissions > openid – Sign users in*
      - *Openid permissions > profile – View users' basic profile*
      - *User > User.Read – Sign in and read user profile*
7. Click *Add permissions*.
8. In the *API permissions* page, click *Grant admin consent for <domain name>*. If this option is grayed out, you must log into an Entra ID admin account to perform this step. Click *Yes* in the *Grant admin consent* confirmation prompt. Observe the *Grant consent successful* notification at the top-right.
   Also, observe the *Status* field shows *Granted for <domain>* for all the permissions added.



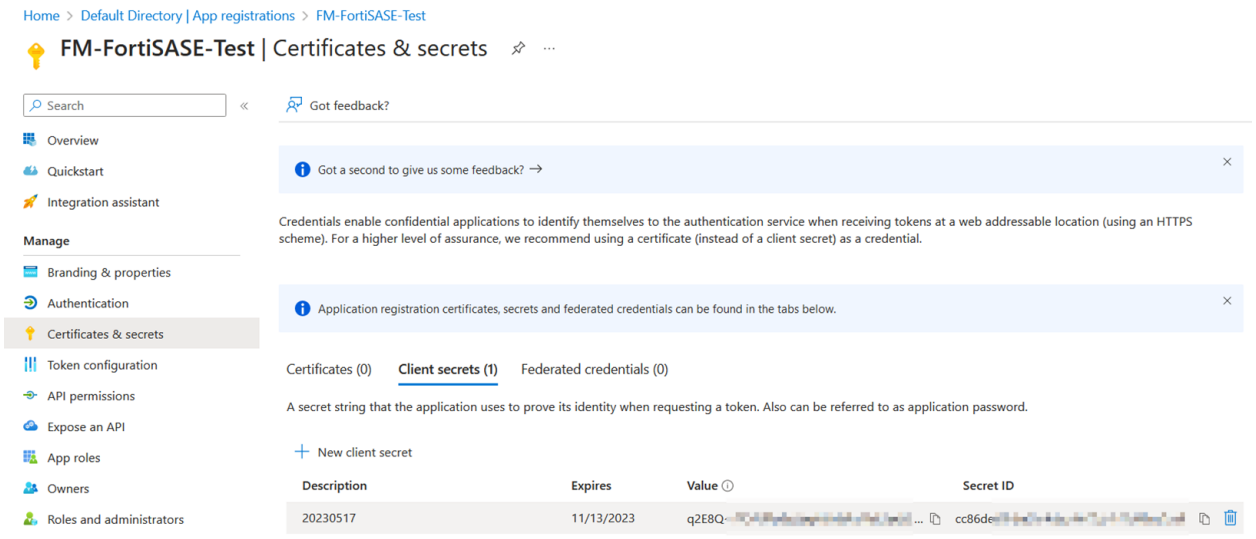
This step is important since it ensures that the administrator grants permissions for the enterprise application from Entra ID instead of end users requiring the administrator to log in to each instance and provide permissions.

Therefore, in summary, you should add the following Microsoft Graph permissions to support the following Entra ID features:

Feature	API permission group	Permission name	Type
Tunnel autoconnect	*OpenId permissions*	*offline_access*	Delegated
	OpenId permissions	*openid*	
	OpenId permissions	*profile*	
	User	*User.read*	
Group searching	*Group*	*Group.Read.All*	Application
	GroupMember	*GroupMember.Read.All*	

To add a client secret string and determine the value of the client secret string:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *Certificates & secrets*, and click *New client secret*.
4. In the *Add a Client Secret* slide-in, add a *Description* and select the *Expires* option of your choice. Click *Add*.
5. Observe that a new client secret has been created. Immediately after creation, ensure you copy the *Value* of the client secret string, which FortiSASE uses as the *Client Secret*. This value is not visible after this initial creation step and moving to another page.



To determine the tenant and client IDs:

1. In the left menu, click *App registrations*, then click *All applications*.
2. Look for your FortiSASE enterprise application name and click the hyperlinked name.
3. In the left menu, click *Overview* and note the following values:
   - *Application (client) ID*, which FortiSASE uses as the *Client ID*
   - *Directory (tenant) ID*, which FortiSASE uses as the *Tenant ID*

Entra ID page within specific enterprise application	Entra ID field	FortiSASE field
Overview	*Directory (tenant) ID*	*Tenant ID*
	Application (client) ID	*Client ID*
Certificates & Secrets	*Value*	*Client Secret*

Configuring Microsoft Entra ID options for agent-based autoconnect

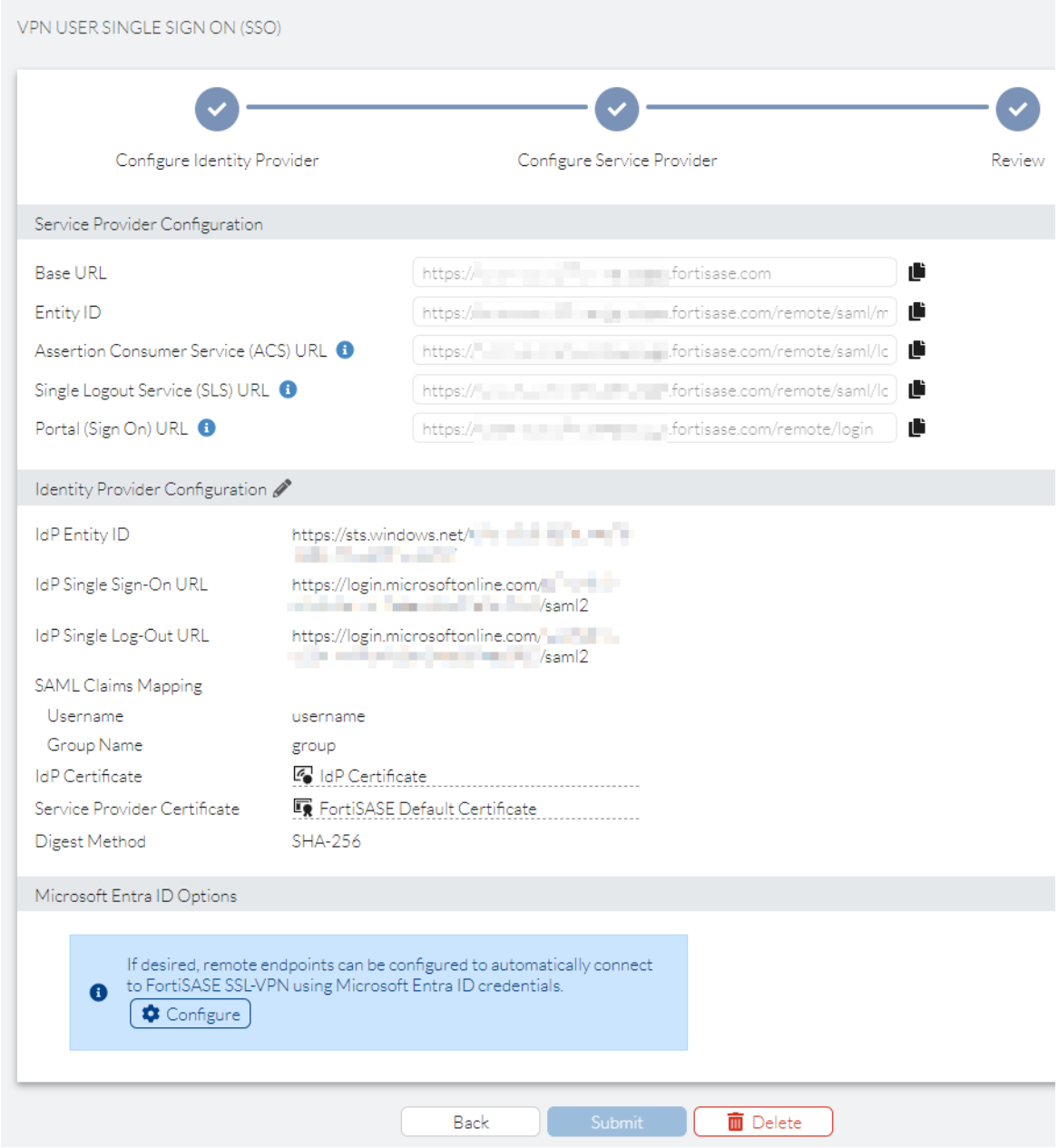
You must configure FortiSASE with Entra ID options, namely the domain name and application ID, to automatically connect to FortiSASE remote tunnel using Entra ID credentials. The FortiSASE Endpoint Management Service uses this information to configure the remote access profile on the FortiClient agent installed on a Windows endpoint. The FortiClient agent for Windows also uses this information to automatically establish a remote tunnel connection immediately after FortiClient is installed, and every time a user logs into Windows.

To configure FortiSASE with Entra ID options:

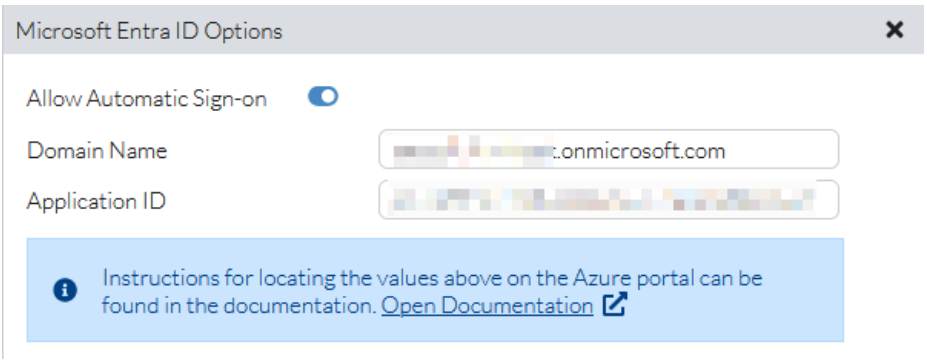
1. In *Access & authentication > Authentication Sources > SSO*, ensure that *Configure Identity Provider* and *Configure Service Provider* are already configured as Configuring FortiSASE with Microsoft Entra ID SSO in

FortiClient agent-based mode on page 517 describes.

2. Under *Microsoft Entra ID Options*, click *Configure*.



3. In the *Microsoft Entra ID Options* slide-in, select *Allow Automatic Sign-on* and enter the domain name and application ID.



For instructions for locating the domain name and application ID on the Azure portal and deployment details for configuring remote Windows endpoints with the FortiClient agent for Windows to automatically connect to FortiSASE remote tunnel using Entra ID credentials, see the FortiSASE Agent-based Tunnel Using OAuth.

Considerations

- Tunnel OAuth authentication is a feature that only FortiClient (Windows) supports. Therefore, *Microsoft Entra ID Options* and the FortiSASE agent-based autoconnect tunnel using Entra ID use case apply to Windows endpoints only.
- A FortiSASE instance with IPsec remote users enabled does not support Microsoft Entra ID automatic login using OAuth. Only an SSL-enabled FortiSASE instance supports Entra ID automatic login using OAuth.
- OAuth support is currently limited to Entra ID as the IdP and Windows endpoints installed with FortiClient agent software.
- FortiSASE cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE as well.

Searching user groups from Entra ID SSO

After performing preliminary steps and determining the Microsoft Entra ID single sign on (SSO) credentials, you can proceed to configure them in FortiSASE to allow dynamic group discovery from Entra ID SSO and select a group for SAML group matching.

The following example is for searching user groups from Entra ID SSO from FortiSASE for a FortiClient agent-based mode SSO configuration and demonstrates general steps that also apply to a proxy mode SSO configuration.

FortiSASE cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE as well.

To search user groups from Entra ID SSO in FortiClient agent-based mode:

1. Go to *Access & authentication > Authentication Sources > SSO*.
   a. For a new configuration, enter the Entra ID SSO fields.
   b. For an existing configuration, click the pencil icon to the right of *Identity Provider Configuration*.
2. Select *SAML Group Matching* and click *Search*.
3. From the *SAML Provider Type* dropdown list, select *Entra ID*. Next to *SAML Provider Credential*, click *Change*.
4. Enter the Entra ID credentials obtained from the Entra ID portal:
   - *Tenant ID*
   - *Client ID*
   - *Client Secret*
5. Click *OK* to save the credentials.
6. Click *Select group* next to *SAML Remote User Groups* and notice that FortiSASE dynamically obtains the groups from Entra ID and populates the field. Select a remote user group from the table and click *OK* to save the changes.
7. Notice that the *Configure Service Provider* page has the *Group Name* automatically filled in with the selected user group name. Click *Next* to advance this page and click *Submit* on the *Review* page to submit the agent SSO configuration settings.

Configuring FortiSASE with Entra ID SSO in proxy agentless mode

You can configure a single sign on (SSO) connection with Microsoft Entra ID, where Entra ID is the identity provider (IdP) and FortiSASE is the service provider (SP). This feature allows end users to configure FortiSASE as their proxy server and authenticate using their Entra ID credentials.

Before completing the following steps, see Configuring FortiSASE with Microsoft Entra ID SSO: SAML configuration fields on page 515 for how Entra ID SAML fields map to FortiSASE SAML fields.

Configuring FortiSASE with Entra ID SSO

To configure FortiSASE with Entra ID SSO:

1. In FortiSASE, go to *Access & authentication > Authentication Sources > SSO > Proxy*. The first step of the SSO configuration wizard displays the entity ID, SSO URL, and single logout URL. You use these values to configure FortiSASE as an SP in Azure. Copy these values.
2. Create and configure your FortiSASE environment in Azure:
   a. In the Azure portal, go to *Microsoft Entra ID > Enterprise applications > New application*.
   b. Search for and select FortiSASE.
   c. Click *Create*.
   d. Assign Entra ID users and groups to FortiSASE.
   e. Go to *Set up single sign on*.
   f. For the SSO method, select *SAML*.

g. In *Basic Configuration*, enter the values that you copied in step 1 in the *Identifier (Entity ID)*, *Reply URL*, *Sign on URL*, and *Logout URL* fields. Click *Save*.

3. Obtain the IdP information from Azure:
   a. The *SAML Signing Certificate* box contains links to download the SAML certificate. Download the certificate.
   b. The *Set up <FortiSASE instance name>* box lists the IdP information that you must provide to FortiSASE. Copy the values in the *Login URL*, *Entra ID Identifier*, and *Logout URL* fields.
4. Configure the IdP information in FortiSASE:
   a. In FortiSASE, click *Next* in the SSO wizard. In the *IdP Entity ID*, *IdP Single Sign-On URL*, *IdP Single Log-Out URL* fields, paste the values that you copied from the *Entra ID Identifier*, *Login URL*, and *Logout URL* fields, respectively.
   b. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
   c. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click *+* to add your own custom certificate.
   d. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Azure if *Certificate Verification* is enabled on Azure.

   > *FortiSASE Default Certificate* is a built-in wildcard certificate on FortiSASE that a well-known public CA signed and remains same across all of your points of presence.
   >
   > *FortiSASE Default Certificate* periodically renews. Thus, if IdPs use *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with the new SP certificate. To avoid updating your IdP configuration frequently, uploading your own certificate is recommended.

5. Review the SAML configuration, then click *Submit*.
6. (Optional) If you want Entra ID to perform SP signature verification, download the *Service Provider Certificate* from FortiSASE from *System > Certificates*, select *FortiSASE Default Certificate* and click *Download*. On the Azure application, under *SAML Certificates*, upload the FortiSASE Default Certificate and select the digest method that matches to what is configured on FortiSASE in step 4.d.

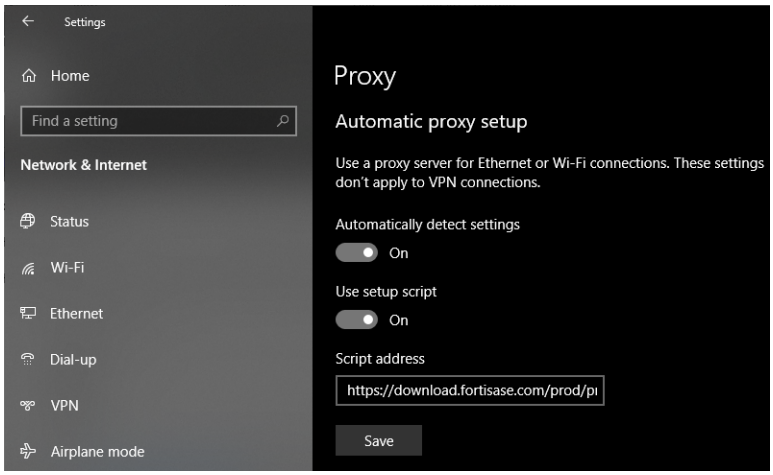
Configuring FortiSASE as a proxy server

The end user follows these instructions to configure proxy agentless mode on their machine. The end user can configure proxy settings at the OS level or in a browser. When the user configures proxy settings at the OS level, the settings are applied to all installed browsers. The following gives instructions for configuring proxy settings at the OS level on a Windows 10 device.

To configure Windows 10 to use the FortiSASE proxy server:

1. In Windows, go to *Windows Settings > System > Proxy Settings*.
2. Enable *Use setup script*.

3. In the *Script address* field, enter the *Hosted PAC File* URL.



4. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their Entra ID credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

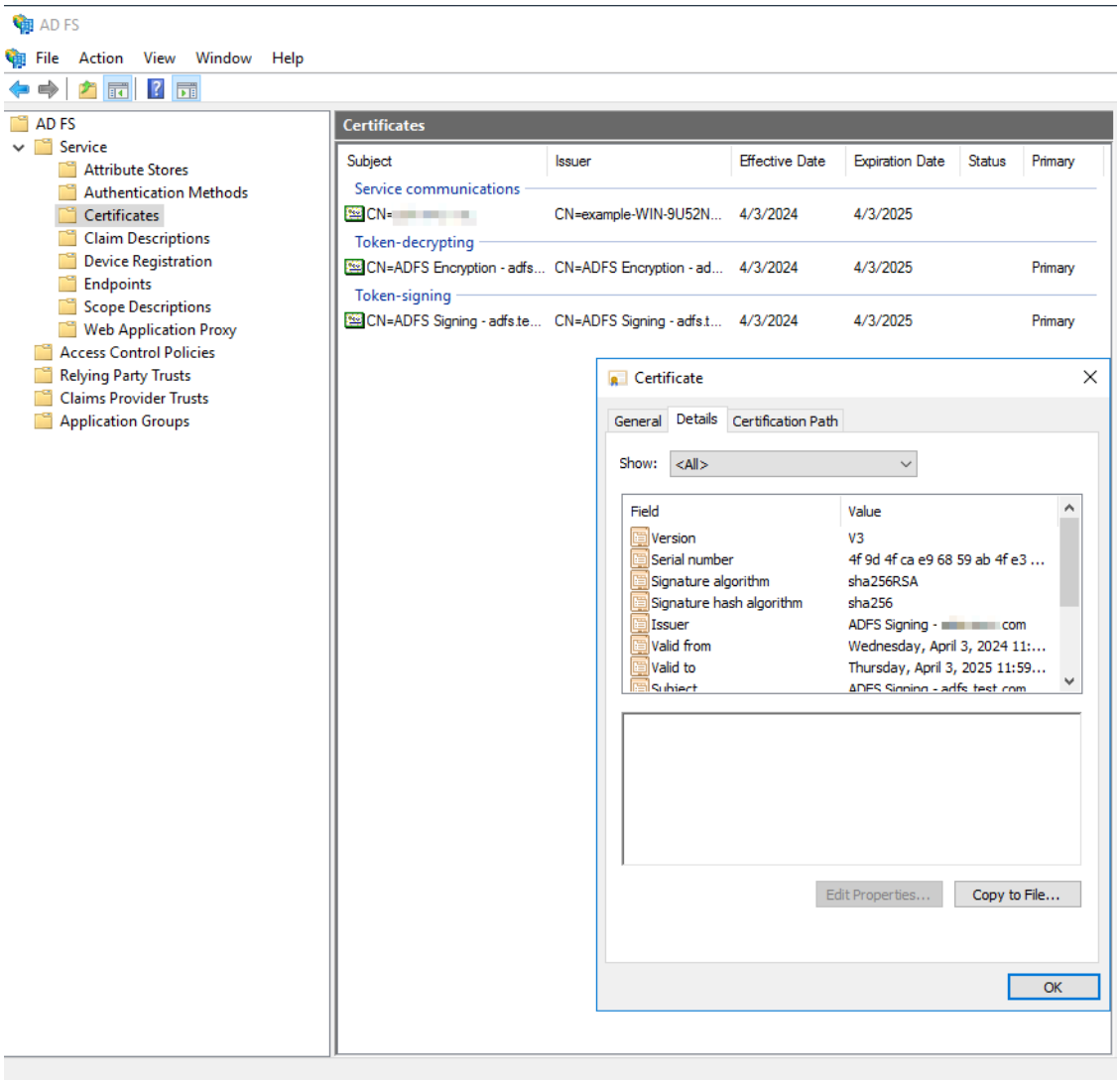
Configuring FortiSASE with AD FS SSO

FortiSASE supports claims-based SAML user authentication using Active Directory Federation Services (AD FS). FortiSASE acts as a service provider (SP) and AD FS acts as an identity provider (IdP) in the SAML authentication flow. In AD FS terminology, FortiSASE is also called a relying party.

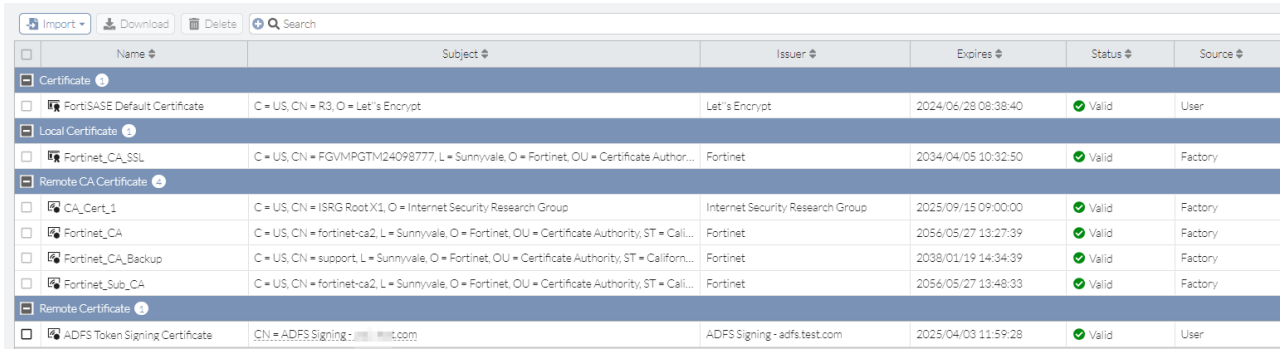
The example that this topic discusses assumes that you have completed prerequisites to install AD FS, and the AD FS service is already installed on Windows Server 2016. See AD FS Requirements.

To export an IdP certificate from AD FS and import it in FortiSASE:

1. On Windows 2016 Server Manager, open the AD FS management snap-in from *Server Manager* > *Tools* > *AD FS Management*.
2. From the *Service* dropdown list, select *Certificates*. Double-click the certificate under *Token-signing*. In the *Certificate* menu, go to the *Details* tab and select *Copy to File* to export it to a suitable location using either .CER format.



3. To import this certificate to FortiSASE, move it to a location that the machine where you will open the FortiSASE GUI can access.
4. In FortiSASE, go to *System* > *Certificates*. Select *Import* > *Remote Certificate*. For *Type*, select *Remote Certificate* and click *Upload* to import the IdP certificate. Give a suitable *Certificate Name* as desired.
5. Click *OK*. The certificate is visible under *System* > *Certificates* > *Remote Certificate*. In this example, FortiSASE successfully imported *ADFS Token Signing Certificate*.



To export an SP certificate from FortiSASE:

In FortiSASE, go to *System > Certificate*, click *FortiSASE Default Certificate* and click *Download* from the toolbar. You will import this certificate to AD FS as the SP certificate in To configure AD FS relying party trust: on page 531.

FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE that a well-known public CA signed and remains same across all of your points of presence.

FortiSASE Default Certificate periodically renews. Thus, if IdPs use *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with the new SP certificate. To avoid updating your IdP configuration frequently, uploading your own certificate is recommended.

To retrieve IdP Configuration from AD FS:

1. On the Windows server where AD FS is installed, open a web browser to download the Federation metadata XML file using the URL https://<your-adfs.domain.com>/federationmetadata/2007-06/FederationMetadata.xml>, where your-adfs.domain.com is the FQDN of your AD FS server.
2. Open the XML file and search for *entityID*, *SingleSignOnService Location*, and *SingleLogoutService Location* and copy the values (i.e. URLs) for these fields in a notepad file:

   ```
   entityID="http://<your-adfs.domain.com>/adfs/services/trust"
   ```

   ```
   <SingleSignOnServiceLocation="https://<your-adfs.domain.com>/adfs/ls/"
   ```

   ```
   <SingleLogoutServiceLocation="https://<your-adfs.domain.com>/adfs/ls/"
   ```

   You will use these URLs to configure IdP details on FortiSASE in To configure AD FS SSO on FortiSASE: on page 530.

To configure AD FS SSO on FortiSASE:

1. In FortiSASE, to configure SSO for agent-based users, go to *Access & authentication > Authentication Sources > SSO > Agent*. Similarly, for agentless users using FortiSASE proxy, go to *Access & authentication > Authentication Sources > SSO > Proxy*.
2. For *Configure Identity Provider*, copy the values in the *Entity ID*, *Assertion Consumer Service (ACS) URL*, and *Single Logout Service (SLS) URL* fields to a Notepad file. You will use these URLs in To configure AD FS relying party trust: on page 531. Click *Next*.
3. In *Configure Service Provider*, paste the values (i.e. URLs) from Notepad that you retrieved in To retrieve IdP Configuration from AD FS: on page 530 with the following mapping:

FortiSASE	Values copied from AD FS
IdP Entity ID	http://<your-adfs.domain.com>/adfs/services/trust
IdP Single Sign-On URL	https://<your-adfs.domain.com>/adfs/ls/
IdP Single Log-Out URL	https://<your-adfs.domain.com>/adfs/ls/

4. For *SAML Claims Mapping*, in the FortiSASE *Username* field, enter username as copied from AD FS.
5. Disable *SAML Group Matching*.

6. From the dropdown list, select the IdP certificate that was imported into FortiSASE in To export an IdP certificate from AD FS and import it in FortiSASE: on page 528:
7. For *Service Provider Certificate*, select *FortiSASE Default Certificate*.

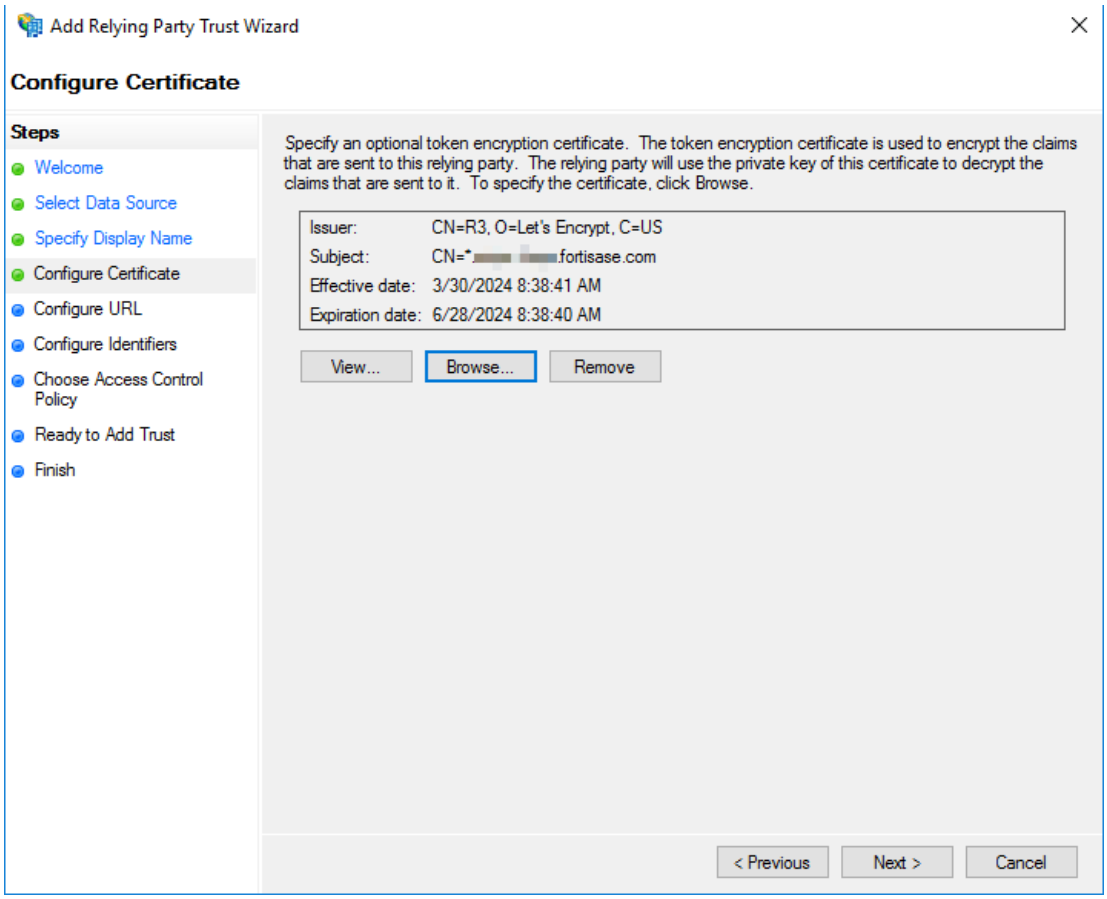
   While configuring *Service Provider Certificate*, the FortiSASE instances that have existing or old SSO configuration, are by default configured with the legacy default certificate (i.e. *Fortinet_Factory*) as its service provider (SP) certificate.

   FortiSASE administrators can change the legacy default certificate (i.e. *Fortinet_Factory*) to use the new *FortiSASE Default Certificate*. Once FortiSASE is configured to use *FortiSASE Default Certificate*, FortiSASE administrators can no longer configure and use the legacy default certificate (i.e. *Fortinet_Factory*). Thus, ensure to update the SP certificate in your IdP configuration. Other FortiSASE instances with fresh SSO configuration have the direct option to use the *FortiSASE Default Certificate* in the *Service Provider Certificate* dropdown menu.

   FortiSASE Default Certificate periodically renews. Thus, if IdPs use *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with the new SP certificate. To avoid updating your IdP configuration frequently, uploading your own certificate is recommended.
8. For *Digest Method*, select *SHA-256*. FortiSASE supports both SHA-1 and SHA-256, but AD FS is by default configured with SHA-256 and Microsoft also recommends this hash algorithm.
9. Click *Next* and then click *Submit*. Click *OK* after reading the Caution prompt.

To configure AD FS relying party trust:

1. On Windows Server, open the *AD FS Management* snap in.
2. Right-click *Relying Party Trust* and select *Add Relying Party Trust*.
3. In the *Welcome* step, select *Claims aware*, then *Start*.
4. In the *Select Data Source* step, select *Enter data about the relying party manually*. Click *Next*.
5. In the *Specify Display Name* step, give the relying party a suitable *Display name* (such as SASE). Click *Next*.
6. (Optional) To encrypt the token claims sent to the relying party (i.e. FortiSASE), in the *Configure Certificate* step, copy the certificate *FortiSASE Default Certificate* downloaded in To export an SP certificate from FortiSASE: on page 530 and move it to Windows Server in a suitable directory. Upload the certificate by clicking *Browse* to navigate to directory. Click *Next*.

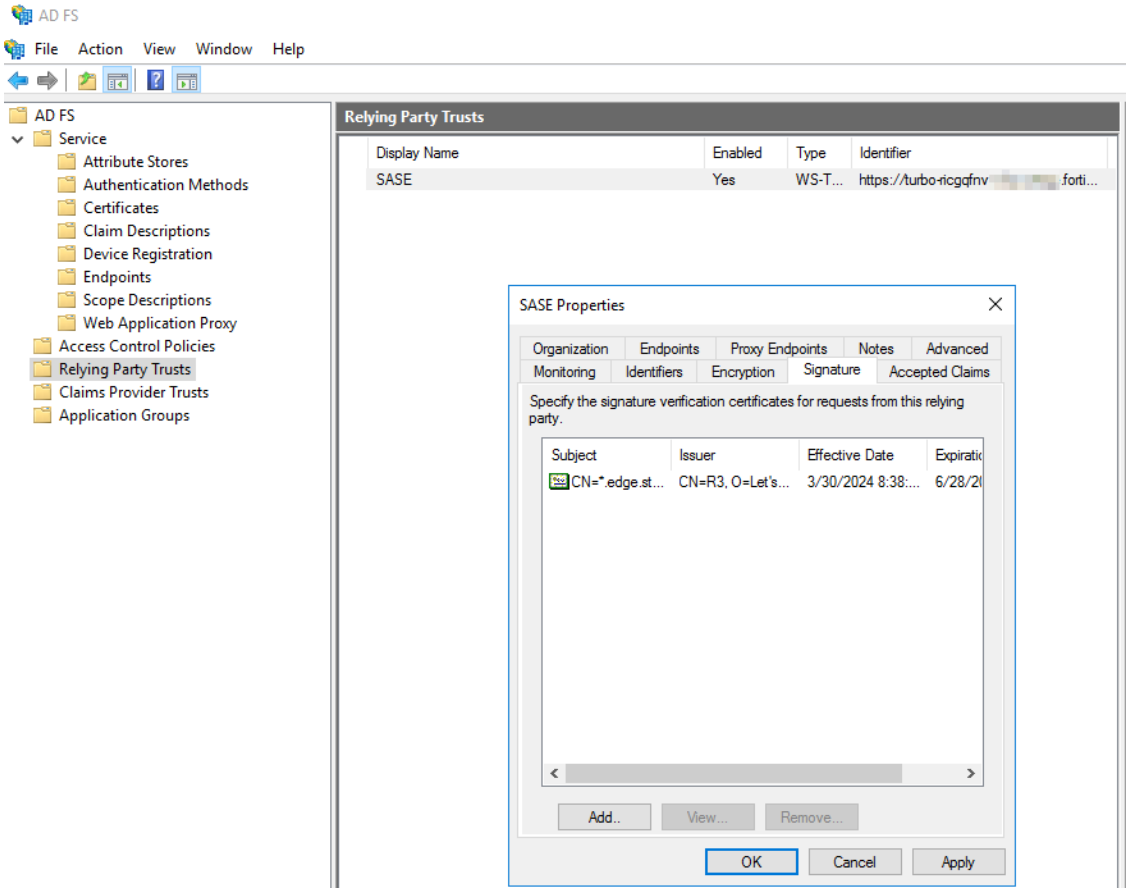


7. In the *Configure URL* step, select *Enable support for the SAML 2.0 WebSSO protocol* and enter the *Assertion Consumer Service (ACS) URL* from To configure AD FS SSO on FortiSASE: on page 530. Click *Next*.
8. In the *Configure Identifiers* step, in the *Relying party trust identifier* field, paste the *Entity ID* value from To configure AD FS SSO on FortiSASE: on page 530. Click *Add*, then *Next*.
9. In the *Choose Access Control Policy* step, *Permit everyone* is selected by default. If desired, restrict the access control policy to a specific group. Click *Next*. In the *Ready to Add Trust* step, click *Next*. In the *Finish* step, click *Close*.

To configure properties of AD FS relying party trusts:

1. On the *AD FS* management snap-in, click *Relying Party Trusts*. Right-click your configured relying party trust and click *Properties*.
2. On the *Signature* tab, click *Add* to go to the folder to add *FortiSASE Default Certificate*.

3. Click *Apply*.

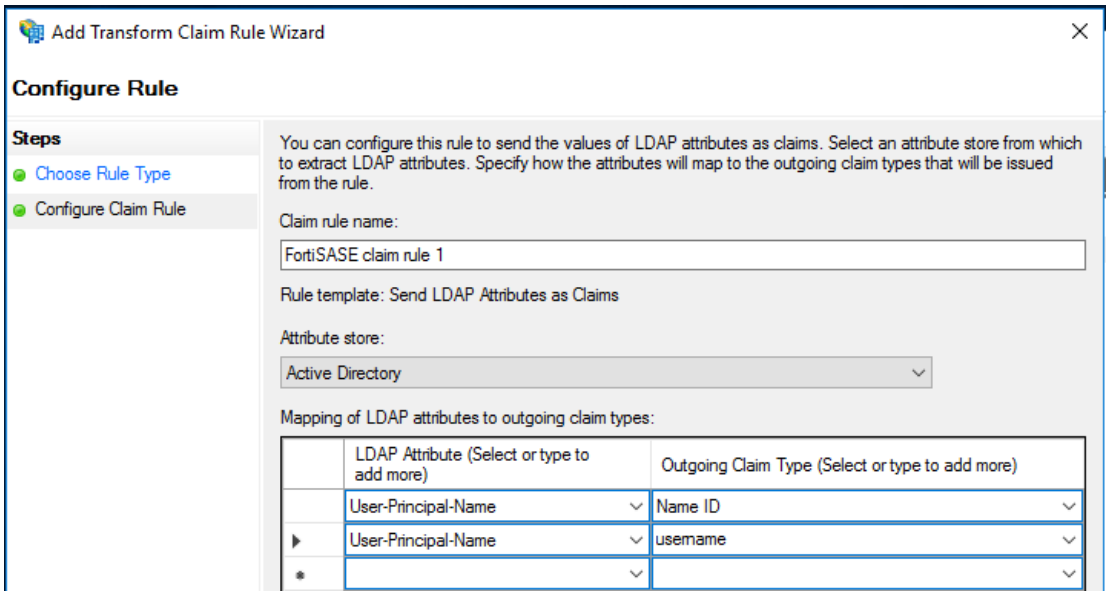


4. On the *Advanced* tab, for *Secure hash algorithm*, select *SHA-256*.
5. Click *OK*.

To configure an AD FS claim issuance policy:

1. On the *AD FS* management snap-in, click *Relying Party Trusts*. Right-click your configured relying party trust and click *Edit Claim Issuance Policy*.
2. In *Issuance Transform Rules*, click *Add Rule*. A new *Add Transform Claim Rule Wizard* opens.
3. For *Choose Rule Type*, in the *Claim rule template*, select *Send LDAP Attributes as Claims* from the dropdown list. Click *Next*.
4. In *Configure Claim Rule*, give a suitable claim rule name.
5. For *Attribute store*, select *Active Directory*.
6. Enter the following claims that FortiSASE supports:

LDAP Attribute	Outgoing Claim Type
User-Principal-Name	Select *Name ID* from the dropdown list.
User-Principal-Name	username. As username is unavailable to select from the dropdown list, enter it manually.



7. Click *Finish*. The claim rule is visible under *Claim Issuance Policy*.
8. Click *Apply*. Click *OK*.

To configure SAML user groups on FortiSASE:

1. On FortiSASE, go to *Access & authentication* > *Access* > *Users and groups*.
2. Click *Create*, select *User Group*.
3. Click *Next*.
4. Enter a suitable *Name* for the group. From the *Remote Groups* table, click *Create*.
5. From the *Remote Server* dropdown list, select *Agent SSO*. You must select *Agent SSO* even if you are using proxy.
6. Click *OK* to save the remote server configuration.
7. Click *OK* to save the user group configuration.
8. Use the user group created inside respective policies for agent-based users or proxy policies for agentless users to authenticate users connecting to FortiSASE using SSO using AD FS. See Policies on page 296 and Proxy policies on page 302.
9. For agentless users, do the following:
   a. Download the PAC file from *Network* > *Proxy configuration*. See Downloading the preconfigured PAC file on page 738.
   b. Customize the PAC file to add IdP URLs to exempt the IdP traffic to flow through FortiSASE. See Customizing the PAC file on page 739.
   c. Configure the proxy setting on your endpoint using the customized PAC file. See Windows on page 744.

While setting up SSO with AD FS or other custom identity providers (IdP) (except Google, Entra ID, FortiTrustID, or Okta) for agentless users, customizing the PAC file to add IdP URLs to it such that the traffic to IdP URLs is not forwarded to the FortiSASE proxy server and instead goes directly to the internet is mandatory. See Customizing the PAC file on page 739.

Configuring FortiSASE with Okta SSO

You can configure a single sign on (SSO) connection with Okta via SAML, where Okta is the identity provider (IdP) and FortiSASE is the service provider (SP). This feature allows end users to connect to a tunnel by logging in with their Okta credentials.

To configure FortiSASE with Okta SSO:

1. In FortiSASE, go to *Access & authentication* > *Authentication Sources* > *SSO*.
2. If *Proxy* or *Authenticated onboarding* is configured, click on the *Agent* tab to ensure *Agent SSO* is being configured.

   The first step of the SSO configuration wizard displays the entity ID, SSO URL, and single logout URL. You use these values to configure FortiSASE as an SP in Okta. Copy these values.
3. Create and configure your FortiSASE environment in Okta.
   a. On the Okta administration page, go to *Applications* > *Applications*.
   b. Click *Create App Integration*.
   c. For *Sign-in method* select *SAML 2.0*.
   d. Click *Next*.
   e. Fill out the fields in *General Settings* and click *Done*.
   f. In *Configure SAML*, copy and paste the SP fields from FortiSASE to Okta:

FortiSASE SAML field	Okta SAML settings configuration field
Entity ID	Audience URI (SP Entity ID)
Assertion Consumer Service (ACS) URL	Single sign-on URL
Single Logout Service (SLS) URL	Used in Show Advanced Settings. See below.
Portal (Sign On) URL	Default RelayState

   g. Click *Show Advanced Settings* and configure these settings:

Field	Value
Response	Signed
Assertion Signature	Signed
Digest Algorithm	SHA256 (default)
Signature Certificate	FortiSASE Default Certificate or your own custom certificate already imported to FortiSASE. Must download from FortiSASE and load it into Okta here.
Enable Single Logout	Enabled
Single Logout URL	Single Logout Service (SLS) URL from FortiSASE
SP Issuer	Entity ID from FortiSASE

h. Click *Next*.
i. In *Feedback*, for *App type* select *This is an internal app that we have created* and click *Finish*.
j. Go to the *Sign On* tab then *Settings* > *Sign on methods*.
   i. Under *Metadata details*, click *More details*.
   ii. Make note of the following Okta fields that you will copy and paste into FortiSASE:

Okta SAML field	FortiSASE SAML settings configuration field
Sign-on URL	IdP Single Sign-on URL
Sign-out URL	IdP Single Log-out URL
Issuer	IdP Entity ID
Signing Certificate	IdP Certificate

   iii. Download the IdP certificate from the provided link in *Signing Certificate*. Save the certificate to your device.
   iv. In *Attribute statements*, go to *Show legacy configuration*:
      i. In *Profile attribute statements*, click *Edit*.
      ii. For *Profile attribute statements*, configure these settings:

Field	Value
Name	username
Name format	Basic
Value	user.login

      iii. For *Group attribute statements*, configure these settings:

Field	Value
Name	group
Name format	Basic
Filter	Matches regex: .*

      iv. Click *Save*.
k. Go to the *Assignments* tab:
   i. From the *Assign* dropdown list, select *Assign to People*.
   ii. In the dialog, assign the desired users to the Okta application.
   iii. From the *Assign* dropdown list, select *Assign to Group*.
   iv. In the dialog, assign the desired groups to the Okta application.

4. Configure the IdP information in FortiSASE:
   a. In FortiSASE, click *Next* in the SSO wizard. Copy and paste the IdP fields from Okta to FortiSASE.

Okta SAML field	FortiSASE SAML settings configuration field
Sign-on URL	IdP Single Sign-on URL
Sign-out URL	IdP Single Log-out URL
Issuer	IdP Entity ID

   b. In *SAML Claims Mapping*, in the *Username* field, enter username. In the *Group Name* field, enter group. Both fields are case-sensitive. If you have configured to use SAML attribute names other than username or group on Okta, you can enter the SAML attribute name in the *Username* and *Group Name* fields accordingly.
   c. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
   d. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click + to add your own custom certificate.
   e. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Okta if *Certificate Verification* is enabled on Okta.
   f. For *Response and assertion signature validity*, select either:
      i. At least one (default): For one of the response or assertion from IdP to be signed and valid.
      ii. Both: For both response and assertion from IdP to be signed and valid.

      This security enforcement feature corresponds to the Okta configuration for the *Response and Assertion* settings in *Advanced Settings* for SAML integration.

      For this example, select *Both* per Okta configuration settings in Step 3.g. above.

      FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE that a well-known public CA signed and remains same across all of your points of presence.

      FortiSASE Default Certificate periodically renews. Thus, if IdPs use *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with the new SP certificate. To avoid updating your IdP configuration frequently, uploading your own certificate is recommended.

5. Review the SAML configuration, then click *Submit*.
6. Invite Okta users to FortiSASE:
   a. (Optional) If you want to define a group of users, create a user group:
      i. Go to *Access & authentication > Access > Users and groups*.
      ii. Click *Create > User Group*.
      iii. In the *Members* field, click +.
      iv. In the *Select Entries* pane, select the desired users to add to this user group.
      v. In the *Remote Groups* field, select *Create*.
      vi. From the *Remote Server* dropdown list, select the desired server.
      vii. In the *Groups ID* field, add the desired group name as it is named in Okta. Click + to add more Group IDs. If needed, click *OK*.
      viii. Click *OK*.
   b. In *Access & authentication > Authentication Sources > SSO*, click *Onboard Users*.

c. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE.
d. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Configuring FortiSASE with FortiAuthenticator Cloud as SAML IdP proxy for Entra ID SSO

FortiAuthenticator Cloud performs the function of a SAML identity provider (IdP) as well as an IdP proxy and enforces multifactor authentication (MFA). FortiAuthenticator Cloud is available for IdP and IdP proxy functionality and FortiToken Cloud for MFA including adaptive authentication.

A use case for IdP proxy is when using multiple IdPs to authenticate different user types. For example, you may authenticate employees using Microsoft Entra ID while contractors use Google Workspace or Okta.

You can configure a single sign on (SSO) connection with FortiAuthenticator Cloud via SAML, where FortiAuthenticator Cloud is the IdP, namely, an IdP proxy, and FortiSASE is the service provider (SP). This feature allows end users to connect to a tunnel by logging in with their corresponding IdP credentials.

This example describes how to set up FortiAuthenticator Cloud as a SAML IdP proxy for Entra ID.

⚠ These steps require FortiAuthenticator Cloud 6.5.0 or later to support the following features to help with compatibility with third-party IdPs:

- **Sends username in this parameter**: specify the parameter name in which the remote IdP receives the username so as to prefill the username login field.
- **Strip realm from username before sending.**

To upgrade to FortiAuthenticator Cloud instance, see the FortiAuthenticator Cloud Release Notes corresponding to your version, specifically, the *Upgrade Information* section.

1. In the Azure portal, do the following:
   a. Create an enterprise application using FortiSASE as a template from the Azure App Gallery and copy its application ID. See To create an enterprise application using FortiSASE as a template from the gallery and find the application ID of the FortiSASE enterprise application: on page 539.
   b. Register the enterprise application with Microsoft identity platform and generate an authentication key. See To register the enterprise application: on page 539.
   c. Add the enterprise application as an assignment. See To add the enterprise application as an assignment: on page 540.
2. In FortiAuthenticator Cloud, do the following:
   a. Enable the SAML IdP service on the publicly facing interface. See To enable SAML IdP service on interface: on page 540.
   b. Create a remote OAuth server with Azure application ID and authentication key. See To create a remote OAuth server: on page 540.
   c. Start to create a remote SAML server. See To partially configure the remote SAML server on FortiAuthenticator Cloud: on page 540.
3. In the Azure portal, configure SAML settings for the FortiSASE application in Azure. See To configure SAML settings for the FortiSASE application in Azure: on page 541 and To collect SAML IdP URL information: on page 541.

4. In FortiAuthenticator Cloud, do the following:
   a. Continue to create a remote SAML server. See To fully configure the remote SAML server on FortiAuthenticator Cloud: on page 541.
   b. Create a realm for domain name. See To create an Azure realm and add it to the IdP: on page 542.
   c. Enable SAML IdP portal. See To enable the SAML IdP portal: on page 542.
   d. Download IdP certificate. See To download the IdP certificate: on page 542.
   e. Start to create a SAML Service Provider (SP) entry for FortiSASE. See To partially configure a SAML SP entry for FortiSASE in FortiAuthenticator Cloud: on page 542.
5. In FortiSASE, configure FortiSASE with FortiAuthenticator Cloud in FortiClient agent-based mode. See Configuring FortiSASE with FortiAuthenticator Cloud in FortiClient agent-based mode on page 543.
6. In FortiAuthenticator Cloud, continue to create a SAML SP entry for FortiSASE. See Configuring FortiAuthenticator Cloud - III on page 544.

Configuring Entra ID

Create a new Entra enterprise application using the FortiSASE application as a template from the Entra app gallery, configure your Microsoft Entra ID environment with users and groups and configure the enterprise application for SAML single sign-on (SSO) for the agent-based deployment.

To create an enterprise application using FortiSASE as a template from the gallery and find the application ID of the FortiSASE enterprise application:

1. Log into the Azure portal.
2. Go to *Microsoft Entra ID* > *Enterprise applications* > *New application*.
3. Search for and select *FortiSASE*.
4. Click *Create*.
5. In *Overview* > *Properties*, copy the application ID. You need this information in a later step.
6. Assign Entra ID users and groups to FortiSASE.

To register the enterprise application:

1. Log into the Azure portal.
2. Go to the directory home, and select *App registrations*.
3. In the *App registrations* window, select *All applications*, and search your application by name.
4. In the list, select your application.
5. Go to *Manage* > *Certificates & secrets*, and select *+ New client secret*.
6. In the *Add a client secret window*, do the following:
   a. In the *Description* field, enter a description for the client secret.
   b. From the *Expires* dropdown list, select a time period after which the client secret expires.
   c. Select *Add*.

> ⚠ In *Client secrets*, make note of the *Value*.
>
> Since this key is visible only once (immediately after creation), you must recreate the key if you do not copy and store it.
>
> Setting up an OAuth server requires the key.

To add the enterprise application as an assignment:

1. Go to the Microsoft Entra ID directory home, and select *Roles and administrators*.
2. From the *Administrative roles* list, select *Directory readers*.
3. Select the ellipsis for *Directory readers*, then select *Description*.
4. Go to *Assignments* and select *Add assignment*.
5. In the *Add assignments* window, search your application by name, and select *Add*.

Configuring FortiAuthenticator Cloud - I

To enable SAML IdP service on interface:

1. In FortiAuthenticator Cloud, go to *System > Administration > Access Rights*.
2. In *Services*, ensure *HTTPS (TCP/443)* is already enabled and enable *SAML IdP (/saml-idp)*.
3. Select *Save* to apply the edits to the network interface.

To create a remote OAuth server:

1. In FortiAuthenticator Cloud, Go to *Authentication > Remote Auth. Servers > OAUTH* and select *Create New*.
2. Enter a name for the remote OAuth server.
3. In the *OAuth source* dropdown list, select *Azure Directory*.
4. In the *Client ID* field, enter the Entra enterprise application ID that you saved previously.
5. In the *Client Key* field, enter the Client secrets *Value* created previously.
6. Select *OK* to add the remote OAuth server.

To partially configure the remote SAML server on FortiAuthenticator Cloud:

1. In FortiAuthenticator Cloud, go to *Authentication > Remote Auth. Servers > SAML*, and click *Create New*. In the *Create New Remote SAML Server* page, configure the following:
   a. Select *Proxy* as the *Type*.
   b. For the *Entity ID*, click the dropdown menu and select the Azure identity provider (IdP) option.
   c. Under *Single Logout*, ensure *Enable SAML single logout* is checked.
   d. Copy these SAML fields:
      - Portal URL
      - Entity ID
      - ACS (login) URL
      - SLS (logout) URL
2. Keep this page open in your web browser since you will continue configuring it after configuring Entra ID.

Configuring SAML settings for the FortiSASE application in Azure

To configure SAML settings for the FortiSASE application in Azure:

1. Log into the Azure portal.
2. Go to *Microsoft Entra ID > Enterprise applications*.
3. Select the enterprise application you created previously.
4. Go to *Set up single sign on*.
5. For the *SSO method*, select *SAML*.
6. In *Basic SAML Configuration*, enter the values that you copied in the FortiAuthenticator Cloud Remote *SAML Server* in these fields:

Microsoft Entra ID > Basic SAML Configuration	FortiAuthenticator Cloud > Edit Remote SAML Server
Identifier (Entity ID)	Entity ID
Reply URL (ACS URL)	ACS (login) URL
Sign on URL	Portal URL
Logout URL	SLS (logout) URL

7. Click *Save* and click *X* to close the window.

To collect SAML IdP URL information:

While still in the SAML-based Sign-on page for the enterprise application you created, in the SAML certificates box, do the following:

1. Download the Certificate (Base64) by clicking *Download* and selecting a file location for downloading the certificate file.
2. Download the Federation Metadata XML by clicking *Download* and selecting a file location for downloading the XML file.

Configuring FortiAuthenticator Cloud - II

To fully configure the remote SAML server on FortiAuthenticator Cloud:

1. Go to the open web browser and continue configuring *Create New Remote SAML Server* in FortiAuthenticator Cloud.
2. Confirm *Type* is still set to *Proxy*.
3. For the *Entity ID*, ensure the Azure identity provider (IdP) option is still selected.
4. Since by this point you have already completed the Entra ID SAML configuration and obtained the IdP metadata file, under *IdP Metadata*, click *Import IdP metadata*, select the Federation Metadata XML file saved previously, and click *OK* to import the file. After importing the XML file, observe that the *IdP entity ID* and *IdP single sign-on URL* fields have been populated accordingly.
5. For *Send username in this parameter*, enter *login_hint*.
6. Ensure *Strip realm from username before sending* is unchecked.

7. In *Single logout*, confirm *Enable SAML single logout* is still checked.
8. In *Group Membership*, select *Cloud* and choose the previously created Azure OAuth server. Update the *Groups* field to match what is configured on the Azure side.
9. Click *OK* to save changes.

To create an Azure realm and add it to the IdP:

1. In FortiAuthenticator Cloud, go to *Authentication > User Management > Realms*.
2. Click *Create New*.
3. Enter the realm name. This should be the domain of the SAML usernames. For example, for usernames such as jsmith@domain.com, the realm name should be set as domain.com.
4. Select the *User source* as the newly created remote SAML authentication server.
5. Click *OK*.

To enable the SAML IdP portal:

1. In FortiAuthenticator Cloud, go to *Authentication > SAML IdP > General*.
2. Enable *SAML identity provider portal*, and enter the following:
   a. *Username input format*: *username@realm (default)*
   b. *Realms*: click *Add a realm* to add the realm associated with the remote server for Azure IdP.
   c. *Default IdP certificate*: select a default certificate to use.
3. Ensure *Legacy login sequence* is disabled.
4. Click *OK* to save changes.

To download the IdP certificate:

1. In FortiAuthenticator Cloud, go to *Certificate Management > End Entities > Local Services*.
2. Click *Export Certificate* to export the certificate being used as the *Default IdP certificate*.
3. In the file browser, choose where to save the file and click *Save*.

To partially configure a SAML SP entry for FortiSASE in FortiAuthenticator Cloud:

1. In FortiAuthenticator Cloud, go to *Authentication > SAML IdP > Service Providers* and create a new reference for the service provider that you will be using as your SAML client.
2. Enter the following information:
   a. *SP name*: enter a name for the service provider (SP) device.
   b. *IdP prefix*: select *+*, enter an IdP prefix in the *Create Alternate IdP Prefix* dialog or select *Generate prefix*, and click *OK*.
   c. *Server certificate*: select the same certificate as the default IdP certificate used in *Authentication > SAML IdP > General*. See Configuring SAML IdP settings.
3. Copy the following information to use for configuring FortiSASE later:
   - IdP entity id
   - IdP single sign-on URL
   - IdP single logout URL
4. Click *Save*.
5. Keep this page open in your web browser since you will continue configuring it after configuring FortiSASE.

Configuring FortiSASE with FortiAuthenticator Cloud in FortiClient agent-based mode

To configure the FortiAuthenticator Cloud IdP information in FortiSASE:

1. In FortiSASE, go to *Access & authentication* > *Authentication Sources* > *SSO*.
2. Copy the following fields from the *Configure Identity Provider* page. You use these fields to complete the FortiAuthenticator Cloud SAML service provider configuration.
   - Entity ID
   - ACS URL
   - SLS URL
3. Click *Next* in the single sign on (SSO) wizard.
4. In the *IdP Entity ID*, *IdP Single Sign-On URL*, and *IdP Single Log-Out URL* fields, paste the corresponding values that you copied from the FortiAuthenticator Cloud *SAML IdP* > *Service Providers* fields.
5. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded from FortiAuthenticator Cloud. Click *Next*.
6. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click *+* to add your own custom certificate.
7. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Azure if *Certificate Verification* is enabled on Azure.

   FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE that a well-known public CA signed and remains same across all of your points of presence.

   FortiSASE Default Certificate periodically renews. Thus, if IdPs use *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with the new SP certificate. To avoid updating your IdP configuration frequently, uploading your own certificate is recommended.

8. Review the SAML configuration, then click *Submit*.
9. Click *OK* to confirm that SSO authentication will take priority over existing LDAP and RADIUS authentication methods.
10. Invite Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) users to FortiSASE:
    a. (Optional) If you want to define a group of users, create a user group:
       i. Go to *Access & authentication* > *Access* > *Users and groups*.
       ii. Click *Create* > *User Group*.
       iii. In the *Members* field, click *+*.
       iv. In the *Select Entries* pane, select the desired users to add to this user group.
       v. In the *Remote Groups* field, select *Create*.
       vi. From the *Remote Server* dropdown list, select the desired server.

vii. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK*.

> FortiSASE cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE as well.

viii. Click *OK*.

b. In *Access & authentication > Authentication Sources > SSO*, click *Onboard Users*.
c. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE.
d. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Configuring FortiAuthenticator Cloud - III

To fully configure a SAML SP entry for FortiSASE in FortiAuthenticator Cloud:

1. Go to the open web browser and continue configuring *Edit SAML Service Provider* in FortiAuthenticator Cloud.
2. In the *SP Metadata* pane, enter the SP information from FortiSASE, which you will use as the SAML SP:

FortiSASE > Access & authentication > SSO	FortiAuthenticator Cloud > Edit SAML Service Provider
Entity ID	SP entity ID
ACS URL	SP ACS (login) URL
SLS URL	SP SLS (logout) URL

3. In *Assertion Attribute Configuration*, configure the following:
   a. Select *Username* from the *Subject NameID* dropdown list.
   b. Select *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified* in *Format*.
4. In *Assertion Attributes*, select *Add Assertion Attribute* and add the following attributes:
   a. SAML attribute: *username*
      User attribute: SAML username
   b. SAML attribute: *groups*
      User attribute: SAML group membership
5. Click *OK* to save changes.

Configuring FortiSASE with FortiAuthenticator as SAML IdP for SSO

In this configuration, FortiSASE relies on SAML for single sign on (SSO) authentication. FortiSASE acts as a SAML service provider (SP) requesting authentication from FortiAuthenticator, which acts as a SAML identity provider (IdP).

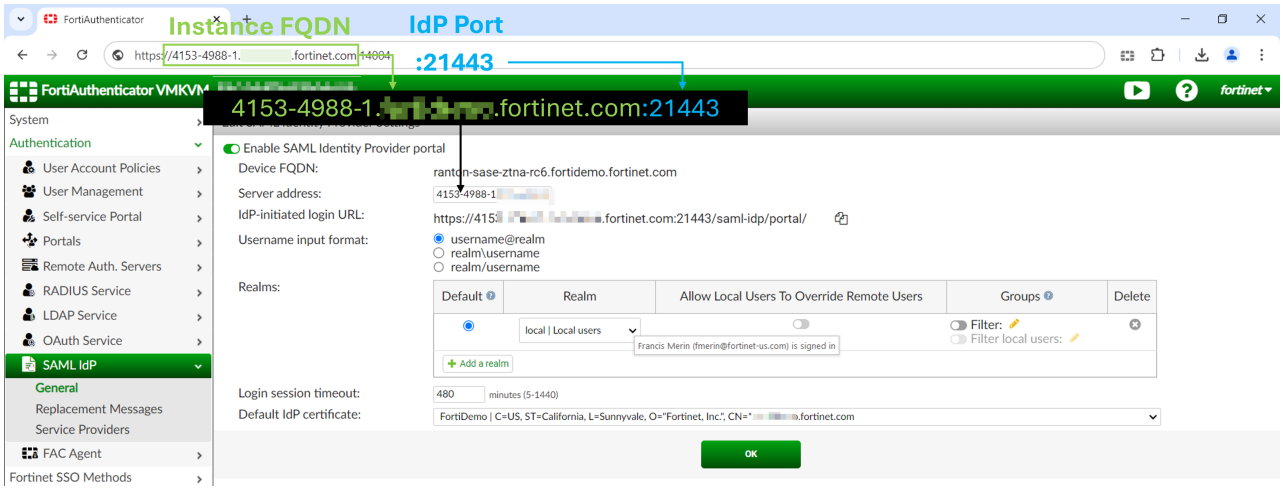
During the authentication process, the SAML SP and IdP must verify each other. This means that they must verify certificates on both ends. FortiAuthenticator has been preloaded with a server certificate signed by a well-known, third-party certificate authority (CA) that the FortiAuthenticator IdP server uses. You must export the SAML IdP certificate from FortiAuthenticator and load it into FortiSASE.

To export the IdP certificate from FortiAuthenticator:

1. Log into FortiAuthenticator.
2. Go to *Certificate Management* > *End Entities* > *Local Services*.
3. Select the active certificate by clicking the left checkbox for the certificate entry in the table and clicking *Export Certificate*.
4. Go to the file location on your local computer and click *Save*.

To configure FortiAuthenticator as SAML IdP:

1. In FortiAuthenticator, go to *Authentication* > *SAML IdP* > *General*.
2. Locate the *instance FQDN* and add the IdP port, in this example 21443, to the end. Enter this address in the *Server address* field.



3. Confirm the default IdP certificate has already been configured as the desired certificate. Click *OK*. You see *Successfully saved SAML Identity Provider Settings* at the top of the window.
4. Go to *Authentication* > *SAML IdP* > *Service Providers*.
5. Click *Create New* to create a new SAML service provider for FortiSASE. See Service providers.
6. In *Edit SAML Service Provider*, observe the following fields:
   - *IdP entity id*
   - *IdP single sign-on URL*

- *IdP single logout URL*

7. Keep this page open in your browser since you will copy values from *Edit SAML Service Provider* to FortiSASE.

To import the IdP certificate into FortiSASE:

1. In FortiSASE, go to *System* > *Certificates*.
2. Click *Import* > *Remote Certificate*.
3. For *Import Remote Certificate*, configure the following settings:

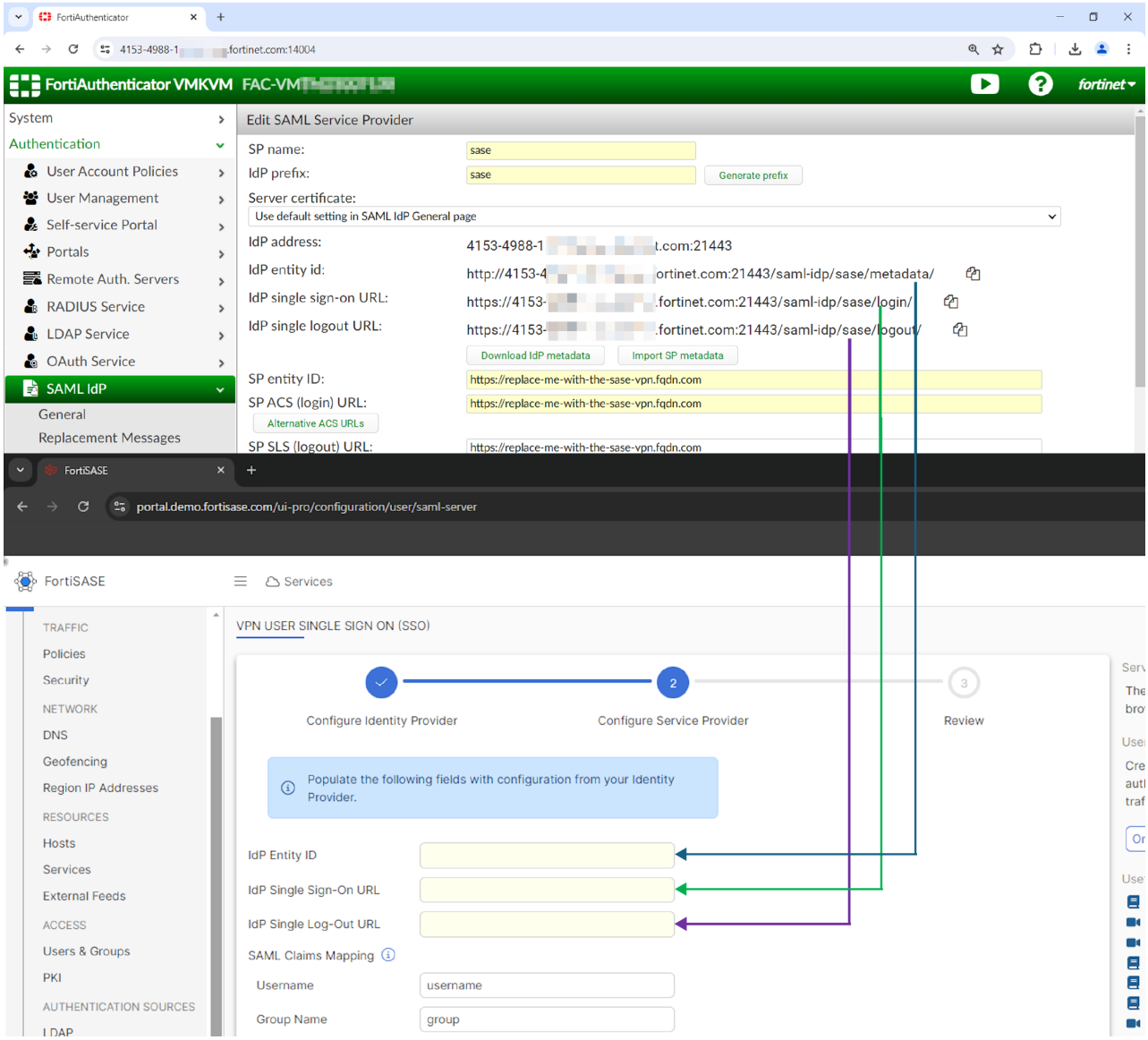
Field	Value
Type	*Remote Certificate*
Certificate File	Click *Upload* and select the saved certificate from the saved file location on your local computer.
Certificate Name	By default, this field contains the certificate file name without the file extension. You can modify it as desired.

4. Click *OK*.

To configure FortiSASE as SAML SP:

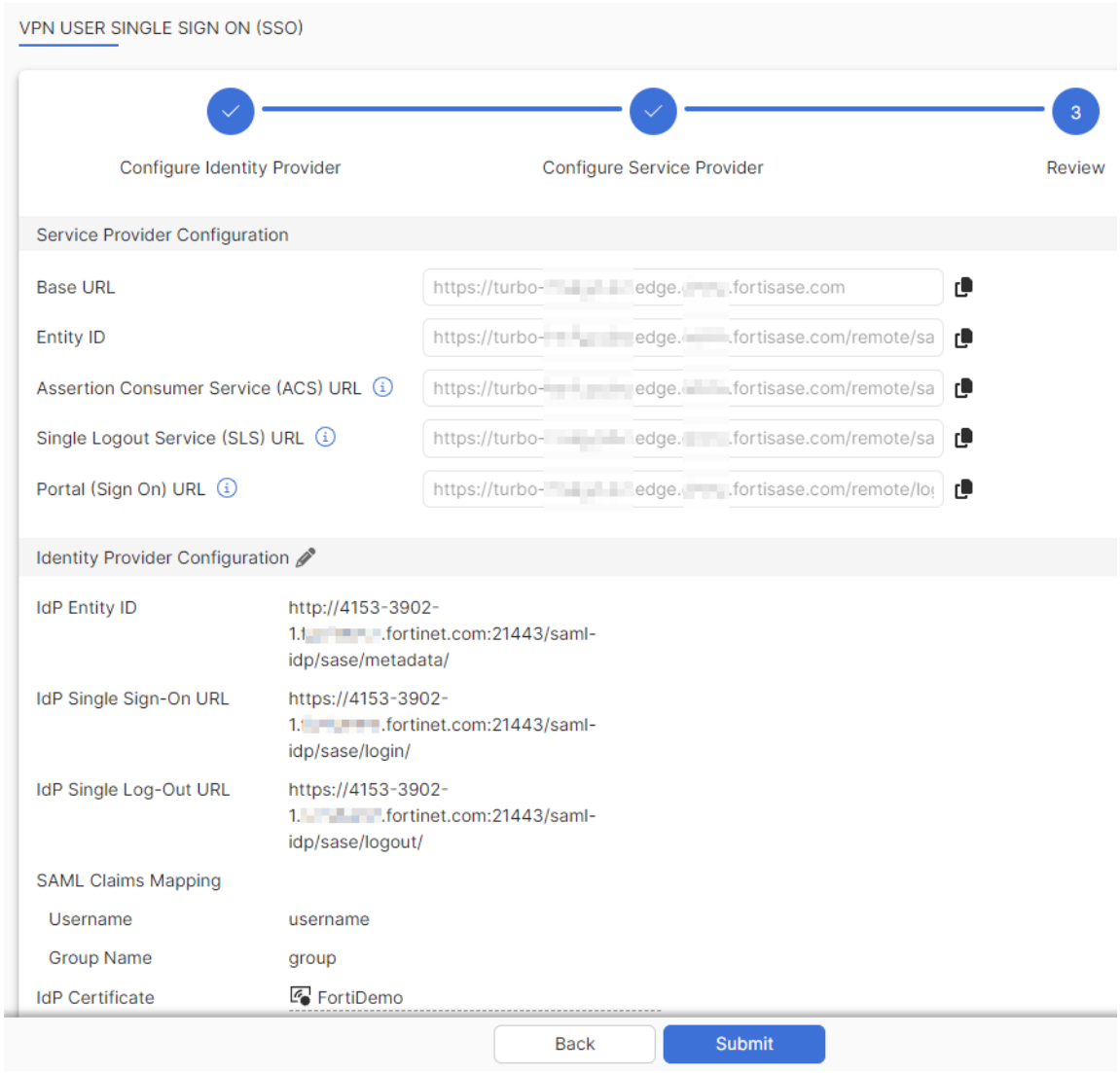
1. In FortiSASE, go to *Access & authentication* > *Authentication Sources* > *SSO*. Click *Next* in the SSO wizard.
2. In *Configure Service Provider*, copy the FortiAuthenticator *SAML IdP* > *Service Providers* fields in the FortiSASE SAML service provider page and paste them into matching IdP fields.

FortiAuthenticator > Edit SAML Service Provider	FortiSASE > Access & authentication > SSO
IdP entity id	*IdP Entity ID*
IdP single sign-on URL	*IdP Single Sign-On URL*
IdP single logout URL	*IdP Single Log-Out URL*



Field	Value
IdP Certificate	Certificate downloaded from FortiAuthenticator
Service Provider Certificate	FortiSASE Default Certificate
Digest Method	Select the desired digest method. SHA-256 is recommended.

3. Click *Next*. For *Review*, click *Submit*.



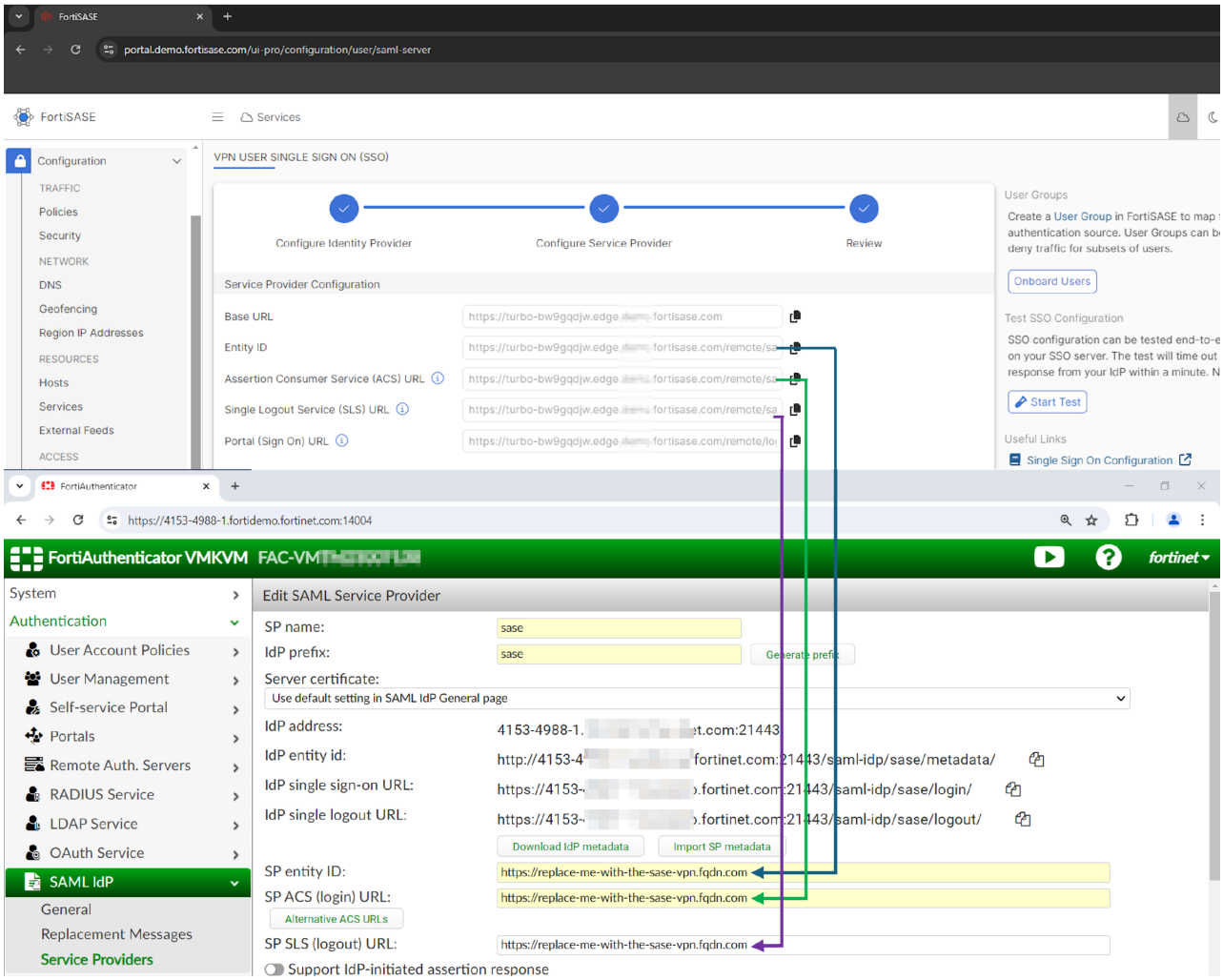
A dialog informs you that SSO authentication takes priority over existing LDAP and RADIUS authentication methods. Click *OK*.

4. In *Service Provider Configuration*, observe the following fields:
   - *Entity ID*
   - *Assertion Consumer Service IdP (ACS) URL*
   - *IdP single logout URL*
5. Keep this page open in your web browser since you will copy values from *Service Provider Configuration* to FortiAuthenticator.

To configure FortiAuthenticator as SAML IdP:

1. Go to the open web browser and continue configuring *Edit SAML Service Provider* for the FortiSASE SAML SP in FortiAuthenticator.
2. Copy the SP fields from FortiSASE, which you will paste in the SAML SP fields. You can replace the placeholder values predefined in the FortiAuthenticator fields:

FortiSASE > Access & authentication > SSO	FortiAuthenticator > Edit SAML Service Provider
Entity ID	*SP entity ID*
ACS URL	*SP ACS (login) URL*
SLS URL	*SP SLS (logout) URL*



3. Click *OK*.

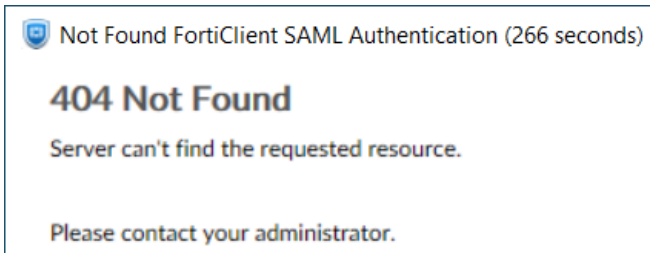
Troubleshooting

After clicking SAML Login, I receive an error when the FortiClient SAML authentication prompt appears. What do the error messages mean and how can I resolve the issues?

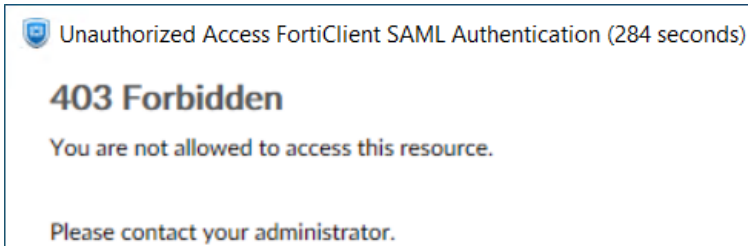
If you have issues with displaying the SAML login prompt from FortiClient, examine the error message:

- A *404 Not Found* error in the SAML login prompt indicates that FortiClient could not successfully access the IdP SSO URL. This error indicates an issue with configuring the *IdP Single Sign-On URL* field in the *Identity*

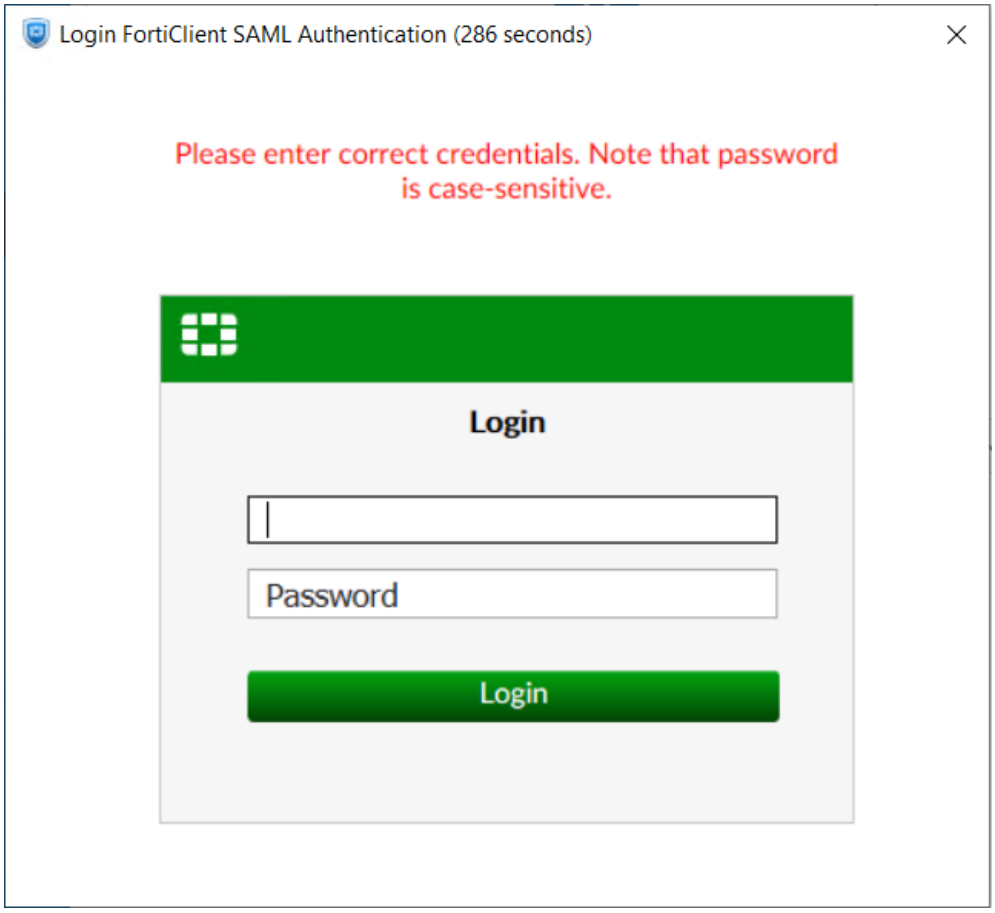
Provider Configuration section of the *SSO > Agent* wizard in FortiSASE.
To resolve this issue, ensure that this field was copied correctly from *Edit SAML Service Provider* on FortiAuthenticator.



- A *403 Forbidden* error in the SAML login prompt indicates that the username provided does not have permission to log into the SP, in this case, FortiSASE. This error indicates an issue with configuring the *SP ACS (login) URL* field in the *Edit SAML Service Provider* page in FortiAuthenticator.
  To resolve this issue, ensure that this field has not been left with the predefined placeholder value *https://replace-me-with-the-sase-vpn.fqdn.com* and is replaced with the correct URL in the *Assertion Consumer Service (ACS) URL* field in the *Service Provider Configuration* section of the *SSO > Agent* wizard in FortiSASE.



After clicking SAML Login, the FortiClient SAML authenticator prompt displays as desired. When I enter my credentials, I see the error message Please enter correct credentials. Note that password is case-sensitive. What does this mean and how can I resolve the issue?



This error message indicates that you entered the username or password incorrectly. To resolve this issue, ensure that you are correctly entering in the credentials.

Considerations

- When using Chrome, ensure that an extra http:// or https:// is not added in these cases:
  - Copying the instance address from the address bar and pasting it to FortiAuthenticator in *Authentication > SAML IdP > General > Server address*
  - Copying the IdP values from FortiAuthenticator and pasting them to IdP fields in FortiSASE in *Access & authentication > Authentication Sources > SSO*
- In FortiSASE, if *SSO* is not visible in the *Access & authentication > Authentication Sources* menu, this indicates that the FortiSASE Endpoint Management Service (EMS) connection failed.

Searching user groups from SAML IdP

From FortiSASE, it is possible to search the user groups on the remote SAML provider configured for agent and proxy SSO by configuring SAML provider credentials in the *Search User Groups from SAML Provider* slide-in window. You can then configure the user groups for SAML group matching. Dynamically discovering a user group from the SAML identity provider (IdP) is more convenient than manually finding a user group's identifier (ID) from the remote SAML provider's portal and configuring it for SAML group matching.

Before you can configure the SAML provider credentials, you must perform some setup and obtain these credentials from the SAML IdP.

Currently, searching user groups from a SAML provider from FortiSASE is supported with Entra ID SSO via *Access & authentication > Authentication Sources > SSO*. See Configuring API permissions and determining Entra ID SSO credentials on page 552 and Searching user groups from Entra ID SSO on page 555.

FortiSASE cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE as well.

Configuring API permissions and determining Entra ID SSO credentials

Before you can autoconnect to a tunnel using Microsoft Entra ID SSO and search user groups from Entra ID single sign on (SSO), you must configure API permissions for autoconnect and group searching, and then determine the SAML provider credentials from the Entra ID portal.

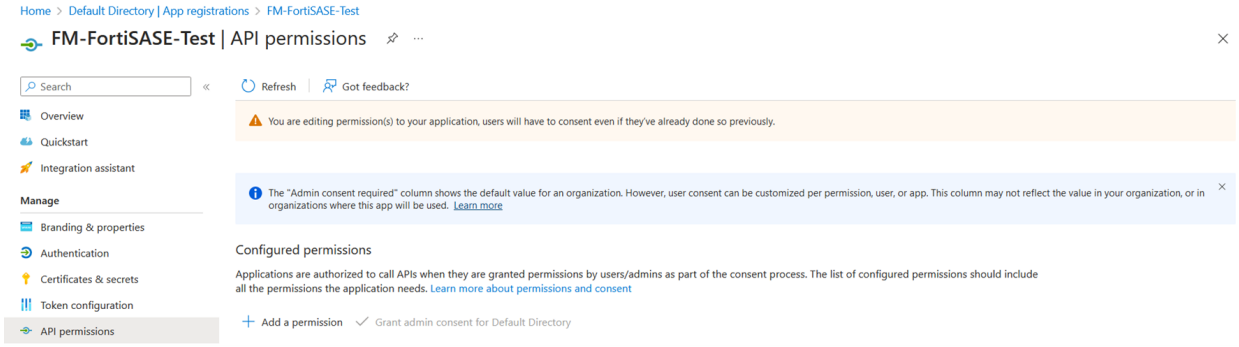
To access the Entra ID portal:

1. Log into the Azure portal. You should already have an enterprise application created in Entra ID. If this has not been created, see Creating an enterprise application using FortiSASE as a template from the gallery and collecting SAML IdP URL information.
2. On the homepage, do one of the following:
   - Under *Azure Services*, click *Microsoft Entra ID*.
   - Click the navigation menu and under *All Services*, click *Microsoft Entra ID*.

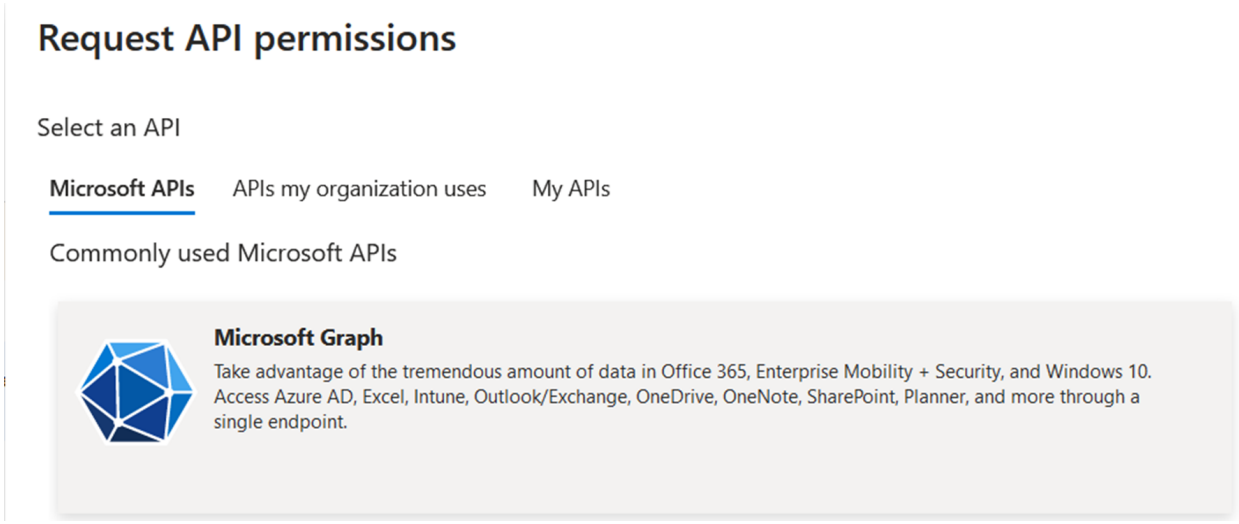
To add Microsoft Graph API application permissions required for autoconnect and searching user groups:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.

3. In the left menu, click *API permissions*, and click *Add a permission*.

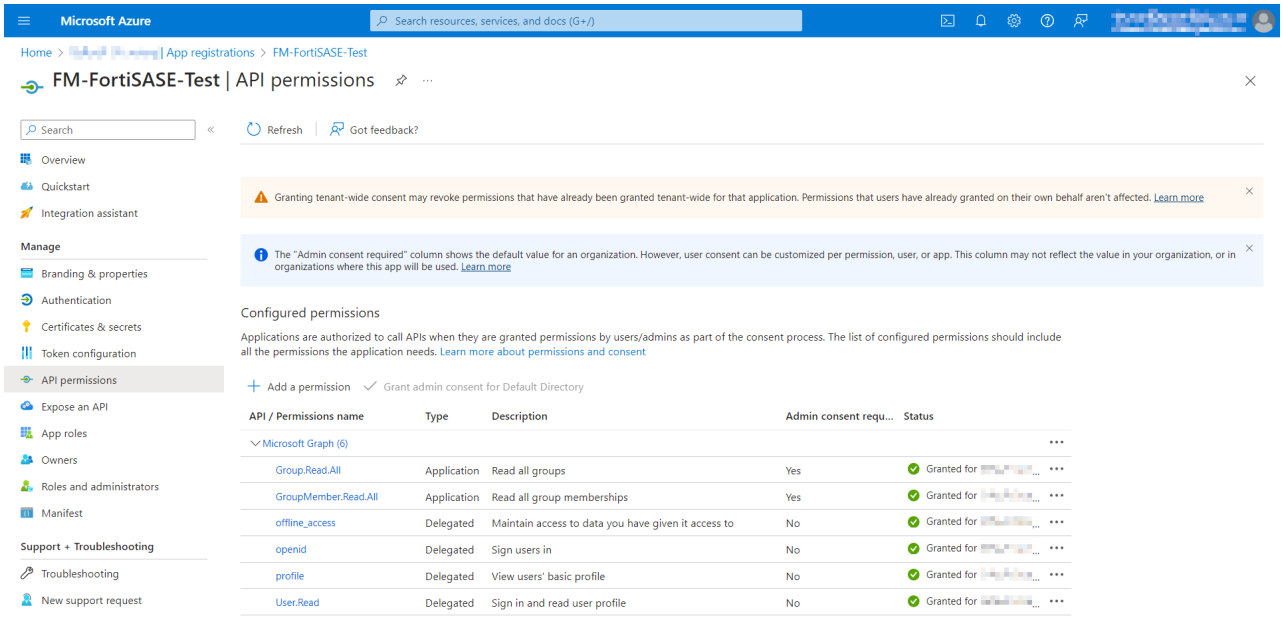


4. In the *Request API permissions* slide-in, click *Microsoft Graph*.



5. Add application permissions:
   a. Select *Application permissions*.
   b. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for group searching:
      - *Group > Group.Read.All – Read all groups*
      - *GroupMember > GroupMember.Read.All – Read all group memberships*
   c. Click *Add permissions*.
6. Add delegated permissions:
   a. Repeat steps 1-4 to add a permission.
   b. Select *Delegated permissions*.
   c. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for autoconnect:
      - *Openid permissions > offline_access – Maintain access to data you have given it access*
      - *Openid permissions > openid – Sign users in*
      - *Openid permissions > profile – View users' basic profile*
      - *User > User.Read – Sign in and read user profile*
7. Click *Add permissions*.
8. In the *API permissions* page, click *Grant admin consent for <domain name>*. If this option is grayed out, you must log into an Entra ID admin account to perform this step. Click *Yes* in the *Grant admin consent*

confirmation prompt. Observe the *Grant consent successful* notification at the top-right. Also, observe the *Status* field shows *Granted for <domain>* for all the permissions added.



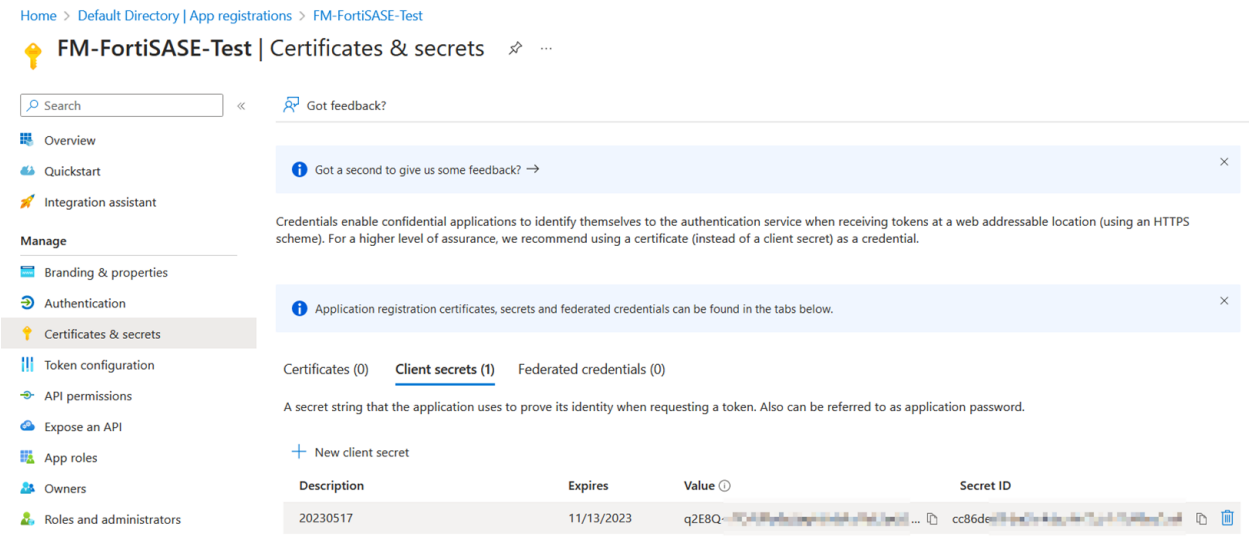
This step is important since it ensures that the administrator grants permissions for the enterprise application from Entra ID instead of end users requiring the administrator to log in to each instance and provide permissions.

Therefore, in summary, you should add the following Microsoft Graph permissions to support the following Entra ID features:

Feature	API permission group	Permission name	Type
Tunnel autoconnect	*OpenId permissions*	*offline_access*	Delegated
	OpenId permissions	*openid*	
	OpenId permissions	*profile*	
	User	*User.read*	
Group searching	*Group*	*Group.Read.All*	Application
	GroupMember	*GroupMember.Read.All*	

To add a client secret string and determine the value of the client secret string:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *Certificates & secrets*, and click *New client secret*.
4. In the *Add a Client Secret* slide-in, add a *Description* and select the *Expires* option of your choice. Click *Add*.
5. Observe that a new client secret has been created. Immediately after creation, ensure you copy the *Value* of the client secret string, which FortiSASE uses as the *Client Secret*. This value is not visible after this initial creation step and moving to another page.



To determine the tenant and client IDs:

1. In the left menu, click *App registrations*, then click *All applications*.
2. Look for your FortiSASE enterprise application name and click the hyperlinked name.
3. In the left menu, click *Overview* and note the following values:
   - *Application (client) ID*, which FortiSASE uses as the *Client ID*
   - *Directory (tenant) ID*, which FortiSASE uses as the *Tenant ID*

Entra ID page within specific enterprise application	Entra ID field	FortiSASE field
Overview	*Directory (tenant) ID*	*Tenant ID*
	Application (client) ID	*Client ID*
Certificates & Secrets	*Value*	*Client Secret*

Searching user groups from Entra ID SSO

After performing preliminary steps and determining the Microsoft Entra ID single sign on (SSO) credentials, you can proceed to configure them in FortiSASE to allow dynamic group discovery from Entra ID SSO and select a group for SAML group matching.

The following example is for searching user groups from Entra ID SSO from FortiSASE for a FortiClient agent-based mode SSO configuration and demonstrates general steps that also apply to a proxy mode SSO configuration.

FortiSASE cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE as well.

To search user groups from Entra ID SSO in FortiClient agent-based mode:

1. Go to *Access & authentication > Authentication Sources > SSO*.
   a. For a new configuration, enter the Entra ID SSO fields.
   b. For an existing configuration, click the pencil icon to the right of *Identity Provider Configuration*.
2. Select *SAML Group Matching* and click *Search*.
3. From the *SAML Provider Type* dropdown list, select *Entra ID*. Next to *SAML Provider Credential*, click *Change*.
4. Enter the Entra ID credentials obtained from the Entra ID portal:
   - *Tenant ID*
   - *Client ID*
   - *Client Secret*
5. Click *OK* to save the credentials.
6. Click *Select group* next to *SAML Remote User Groups* and notice that FortiSASE dynamically obtains the groups from Entra ID and populates the field. Select a remote user group from the table and click *OK* to save the changes.
7. Notice that the *Configure Service Provider* page has the *Group Name* automatically filled in with the selected user group name. Click *Next* to advance this page and click *Submit* on the *Review* page to submit the agent SSO configuration settings.

Testing SSO configuration from FortiSASE

From FortiSASE, you can test the single sign on (SSO) configuration settings end-to-end by logging into a user account configured on your SSO server. This feature allows you to open a popup test window that points to the SSO login page.

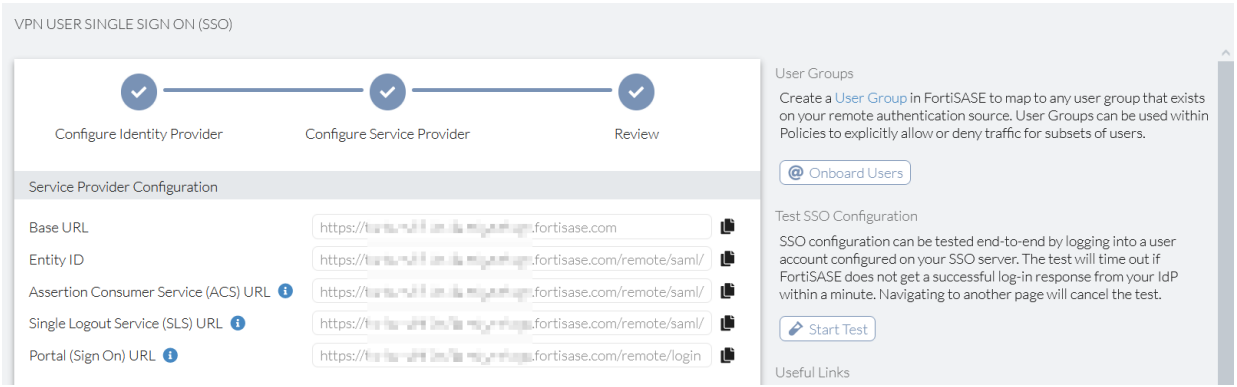
This test provides SSO configuration test results and raw log output of SAML debug from the security PoP that can help you troubleshoot issues with any misconfigured SSO configuration settings.

The example is for testing a Microsoft Entra ID SSO configuration and demonstrates general steps that also apply to Okta SSO.

To test SSO configuration from FortiSASE using Entra ID SSO:

1. Go to *Access & authentication > Authentication Sources > SSO*. Ensure that you configured Entra ID SSO and that you clicked *Submit* at the end of the configuration steps. For details, see Configuring FortiSASE with Microsoft Entra ID SSO in FortiClient agent-based mode on page 517.

2. In right-hand gutter, click *Start Test*.

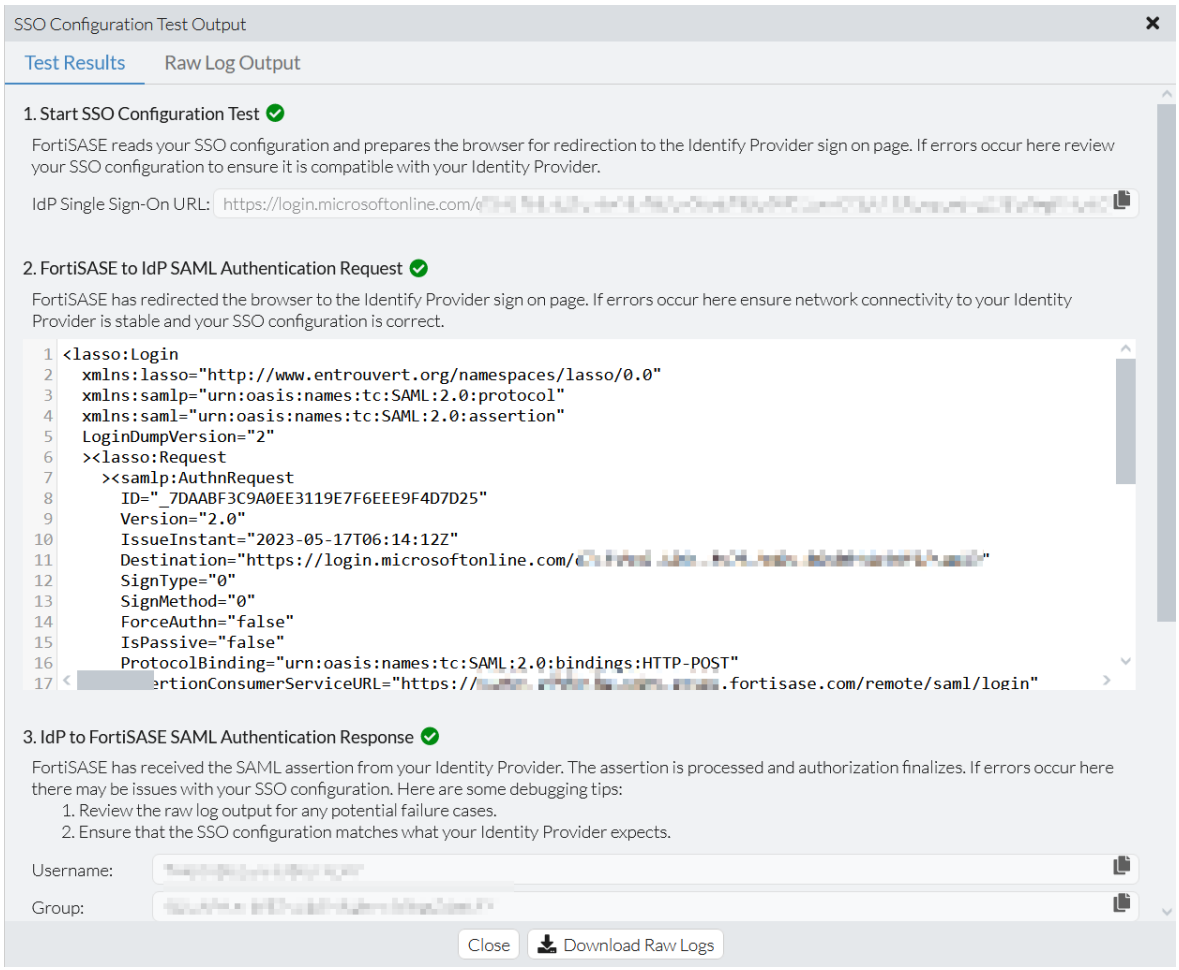


3. A popup from the SSO provider prompts for login information. This is the user account that has already been set up on the SSO server that you want to use for the test. When prompted, enter the username and password of the user account to use for the test.

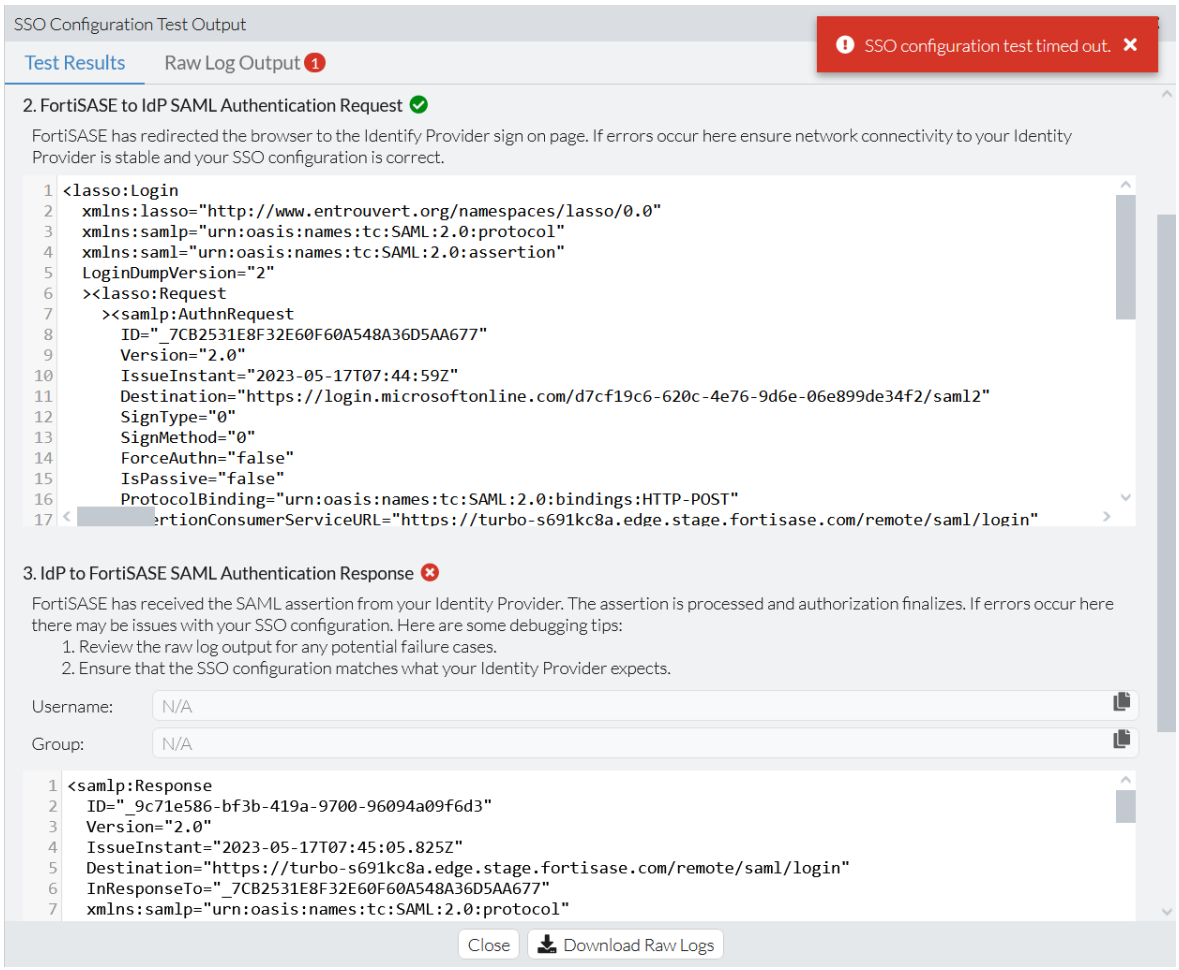
> Ensure that you enter the username and password of the user account within one minute. The test times out if FortiSASE does not get a successful login response within a minute with the error message *SSO configuration test timed out*.

4. You see that the notification *SSO configuration verified successfully* displays in the right-hand gutter when the SAML connection test succeeds. If the test fails, one of the following error messages displays:
   - *Failed to trigger SSO configuration test.*
   - *SSO configuration test timed out.*
   - Within one minute of starting the test, the *SSO Configuration Test Output* slide-in window appears.
     i. In the *Test Results* tab, you see the corresponding icons that help you to narrow down your SAML troubleshooting steps:
        - Green checkmark next to test steps that succeeded
        - Red X next to test steps that failed, which suggests issues with the SSO configuration. The window displays debugging/troubleshooting steps when this occurs.

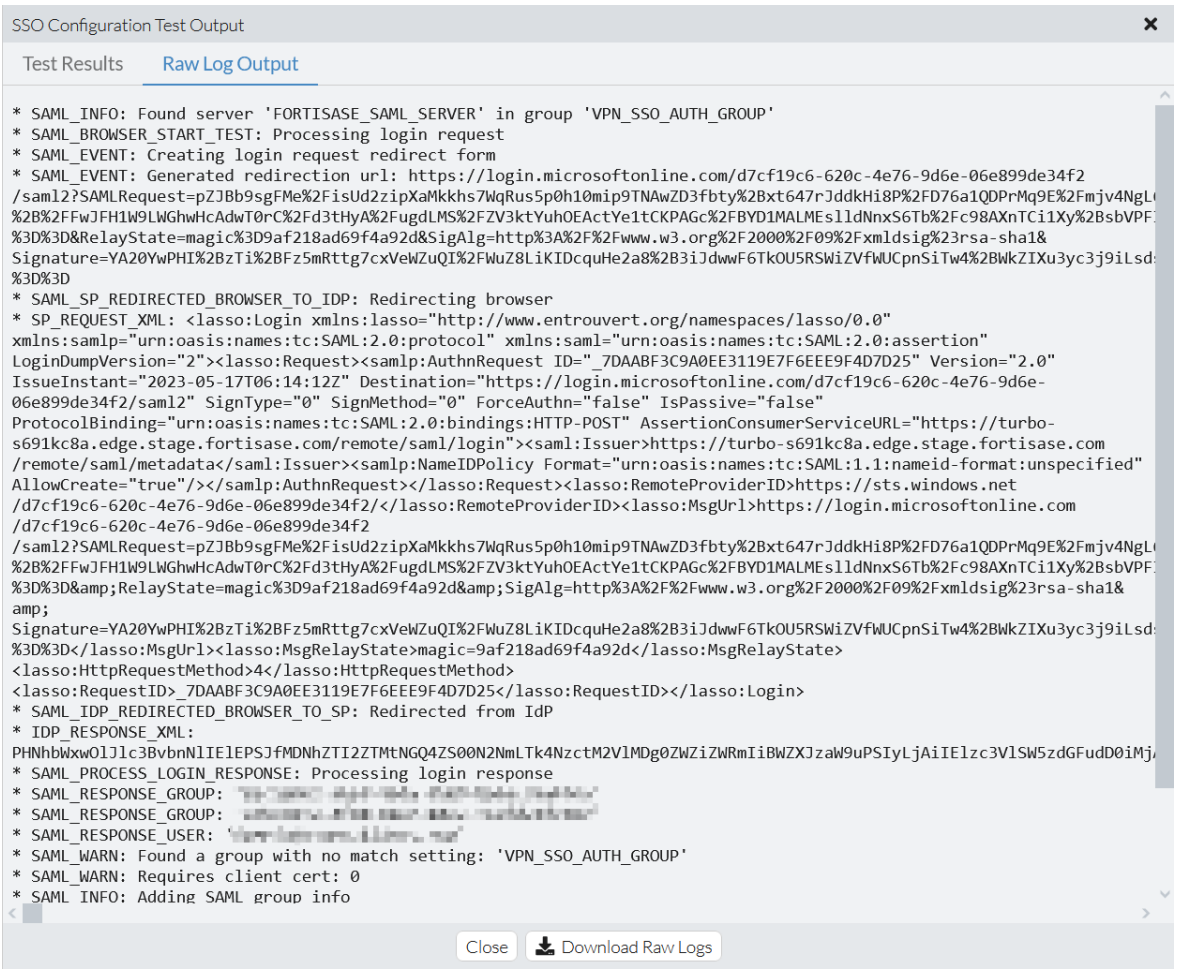
     The following shows an example *Test Results* tab with successful test steps.



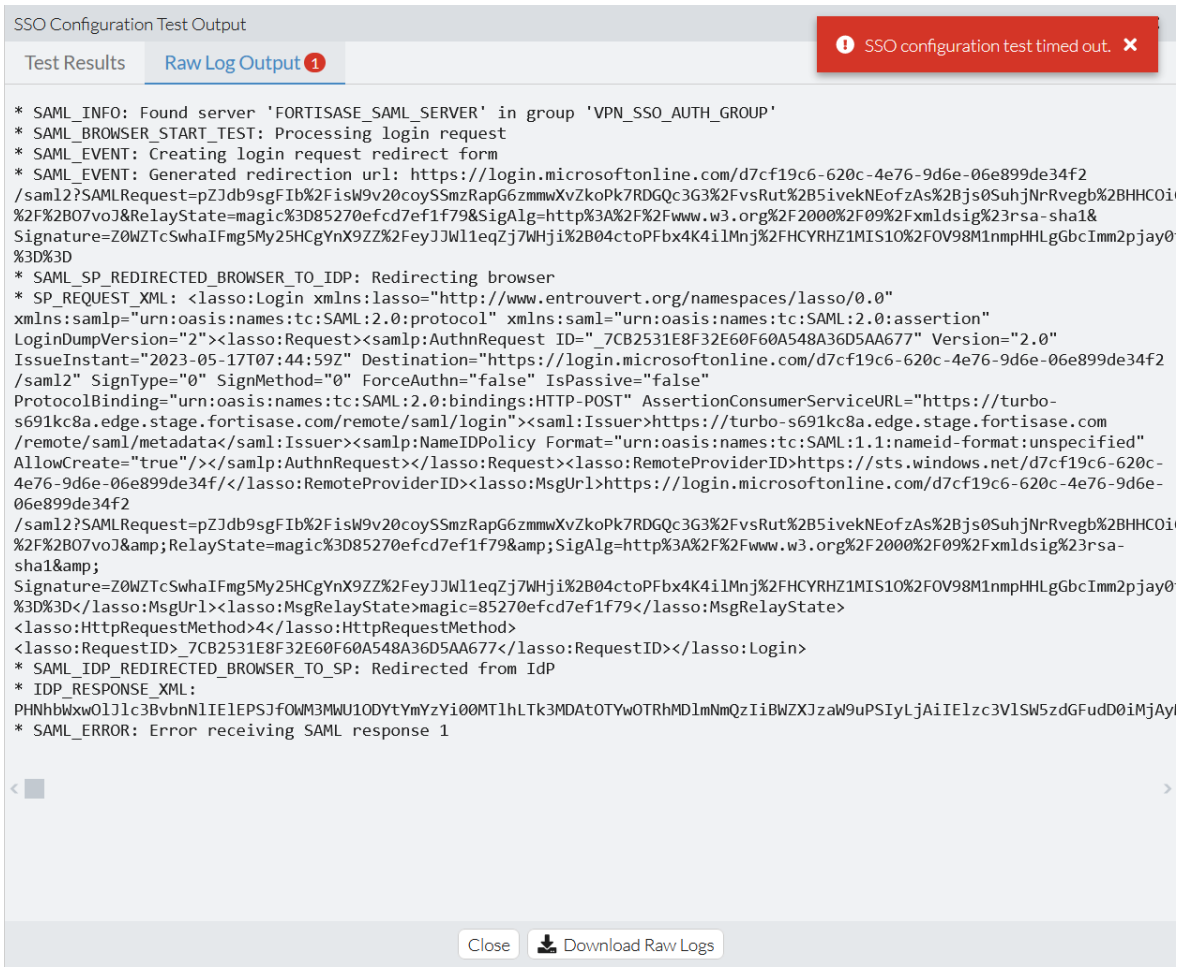
The following shows an example *Test Results* tab with a failed test step that an identity provider entity ID misconfiguration caused.



ii. In the *Raw Log Output* tab, observe the SAML debug raw log output from the security point of presence with sensitive information removed. The following shows an example of the *Raw Log Output* tab with successful test steps.



The following shows an example *Raw Log Output* tab with a failed test step that an identity provider entity ID misconfiguration caused.



Notice the number next to the *Raw Log Output* tab title indicating the number of error messages in the output. See the *SAML_ERROR: Error receiving SAML response 1* as the last line of the output.

Prerequisites and considerations

Prerequisites

- Testing single sign on (SSO) configuration from FortiSASE via the *Start Test* button in *Access & authentication > Authentication Sources > SSO* is only visible and supported in FortiSASE instances with SSL remote agent connectivity.
- When using the Chrome web browser for testing SSO configuration, you must disable *TLS 1.3 hybridized Kyber support* via *chrome://flags* for this test to work.
- Testing SSO configuration from FortiSASE supports FortiClient agent-based mode using Microsoft Entra ID SSO or Okta SSO via *Access & authentication > Authentication Sources > SSO*.
- Ensure that you disable or exempt any web browser popup blockers to allow popups for the *Access & authentication > Authentication Sources > SSO* page prior to clicking *Start Test*. Otherwise, you see the error message *Failed to trigger SSO configuration test* and the test SSO configuration feature does not work as desired.

Considerations

Ensure that the web browser remains on the *Access & authentication* > *Authentication Sources* > *SSO* page for the test duration. Going to another page cancels the test.

Authenticated onboarding

This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

FortiSASE cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE as well.

FortiSASE enhances security during managed endpoint client onboarding by enforcing user authentication via SAML SSO, ensuring only authenticated users and endpoints can register. This prevents unauthorized endpoints, even those with a valid invitation code to connect to FortiSASE Management service. For details on client onboarding using Invitation code, see Client onboarding on page 730 and Managed endpoint client onboarding on page 731.

In this process, the FortiSASE Management service functions as the SAML Service Provider (SP) and integrates seamlessly with other SAML Identity providers (IdPs), including FortiAuthenticator, Okta, and Entra ID.

Once the feature is configured, following updates take effect:

- **New invitation code generation**: FortiSASE generates a new invitation code for endpoints to connecting to FortiSASE Management service, replacing previously issued invitation codes. This ensures that only endpoints that are authenticated via configured SAML IdP can connect.
- **Automatic migration to use new invitation code**: All currently managed endpoints are automatically migrated to use the new invitation code, reducing administrative overhead and ensuring a smooth transition.
- **Updated Pre-configured Installers**: Pre-configured FortiClient installers available for download from the FortiSASE Management portal are automatically updated with the latest invitation code. Organizations using these installers for bulk deployment must ensure they distribute the latest versions.
- **Enterprise Mobility management considerations**: If your organization deploys endpoints using an Enterprise Mobility Management (EMM) solution, such as Microsoft Intune, you must update the configurations to reflect the new FortiClient installer. For details, see Enterprise mobility management on page 752.
- **Re-authentication required for existing endpoint**: All previously registered endpoints are prompted and required to re-authenticate with FortiSASE. This ensures that only authorized users and devices remain connected to FortiSASE Management service.

Starting in 25.4.b Feature, authenticated onboarding can be used with endpoints with users authenticated using an Entra ID account by enabling *Include associated domain*, selecting an Entra ID domain, and adding a *Domain identification claim*.

- If authenticated onboarding was enabled prior to 25.4.b Feature, then to enable *Include associated domain* you must first delete the existing authenticated onboarding configuration and then reconfigure the feature fully.

The example below uses Microsoft's Entra ID as IdP to configure authenticated onboarding. Review following tables to understand how Entra ID's basic SAML configuration fields map to FortiSASE SAML fields.

- **Mapping FortiSASE SAML fields to Entra ID fields**: When configuring Entra ID as the IdP, the following fields are required to be copied from SAML fields from FortiSASE's *Configure Identity Provider* step, and be configured in respective fields in Entra ID, as shown below:

FortiSASE SAML field	Entra ID Basic SAML configuration field
Entity ID	*Identifier (Entity ID)*
Assertion Consumer Service (ACS) URL	*Reply URL (Assertion Consumer Service URL)*
Single Logout Service (SLS) URL	*Logout Url (Optional)*
Portal (Sign On) URL	*Sign on URL*

- **Mapping Entra ID SAML fields to FortiSASE fields**: When configuring FortiSASE as the SP, the following fields required to be copied from SAML fields of Enterprise application > Single sign-on, and be configured in respective fields for FortiSASE's *Configure Service Provider* step.

FortiSASE SAML field	Entra ID Basic SAML configuration field
IdP Entity ID	*Microsoft Entra Identifier*
IdP Single Sign-On URL	*Login URL*
IdP Certificate	*Certificate (Base 64)* Available to be downloaded from Azure application under *SAML Certificates* section.

To configure authenticated onboarding with Entra ID as IdP:

1. In FortiSASE, go to *Access & authentication > Authentication Sources > SSO > Authenticated onboarding*.
2. For *Configure Identity Provider* step, configuration wizard displays the *Entity ID*, *Assertion Consumer Service (ACS) URL*, and *Portal (Sign On) URL*. You use these values to configure FortiSASE as an SP in Azure portal. Copy these values.
3. (When using authenticated onboarding with endpoints with users authentication using an Entra ID account only) Enable *Include associated domain*, click *+*, and select an Entra ID domain previously configured through *Access & authentication > Authentication Sources > Domains*. See Entra ID domains on page 581.

   This step allows an endpoint profile configured with a matching AD group from the domain to be assigned to matching endpoints with users authenticated using an Entra ID account.

   If authenticated onboarding was enabled prior to 25.4.b Feature, then to enable *Include associated domain* you must first delete the existing authenticated onboarding configuration and then reconfigure the feature fully.

   a. For *Domain identification claim*, make note of the default claim name of username or change it to a claim name of your choosing.

   b. As mentioned in the inline message, the following claim must be added on your Identity Provider (Entra ID):
      - Name: *username*
      - Source Attribute: *user.localuserprincipalname*
4. Click *Next* to move to *Configure Service Provider* section and keep this page open.
5. Create and configure an Enterprise application on Azure for FortiSASE:
   a. In the Azure portal, go to *Microsoft Entra ID > Enterprise applications > New application*.
   b. Search for and select *FortiSASE*.
   c. Click *Create*.
   d. Go to *Users and groups* to assign Entra ID users and groups to authenticate remote FortiClient users against it.
   e. Select *Single sign on* and for the SSO method, select *SAML*.
   f. In *Basic Configuration*, enter the values that you copied in step 1 in the *Identifier (Entity ID)*, *Reply URL (Assertion Consumer Service URL)*, *Sign on URL*, and *Logout URL* fields. Click *Save*.
6. Obtain the IdP information from Azure:
   a. The *SAML Signing Certificate* box contains links to download the SAML certificate. Download the certificate.
   b. The *Set up <Enterprise-application-name>* box lists the IdP information that you must provide to FortiSASE. Copy the values in the *Login URL*, *Entra ID Identifier* fields.
7. Configure IdP information in *Configure Service Provider* section on FortiSASE:
   a. In the *IdP Entity ID*, *IdP Single Sign-On URL* fields, paste the values that you copied from the *Entra ID Identifier*, *Login URL* respectively.
   b. From the *IdP Certificate* dropdown list, select *+*, then upload the certificate that you downloaded in step 5.a.
8. Click *Next*.
9. Review the SAML configuration.
10. Click *Submit*.
11. In the warning prompt, click *Continue*.
12. (When using authenticated onboarding with Entra ID-joined endpoints only) Upon successful configuration of authenticated onboarding, the following inline message is displayed at the top of the page:

    Authenticated onboarding enabled and invitation code has been updated. Previously onboarded endpoints will be migrated to the new invitation code on their next reboot. The legacy invitation code is still valid in case of migration errors. Once migration is complete, delete the legacy invitation code.

    If migration of endpoints has been completed, you can delete the legacy invitation code by clicking the *Delete legacy invitation code* button that follows the inline message above.

SCIM server support

FortiSASE supports acting as a System for Cross-domain Identity Management (SCIM) server for automated user provisioning from Entra ID, FortiAuthenticator, and Okta SAML IdPs. The SCIM client (IdP) sends user and group information to the SCIM server (FortiSASE as SP).

Prerequisites

- SCIM server support is a select availability feature. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
- Only available for FortiSASE instances enabled with IPsec remote agent support.
- Not supported in instances with hybrid IPsec/SSL enabled.

The following subtopics cover the following supported SCIM clients:

- Configuring Entra ID as SCIM client on page 565
- Configuring FortiAuthenticator as SCIM client on page 569
- Configuring Okta as SCIM client on page 574

Configuring Entra ID as SCIM client

Entra ID can be configured as a SCIM client for FortiSASE as a SCIM server.

This example demonstrates how to configure Entra ID as a SCIM client by creating a new enterprise application that supports SCIM integration.

Prerequisites and considerations

Prerequisites

- The default FortiSASE enterprise application template available in the Microsoft Entra gallery does not support SCIM integration. You must create a new application using the *+Create your own application* wizard with the *Integrate any other application you don't find in the gallery (Non-gallery)* option.
- Creating your own application requires configuring the *User Attributes & Claims*, namely, for username and group. See Configuring FortiSASE with Microsoft Entra ID SSO: SAML configuration fields on page 515.

Considerations

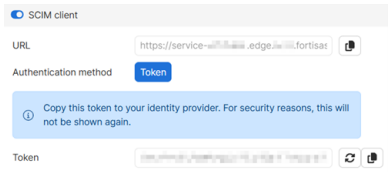
- Currently, FortiSASE does not support these SCIM synchronization operations upon user or group deletion in Entra ID:
  - When a user is deleted from Entra ID, the user remains enabled in local SCIM user groups that it is a member of in FortiSASE. However, policy is not enforced on this user.
- Since the default *FortiSASE* enterprise application template available in the Microsoft Entra gallery does not support SCIM integration, you can use a new Entra ID custom app for SCIM only. Users and groups from that app will sync to FortiSASE without replacing the existing IdP configuration.
- When a previously assigned user has been removed and then added back to the Entra ID application, FortiSASE should match a policy when this user is part of a local SCIM user group specified as the source in the policy.
  - To support this use case, you must configure the the Entra ID provisioning settings with the *aadOptscim062020* feature flag in the *Tenant URL* field. See Flags to alter the SCIM behavior.
  - For example, when the SCIM server URL is *https://service-a1bcd2ef.edge.prod.fortisase.com:44559/fortisase_saml_server_scim/scim/v2*, then you must configure *https://service-a1bcd2ef.edge.prod.fortisase.com:44559/fortisase_saml_server_*

scim/scim/v2/?aadOptscim062020 in the *Tenant URL* field.

- When a user is soft-deleted in Entra ID, the object ID is added to the username in Entra ID. Upon the next SCIM synchronization event to FortiSASE, the synchronized username will be displayed in FortiSASE with the appended ID.
  - To ensure the object ID is not appended to the username, if the user is no longer needed, delete it permanently from Entra ID through *Entra ID > Users > Deleted users*.
  - Alternatively, wait for the user to be automatically deleted permanently by Entra ID in 30 days. In the meantime before the permanent deletion, note the above behavior is expected.

To configure Entra ID as SCIM client:

1. In FortiSASE, go to *Access & authentication > Authentication Sources > SSO*.
2. If *Proxy* or *Authenticated onboarding* are configured, click the *Agent* tab to ensure *Agent SSO* is being configured.
3. Click the pencil icon next to *SCIM client* to edit these settings.
   a. Enable *SCIM client*.
   b. Click the copy button next to the text field to the right of *URL* to copy the SCIM server URL to be used in Entra ID. Paste this URL to a document or text file for later use.
   c. Click the regenerate button next to the text field to the right of *Token* to generate a new token. Click the copy button to copy the token. Paste this token to a document or text file for later use.



   Copy this token to your identity provider. For security reasons, this will not be shown again.
4. Click *Next*.
5. Click *Submit*.
   Once the SSO configuration has been saved, observe the *Token* text field now contains *ENC XXXX* which is expected for security reasons.
6. Configure a new enterprise application with SCIM integration since the default FortiSASE template does not currently support SCIM integration.
   a. In the Entra ID portal, go to *Microsoft Entra ID > Enterprise applications > New application*.
   b. Click *+Create your own application*.
      i. Enter a name for your app. This is an arbitrary value that is used to reference the enterprise application in your Entra environment.
      ii. Select *Integrate any other application you don't find in the gallery (Non-gallery)*.
      iii. Click *Create*.
   c. Go to *Microsoft Entra ID > Enterprise applications* and select your newly created application.
   d. From *Manage > Users and groups*, assign users and groups to the enterprise application by searching for specific users and groups, selecting them and clicking *+Add user/group*.
   e. Creating your own application requires configuring the *User Attributes & Claims*, namely, for username and group. See Configuring FortiSASE with Microsoft Entra ID SSO: SAML configuration fields on page 515.

f. Configure the enterprise application and FortiSASE for SSO using Entra ID. See Configuring FortiSASE with Microsoft Entra ID SSO in FortiClient agent-based mode on page 517.

7. Initially configure SCIM integration on the newly created enterprise application.
   a. Go to *Microsoft Entra ID > Enterprise applications* and select your newly created application.
   b. Click *Manage > Provisioning*.
   c. In the *Overview (Preview)* page, click *+New configuration*.
   d. In the *New provisioning configuration* page, configure these settings:

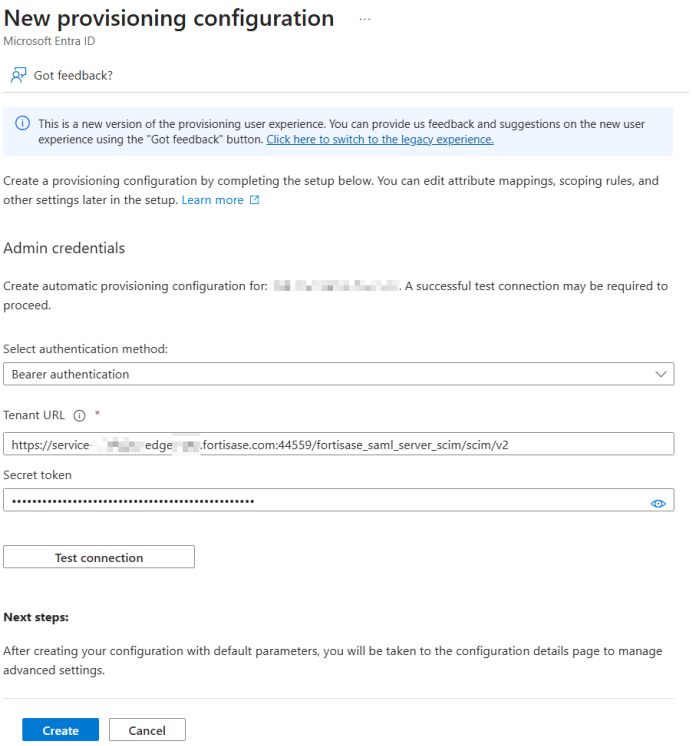
Field	Value
Select authentication method	*Bearer authentication*
Tenant URL	Paste the SCIM server URL copied from FortiSASE here. In this example, use *https://service-a1bcd2ef.edge.prod.fortisase.com:44559/fortisase_saml_server_scim/scim/v2*.
Secret token	Paste the token copied from FortiSASE here.



When a previously assigned user has been removed and then added back to the Entra ID application, FortiSASE should match a policy when this user is part of a local SCIM user group specified as the source in the policy.

- To support this use case, you must configure the the Entra ID provisioning settings with the *aadOptscim062020* feature flag in the *Tenant URL* field. See Flags to alter the SCIM behavior.
- For example, when the SCIM server URL is *https://service-a1bcd2ef.edge.prod.fortisase.com:44559/fortisase_saml_server_scim/scim/v2*, then you must configure *https://service-a1bcd2ef.edge.prod.fortisase.com:44559/fortisase_saml_server_scim/scim/v2/?aadOptscim062020* in the *Tenant URL* field.

   e. Click *Test connection*.

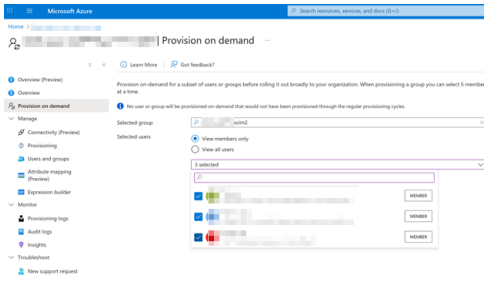


f. After the test succeeds, click *Create*.

g. Click *Start provisioning* and click *Yes* in the resulting dialog to enable synchronization using SCIM. Entra ID periodically synchronizes users and groups assigned to the application.

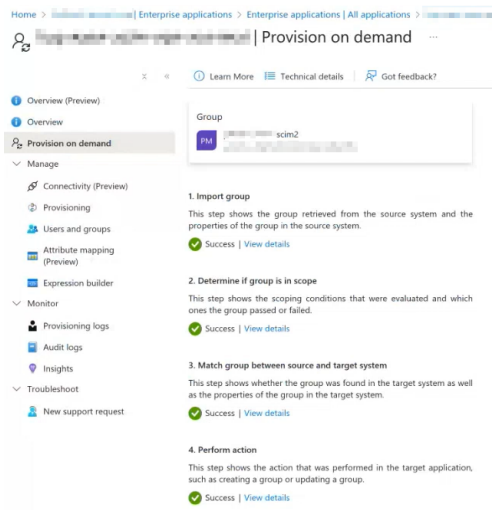
8. You can manually trigger SCIM synchronization on Entra ID from the *Provision on demand* page.

a. Search for users or groups to manually synchronize and select them.



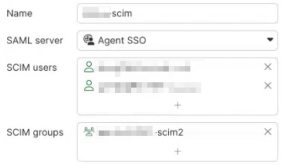
b. Click *Provision*.

Upon provisioning you will see a status page indicating whether the synchronization operations were successful and the options to see details about each synchronization operation.



9. In FortiSASE, go to *Access & authentication > Access > Users and groups > SCIM users and groups* to observe the local users and groups synchronized using the Entra ID SCIM client.
10. Go to *Access & authentication > Access > Users and groups* and click *+Create*:
    a. Select *SCIM user group* and click *Next*.
    b. In the *Create New Local SCIM User Group* pane, configure these settings:

Field	Value
Name	A name for the group. For example, *prod-scim*.
SAML server	*Agent SSO*
SCIM users	Click + to select SCIM users learned from synchronization with SCIM client.
SCIM groups	Click + to select SCIM groups learned from synchronization with SCIM client.



    c. Click *OK*.
11. When creating or editing a policy within *Security > Traffic > Policies*, configure a local SCIM user group with *User > Specify* to make an identity-based traffic policy dependent on Entra ID SSO users and groups.
12. After making changes to users and groups within Entra ID, either after the fixed 40-minute interval elapses (recommended) or after manually triggering *Provision on demand* (for verification), Entra ID synchronizes users and groups with FortiSASE.

Configuring FortiAuthenticator as SCIM client

FortiAuthenticator including FortiAuthenticator Cloud can be configured as a SCIM client for FortiSASE as a SCIM server.

This example demonstrates how to configure FortiAuthenticator as a SCIM client for an existing FortiAuthenticator already configured using steps in Configuring FortiSASE with FortiAuthenticator as SAML IdP for SSO on page 545. It is also possible to configure FortiSASE with FortiAuthenticator as SAML IdP for SSO for the first time with steps in this topic to configure FortiAuthenticator as a SCIM client.

The steps in Configuring FortiSASE with FortiAuthenticator as SAML IdP for SSO on page 545 and this topic apply to both FortiAuthenticator and FortiAuthenticator Cloud as SAML IdP.

Prerequisites and considerations

Prerequisites

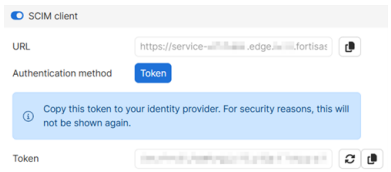
- FortiAuthenticator and FortiAuthenticator Cloud must be running version 6.6.0 and later to support SCIM client service.
  - This example uses steps that were validated in:
    - FortiAuthenticator running version 6.6.8
    - FortiAuthenticator Cloud running version 6.6.7

Considerations

- Currently, FortiAuthenticator and FortiAuthenticator Cloud only support manual SCIM synchronization performed by the administrator from the FortiAuthenticator GUI.
- Currently, only local users and local groups can be synchronized using FortiAuthenticator as SCIM client.

To configure FortiAuthenticator as SCIM client:

1. In FortiSASE, go to *Access & authentication* > *Authentication Sources* > *SSO*.
2. If *Proxy* or *Authenticated onboarding* are configured, click the *Agent* tab to ensure *Agent SSO* is being configured.
3. Click the pencil icon next to *SCIM client* to edit these settings.
   a. Enable *SCIM client*.
   b. Click the copy button next to the text field to the right of *URL* to copy the SCIM server URL to be used in FortiAuthenticator. Paste this URL to a document or text file for later use.
   c. Click the regenerate button next to the text field to the right of *Token* to generate a new token. Click the copy button to copy the token. Paste this token to a document or text file for later use.

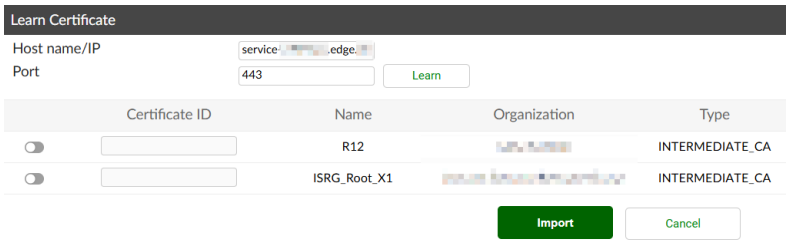


   Copy this token to your identity provider. For security reasons, this will not be shown again.
4. Click *Next*.
5. Click *Submit*.
   Once the SSO configuration has been saved, observe the *Token* text field now contains *ENC XXXX* which is expected for security reasons.
6. To ensure FortiAuthenticator includes the CA certificates required to trust the server certificate presented to the FortiSASE SCIM server during its HTTPS handshaking operation, you must learn certificates from the

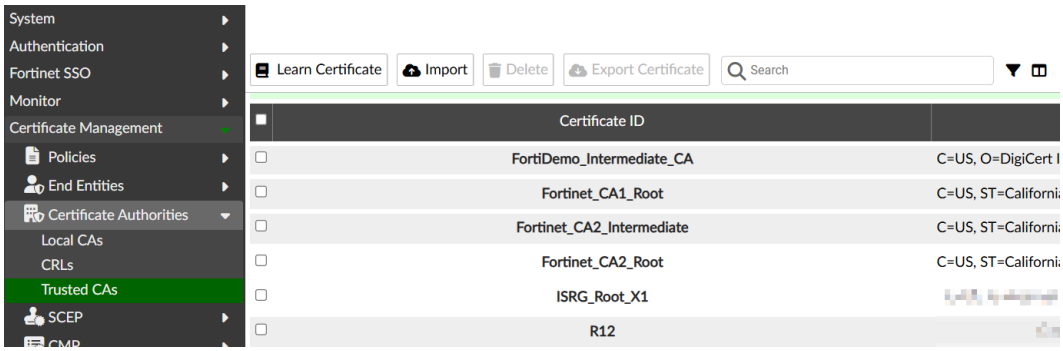
FortiSASE SCIM server URL.

a. In FortiAuthenticator, go to *Certificate Management* > *Trusted CAs* and click *Learn Certificate* to learn the CA certificates from the FortiSASE SCIM server URL.
b. In *Host Name/IP* copy the hostname of the FortiSASE SCIM server URL.

   For example, if the FortiSASE SCIM server URL is *https://service-a1bcd2ef.edge.prod.fortisase.com:44559/fortisase_saml_server_scim/scim/v2* then use *service-a1bcd2ef.edge.prod.fortisase.com*.
c. Leave *Port* as *443*.
d. Click *Learn*. After some time, FortiAuthenticator will return the CA certificates used by the FortiSASE SCIM server.
e. For each CA certificate learned, enable the CA certificate using the toggle button and enter a Certificate ID conforming to FortiAuthenticator input text validation.

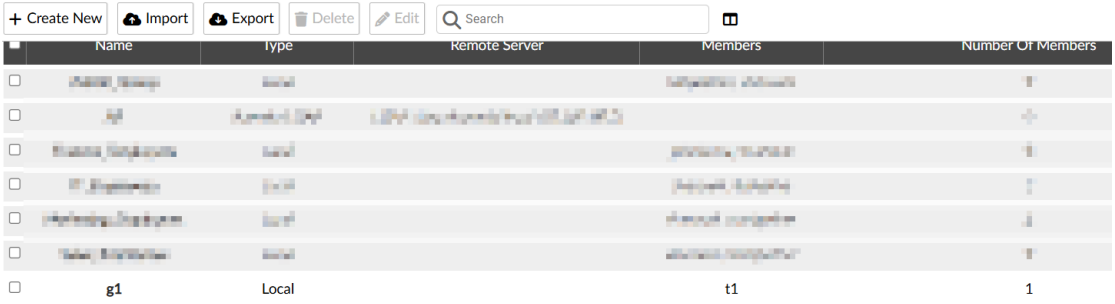


f. Click *Import*. Observe the CA certificates have been successfully imported to FortiAuthenticator.



7. Go to *Authentication* > *User Management* > *User Groups* to add local users to groups. If needed, you can create, edit, or delete local users from *Authentication* > *User Management* > *Local Users*.

   In this example, group *g1* with local user *t1* as its sole member is to be synchronized using the SCIM client.



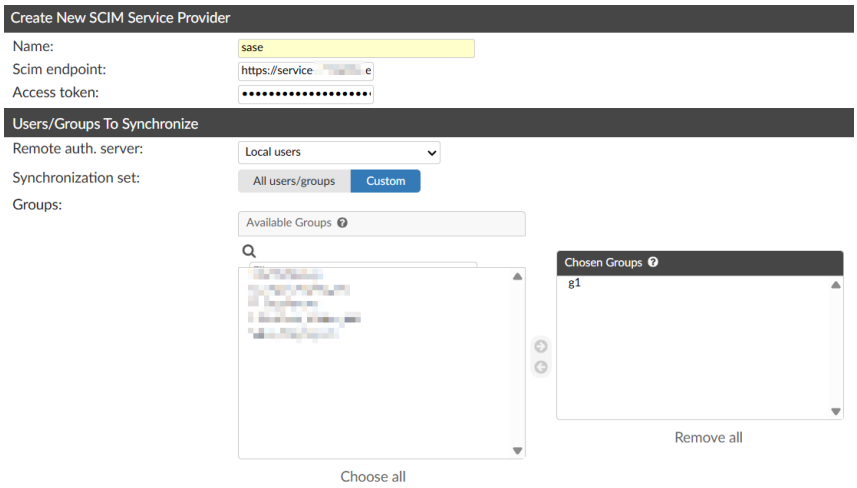
8. Go to *Authentication* > *SCIM* > *Service Provider* and click *+Create New*.

a. Configure these settings:

Field	Value
Name	Name of the SCIM service provider. For example, *sase*.
Scim endpoint	Paste the SCIM server URL copied from FortiSASE here. In this example, use *https://service-a1bcd2ef.edge.prod.fortisase.com:44559/fortisase_saml_server_scim/scim/v2*.
Access token	Paste the token copied from FortiSASE here.

b. In *Users/Groups to Synchronize*, configure these settings:

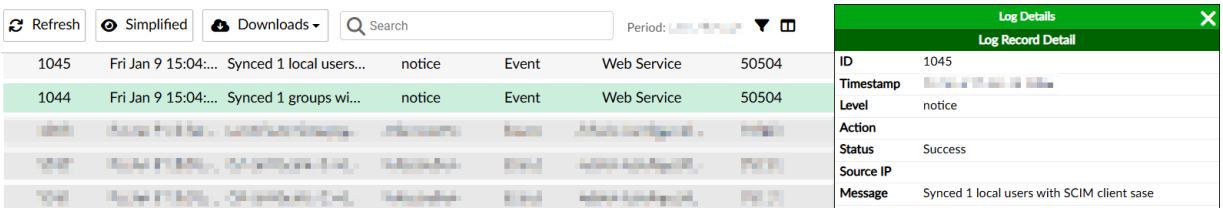
Field	Value
Remote auth. server	*Local users*
Synchronization set	*Custom*
Groups	Select groups from the left column and click the right arrow to move them to the *Chosen Groups* column.



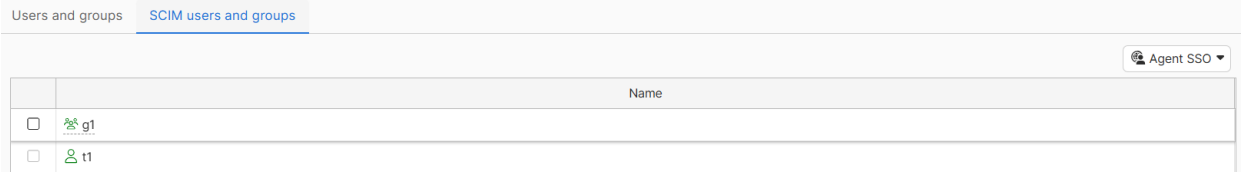
c. As needed, configure the *User Attributes Mapping* and *Group Attributes Mapping*. For this example, the defaults should suffice.

d. Click *Save*. Upon saving, FortiAuthenticator should initially synchronize users and groups with FortiSASE using the SCIM protocol over TCP port 44559.

9. Go to *Logging* > *Log Access* > *Logs* to confirm the SCIM client has successfully synchronized groups and local users with FortiSASE.

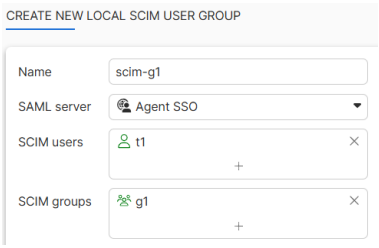


10. In FortiSASE, go to *Access & authentication* > *Access* > *Users and groups* > *SCIM users and groups* to observe the local users and groups synchronized using the FortiAuthenticator SCIM client.

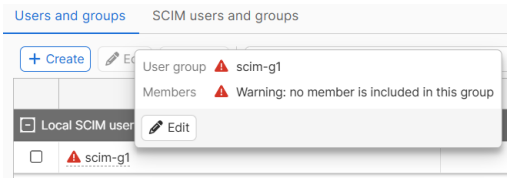


11. Go to *Access & authentication* > *Access* > *Users and groups* and click *+Create*:
    a. Select *SCIM user group* and click *Next* .
    b. In the *Create New Local SCIM User Group* pane, configure these settings:

Field	Value
Name	A name for the group. For example, *scim-g1*.
SAML server	*Agent SSO*
SCIM users	Click + to select SCIM users learned from synchronization with SCIM client.
SCIM groups	Click + to select SCIM groups learned from synchronization with SCIM client.



    c. Click *OK*.
12. When creating or editing a policy within *Security* > *Traffic* > *Policies*, configure a local SCIM user group with *User* > *Specify* to make an identity-based traffic policy dependent on FortiAuthenticator SSO local users and groups.
13. After making changes to local users and local groups on FortiAuthenticator, whenever needed, in FortiAuthenticator, edit the SCIM service provider created in Step 8, and repeat Steps 7 and 8b above to add, remove, or change local users, local group memberships, and local groups.
    a. In *Edit SCIM Service Provider*, observe the button has changed from *Save* to *Sync*. Click *Sync* to manually synchronize users and groups between FortiAuthenticator and FortiSASE.
    b. If all SCIM users and SCIM groups are removed from the FortiAuthenticator SCIM client and are synchronized with FortiSASE, in FortiSASE observe the message *Warning: no member is included in the group*. This is expected operation.



Configuring Okta as SCIM client

Okta can be configured as a SCIM client for FortiSASE as a SCIM server.

This example demonstrates how to configure Okta as a SCIM client.

To configure Okta as a SCIM client:

1. In FortiSASE, go to *Access & authentication* > *Authentication Sources* > *SSO*.
2. If *Proxy* or *Authenticated onboarding* are configured, click the *Agent* tab to ensure *Agent SSO* is being configured.
3. The first step of the SSO configuration wizard displays the entity ID, SSO URL, and single logout URL. You use these values to configure FortiSASE as an SP in Okta. Copy these values.
4. Create and configure your FortiSASE environment in Okta.
   a. On the Okta administration page, go to *Applications* > *Applications*.
   b. Click *Create App Integration*.
   c. For *Sign-in method*, select *SAML 2.0*.
   d. Click *Next*.
   e. Fill out the fields in *General Settings* and click *Done*.
   f. In *Configure SAML*, copy and paste the SP fields from FortiSASE to Okta:

FortiSASE SAML field	Okta SAML settings configuration field
Entity ID	*Audience URI (SP Entity ID)*
Assertion Consumer Service (ACS) URL	*Single sign-on URL*
Single Logout Service (SLS) URL	Used in *Show Advanced Settings*. See below.
Portal (Sign On) URL	*Default RelayState*

   g. Click *Show Advanced Settings* and configure these settings:

Field	Value
Response	*Signed*
Assertion Signature	*Signed*
Digest Algorithm	*SHA256* (default)
Signature Certificate	*FortiSASE Default Certificate* or your own custom certificate already imported to FortiSASE. Must download from FortiSASE and load it into Okta here.
Enable Single Logout	*Enabled*
Single Logout URL	*Single Logout Service (SLS) URL* from FortiSASE
SP Issuer	*Entity ID* from FortiSASE

   h. Click *Next*.

i. In *Feedback*, for *App type* select *This is an internal app that we have created* and click *Finish*.
j. In the *Sign On* tab, go to *Settings* > *Sign on methods*.
   i. Under *Metadata details*, click *More details*.
   ii. Make note of the following Okta fields that you will copy-and-paste into FortiSASE:

Okta SAML field	FortiSASE SAML settings configuration field
Sign-on URL	IdP Single Sign-on URL
Sign-out URL	IdP Single Log-out URL
Issuer	IdP Entity ID
Signing Certificate	IdP Certificate

   iii. Download the IdP certificate from the provided link in *Signing Certificate*. Save the certificate to your device.
   iv. In *Attribute statements*:
      i. Go to *Show legacy configuration* and in *Profile attribute statements* click *Edit*.
      ii. For *Profile attribute statements*, configure these settings:

Field	Value
Name	*username*
Name format	*Basic*
Value	*user.login*

      iii. For *Group attribute statements*, configure these settings:

Field	Value
Name	*group*
Name format	*Basic*
Value	*Matches regex: .**

      iv. Click *Save*.

5. Configure the IdP information in FortiSASE:
   a. Click *Next* in the SSO wizard. Copy and paste the IdP fields from Okta to FortiSASE:

Okta SAML field	FortiSASE SAML settings configuration field
Sign-on URL	IdP Single Sign-on URL
Sign-out URL	IdP Single Log-out URL
Issuer	IdP Entity ID

   b. In *SAML Claims Mapping*, in the *Username* field, enter *username*. In the *Group Name* field, enter *group*. Both fields are case-sensitive. If you have configured to use SAML attribute names other than *username* or *group* on Okta, you can enter the SAML attribute name in the *Username* and *Group Name* fields accordingly.

c. From the *IdP Certificate* dropdown list, select *Create*, then upload the *Signing Certificate* that you downloaded. Click *Next*.

d. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click + to add your own custom certificate.

e. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Okta if *Certificate Verification* is enabled on Okta.

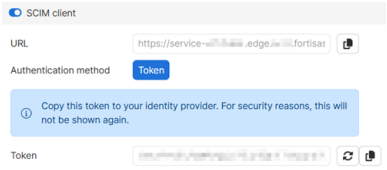
> *FortiSASE Default Certificate* is a built-in wildcard certificate on FortiSASE that a well-known public CA signed and remains the same across all of your points of presence.
>
> *FortiSASE Default Certificate* periodically renews. Thus, if IdPs use *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with the new SP certificate. To avoid updating your IdP configuration frequently, uploading your own certificate is recommended.

f. Review the SAML configuration, then click *Submit*.

g. Enable *SCIM client*.

i. Click the copy button next to the text field to the right of *URL* to copy the SCIM server URL to be used in Entra ID. Paste this URL to a document or text file for later use.

ii. Click the regenerate button next to the text field to the right of *Token* to generate a new token. Click the copy button to copy the token. Paste this token to a document or text file for later use.



Copy this token to your identity provider. For security reasons, this will not be shown again.

iii. Click *Next*.

h. Click *Submit*. Once the SSO configuration has been saved, observe the *Token* text field now contains *ENC XXXX* which is expected for security reasons.

6. Configure SCIM provisioning in Okta:

a. On the Okta administration page, go to *Applications* > *Applications*.

b. Select the previously created application.

c. Go to the *General* tab and in *App Settings*, click *Edit*.

d. For *Provisioning*, select *SCIM* and click *Save*.

e. Go to the *Provisioning* tab under *Settings* > *Integration*.

i. In *SCIM Connection*, click *Edit* and configure these settings:

Okta SCIM field	Value
SCIM Connection	
SCIM connector base URL	Copy and paste the FortiSASE SCIM server URL.
Unique identifier field for users	*userName*
Supported provisioning actions	*Select all*
Authentication mode	*HTTP Header*
HTTP Header	
Authorization	Copy and paste the SCIM token.

ii. Click *Test Connector Configuration*.
iii. If the communication is successful, you should see a message *Connector configured successfully*. Click *Close*.
iv. Click *Save*.

f. Go to the *Provisioning* tab and click *Settings* > *To App*.
i. In *Provisioning to App*, click *Edit* and enable the *Create Users*, *Update User Attributes*, and *Deactivate Users* options.
ii. Click *Save*.

g. On the *Assignments* tab, assign groups to the application:
i. From the *Assign* dropdown list, select *Assign to People*.
ii. In the dialog, assign the desired users to the Okta application.
iii. From the *Assign* dropdown list, select *Assign to Group*.
iv. In the dialog, assign the desired groups to the Okta application.

h. You will need to set up push groups to ensure users and groups from Okta can be synchronized to FortiSASE using SCIM.
i. On the Okta administration page, go to *Applications* > *Applications*.
ii. Select the previously created application.
iii. Go to the *Push Groups* tab.
iv. Click *Push Groups* > *Find groups by name*. Ensure the *Push group memberships immediately* option is checked (default).

i. Find a group and click *Save*.
j. In the *Push Group* tab, observe the *Push Status* change from *Pushing* to *Active*.

7. In FortiSASE, go to *Access & authentication* > *Access* > *Users and groups* > *SCIM users and groups* to observe the users and groups synchronized using the Okta SCIM client.
8. Go to *Access & authentication* > *Access* > *Users and groups* and click *+Create*:
a. Select *SCIM user group* and click *Next*.
b. In the *Create New Local SCIM User Group* pane, configure these settings:

Field	Value
Name	A name for the group. For example, *scim-g1*.
SAML server	*Agent SSO*
SCIM users	Click + to select SCIM users learned from synchronization with SCIM client.
SCIM groups	Click + to select SCIM groups learned from synchronization with SCIM client.

   c. Click *OK*.

9. When creating or editing a policy within *Security* > *Traffic* > *Policies*, configure a local SCIM user group with *User* > *Specify* to make an identity-based traffic policy dependent on Okta SSO users and groups.
10. After making changes to user and group memberships on Okta, Okta will automatically push group changes to FortiSASE.

Fortinet Single Sign On (FSSO)

FortiSASE supports SSO capabilities for domain-joined Windows users or machines by leveraging the FSSO solution. It requires using a FSSO collector agent. When a user logs into a domain-joined workstation, the domain controller logs this event under Windows security event logs. The FSSO collector agent detects this logon event and extracts the following key details:

- Username
- User IP address
- Group membership (from Active Directory)

The collector agent then forwards this user information to FortiSASE, which can be leveraged using the FSSO user group on FortiSASE. FortiSASE can use FSSO user groups in policies to allow or restrict user traffic access to resources protected by it. Thus, when a domain user logs in to a domain, their user information is available in FortiSASE in the form of the FSSO user group, preventing the need to reauthenticate to access any resources.

FSSO is meant to be used with domain-joined Windows clients behind branch on-ramp devices or edge devices. FSSO provides the mapping of the Windows client's IP address with its currently logged-in username for these use cases.

You can deploy an FSSO agent can using one of the following methods:

Method	Description
FortiAuthenticator	You can configure FortiAuthenticator to act as a collector agent for domain controller (DC) agent installed on the Windows DC or to poll the Windows DC for Window logon event logs. See Methods and Windows event log.
Windows DC	Install independent FSSO collector agent software directly on a Windows DC. Ensure that the installed collector agent software has the necessary domain permissions to collect user login events. During collector agent installation, a DC agent is installed automatically. You can download the collector agent from the Fortinet Support portal.

To configure an FSSO connector on FortiSASE:

1. Go to *Access & authentication > Authentication Sources > Fortinet Single Sign On (FSSO)* and click *Create* and enter the following information:

Field	Description
Name	Enter a suitable name for the FSSO connector.
Server	Enter the FQDN or IP address of the FortiAuthenticator or Windows Server hosting the collector agent.
Password	Enter the shared secret. This must match the password configured on the FSSO agent.
Certificate	Select the CA certificate that signed the agent's SSL certificate. To upload the certificate, click *+* and upload the remote CA certificate.

2. (Optional) If you have redundant FSSO agents as backup if the primary FSSO server fails, click *+* to add them and specify their IP address or FQDN. A maximum of four redundant FSSO agents are configurable.
3. Click *OK*.

To view AD groups and FSSO logon users:

1. Go to *Access & authentication > Authentication Sources > Fortinet Single Sign On (FSSO)* and verify the *Status* column value for the FSSO collector agent shows *Connected*.
2. Select the FSSO connector and click *View AD groups* to see the available AD groups fetched by the collector agent. If the AD groups are not visible, click *Refresh AD groups*.
3. To see the users who are logged onto the domain and information about their usernames, IP address, AD group membership, and login duration, double-click to open the FSSO connector and click *Show FSSO logons*.

To configure FSSO user groups:

1. To configure FSSO user groups, go to *Access & authentication > Access > Users and groups*. Click *Create*.
2. Select *FSSO user group* and click *Next*.
3. Enter a suitable name. Under *FSSO active directory groups*, click *+* to select the desired AD user groups.
4. Click *OK*.

You can now use the FSSO user groups for secure internet access and secure private (SPA) access policies under *Security > Traffic > Policies*, to allow or deny access to domain users who have successfully logged into their domain. For user traffic incoming from Edge devices, you can use FSSO user groups to authorize user traffic as per configured policies without requiring users to reauthenticate.

Prerequisites

- FortiAuthenticator or the Windows server hosting the collector agent are reachable from FortiSASE security PoPs over the internet or via a SPA connection.
- FortiSASE uses an encrypted channel for communication between the security PoPs and a collector agent that uses TCP port 8001. Therefore, you must ensure to configure proper firewall rules to allow inbound

connections on TCP 8001. By default, FortiAuthenticator listens on TCP port 8000 for FSSO and TCP port 8001 for the FortiClient FSSO Mobility Agent (FSSOMA).

- One option is to reconfigure FSSOMA to use a port other than TCP port 8000 and then reconfigure FSSO to use TCP port 8001.
- An alternative option is to use the default FSSO port 8000 on FortiAuthenticator and then configure an externally-facing firewall with a port forwarding (destination NAT) rule from external TCP port 8001 to internal TCP port 8000 destined for the FortiAuthenticator internal IP address.

Considerations

- Typically, FortiAuthenticator should be fully configured with respect to both the FSSO port, method, and filtering settings before configuring FSSO in FortiSASE. Otherwise, if FortiAuthenticator is fully configured after configuring FortiSASE, then Refresh AD groups must be used in *Access & authentication > Authentication Sources > Fortinet Single Sign-On (FSSO)* to refresh the AD groups used for FSSO.
- Currently, FortiSASE only supports establishing an FSSO connection to a private FortiAuthenticator behind an SPA hub configured for BGP per overlay.

Domains

FortiSASE supports Active Directory (AD) domains, which work with these features:

- In *Access & authentication > Authentication Sources > Domains*, configuring FortiSASE Endpoint Management Service to connect to AD domains to allow viewing and selecting AD domains, users, and groups.
- Assigning endpoint profiles to AD-joined endpoints based on matching AD users or groups
- Zero trust network access tagging when these Windows rule types are configured and matching:
  - *User in AD Group*
  - *Domain*

For details on Entra ID domains, see Entra ID domains on page 581.



For demonstrations of various configuration options for implementing FortiSASE endpoint management features, such as custom endpoint profiles, tunnel autoconnect, split tunnel, vulnerability scan, zero trust network access (ZTNA), and more, see the FortiSASE Endpoint Management Deployment Guide.

To configure an AD connection:

1. Go to *Access & authentication > Authentication Sources > Domains* and click *Create > Active Directory (AD) connection*.

2. Configure the AD server settings to match those on your AD server. Modify these to match your setup:

Field	Value
Name	Domain name from AD server
Server address	<AD server IP address or name>
Server Port	389
Username	administrator
Password	<Password>
Sync every	60 minutes
LDAPS connection	Disabled

3. Click *Create*. Upon success, observe the message *Connection to the Active Directory successfully authorized*.

Considerations

- This feature does not apply for proxy mode users. See Proxy agentless mode on page 15.
- When the FortiSASE Endpoint Management Service uses AD servers with domains for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

Entra ID domains

Supporting Entra ID domains only works with Windows endpoints running FortiClient 7.0.13 or later that are joined to Entra ID domains and are connected to the FortiSASE Endpoint Management Service.

FortiSASE cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE as well.

FortiSASE supports Entra ID domains to work with these features:

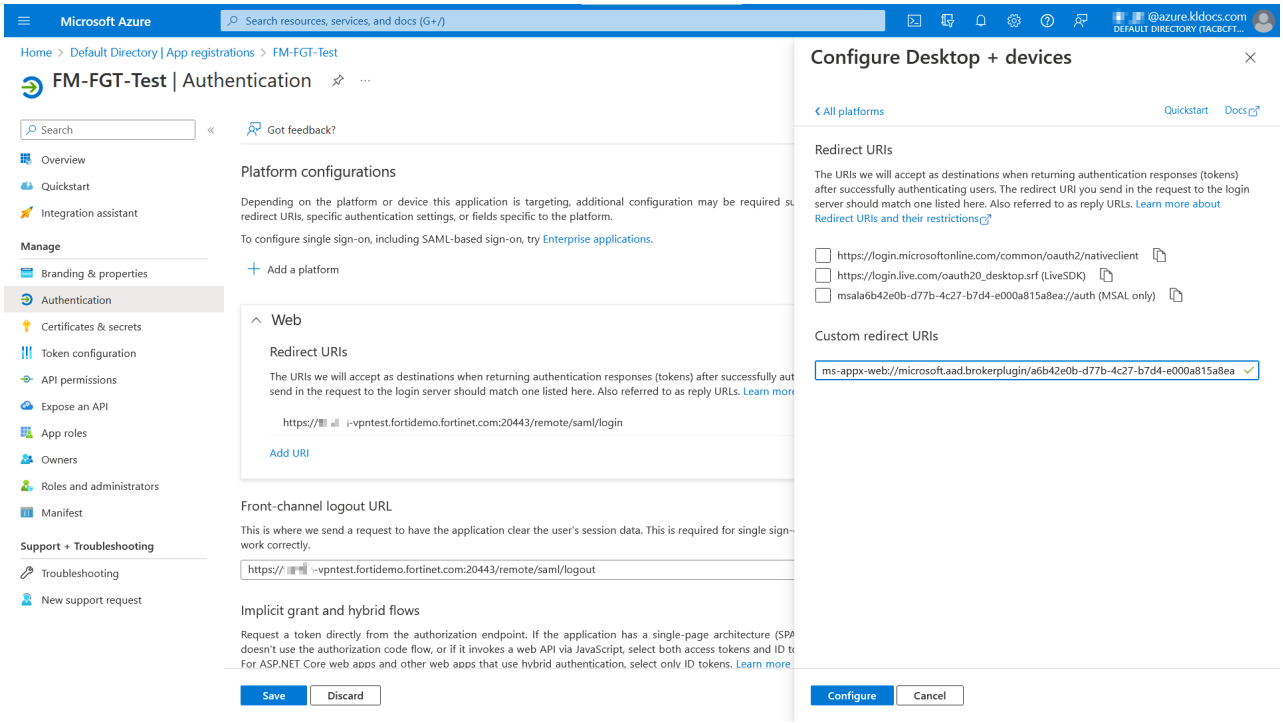
- In *Access & authentication > Authentication Sources > Domains*, configuring FortiSASE Endpoint Management Service to connect to Entra ID domains to allow viewing and selecting Entra ID domains, users, and groups.
- Assigning endpoint profiles to Entra ID-joined endpoints based on matching Entra ID users or groups

- Zero trust network access tagging when these Windows rule types are configured and matching:
  - *User in AD Group*
  - *Domain*

To register FortiSASE as a mobile/desktop application with a custom redirect URI:

In Entra ID, add a custom redirect URI as follows:

1. Log into the Azure portal.
2. On the homepage, do one of the following:
   - Under *Azure Services*, click *Entra ID*.
   - Click the navigation menu and under *All Services*, click *Entra ID*.
3. In the left menu, click *App registrations*, then click the *All applications* tab.
4. Look for the name of your FortiSASE SSL enterprise application and click the hyperlinked name.
5. Click *Authentication* and under *Platform configurations*, click *Add a platform*.
6. In the slide-in, select *Mobile and desktop applications*.
7. In the *Configure Desktop + Devices* slide-in, in the *Custom redirect URIs* field, enter *ms-appx-web://microsoft.aad.brokerplugin/<followed by the "Application ID" noted down earlier>*. This custom redirect URI is the specific URI format corresponding to the FortiClient application implementation used for obtaining an access token from Entra ID.
   For example, if the application ID is *dfa94502-5f95-48c0-9a6a-9be1af6de562* then the custom redirect URL is: *ms-appx-web://microsoft.aad.brokerplugin/dfa94502-5f95-48c0-9a6a-9be1af6de562*



8. Click *Configure* at the bottom of the page to save the configuration. For details on redirect URIs, see Authentication and authorization basics and Redirect URI (reply URL) restrictions and limitations.

Configuring API permissions and determining Entra ID SSO credentials

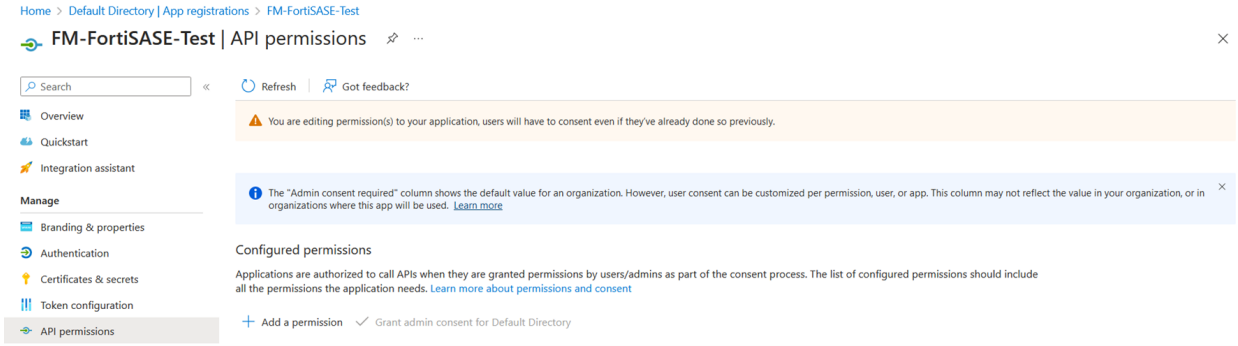
Before you can autoconnect to a tunnel using Microsoft Entra ID SSO and search user groups from Entra ID single sign on (SSO), you must configure API permissions for autoconnect and group searching, and then determine the SAML provider credentials from the Entra ID portal.

To access the Entra ID portal:

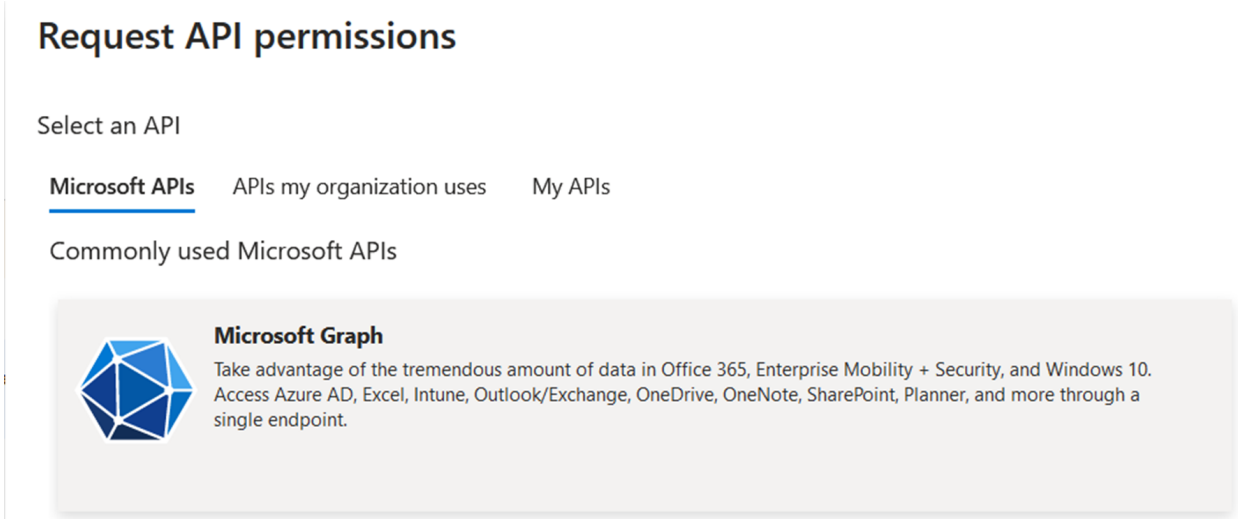
1. Log into the Azure portal. You should already have an enterprise application created in Entra ID. If this has not been created, see Creating an enterprise application using FortiSASE as a template from the gallery and collecting SAML IdP URL information.
2. On the homepage, do one of the following:
   - Under *Azure Services*, click *Microsoft Entra ID*.
   - Click the navigation menu and under *All Services*, click *Microsoft Entra ID*.

To add Microsoft Graph API application permissions required for supporting an Entra ID domain:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *API permissions*, and click *Add a permission*.



4. In the *Request API permissions* slide-in, click *Microsoft Graph*.



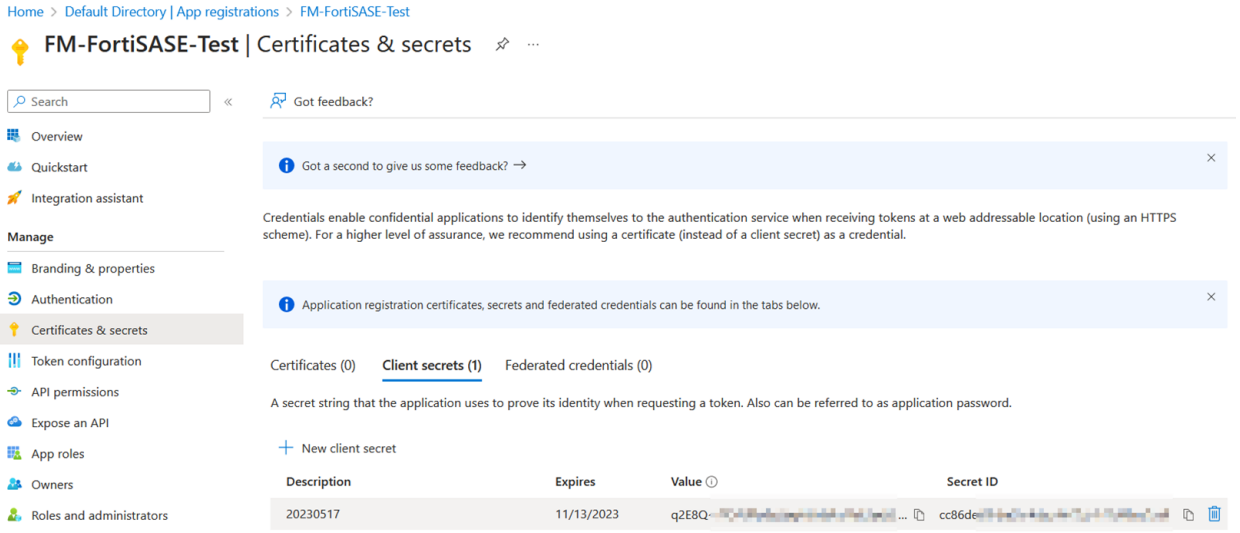
5. Add application permissions:
   a. Select *Application permissions*.
   b. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for group searching:
      - *Device > Device.Read.All – Read all devices*
      - *Domain > Domain.Read.All – Read domains*
      - *Group > Group.Read.All – Read all groups*
      - *GroupMember > GroupMember.Read.All – Read all group memberships*
      - *User > User.Read.All – Read all users' full profiles*
   c. Click *Add permissions*.
6. Add delegated permissions:
   a. Repeat steps 1-4 to add a permission.
   b. Select *Delegated permissions*.
   c. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for autoconnect:
   User > User.Read – Sign in and read user profile
7. Click *Add permissions*.
8. In *API permissions*, click *Grant admin consent for <domain name>*. If this option is grayed out, you must log into an Entra ID admin account to perform this step. Click *Yes* in the *Grant admin consent* confirmation prompt. Observe the *Grant consent successful* notification at the top-right.
   Also, observe the *Status* field shows *Granted for <domain>* for all the permissions added.
   This step is important since it ensures that the administrator grants permissions for the enterprise application from Entra ID instead of end users requiring the administrator to log in to each instance and provide permissions.
   Therefore, in summary, you should add the following Microsoft Graph permissions to support the following Entra ID features:

API permission group	Permission name	Type
Device	*Device.Read.All*	Application
Domain	*Domain.Read.All*	
Group	*Group.Read.All*	
GroupMember	*GroupMember.Read.All*	
User	*User.Read.All*	
	User.Read	Delegated

To add a client secret string and determine the value of the client secret string:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *Certificates & secrets*, and click *New client secret*.
4. In the *Add a Client Secret* slide-in, add a *Description* and select the *Expires* option of your choice. Click *Add*.
5. Observe that a new client secret has been created. Immediately after creation, ensure you copy the *Value* of the client secret string, which FortiSASE uses as the *Client Secret*. This value is not visible after this initial

creation step and moving to another page.



To determine the tenant and client IDs:

1. In the left menu, click *App registrations*, then click *All applications*.
2. Look for your FortiSASE enterprise application name and click the hyperlinked name.
3. In the left menu, click *Overview* and note the following values:
   - *Application (client) ID*, which FortiSASE uses as the *Client ID*
   - *Directory (tenant) ID*, which FortiSASE uses as the *Tenant ID*

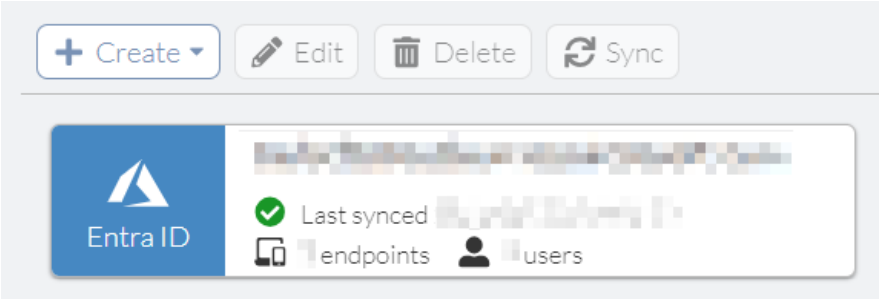
Entra ID page within specific enterprise application	Entra ID field	FortiSASE field
Overview	*Directory (tenant) ID*	*Tenant ID*
	Application (client) ID	*Client ID*
Certificates & Secrets	*Value*	*Client Secret*

To configure an Entra ID connection:

1. Go to *Access & authentication* > *Authentication Sources* > *Domains* and click *Create* > *Entra ID connection*.
2. Configure the Entra ID domain settings to match those for your Entra ID tenant and application. Modify these to match your setup.

Field	Value
Name	Domain name from Entra ID
Tenant ID	*Directory (tenant) ID* from Entra ID
Client ID	*Application (client) ID* from Entra ID
Client secret	Value of *Client Secret* from Entra ID

3. Click *Authorize*. Upon success, observe the message *Connection to Entra ID successfully authorized. Click "Next" to synchronize groups*. Click *Next*.
4. Configure settings related to synchronizing groups:
5. Click *Sync*. You will return to the *Access & authentication > Authentication Sources > Domains* page with a card with details about the newly added AD domain.



6. To manually sync with Entra ID, select the card corresponding to the Entra ID domain and click *Sync*.

System

Administration

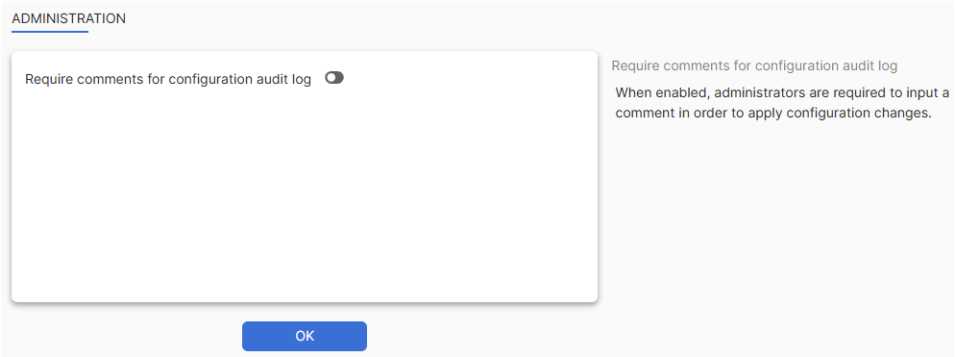
The *System > Administration* page includes the *Require comments for configuration audit* option. When enabled, this feature ensures any configuration changes made by an administrator require a change summary to be entered. This includes all configuration changes on FortiSASE, such as those to objects, endpoint profiles, and analytics and reporting configurations. The change summary will include information on the object being changed, the administrator that made the change, and a short description of the change made.

Configuration audit logs can be reviewed in *Operations > Logs > Events > Administrator Events*. If *Require comments for configuration audit log* is disabled in *System > Administration*, the *Configuration audit log* change summary pane will no longer display when changes are submitted. Existing change summaries are retained for 30 days.

New logs can be reviewed in *Administrator Events* after some delay. See Administrator Events on page 245.

To enable configuration audit logs:

1. Go to *System > Administration*.



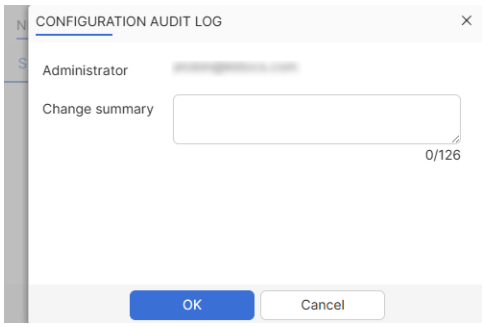
2. Enable *Require comments for configuration audit log*.
3. Click *OK*.

Example

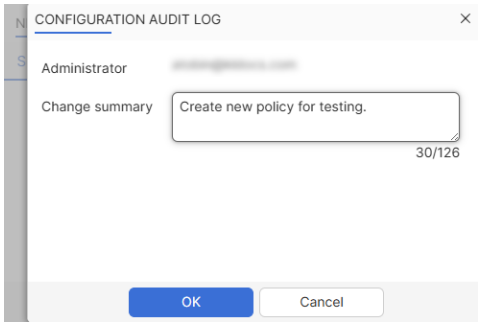
The following example demonstrates configuring a new traffic policy in *Security > Traffic > Policies*. Once the new policy is completed and submitted, the *Configuration audit log* pane will require a change summary to be submitted before the action can be completed.

To submit a change summary:

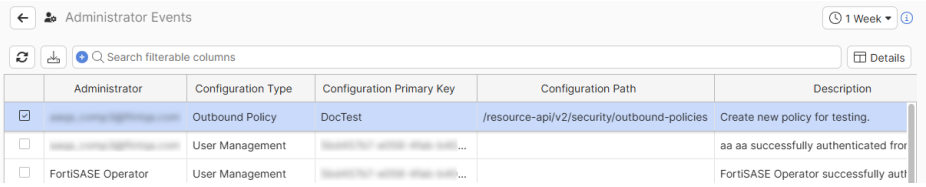
1. Go to *Security* > *Traffic* > *Policies*.
2. Click *Create*.
3. Configure the policy details. See Policies on page 296 for more information.
4. Click *OK*. The *Configuration audit log* pane is displayed.



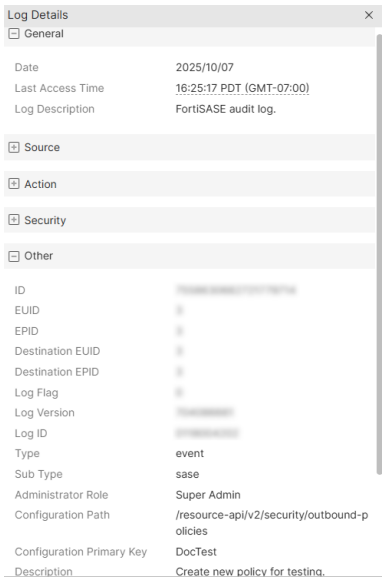
5. Enter a *Change summary* describing the purpose of the change.



6. Click *OK*. The policy is created.
7. Go to *Operations* > *Logs* > *Events* > *Administrator Events* to view the configuration audit log.



8. Click *Details* to view the *Log Details*.



HTML templates

You can customize pages that display on endpoints in certain situations, such as if FortiSASE blocks access based on Application Control With Inline-CASB settings.

The following lists the HTML templates for block pages, email, and warning pages that you can customize in FortiSASE:

Name	Description
Block page	
Application Control Block page	Replacement HTML for Application Control With Inline-CASB block page
Banned Word Block Page	Replacement HTML for Banned Word/Content Web Filter block page
Captive Portal Disclaimer	FortiSASE does not currently support this option.
Captive Portal Login Failed Page	Replacement HTML for Captive Portal login failed page
Captive Portal Login Page	Replacement HTML for Captive Portal login page
Captive Portal Reject Page	FortiSASE does not currently support this option.
Captive Portal SAML Login Page	Replacement HTML for Captive Portal SAML login page
Data Loss Prevention Block Page	Replacement HTML for Data Loss Prevention block page
FortiGuard Block Page	Replacement HTML for FortiGuard Category Based Web Filter block page

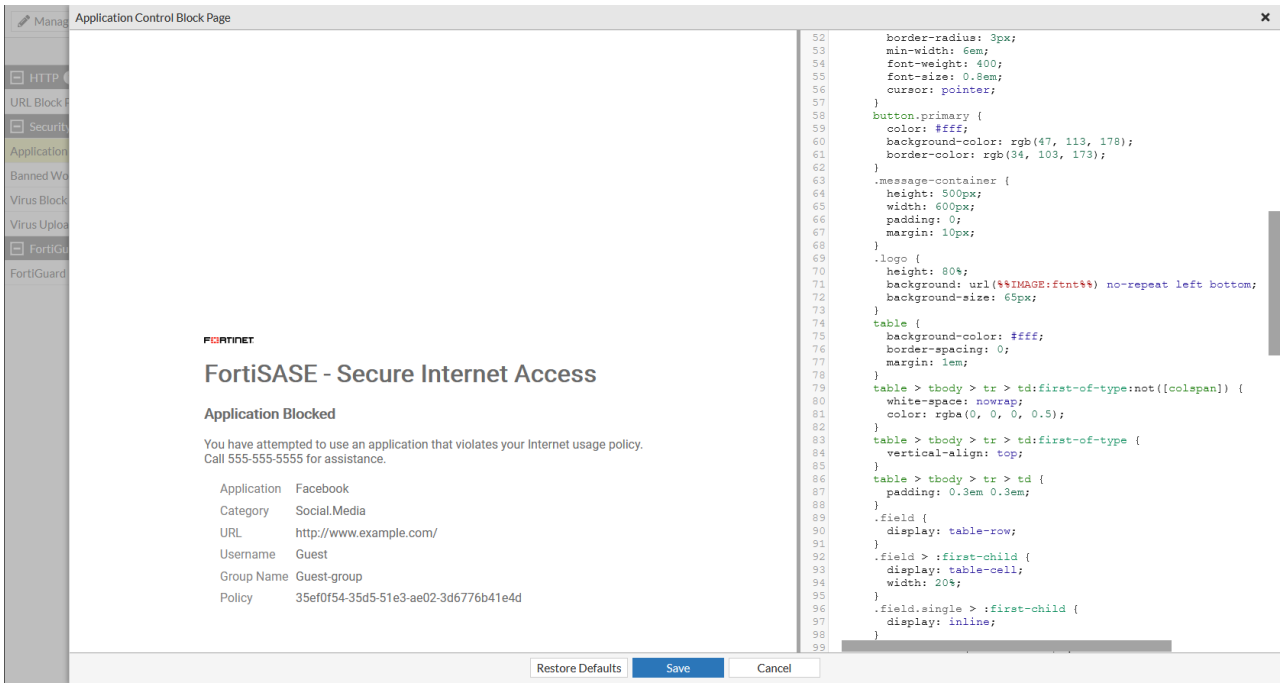
Name	Description
Intrusion Prevention Block Page	Replacement HTML for Intrusion Prevention block page
URL Block Page	Replacement HTML for HTTP URL block page
Video Block Page	Replacement HTML for FortiGuard category-based video filter block page
Virus Block Page	Replacement HTML for AntiVirus block page
Virus Upload Block Page	Replacement HTML for virus infected file upload block page
YouTube Embedded Custom Block Message	Plain text message that shows in the YouTube embedded player when FortiSASE blocks a video
Email	
Invitation Email	HTML email content for inviting users to FortiSASE
Warning Page	
FortiGuard Warning Page	Replacement HTML for FortiGuard Category Based Web Filter warning page

For example, you can customize the message to add your company logo and include your helpdesk phone number so that users can contact the network administrator about their machine. You can also customize the email to send to users to invite them to FortiSASE.

This example modifies the Application Control block page to use the Fortinet logo instead of the FortiSASE logo and include a phone number.

To customize the Application Control block page:

1. Go to *System* > *HTML templates*.
2. On the *Images* tab, click *Create*.
3. In the *Name* field, enter the desired name. This example uses ftnt.
4. Upload the desired logo.
5. Click *OK*.
6. On the *Templates* tab, select *Application Control Block Page*, then click *Edit*.
7. To replace the FortiSASE logo, replace `%%IMAGE:logo_fortisase_sia&%%` with `%%IMAGE:<image name>%%`. This example replaces it with `%%IMAGE:ftnt%%`.
8. To add a phone number to the message, modify the `<body><div class="message-container"><p>You have attempted...</p>` element as desired.
9. Click *Save*. The endpoint user sees this page when they attempt to view an application that FortiSASE Application Control With Inline-CASB blocks access to.



API-based CASB

The goal of the API-based cloud access security broker (CASB) feature that FortiCASB powers is to act as a mediator between the cloud provider and user to implement preconfigured or customized security policies of the organization on cloud application usage.

API-based CASB offers an API-based approach by obtaining data directly from SaaS cloud applications using REST API queries with OAuth 2.0 authentication. Therefore, API-based CASB can essentially perform deep inspection of cloud traffic, providing advanced monitoring, analysis, and notifications when suspicious activity is triggered.

Since API-based CASB performs out-of-band communication with SaaS applications, there is no performance impact on user cloud application traffic.

API-based CASB provides insights on suspicious activity on past and current cloud user activity and relies on the network administrator to review and act upon these insights after they occur.

This section describes how to enable API-based CASB and its prerequisites and considerations. See:

- For details on monitoring onboarded cloud applications, see API-based CASB monitoring on page 64.
- For onboarding details, see Applications on page 413.
- For data protection details, see Data Protection on page 414. Currently, Data Protection view offers limited customization.

To enable API-based CASB on FortiSASE:

1. Go to *System* > *API-based CASB*.
2. Set *Status* as *Enabled*.

3. Click *OK*.
4. After enabling the API-based CASB feature, a CASB region selection prompt appears. Select either *Global* or *Europe*.
5. Click *OK* to provision the API-based CASB feature for your instance.

Prerequisites and considerations

Prerequisites

The Cloud API CASB & DLP license is required for API-based CASB support in FortiSASE. This license is included with FortiSASE remote user subscriptions. An add-on subscription is required for FortiSASE Thin-Edge and On-ramp locations. See the FortiSASE Ordering Guide.

Considerations

- The API-based CASB feature supports onboarding these cloud applications:
  - AWS S3
  - Google Cloud Storage
  - Office 365
- You must perform configuration steps within the cloud application first before configuring the API-based CASB feature within FortiSASE.

Certificates

You can upload a certificate for use with SSL deep inspection and LDAP and SAML single sign on (SSO) authentication.

To upload a certificate:

1. Go to *System* > *Certificates*.
2. Click *Import*, then do one of the following:
   - Select *Local Certificate* and configure the following:
     i. For *Type*, select *Local Certificate* to upload a custom service provider certificate in SSO configuration or *Local CA Certificate* to upload a custom SSL deep inspection certificate.
     ii. For *Format*, select *PKCS#12 Certificate* or *Certificate*.
     iii. In the *Certificate File* or *Certificate with Key File* field, click *Upload* to upload the certificate file. The certificate name is the same as the uploaded file name and can be a maximum of 35 characters long.
     iv. If you selected *Certificate* for *Format*, in the *Key File* field, click *Upload* to upload the key file.
     v. (Optional) Configure a password.
     vi. Click *OK*.

- Select *Remote Certificate* and configure the following:
  i. For *Type*, select *Remote Certificate* to trust a remote server certificate public key. You can use this to upload an identity provider server certificate in SSO configuration. Select *Remote CA Certificate* to trust a remote server CA certificate. You can use this in LDAPS configuration.
  ii. Click *Upload* to upload the certificate file.
  iii. Enter a certificate name as desired. The certificate name can be a maximum of 35 characters long.

3. Click *OK*. The certificate displays in *System* > *Certificates*.

Central Management

This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

Some customers require a centralized way to manage configuration for their on-premise FortiGate devices and remote users connecting using FortiSASE. FortiSASE integrates with FortiManager to provide central management for a selected set of configuration settings. In FortiManager, configuration settings such as addresses, address groups, and security profile groups are also known as objects.

The following configuration settings synchronize from FortiManager to FortiSASE:

- Policy packages with the following configuration:
  - Firewall policies
  - Firewall proxy policies
  - Firewall schedules
  - Security posture tags
- Security profile group:
  - SSL/SSH Inspection (SSL Inspection only)
  - AntiVirus Profile
  - Web Filter Profile: support for empty custom categories that requires editing and adding web sites to them in FortiSASE after synchronization
  - IPS Profile
  - File Filter Profile including support for blocking password-protected files
  - DLP Profile
  - DNS Filter
  - Application Control
  - Video Filter profile
  - Profile protocol options
    - Handling unknown content encoding
    - Handling oversized files
- External feeds (associated with Web Filter and DNS Filter profiles only):
  - Web filter FQDNs
  - DNS filter domains

  - External hosts (associated with DNS Filter profiles)
- Firewall address and address group
- Services and service groups
- Security profile group
- Local, PKI, and LDAP users and user groups
- Authentication sources (SSO via SAML, LDAP, RADIUS, FSSO)

An administrator follows this configuration workflow for central management:

1. Configure FortiSASE for central management.
2. Configure FortiManager for central management.
3. Verify configuration updates performed using central management.

Prerequisites and considerations

See Prerequisites and considerations on page 594.

For details on using a FortiManager key for synchronizing configuration for MSSP tenants, see Central management for MSSP tenants on page 712.

Prerequisites and considerations

Prerequisites

This section covers prerequisites to using central management in FortiSASE:

- Supported models and firmware on page 595
- FortiCloud account prerequisites on page 595
- Network topology on page 595

> This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

Considerations

- Central management supports only one-way configuration synchronization from FortiManager to FortiSASE. Therefore, avoid deleting objects from FortiManager to prevent any conflicts.
- Central management supports synchronizing a maximum of 3000 objects at once from FortiManager.
- If you attempt to synchronize any security profiles or other configuration settings from FortiManager that FortiSASE does not support, they are ignored and not synchronized to FortiSASE.

  FortiSASE treats all flow-based features synchronized from FortiManager as proxy-based features (best match).

- After enabling central management, objects synchronized from FortiManager to FortiSASE are considered read-only and you cannot modify them directly in FortiSASE.
- FortiManager only supports adding FortiSASE to FortiGate and Fortinet Security Fabric administrative domains (ADOM). This feature does not support other ADOMs where the connector appears including FortiProxy, FortiFirewallCarrier, FortiFirewall, FortiCarrier, and the global database ADOMs. Additionally, you cannot add FortiSASE to ADOMs operating in backup mode. Attempting to do so presents the user with an *An unexpected error has occurred* error.
- Central management does not support synchronizing client-to-client traffic policies, that is, policies where the incoming interface and outgoing interface are both specified as *SASE_ingress_zone*.

Supported models and firmware

For a list of model and firmware version prerequisites, see Central management using FortiManager.



This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

FortiCloud account prerequisites

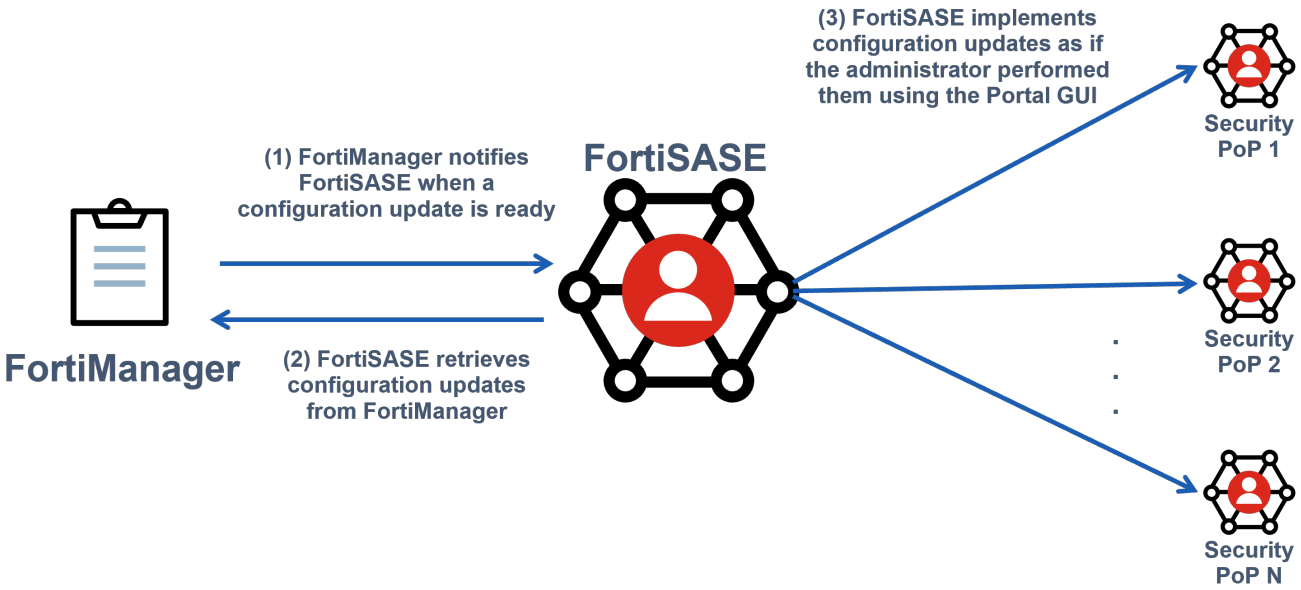
You must register FortiManager used with central management to the same FortiCloud account used to log into FortiSASE before using this feature.

For details on registering products, see Registering assets.

Network topology

FortiSASE integrates with FortiManager by using a connector with the following workflow:

1. FortiManager notifies FortiSASE when a configuration update is ready.
2. FortiSASE retrieves configuration updates from FortiManager.
3. FortiSASE implements configuration updates retrieved from FortiManager using standard orchestration as if you performed these changes using the portal GUI.



Mapping FortiManager objects to FortiSASE configuration settings

Ensure you are aware of Prerequisites and considerations on page 594.

The following FortiManager objects map to the following FortiSASE configuration settings:

FortiManager object	FortiSASE configuration setting
Policies	
Firewall policies	Policies
Firewall proxy policies	Proxy policies
Firewall schedules	Schedules
Security posture tags	Security posture tags
Firewall address and address group	
Firewall address	Host
Address group	Host group
Services	Services
Service groups	Service groups
Security profile group	
Profile group • FortiSASE treats flow-based features as proxy-	Security profile group

FortiManager object	FortiSASE configuration setting
based features (best match). • In FortiManager, all security profiles including SSL/SSH inspection are associated with a security profile group.	In FortiSASE, all security settings including SSL inspection are associated with a security profile group.
SSL/SSH Inspection (SSL Inspection only)	Configure security profile group settings > SSL inspection
Profile Protocol Options • unknown-content-encoding • Options: oversize • uncompressed-oversize-limit • oversize-limit	Configure security profile group settings > Deep/certificate inspection settings • Handling unknown content types Configure security profile group settings > Performance optimization • Handling oversized files • Oversized, uncompressed files are larger than • Oversized, compressed files are larger than
AntiVirus Profile	AntiVirus
Web Filter Profile (custom categories not supported)	Web Filter With Inline-CASB
IPS Profile	Intrusion Prevention
File Filter Profile	File Filter
DLP Profile	Data Loss Prevention (DLP)
DNS Filter	DNS Filter
Application Control	Application Control With Inline-CASB
Video Filter	Video Filter
External feeds Only external feeds defined and then associated with Web Filter or DNS Filter profiles are synchronized.	
External Resource > Category type, Web Filter > Remote Categories	Web Filter FQDN Feeds
External Resource > Domain type, DNS Filter > Remote Categories	DNS Filter Domains Feeds
External Resource > Address type, DNS Filter > Static Domain Filter > External IP Block Lists	External Hosts
Local, PKI, and LDAP users and user groups	
Local user	User
PKI User	PKI User
User group	User group

FortiManager object	FortiSASE configuration setting
Authentication sources (LDAP and RADIUS)	
LDAP server	LDAP server
RADIUS server	RADIUS server
Fortinet Single Sign-On Agent (FSSO connector)	Fortinet Single Sign-On (FSSO)
Single Sign-On with name *SASE_VPN_SAML_SERVER*	SSO > Agent-based User SSO
Single Sign-On with name *SASE_SWG_SAML_SERVER*	SSO > Proxy User SSO

Enabling central management

Ensure you are aware of Prerequisites and considerations on page 594.

To enable central management on FortiSASE:

1. Go to *System* > *Central management*.
2. Set *Status* as *Enabled*.
3. Click *OK*.
4. Refresh the page or go to *System* > *Central management*.

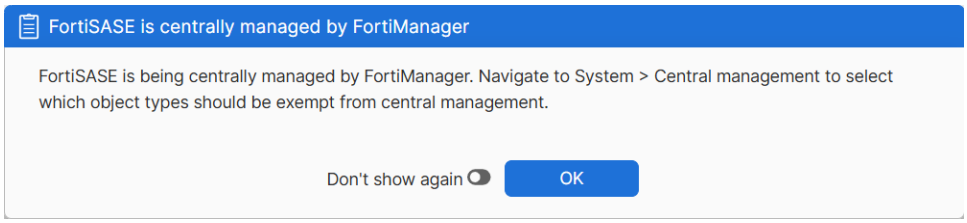
- Observe the prompt indicating that central management has been enabled.
- By default, all objects are enabled to be synchronized.

Objects to be synchronized

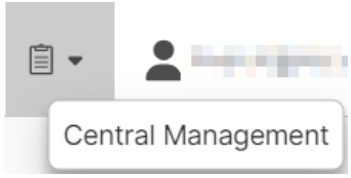
FortiSASE configuration	FortiManager object types	Enabled
Certificates	Local certificate Remote CA certificate Remote certificate	
External feeds	Threat feed	
FSSO	FSSO connector	
Hosts	Address Address group	
LDAP	LDAP server	
PKI	PKI user	
Policies	Firewall policy Proxy policy	
RADIUS	RADIUS server	
Schedules	Schedule group Recurring schedule	
Security profiles	Profile group	
Services	Service Service group	
SSO	SAML server	
Users and groups	Local user User group	

- If an object type is disabled, then it is exempt from central management, that is, not synchronized with FortiManager.
- Object types exempt from central management can be configured by the administrator from the FortiSASE portal.

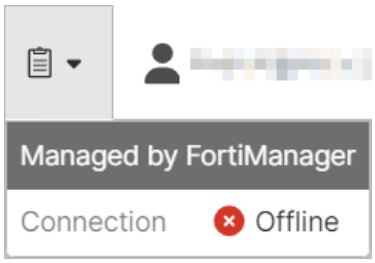
5. Upon each login, observe the prompt indicating that central management has been enabled and that object types can be exempted from central management as described in the previous step.



6. If desired, enable *Don't show again* and click *OK*.
7. Observe a new icon indicating central management is enabled in the FortiSASE header.



8. When you click on the central management icon, observe the connection status to the FortiManager.



When central management is enabled in FortiSASE, the *Connection* will be *Offline*. The *Connection* will change to *Online* only after the FortiSASE Connector has been configured correctly and enabled successfully in FortiManager. See Configuring FortiManager for central management on page 600.

Configuring FortiManager for central management

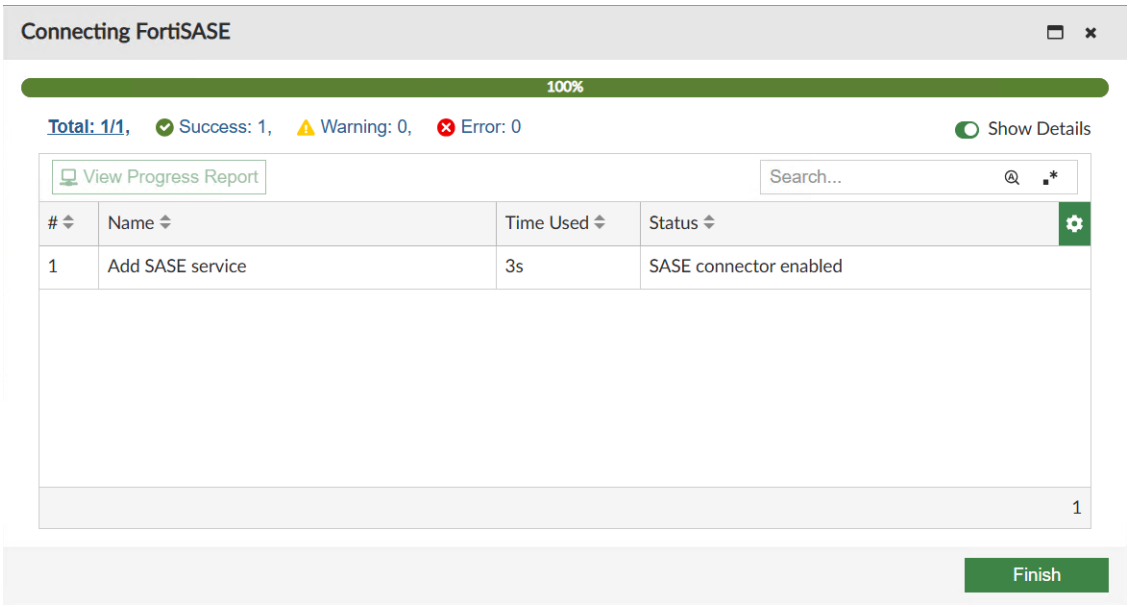
Ensure that you are aware of central management Prerequisites and considerations on page 594.

To configure FortiManager for central management:

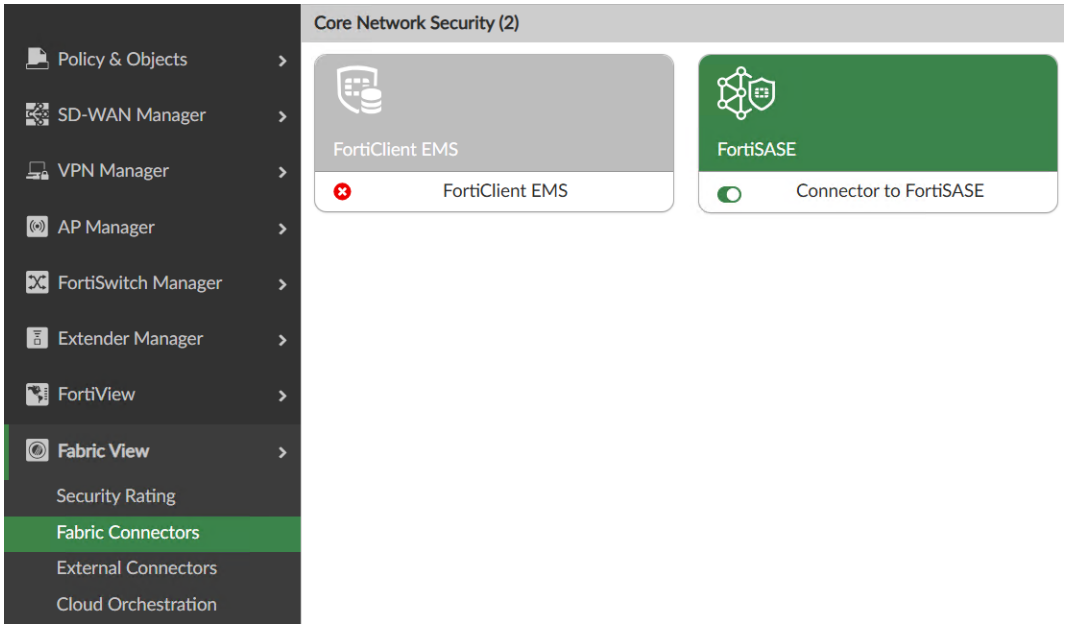
1. When a FortiSASE subscription is registered to the same FortiCloud account as your FortiManager, you receive a notification in the header. Click the notification.



2. Administrative domains (ADOM) enable administrators to manage only devices that they are assigned, based on the ADOMs to which they have access. In the dialog, select the ADOM version.
3. After selecting the ADOM version, the *Edit FortiSASE Connector* dialog appears with *Status* set to enabled. Under *Advanced*, you can define objects. You can leave all object types set to *None* and click *OK*.
4. The *Connecting FortiSASE* dialog appears with the item *Add SASE service*.
   The progress bar should proceed to completed with the Status displaying SASE connector enabled.



5. In *Fabric View* > *Fabric Connectors*, observe that the FortiSASE Connector is enabled.

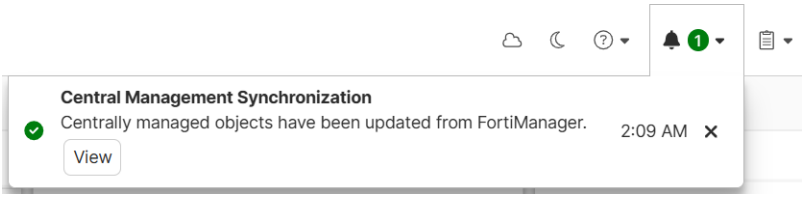


6. FortiManager can now be used to synchronize supported configuration settings with FortiSASE. See the following topics for details:
   - Configuring settings using Device Manager in FortiManager on page 605
   - Configuring settings using policy packages in FortiManager on page 612
   - Configuring security profiles in FortiManager on page 653

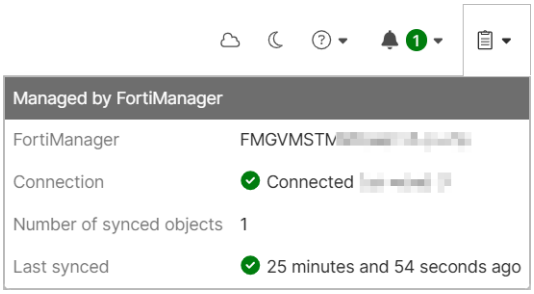
Verifying configuration updates performed using central management

To verify configuration updates performed using central management:

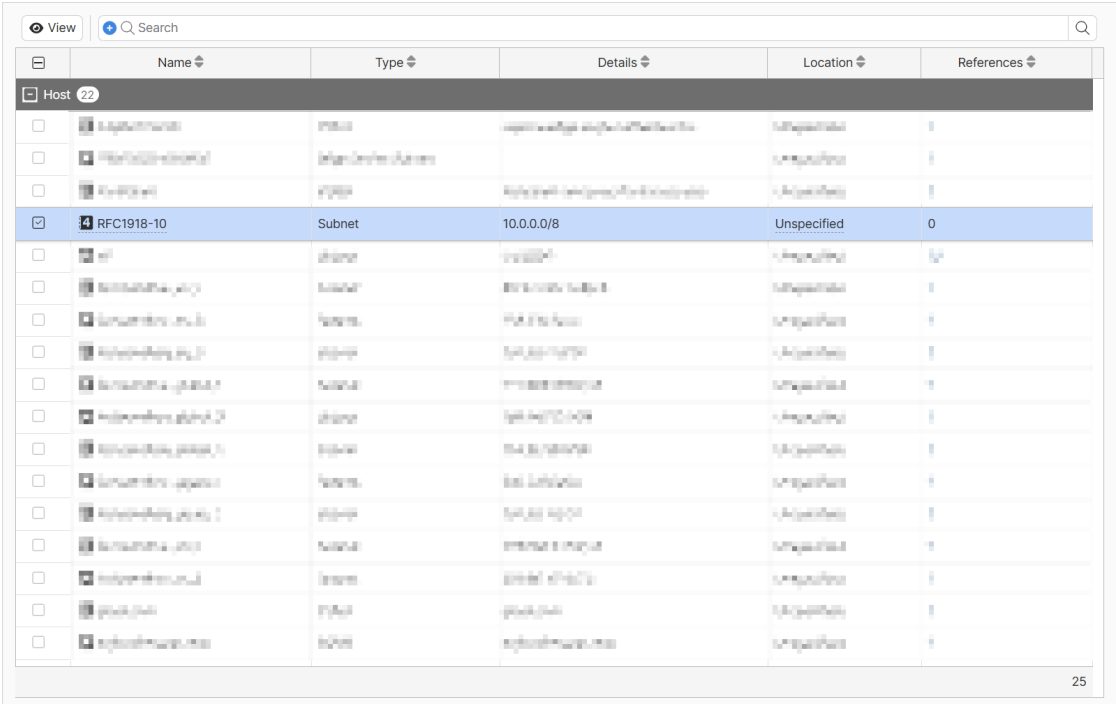
1. Log into the FortiSASE portal.
2. In the header, observe the notification indicating central management synchronization has been performed.



3. In the header, click on the central management icon and observe the connection status, number of synced objects, and last synced time.

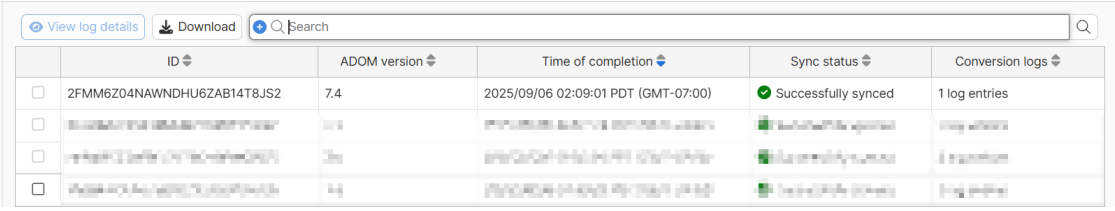


4. Go to the page corresponding to the configuration setting updated using FortiManager. In this example, check *Security* > *Hosts*.

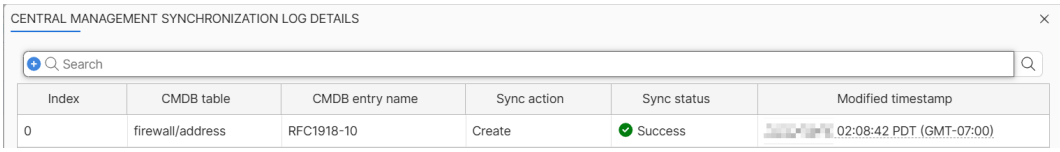


5. Observe that the *RFC1918-10* address has been installed successfully.

6. Go to *Operations* > *Logs* > *Central management synchronizations* and observe a log entry corresponding to the address object synchronization from FortiManager to FortiSASE.



7. Click on the log entry and click *View log details*. Observe the corresponding fields especially the *Sync status* of *success*.



If the logs indicate a configuration synchronization failure, then retry the synchronization again from the FortiManager side. In some cases, network issues can cause synchronization failures.

To troubleshoot configuration synchronization in the FortiManager CLI:

To troubleshoot configuration synchronization progress or errors in the FortiManager CLI, enter these commands and retry the configuration synchronization:

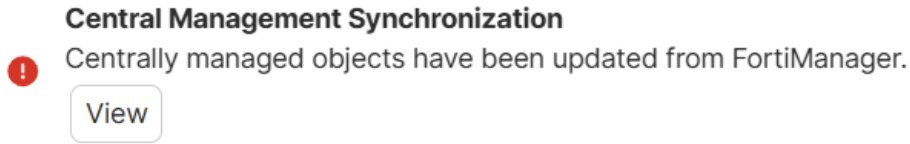
```
diagnose debug enable
diagnose debug application dmsase 255
```

Displaying error messages for failed synchronization attempts

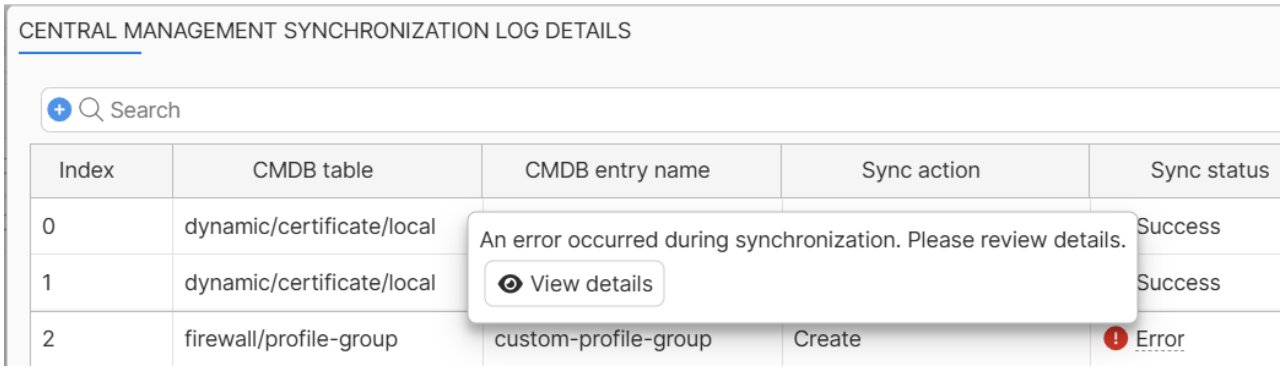
To demonstrate how to display error messages for failed synchronization attempts when using central management, this example shows the error messages that result when a duplicate entry is defined in a security profile, specifically, a duplicate network protocol enforcement entry is defined in a custom application control profile defined in FortiManager.

To display error messages for failed synchronization attempts when using central management:

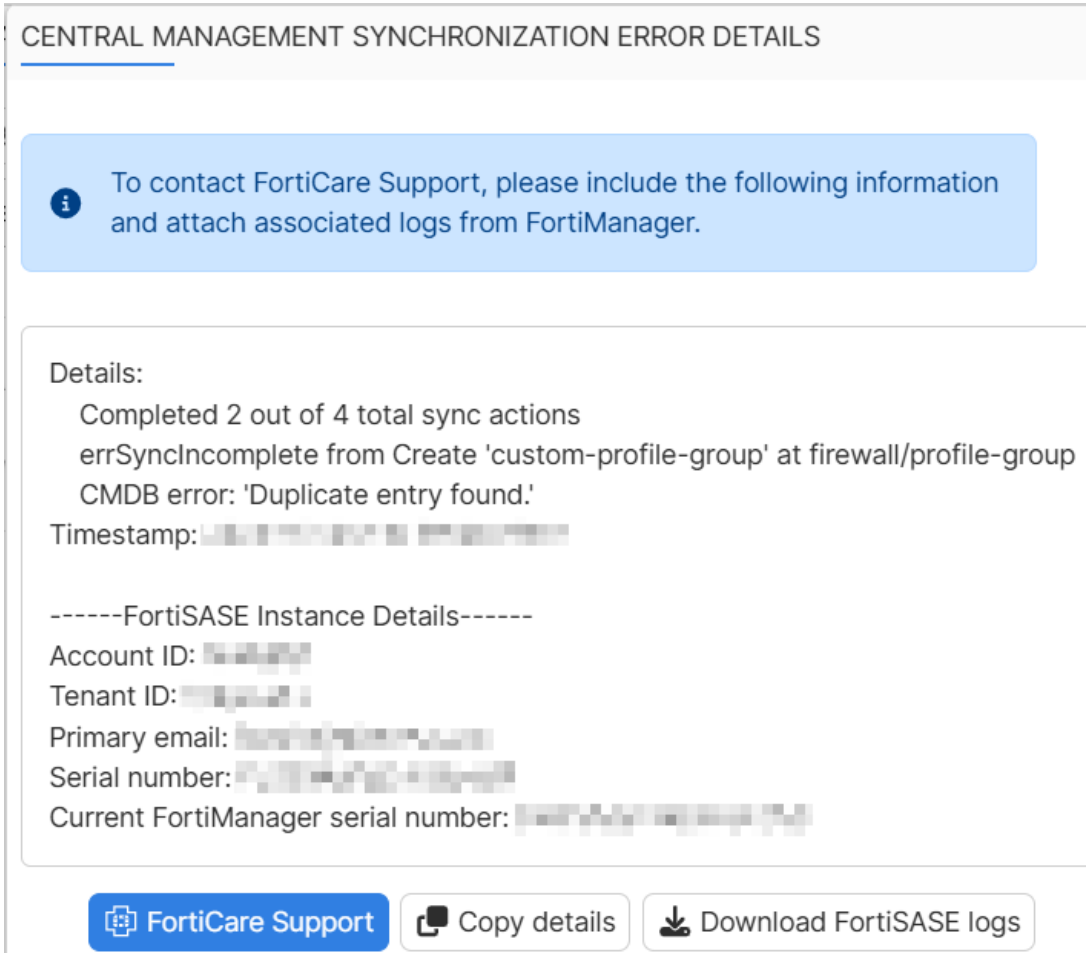
1. Log into the FortiSASE portal.
2. Observe the notification indicating central management synchronization has been performed and an error has resulted. Click *View* to jump to the *Operations* > *Logs* > *Central management synchronizations* page or go to that page directly.



3. In the *Central Management Synchronization Log Details* slide-in, observe the entry with the *Sync status* of *Error*. Hover over the *Error* status and click *View details*.



4. View the *Central Management Synchronization Error Details* slide-in and observe the error log details further. Observe that you can jump to *FortiCare Support* to open a new support ticket, *Copy* details, or *Download FortiSASE logs* as needed.

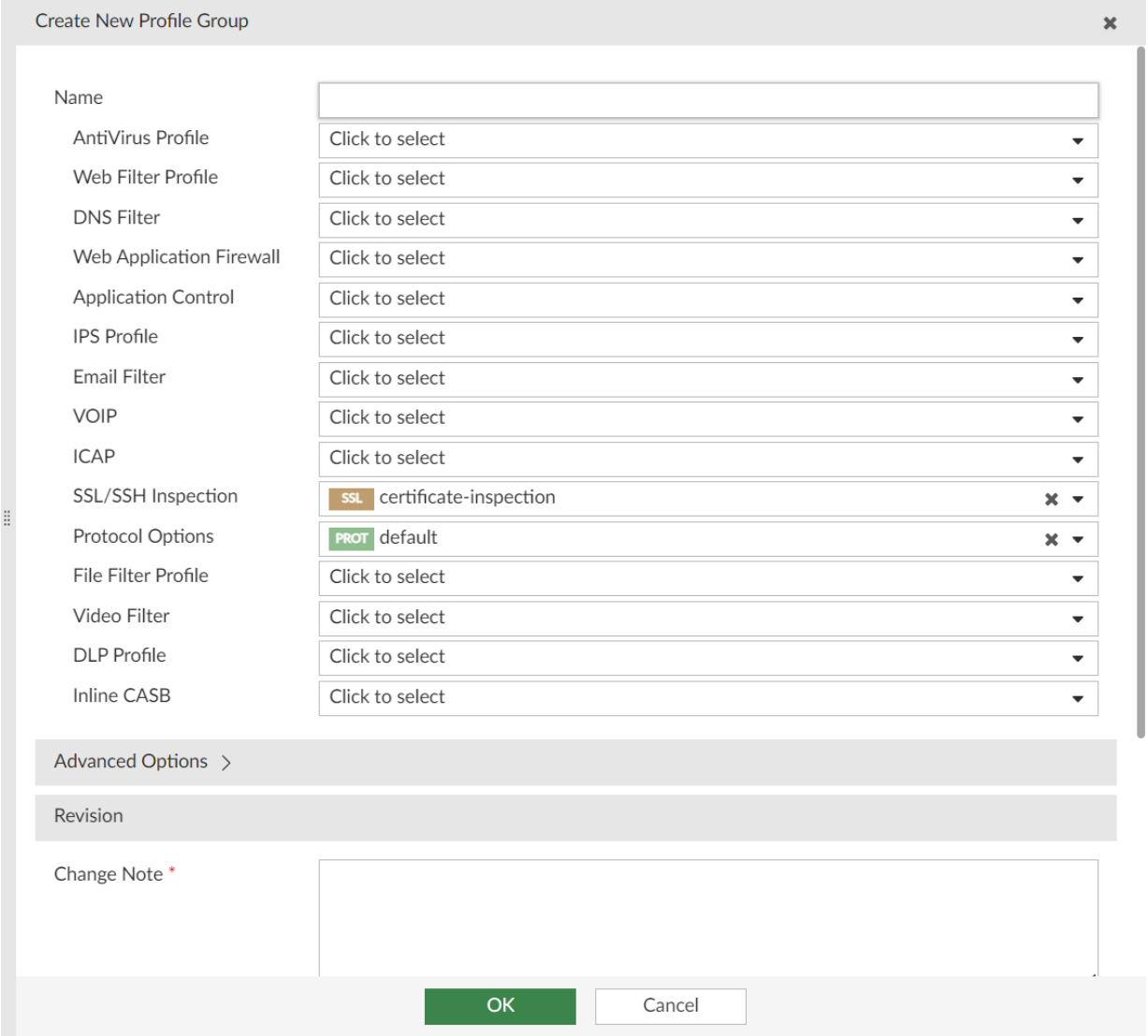


Configuring settings using Device Manager in FortiManager

After Configuring FortiManager for central management on page 600, you can configure and synchronize most supported settings, except for settings covered by policy packages (firewall policies, firewall proxy policies, firewall schedules, security posture tags), using the Device Manager in FortiManager.

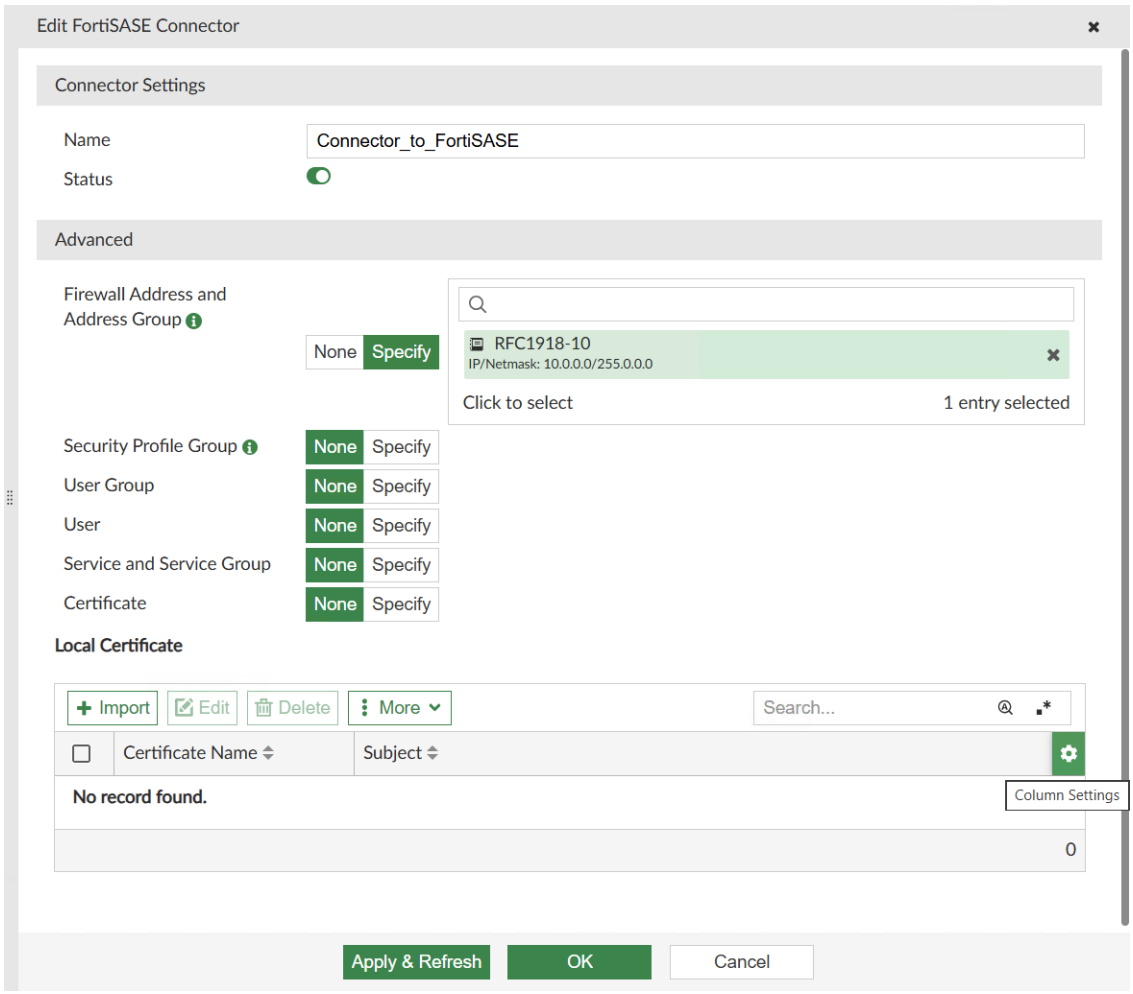
To configure settings using Device Manager in FortiManager:

1. Go to *Fabric View* > *Fabric Connectors*.
2. In *Core Network Security*, right click the *Connector to FortiSASE* card and click *Edit*.
3. Under *Advanced*, you can define objects. Click *Specify* next to the desired object type and then *Click to select*. Click *+v* or *+* and create new settings.
   - *Firewall Address and Address Group*
   - *Security Profile Group*. This feature only supports a few selected types. See Mapping FortiManager objects to FortiSASE configuration settings on page 596.



- *User* (Local User, Peer/PKI user, LDAP server, RADIUS server, or SAML Server)
- *Service and service Group*
- *Certificate*
- *Local Certificate*

In this example, *Firewall Address* and *Address Group* have been set to *Specify* and the *RFC1918-10* predefined firewall address object has been selected to be synchronized from FortiManager to FortiSASE.



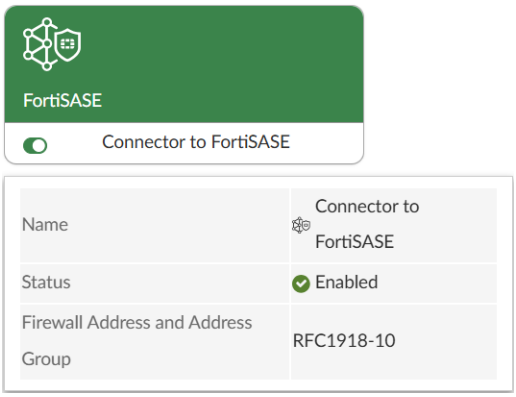
Alternatively, you can define one or more of the supported objects mentioned in Mapping FortiManager objects to FortiSASE configuration settings on page 596. See Creating Objects in the FortiManager Admin Guide.

Once you have defined objects:

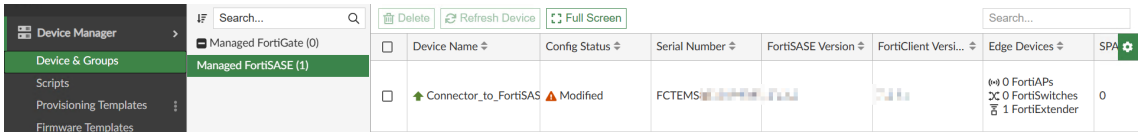
1. Go to *Fabric View* > *Fabric Connectors*.
2. Enable the *FortiSASE Connector* setting the toggle to on.
3. In the *Edit FortiSASE Connector* slide-in, click *Specify* next to the desired object type, then *Click to select* and select the objects previously defined.

4. Click *OK*.

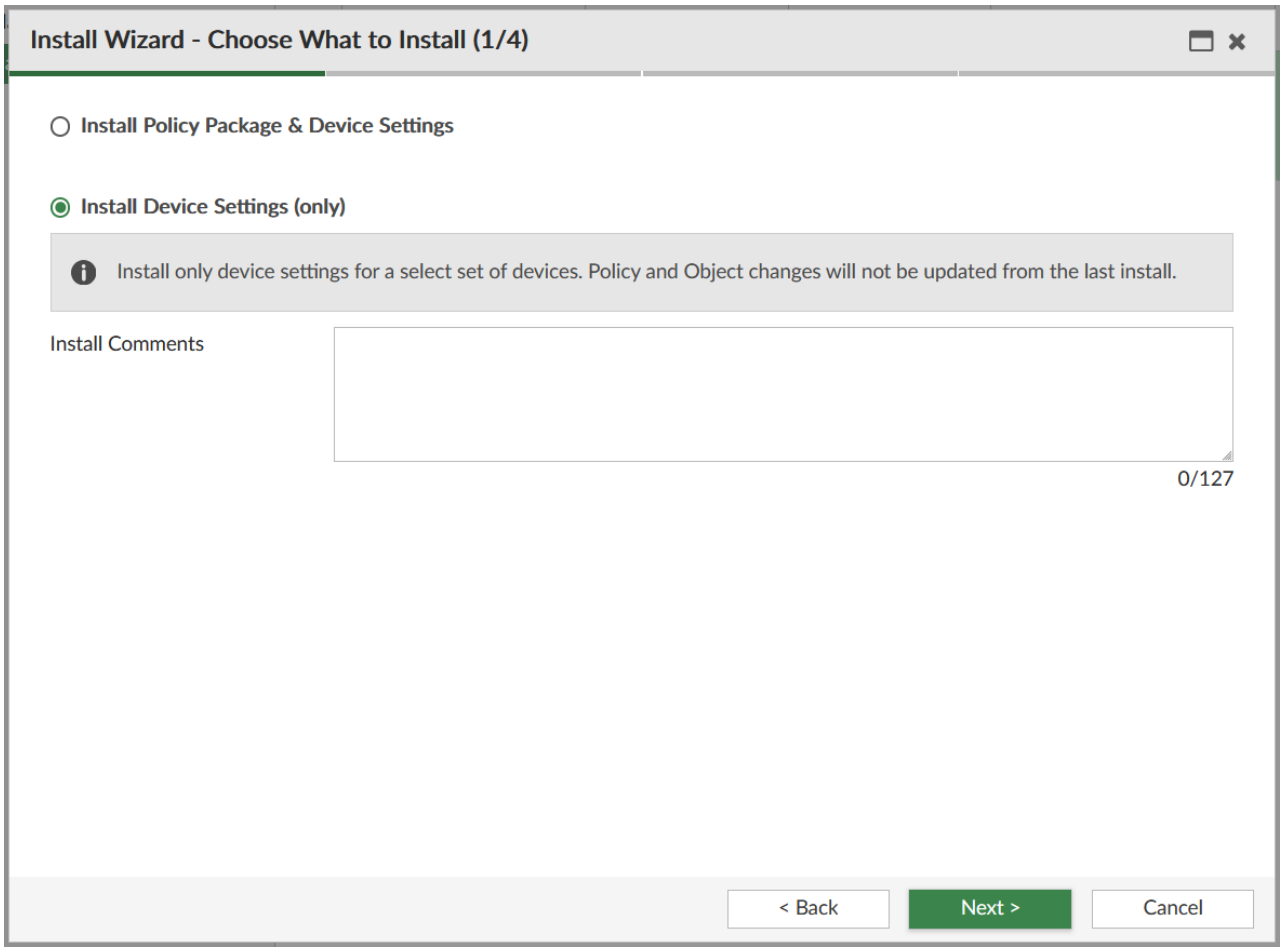
5. When hovering your mouse over the connector, observe the status and the list of synchronized objects.

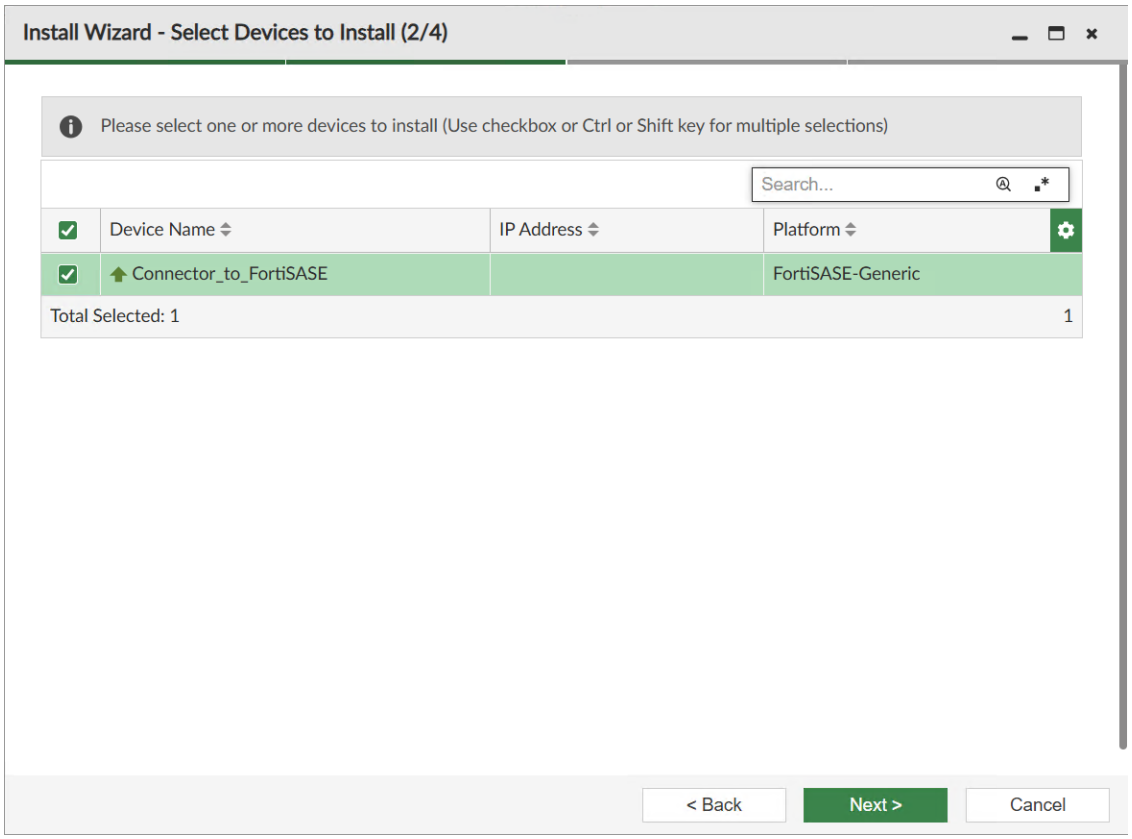


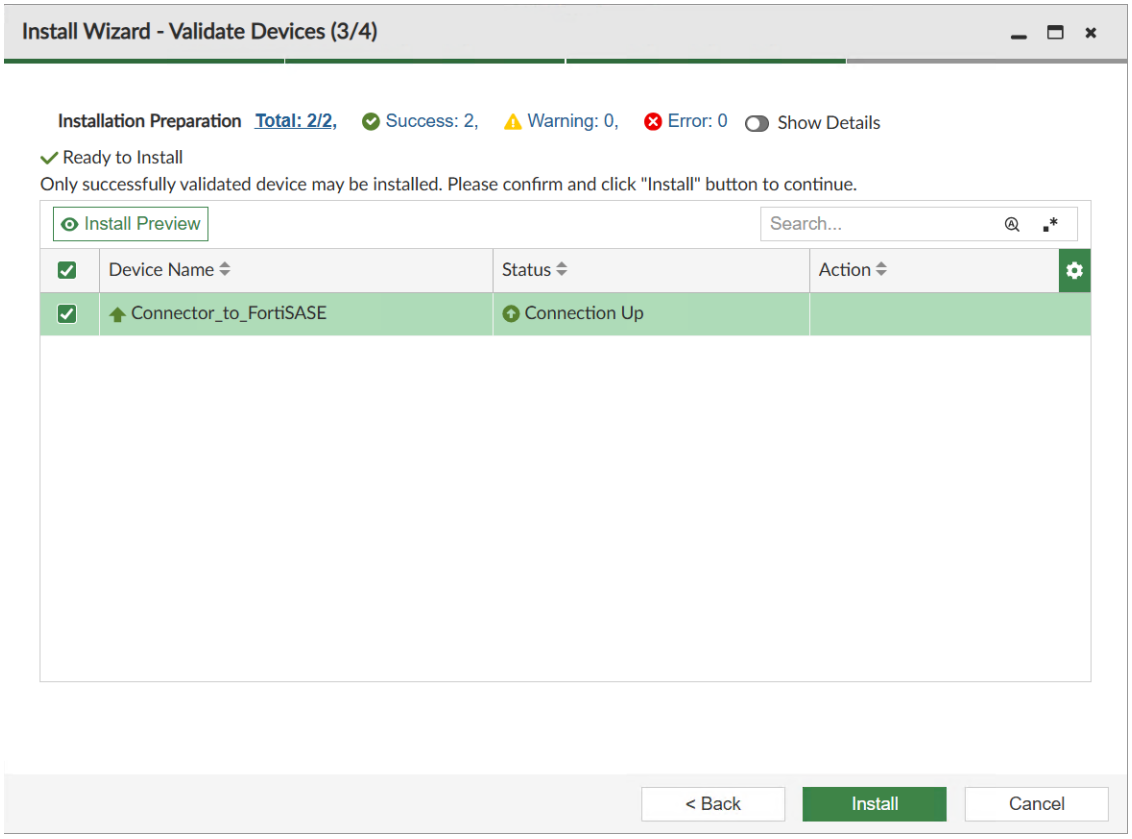
6. Go to *Device Manager > Device & Groups* and observe a Managed FortiSASE device has been added after the FortiSASE Connector has been enabled. Observe that the Managed FortiSASE device has a Config Status of Modified.



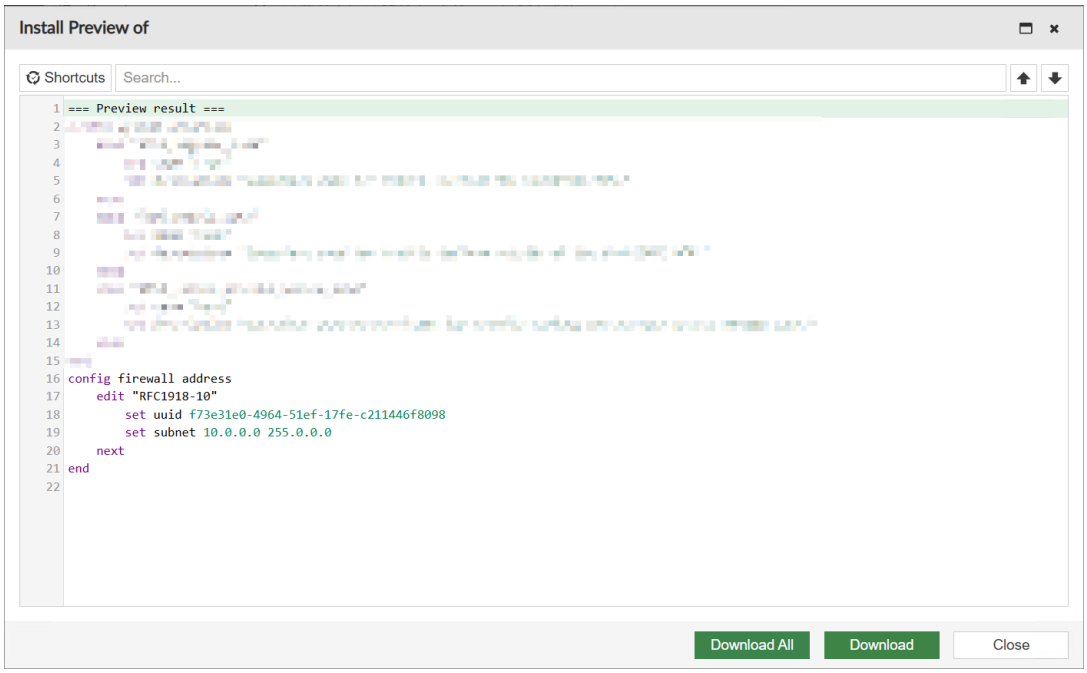
7. Click on *Install Wizard* at the top to install the selected objects from FortiManager to FortiSASE. Select *Install Device Settings (only)* and follow the steps in the wizard until *Installed successfully* appears in the wizard.

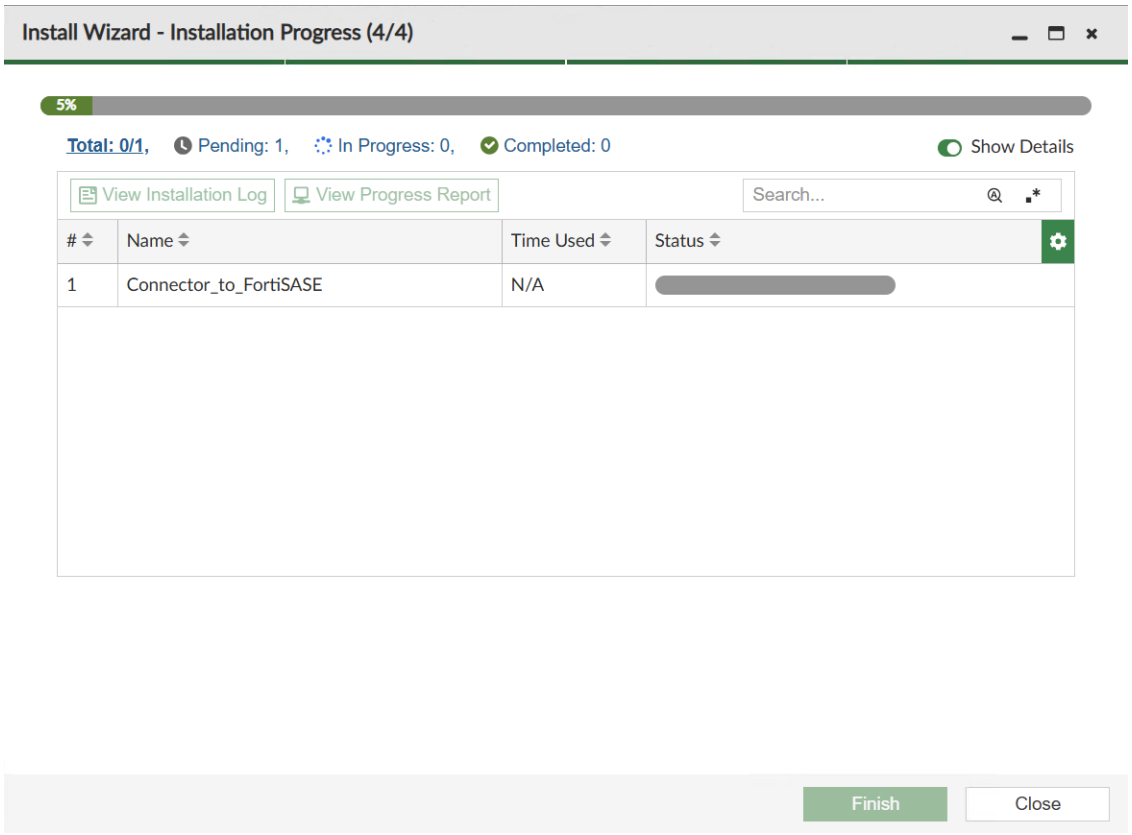

Install Wizard - Choose What to Install (1/4)
Install Policy Package & Device Settings
Install Device Settings (only)
Install only device settings for a select set of devices. Policy and Object changes will not be updated from the last install.
Install Comments
0/127
< Back
Next >
Cancel


Install Wizard - Select Devices to Install (2/4)
Please select one or more devices to install (Use checkbox or Ctrl or Shift key for multiple selections)
Search...
Device Name
IP Address
Platform
Connector_to_FortiSASE
FortiSASE-Generic
Total Selected: 1
1
< Back
Next >
Cancel

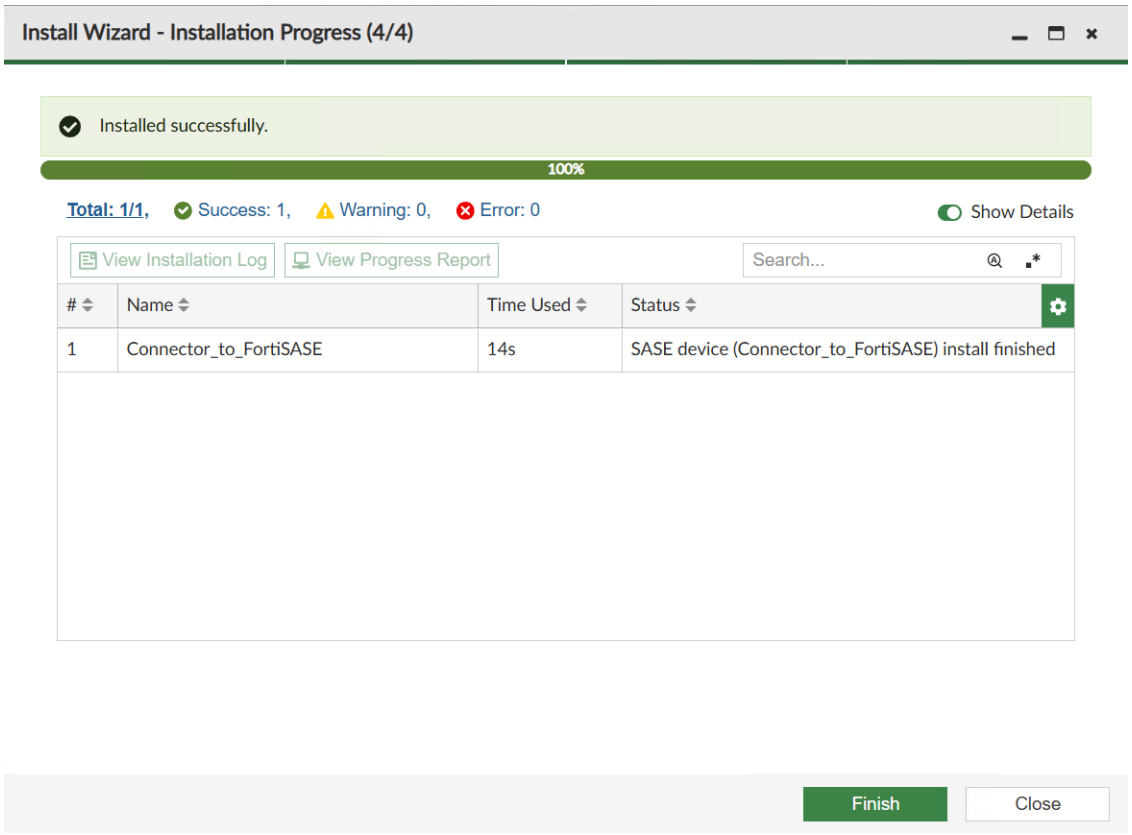

Install Wizard - Validate Devices (3/4)
Installation Preparation
Total: 2/2,
Success: 2,
Warning: 0,
Error: 0
Show Details
Ready to Install
Only successfully validated device may be installed. Please confirm and click "Install" button to continue.
Install Preview
Search...
Device Name
Status
Action
Connector_to_FortiSASE
Connection Up
< Back
Install
Cancel

Optionally, click on *Install Preview* to see a CLI command preview of the configuration settings to be installed in FortiSASE. Click *Close* to exit the preview.

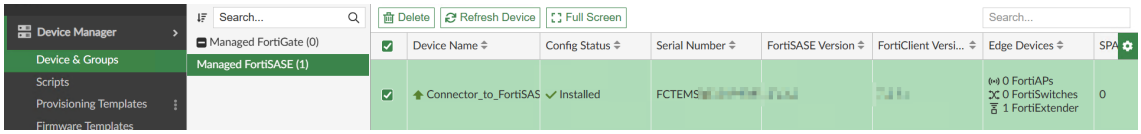




8. Click *Finish* to close the wizard.



9. Observe the *Config Status* has been updated to Installed after completing the *Install Wizard* steps.



Configuring settings using policy packages in FortiManager

Using policy packages in FortiManager ensures seamless and consistent security policy management of FortiSASE and FortiGate devices from a single console used for centralized management.

After Configuring FortiManager for central management on page 600, you can configure and synchronize policy management settings (firewall policies, firewall proxy policies, firewall schedules, security posture tags) using policy packages in FortiManager.

- Objects include items such as firewall addresses, services, security profile groups, external feeds, users and user groups, and authentication sources.
- Objects are used to define policies, and policies are assembled into policy packages that you can install on FortiSASE.
- In FortiManager, policy packages are managed in Policy & Objects > Policy Packages.

Configuration workflow

1. FortiManager:
   a. Create and configure supported objects first using these pages:
      - *Policy & Objects > Firewall Objects*
      - *Policy & Objects > Security Profiles*: Configure individual security profiles and select them in a profile group
      - *Policy & Objects > User & Authentication*
      - *Policy & Objects > Advanced > CLI Configurations*

      You will need to configure desired objects first before they can be selected in firewall or proxy policies. See Supported objects for policies and proxy policies on page 614.
   b. Configure a policy package. See Create new policy packages. FortiSASE only supports the following policy package settings:
      - Central NAT: Either disabled or enabled. This setting has no impact on FortiSASE functionality.
      - NGFW: Profile-based
      - Policy Offload Level: Disable
      - In Folder: Empty.
        i. Create policies within a policy package.
           - For firewall policies, see Create a new firewall policy.
           - For proxy policies, see Create a new proxy policy.
        ii. Add an installation target for the policy package. See Policy package installation targets.
   c. Install the newly created policy package. See Install a policy package.
2. FortiSASE:
   a. Verify the configuration has been synchronized from FortiManager:
      - *Security > Traffic > Policies*
      - *Security > Traffic > Proxy policies*

      See Verifying configuration updates performed using central management on page 602.
   b. If necessary, you may need to troubleshoot failed synchronization attempts. See Displaying error messages for failed synchronization attempts on page 603.

For a demonstration of this configuration workflow, see Example: Creating a Secure Internet-access agent tunnel policy using a policy package in FortiManager on page 633.

Prerequisites and considerations

Prerequisites

The following objects must be enabled when synchronizing policy packages with FortiSASE:

- To use security profiles in firewall or proxy policies, you must enable *Security Profiles > Profile Group*.
- For proxy policy support, enable *Policy > Proxy Policy*.
- To display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page such as *Policy & Objects > Security Profiles or Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

Considerations

- FortiSASE supports global policy packages. See Assign a global policy package.
- FortiSASE interfaces are not created by default in the *Global Database* ADOM when the *Connector to FortiSASE* is enabled.
- In the *Global Database* ADOM, you must manually configure the normalized interfaces that the *Connector to FortiSASE* automatically configures within an ADOM when it is enabled. See Normalized interfaces used with FortiSASE on page 616.

Supported objects for policies and proxy policies

Central management does not support synchronizing client-to-client traffic policies, that is, policies where the incoming interface and outgoing interface are both specified as *SASE_ingress_zone*.

FortiSASE supports selected FortiManager objects that can be synchronized for policies and proxy policies.

Firewall policies

Field	Supported values	Unsupported values
Type	Standard	ZTNA
Incoming interface	SASE_ingress_zone SASE_public_zone SASE_secure_private_access_zone	All other interfaces, predefined or custom.
Outgoing interface	SASE_ingress_zone SASE_public_zone SASE_secure_private_access_zone	All other interfaces, predefined or custom.
Source	Address / address groups • Geography addresses Users / user groups including user groups with SSO via SAML	Internet Service Edge device
Negate Source	Disabled	Enabled
Security Posture Tag	Security posture tags • Tags synchronized and rules mapped. • See Synchronizing security posture tags using FortiClient EMS Connector on page 617. Security posture tag groups	-
Destination	Address / address groups	Internet Service
Negate Destination	Disabled	Enabled

Field	Supported values	Unsupported values
Service	Service / service groups	-
Schedule	always none One-time Recurring Schedule groups	
Action	Accept Deny	IPSEC
Inspection Mode	Proxy-based	Flow-based
Firewall/Network Options	Not supported by FortiSASE	
Display Disclaimer	Not supported by FortiSASE	
Security Profiles > Security Profiles Status	Disabled or enabled	-
Security Profiles > Profile Type	Use Security Profile Group	Use Standard Security Profiles
Block Notification	Not supported by FortiSASE	
Log Allowed Traffic	Security Events All Sessions	-
Traffic Shaping Options	Not supported by FortiSASE	
Enable this policy	Enabled Disabled	-
Advanced Options	Not supported by FortiSASE	

Proxy policies

Field	Supported values	Unsupported values
Explicit Proxy Type	Explicit Web	Transparent Web FTP WAN Optimize
Outgoing interface	SASE_ingress_zone SASE_public_zone SASE_secure_private_access_zone	All other interfaces, predefined or custom.
Source	Address / address groups Use / user groups including user groups with SSO via SAML	-
Negate Source	Disabled	Enabled

Field	Supported values	Unsupported values
Destination	Address / address groups	Internet Service
Negate Destination	Disabled	Enabled
Service	Service / service groups	-
Schedule	always none One-time Recurring Schedule groups	
Action	Accept Deny	-
Firewall/Network Options	Not supported by FortiSASE	
Disclaimer Options	Not supported by FortiSASE	
Security Profiles > Security Profiles Status	Disabled or enabled	-
Security Profiles > Profile Type	Use Security Profile Group	Use Standard Security Profiles
Profile Group	< Any security profile group >	-
Log Allowed Traffic	Security Events All Sessions	-
Enable this policy	Enabled Disabled	-
Advanced Options	Not supported by FortiSASE	

Normalized interfaces used with FortiSASE

When the *Connector to FortiSASE* is enabled in FortiManager, this connector automatically configures normalized interfaces within the selected ADOM to be used for synchronizing with FortiSASE.

Normalized interface	Description
SASE_ingress_zone	Zone for remote agents and edge endpoints
SASE_public_zone	Zone for external networks
SASE_secure_private_access_zone	Zone for private networks.

For example, when the *Connector to FortiSASE* is enabled in the *root* ADOM:

Name	Mapping Rule	Mapped Interface/Zone	Description	Created Time
SASE_ingress_zone			Created by SASE manager	admin /
	Per-device (Connector_to_FortiSASE (root))	SASE_ingress_zone	Created by SASE manager	admin /
	Default	SASE_ingress_zone	Created by SASE manager	admin /
SASE_public_zone			Created by SASE manager	admin /
	Per-device (Connector_to_FortiSASE (root))	SASE_public_zone	Created by SASE manager	admin /
	Default	SASE_public_zone	Created by SASE manager	admin /
SASE_secure_private_access_zone			Created by SASE manager	admin /
	Per-device (Connector_to_FortiSASE (root))	SASE_secure_private_access_zone	Created by SASE manager	admin /
	Default	SASE_secure_private_access_zone	Created by SASE manager	admin /

These interfaces, specified as incoming and outgoing interfaces, and the resulting traffic flow are used to define FortiSASE policy types. See Mapping of FortiManager policies to FortiSASE policies on page 630 .

Considerations

- FortiSASE supports global policy packages. See Assign a global policy package.
  - FortiSASE interfaces are not created by default in the *Global Database* ADOM when the *Connector to FortiSASE* is enabled.
  - In the *Global Database* ADOM, you must manually configure the normalized interfaces that the *Connector to FortiSASE* automatically configures within an ADOM when it is enabled.
- Central management does not support synchronizing client-to-client traffic policies, that is, policies where the incoming interface and outgoing interface are both specified as *SASE_ingress_zone*.

Synchronizing security posture tags using FortiClient EMS Connector

In FortiSASE, security posture tags can be managed in *Endpoint management > Security posture tags*. FortiSASE includes its own EMS instance as part of the service.

In FortiManager, you can use the *FortiClient EMS Connector* to synchronize security posture tags from FortiSASE. These security posture tags retrieved from FortiSASE can then be configured in policies. See Creating FortiClient EMS connectors.

Synchronizing FSSO Connector settings and FSSO user groups

FSSO is meant to be used with domain-joined Windows clients behind branch on-ramp devices or edge devices. FSSO provides the mapping of the Windows client's IP address with its currently logged-in username for these use cases.

In FortiSASE, FSSO Connector settings can be managed in *Access & authentication > Authentication Sources > Fortinet Single Sign-On (FSSO)* and FSSO user groups can be managed in *Access & authentication > Access > Users and groups*.

In FortiManager, you can use SSO/identity connectors for *Fortinet single sign-on (FSSO) agents* to synchronize FSSO connectors to FortiSASE. These FSSO connectors can then be configured in policies. See FSSO user groups.

This example demonstrates how to create an FSSO Connector to be used with a FortiAuthenticator configured as an FSSO collector agent for polling a Windows Active Directory server directly connected to the FortiAuthenticator. This example builds upon an existing and already configured FortiAuthenticator and Windows Active Directory setup. For further details on this use case, see SSO using a FortiGate, FortiAuthenticator, and DC Polling.

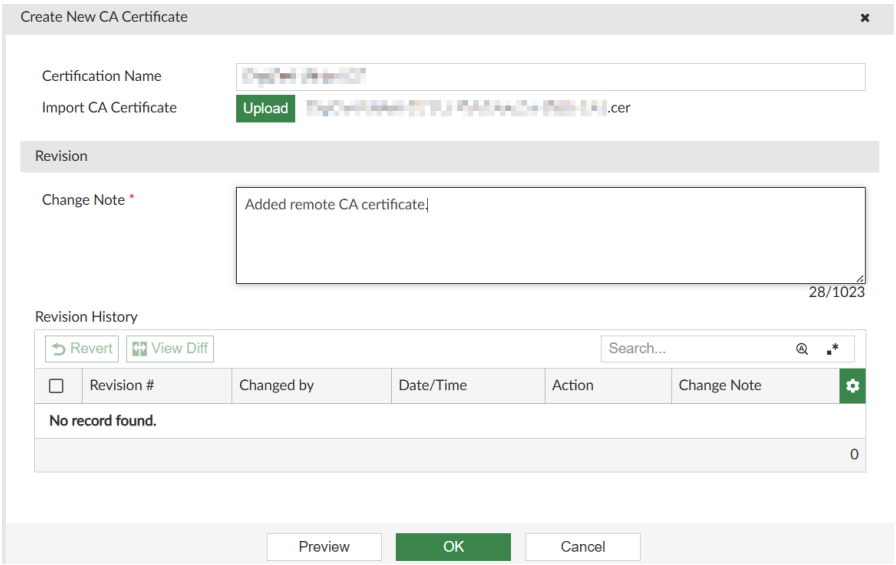
The FSSO Connector is subsequently used to create FSSO user groups, which are used to provide identity-based access in a secure internet-access policy using a policy package in FortiManager. This policy package is synchronized with a FortiSASE instance using central management support.

The central management configuration workflow is as follows:

1. In FortiManager, create a policy package as follows:
   a. Upload a new remote CA certificate. This is used with the FSSO Connector configuration for SSL-encrypted communication between FortiSASE and the FortiAuthenticator.
   b. Create a new FSSO Connector to be used with a FortiAuthenticator.
   c. Create a new FSSO user group.
   d. Configure a security profile and a secure internet access firewall policy that uses the FSSO user group.
2. In FortiManager, synchronize the policy package with FortiSASE.
3. In FortiSASE, confirm the policy package has been synchronized as desired.

To create an FSSO identity-based secure internet-access policy using a policy package in FortiManager:

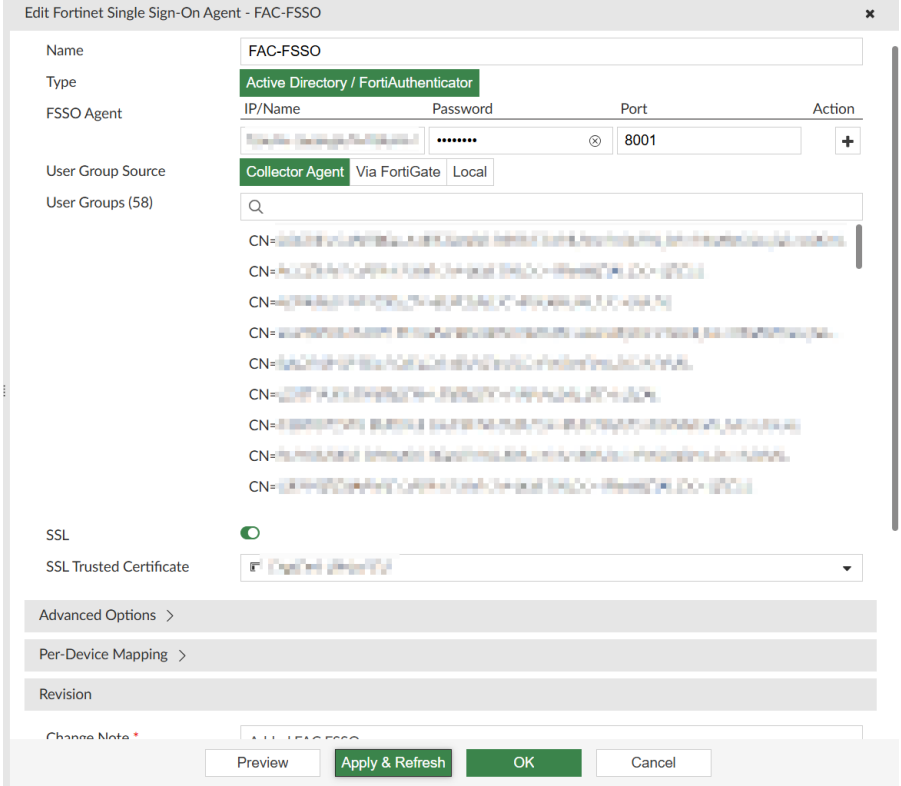
1. In FortiManager, go to *Policy & Objects* > *Advanced* > *CA Certificates* and click *Import*.
   a. In the *Create New CA Certificate* pane, enter the *Certification Name* and click *Upload* next to *Import CA Certificate*.
   b. In the *Upload CA Certificate* pane, either drag and drop or *Browse* to select the CA certificate that signed the certificate used on the FortiAuthenticator for its FSSO collector agent feature.
   c. Click *OK*.
   d. Enter a *Change Note* and click *OK*.



2. Go to *Policy & Objects > Security Fabric > Endpoint/Identity* and click *+Create New > Fortinet Single Sign-On Agent*.
   a. Enter the following settings:

Field		Value
Name		FAC-FSSO (Arbitrary name of FSSO agent)
Type		Active Directory/FortiAuthenticator
FSSO Agent		
	IP/Name	<IP address or hostname of FortiAuthenticator accessible either publicly or via SPA>
	Password	<Shared password configured in FortiAuthenticator settings via *Fortinet SSO > Settings > FortiGate*>
	Port	8001 (used by FortiSASE with SSL-encrypted communications)
	User Group Source	Collector Agent
	SSL	Enabled
	SSL Trusted Certificate	<Select CA certificate uploaded previously>
Change Note		<Arbitrary change note>

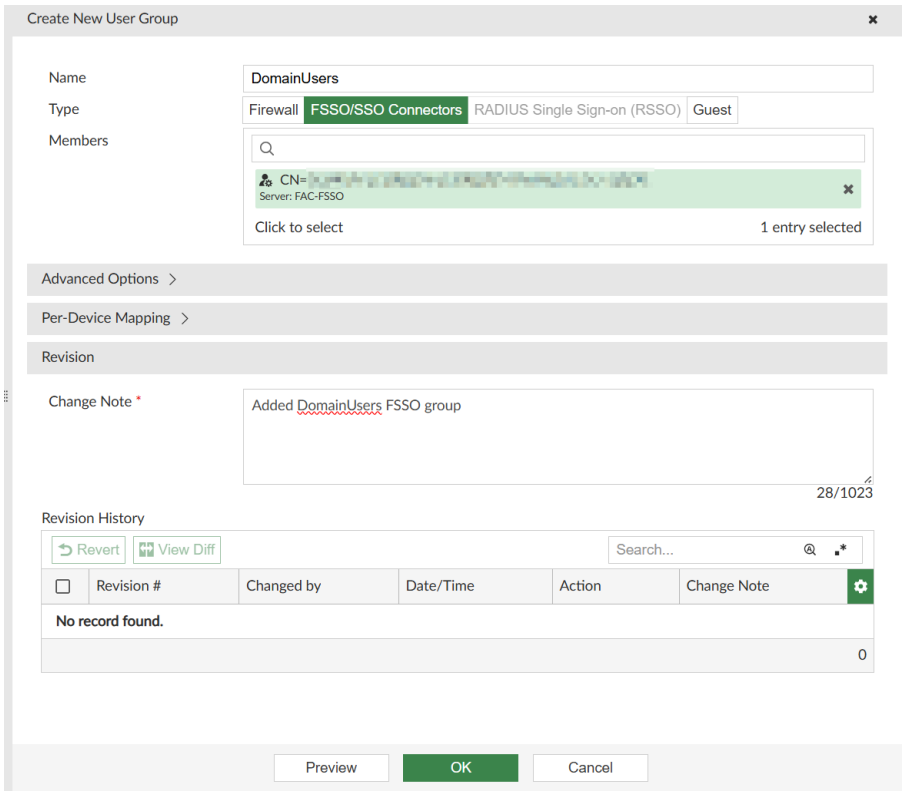
   b. Retrieve FSSO user groups from the FortiAuthenticator by clicking *Apply & Refresh* followed by *Next* in prompt. Observe *User Groups (0)* change to *User Groups (<number of FSSO groups retrieved>)*.
   c. Click *OK*.



3. Go to *Policy & Objects* > *User & Authentication* > *User Groups* and click *+Create New* .
   a. Enter the following settings:

Field	Value
Name	DomainUsers (Arbitrary name of FSSO user group)
Type	FSSO/SSO Connectors
Members	<Click to select> then use checkboxes to select one or more FSSO groups from the list and then click *OK*.
Change Note	<Arbitrary change note>

   b. Click *OK*.



4. Create a new policy package by clicking *Policy Package* > *New*:
   a. Configure these settings:

Field	Value
Name	custom
Central NAT	Disabled
NGFW Mode	Profile-based
Policy Offload Level	Disable
In Folder	<Empty>

   b. Click *OK*.
5. Click the custom policy package, click *Firewall Policy* and then click *+Create New* > *+Create New*.
6. In the *Create New Firewall Policy* dialog:

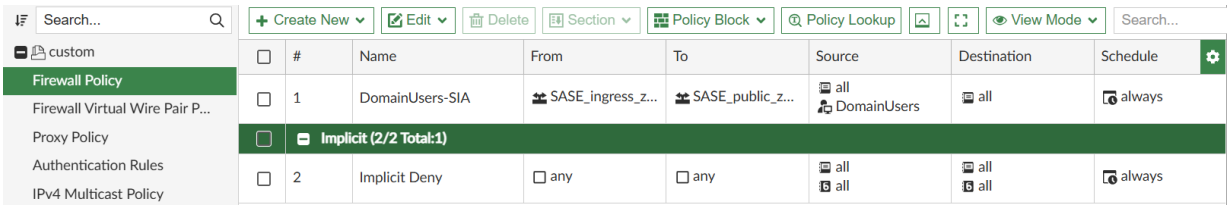
a. Configure these settings:

Field	Value
Name	SIA-Policy-1
Type	Standard
Incoming interface	SASE_ingress_zone
Outgoing interface	SASE_public_zone
Source	Address > all User > User Group > DomainUsers
Negate Source	Disabled
Security Posture Tag	<Empty>
Destination	Address group > all
Negate Destination	Disabled
Service	ALL
Schedule	Always
Action	Accept
Inspection Mode	Proxy-based
Security Profiles > Security Profiles Status	Enabled
Security Profiles > Profile Type	Use Security Profile Group

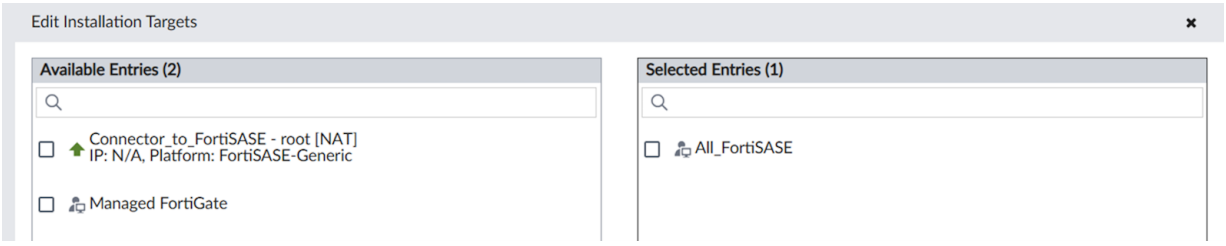
Profile Group	1. Click *+Create*.
	2. Configure a new profile group:
	  a. *Name*: DomainUsers
	  b. *Web Filter Profile*: DomainUsers
	  i. Create new web filter profile with *FortiGuard Category Based Filter* enabled and the *Gambling* category blocked (as an example).
	  c. *SSL/SSH inspection*: certificate-inspection
	  d. *Protocol Options*: default
	3. Add a *Change Note*.
	4. Click *OK*.

Log Allowed Traffic	All Sessions
Enable this policy	Enabled

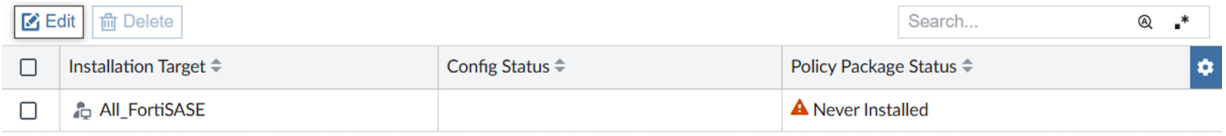
b. Add a *Change Note* then click *OK*.



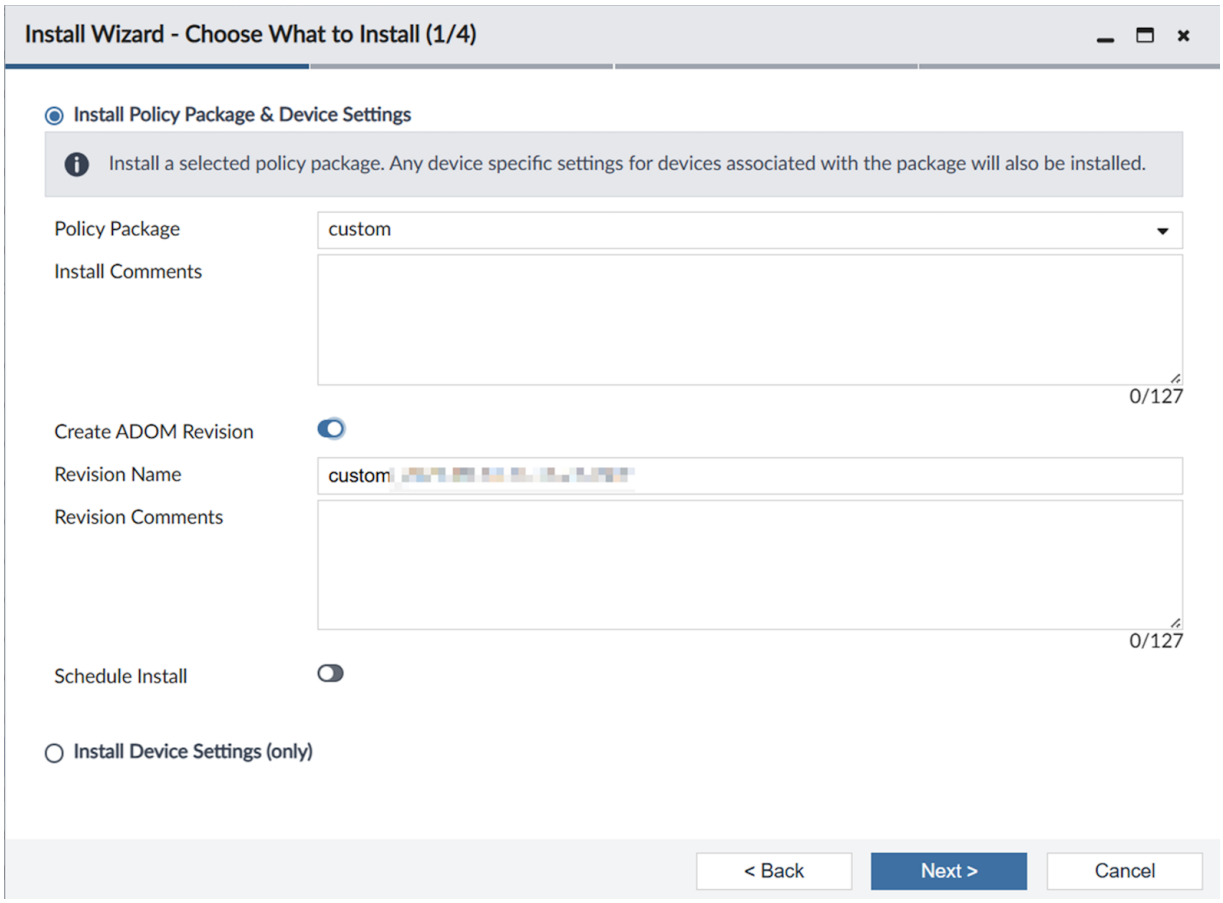
7. In the *custom* policy package, click *Installation Targets*:
   a. Click *Edit*.
   b. In the *Available Entries* column, select *All_FortiSASE* and then click to move it to the *Selected Entries* column.



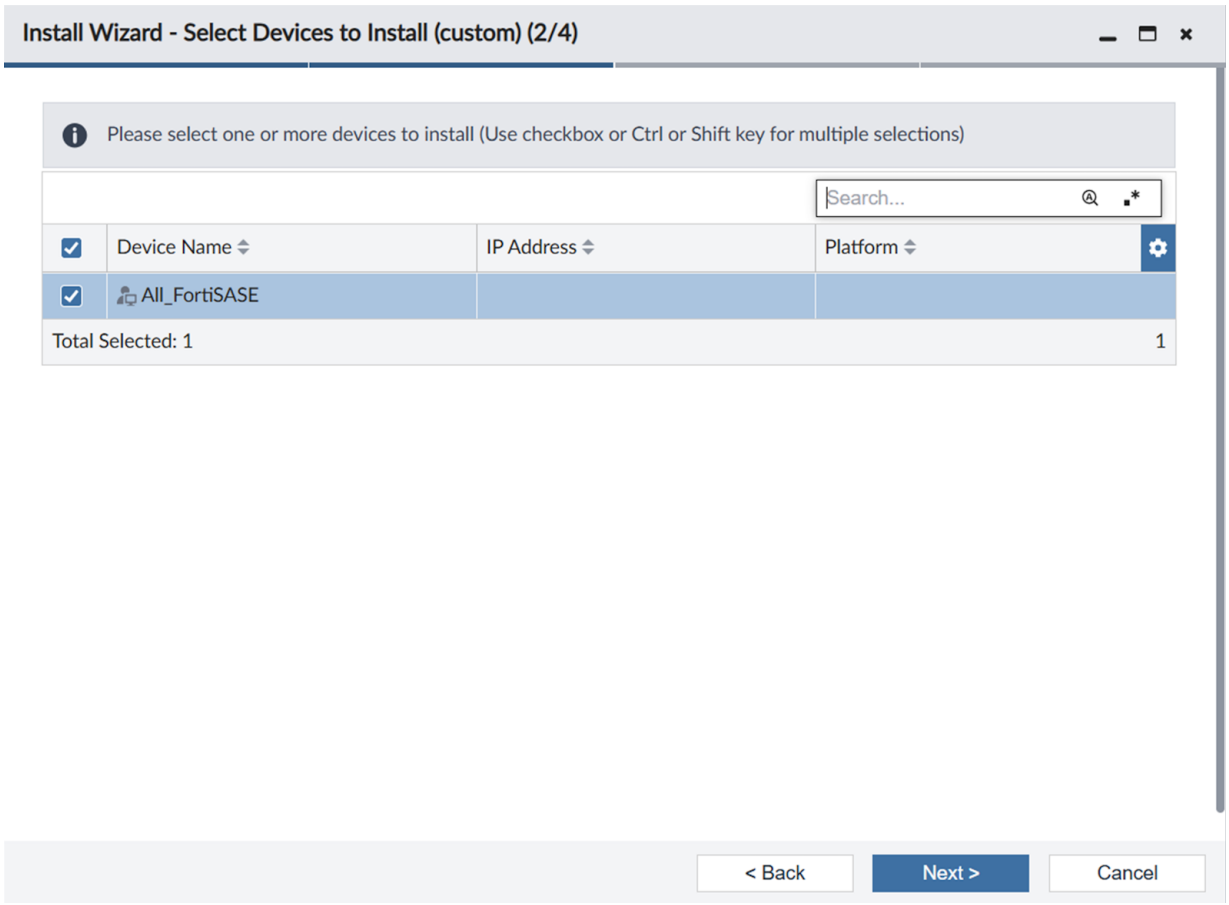
   c. Click *OK*.
   For the *All_FortiSASE* installation target, observe the *Policy Package Status* of *Never Installed*.



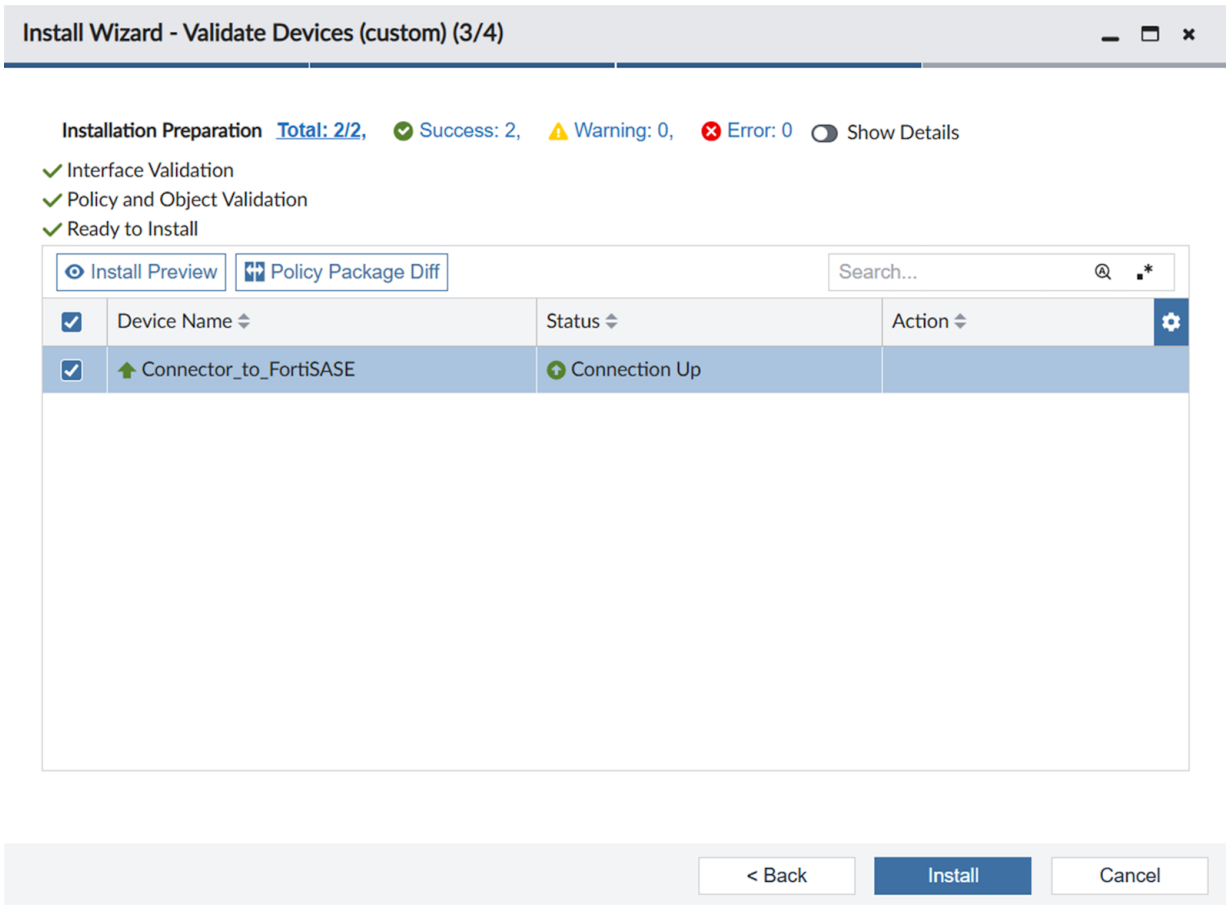
8. Click *Install Wizard*.
   a. Select *Install Policy Package & Device Settings* and observe the *custom Policy Package* is selected. Click *Next*.



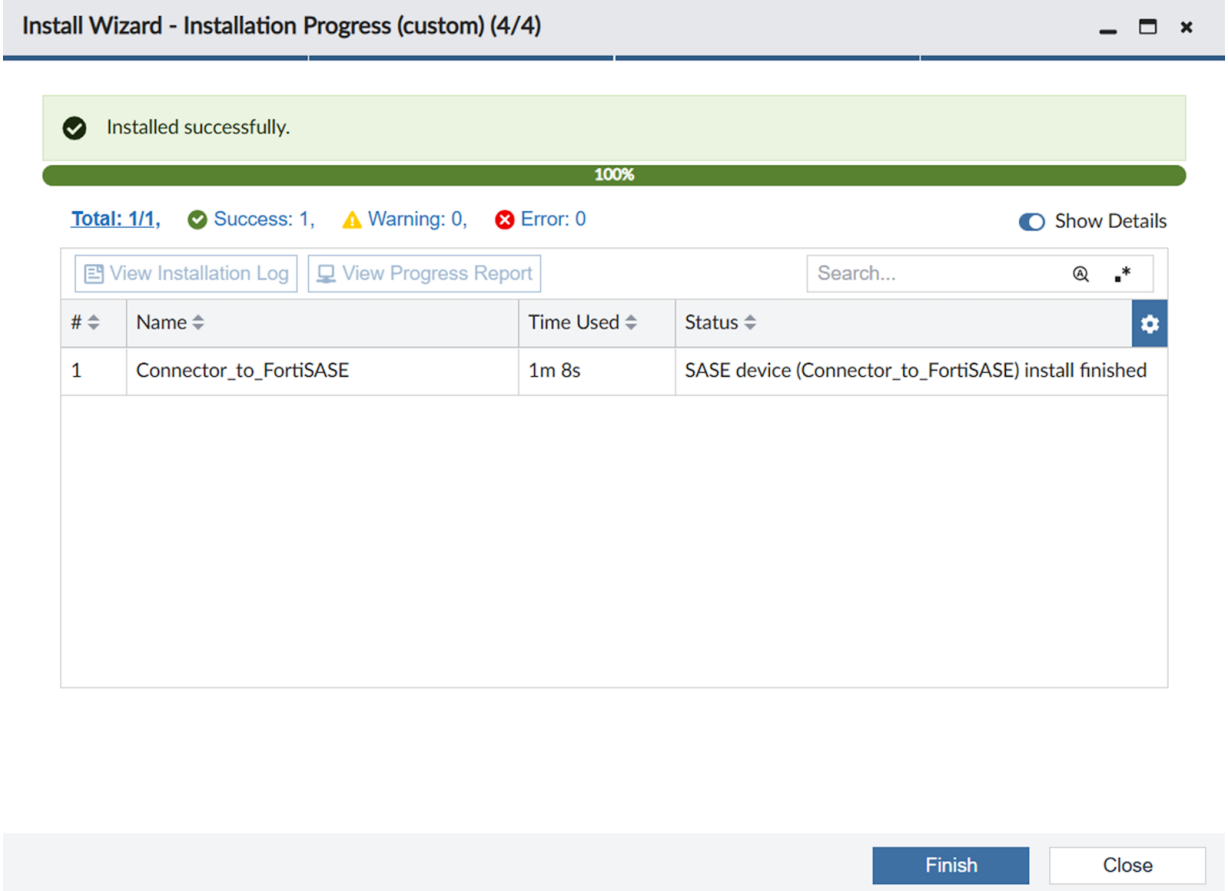
b. Observe the *All_FortiSASE* installation target is selected and click *Next*.



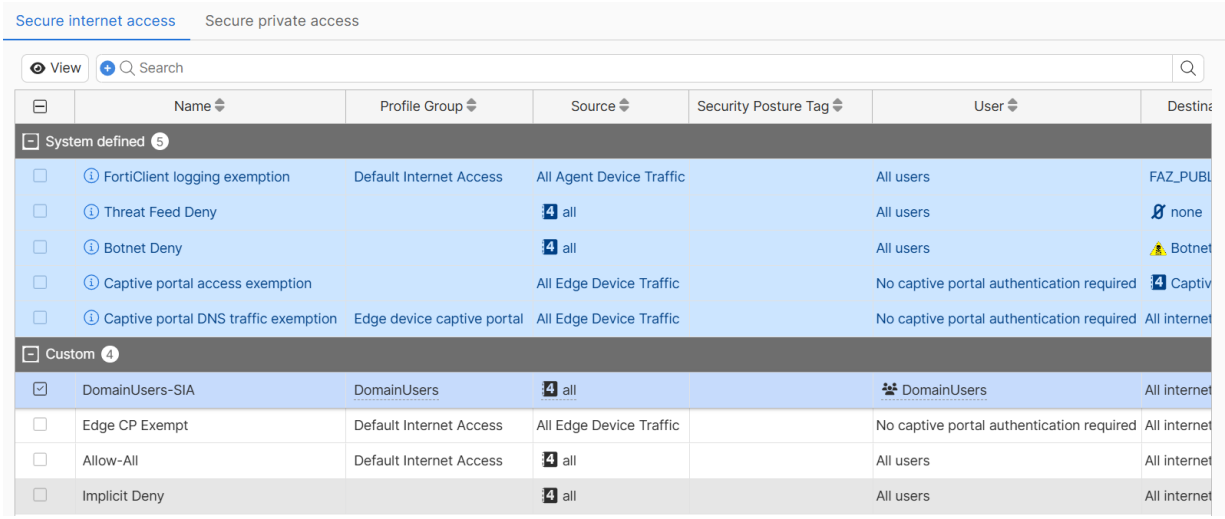
c. Observe validation succeeds and click *Install*.



d. Observe the installation progress. If no errors occur, then observe *Installed successfully*. Click *Finish*.

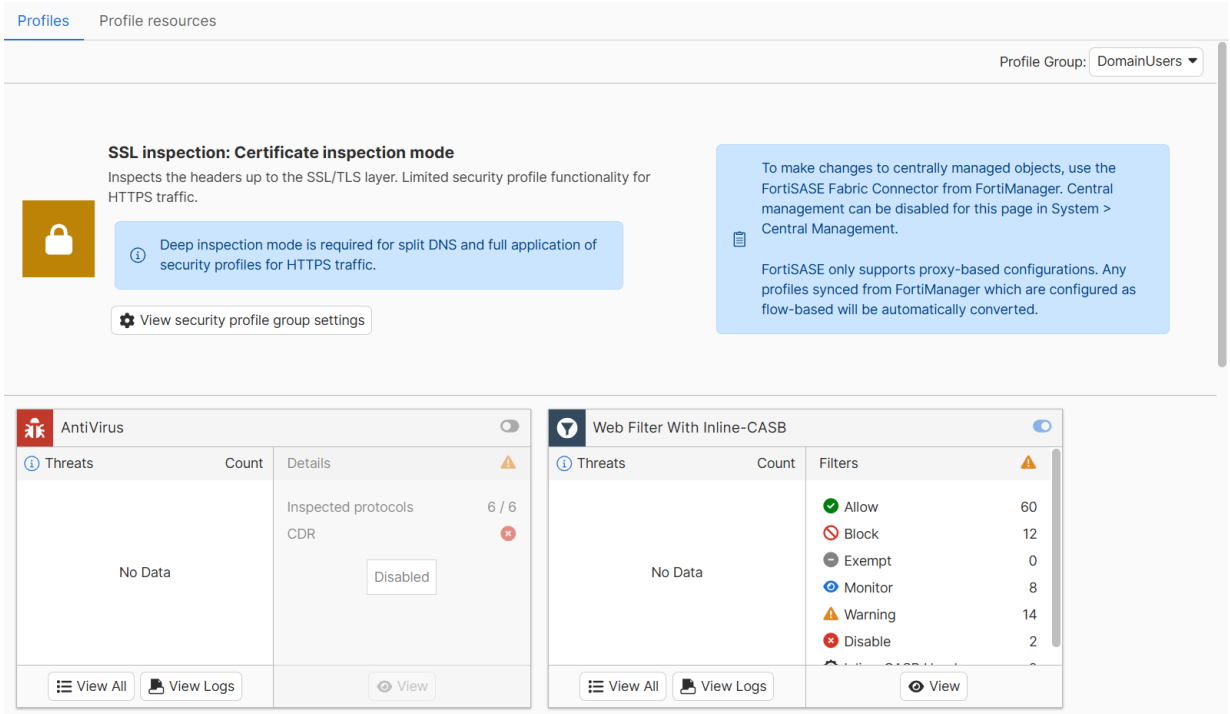


9. In FortiSASE, observe the desired settings have been synchronized as desired:
   a. Go to *Security* > *Traffic* > *Policies* and observe the newly created policy *DomainUsers-SIA*.

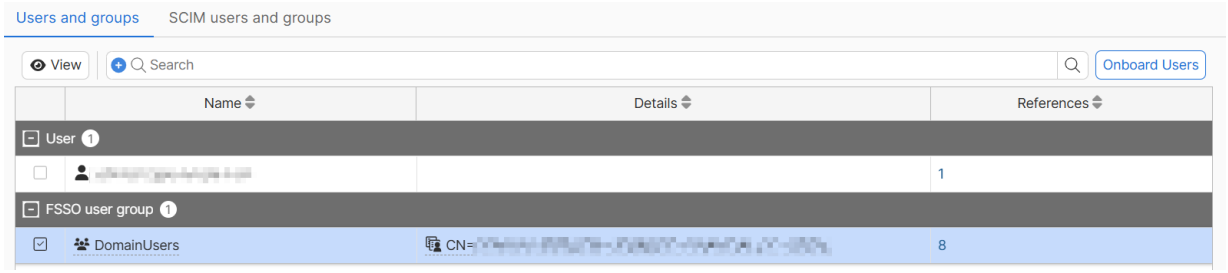


   Observe that there is a captive portal exemption policy *Edge CP Exempt* for *All Edge Device Traffic* in this example setup. Currently, this type of policy is not supported by central management and must be configured through the FortiSASE portal prior to enabling central management. This policy ensures that captive portal authentication is not required for clients behind branch on-ramp devices and edge devices.

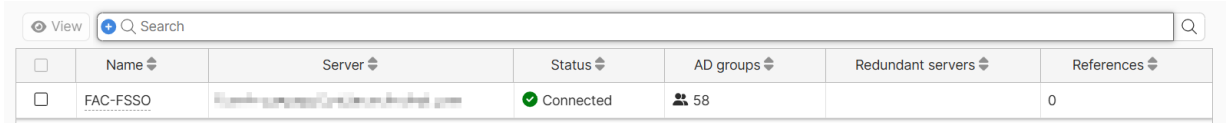
b. Go to *Security > Traffic > Security profiles* and observe the *DomainUsers* security profile group has been created with *Web Filter With Inline-CASB* enabled and certificate inspection configured.



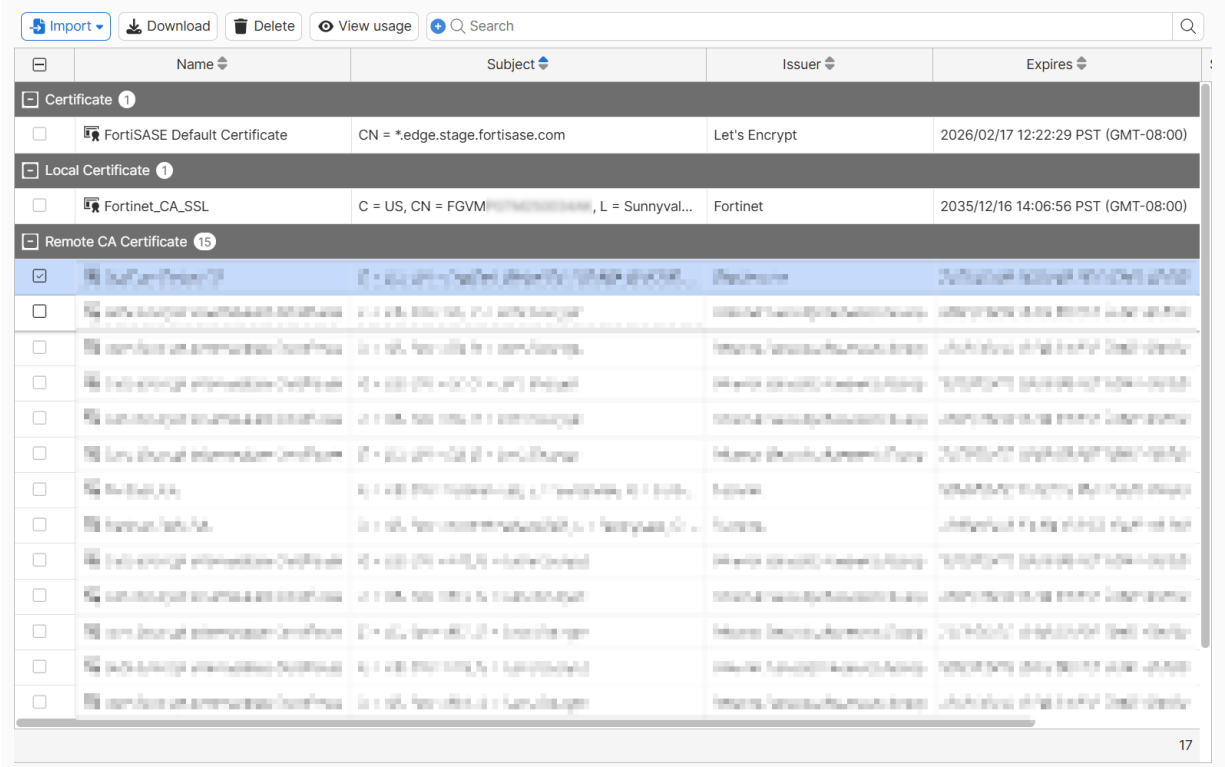
c. Go to *Access & authentication > Access > Users and groups* and observe the FSSO user group *DomainUsers*.



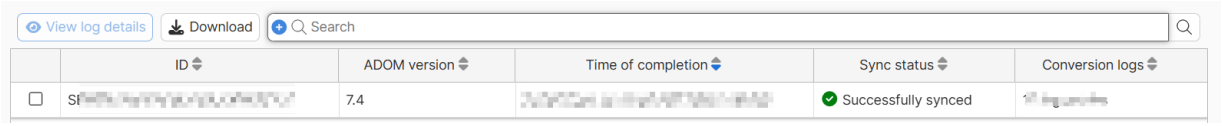
d. Go to *Access & authentication > Authentication Sources > Fortinet Single Sign-On (FSSO)* and observe the new FSSO entry.



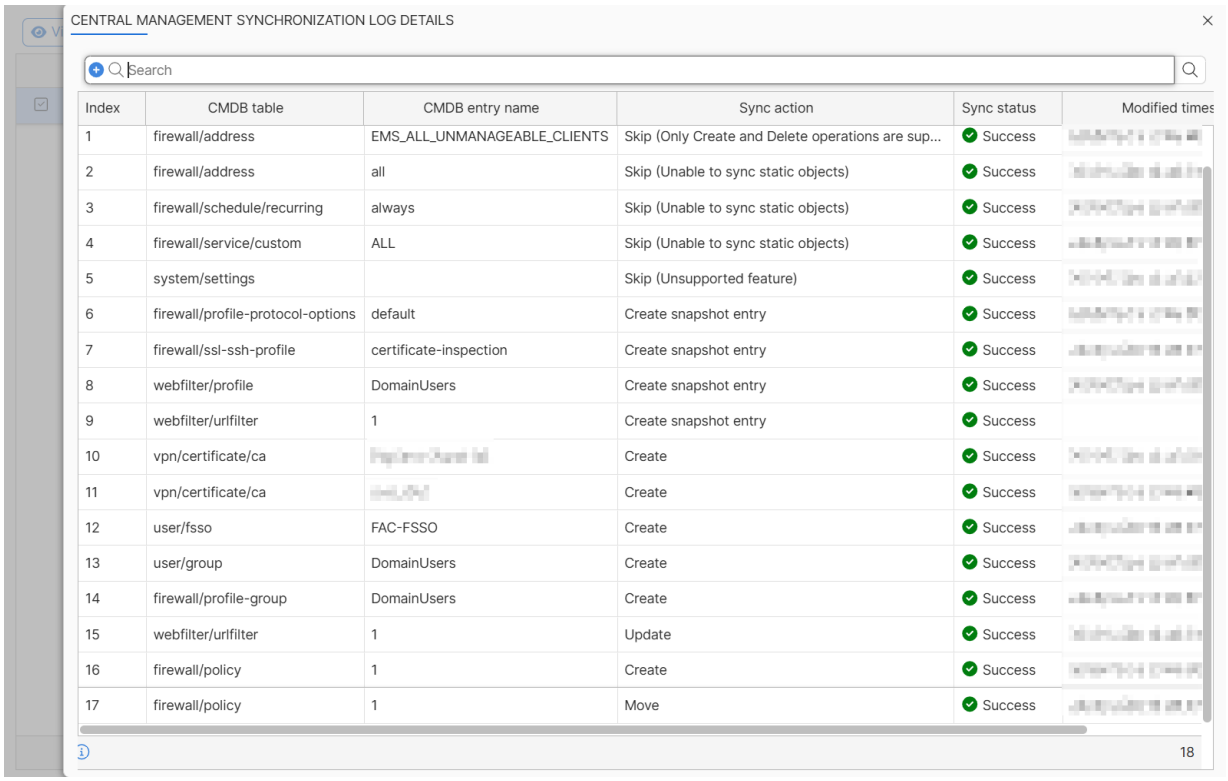
e. Go to *System > Certificates > Remote CA Certificate* and observe the CA certificate has been installed.



10. Go to *Operations* > *Logs* > *Central management synchronizations* to verify the synchronization status.



11. Click on the log entry and click *View log details* to see desired configuration settings have been synchronized from FortiManager.



Mapping of FortiManager policies to FortiSASE policies

Using the normalized interfaces created by the FortiSASE connector, you can configure policies in FortiManager which map to specific FortiSASE policies based on the traffic flow from incoming to outgoing interfaces.

FortiSASE policy type	Visible in FortiSASE	Description	Incoming interface	Outgoing interface
Policy	Always	Secures access from remote agents and edge endpoints to external networks.	Ingress Zone	Public Zone
Private access policy: To Hubs	When SPA feature is licensed and configured.	Secures access from remote agents and edge endpoints to private networks.	Ingress Zone	Private Access Zone
Private access policy: From Hubs	When SPA feature is licensed and configured.	Secures access from private networks to remote agents only.	Private Access Zone	Ingress Zone

FortiSASE policy type	Visible in FortiSASE	Description	Incoming interface	Outgoing interface
Proxy policy	When Proxy feature is enabled.	Secures access from Proxy users to external networks.	Not configurable	Public Zone
Proxy Private Access Policy	When Proxy feature is enabled and SPA feature is licensed and configured.	Secures access from Proxy users to private networks.	Not configurable	Private Access Zone

It is important to note that you can only synchronize a policy type when it is visible in FortiSASE and the corresponding feature is enabled with the proper licensing and configuration dependencies.

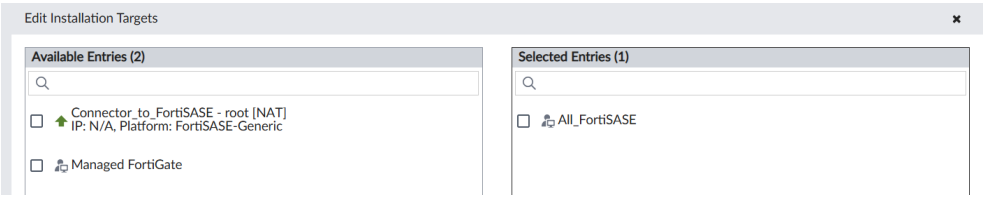
For example, if you attempt to synchronize a Proxy policy from FortiManager to FortiSASE, and the Proxy feature is not enabled, then the synchronization attempt will fail.

Configuring installation targets

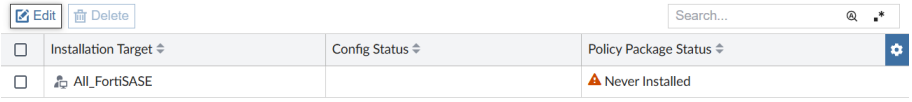
Prior to installing a policy package, FortiSASE must be specified as an installation target.

To configure FortiSASE as an installation target:

1. In the *custom* policy package, click *Installation Targets*:
2. Click *Edit*.
3. In the *Available Entries* column, select *All_FortiSASE* then click > to move it to the *Selected Entries* column.



4. Click *OK*.
   For the *All_FortiSASE* installation target, observe the *Policy Package Status* of *Never Installed*.

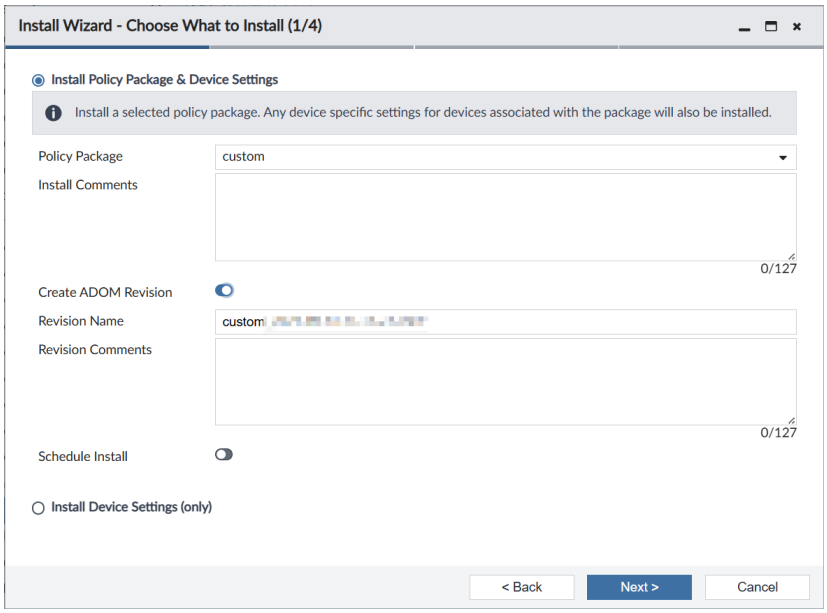


Installing policy package and device settings with the Install Wizard

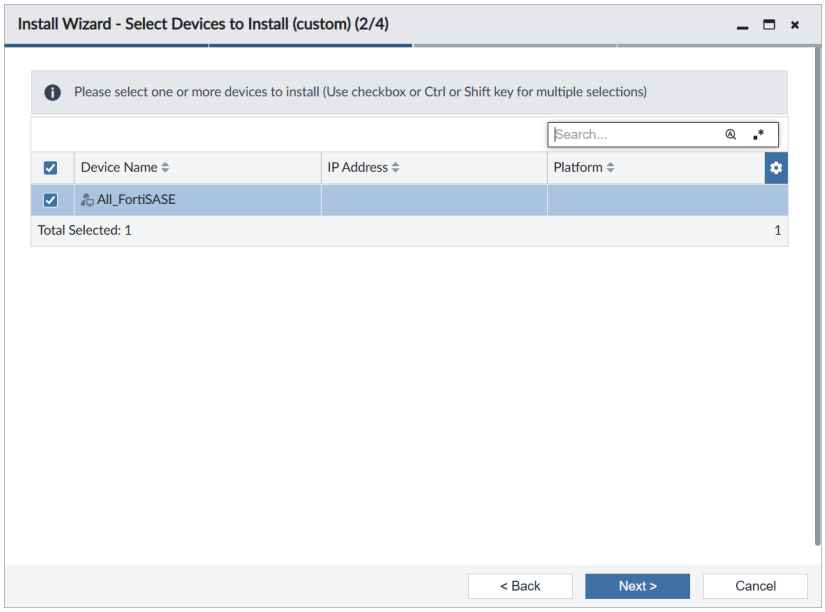
The *Install Wizard* is used to install the specified policy package and device settings.

To install a policy package & device settings with the Install Wizard:

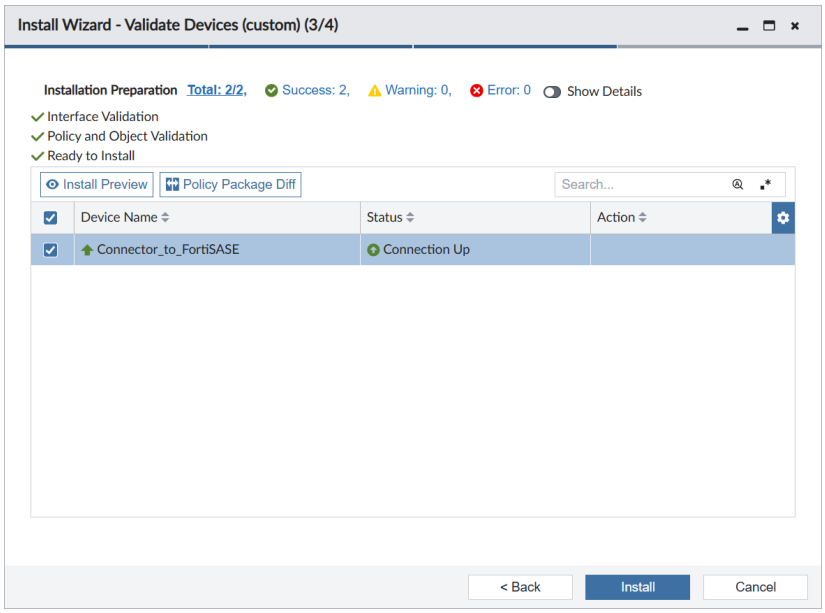
1. Click *Install Wizard*.
2. Select *Install Policy Package & Device Settings* and observe the *custom* Policy Package is selected. Click *Next >*.



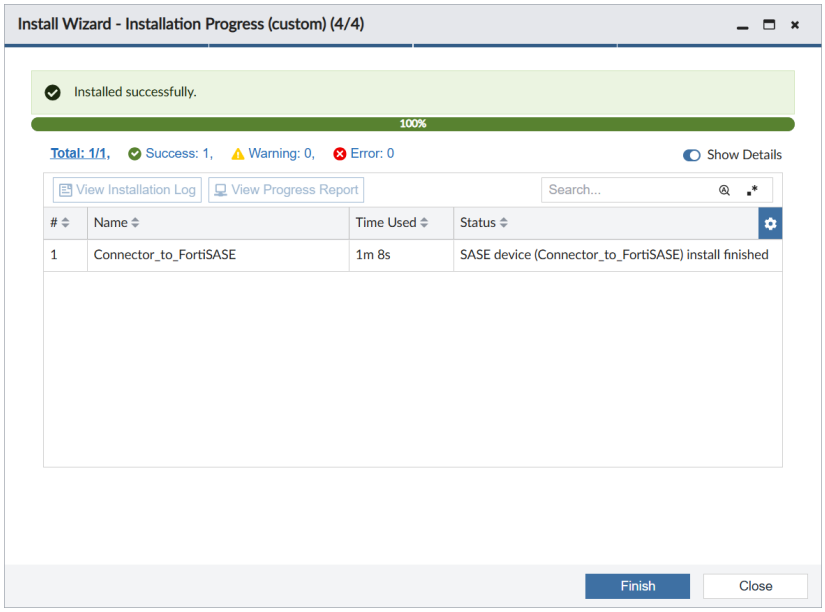
3. Observe the *All_FortiSASE* installation target is selected and click *Next >*.



4. Observe validation succeeds and click *Install*.



5. Observe the installation progress. If no errors occur, then observe *Installed successfully*. Click *Finish*.



Example: Creating a Secure Internet-access agent tunnel policy using a policy package in FortiManager

After Configuring FortiManager for central management on page 600, you can configure and synchronize policy management settings (firewall policies, firewall proxy policies, firewall schedules, security posture tags) using policy packages in FortiManager.

This example demonstrates how to create a secure internet-access agent tunnel policy using a policy package in FortiManager and synchronize it with a FortiSASE instance.

To create a secure internet-access agent tunnel policy using a policy package in FortiManager:

1. In FortiManager, go to *Policy & Objects* > *Policy Packages*.
2. Create a new policy package by clicking *Policy Package* > *New*:
   a. Configure these settings:

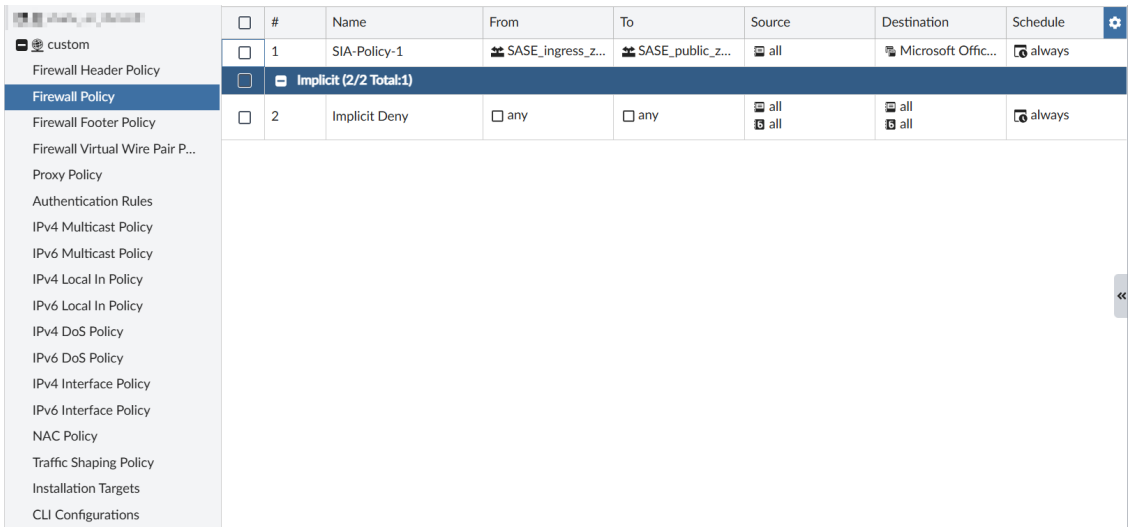
Field	Value
Name	*custom*
Central NAT	*Disabled*
NGFW Mode	*Profile-based*
Policy Offload Level	*Disable*
In Folder	*< Empty >*

   b. Click *OK*.
3. Click the custom policy package, click *Firewall Policy* and then click *+Create New* > *+ Create New*. For this example, the default policy package is used.
4. In the *Create New Firewall Policy* dialog:

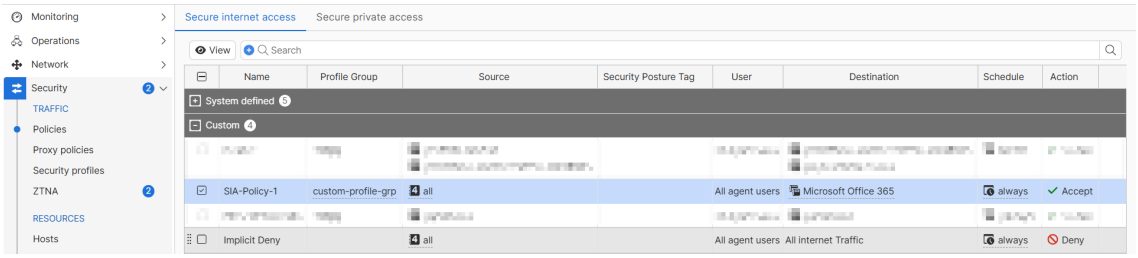
a. Configure these settings:

Field	Value
Name	*SIA-Policy-1*
Type	*Standard*
Incoming interface	*SASE_ingress_zone*
Outgoing interface	*SASE_public_zone*
Source	*All*
Negate Source	*Disabled*
Security Posture Tag	*<Empty>*
Destination	*Address group > Microsoft Office 365*
Negate Destination	*Disabled*
Service	*ALL*
Schedule	*Always*
Action	*Accept*
Inspection Mode	*Proxy-based*
Security Profiles > Security Profiles Status	*Enabled*
Security Profiles > Profile Type	*Use Security Profile Group*
Profile Group	**1.** *+Create* **2.** Configure a new profile group: **a.** *Name: custom-profile-grp* **b.** *AntiVirus Profile: default* **c.** *SSL/SSH inspection: certificate-inspection* **d.** *Protocol Options: default* **3.** Add a *Change Note*. **4.** Click *OK*.
Log Allowed Traffic	*All Sessions*
Enable this policy	*Enabled*

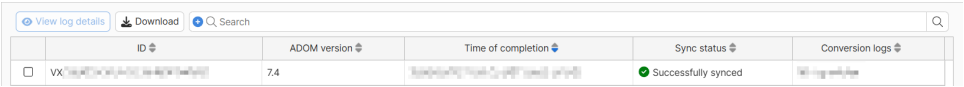
b. Add a *Change Note* then click *OK*.



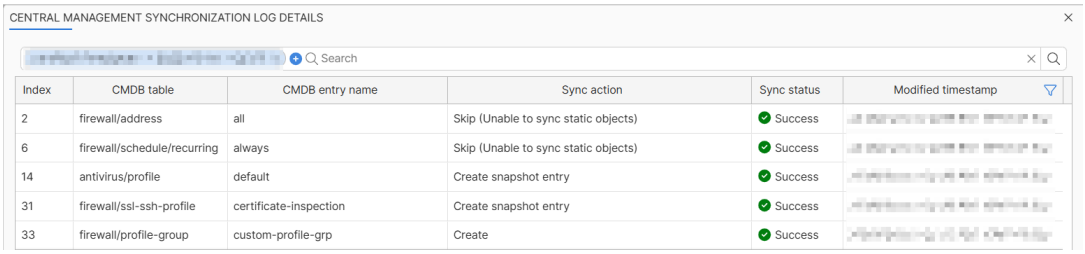
5. In the *custom* policy package, click *Installation Targets*. See Configuring installation targets on page 631.
6. Click *Install Wizard* and install the policy package and device settings. See Installing policy package and device settings with the Install Wizard on page 631.
7. In FortiSASE, go to *Security* > *Traffic* > *Policies* and observe the newly created policy has been synchronized as desired.



8. Go to *Operations* > *Logs* > *Central management synchronizations* to verify the synchronization status.



9. Click on the log entry and click *View log details* to see desired configuration settings have been synchronized from FortiManager.



Example: Creating a Secure Internet-access agent tunnel policy with Entra ID SSO authentication

After Configuring FortiManager for central management on page 600, you can configure and synchronize policy management settings (firewall policies, firewall proxy policies, firewall schedules, security posture tags) using policy packages in FortiManager.

This example demonstrates how to create a secure internet-access agent tunnel policy with Entra ID SSO authentication using a policy package in FortiManager and synchronize it with a FortiSASE instance.

This example is performed after the Entra ID application has already had its Single Sign-on (SSO) settings configured and the Entra ID SAML IdP certificate has already been downloaded to the administrator's endpoint.

To create a secure internet-access agent tunnel policy with Entra ID SSO authentication:

1. Go to *Policy & Objects* > *User & Authentication*.
2. Create a new Single Sign-on server by clicking *+Create New*.

   For Agent-based User SSO, you must configure the Single Sign-on server with the name *SASE_VPN_SAML_SERVER*.

a. Configure these settings:

Field	Value
Name	*SASE_VPN_SAML_SERVER*
Service Provider Configuration	
Address	URL copied from FortiSASE under *Access & authentication* > *Authentication Sources* > *SSO* > *Agent-based User SSO* > *Base URL*
Certificate	*Disabled*
Identity Provider Configuration	
Type	*Custom*
Entity ID	URL copied from Entra ID application Single Sign-on *Microsoft Entra Identifier* setting
Assertion Consumer Service URL	URL copied from Entra ID application Single Sign-on *Login* setting
Single Logout Service URL	URL copied from Entra ID application Single Sign-on *Logout* setting
Certificate	Import a new SAML IdP remote certificate by clicking the dropdown list and clicking *+*: **1.** Configure these settings: **2.** Click *OK*. **3.** Select the newly imported SAML IdP remote certificate.
Additional SAML Attributes	
AD FS Claim	*Disabled*
Attribute Used to Identify Users	*username*
Attibute Used to Identify Groups	*group* See Configuring FortiSASE with Microsoft Entra ID SSO: SAML configuration fields on page 515.
Revision	
Change Note	<Change note>

Field	Value
Certification Name	<Name of certificate>
Import Remote Certificate	Click *Upload*, then *Browse* and look for the SAML IdP remote certificate on your endpoint.
Change Note	<Change note>

   b. Click *OK*.
3. Go to *Policy & Objects* > *User & Authentication* > *User Groups*.
4. Create a new SSO user group using the SSO server by clicking *+Create New*.
   a. Configure these settings:

Field	Value
Name	*SSO Group 1*
Type	*Firewall*
Remote Authentication Servers	1. Click *+Create New*: a. For *Remote Server*, select *SASE_VPN_SAML_SERVER*. b. For *Group Name*, select either *Any* or *Specify* if a Group ID from Entra ID is required to specify the group to match.

   b. Click *OK*.
5. Go to *Policy & Objects* > *Policy Packages*.
6. Create a new policy package by clicking *Policy Package* > *New*:
   a. Configure these settings:

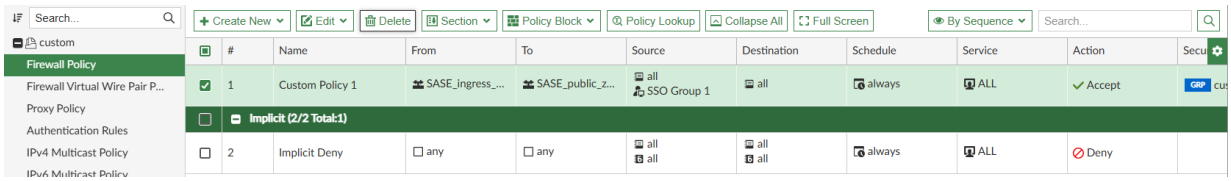
Field	Value
Name	*custom*
Central NAT	*Disabled*
NGFW Mode	*Profile-based*
Policy Offload Level	*Disable*
In Folder	<Empty>

   b. Click *OK*.
7. Click the custom policy package, click *Firewall Policy* and then click *+Create New* > *+ Create New*.
8. In the *Create New Firewall Policy* dialog:

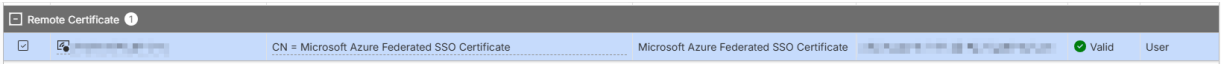
a. Configure these settings:

Field	Value
Name	*Custom Policy 1*
Type	*Standard*
Incoming interface	*SASE_ingress_zone*
Outgoing interface	*SASE_public_zone*
Source	**1.** Click *+*. **a.** In the *Address* tab, select *all*. **b.** In the *User* tab, select the newly created SSO group *SSO Group 1*. **2.** Click *Close*.
Negate Source	*Disabled*
Security Posture Tag	*<Empty>*
Destination	*all*
Negate Destination	*Disabled*
Service	*ALL*
Schedule	*always*
Action	*Accept*
Inspection Mode	*Proxy-based*
Security Profiles > Security Profiles Status	*Enabled*
Security Profiles > Profile Type	*Use Security Profile Group*
Profile Group	**1.** Click *+Create*. **2.** Configure a new profile group: • *Name*: custom-profile-group • *Web File Profile*: custom-profile • *SSL/SSH inspection*: deep-inspection • *Protocol Options*: default **3.** Add a *Change Note*. **4.** Click *OK*.
Log Allowed Traffic	*All Sessions*
Enable this policy	*Enabled*
Change Note	<Change Note>

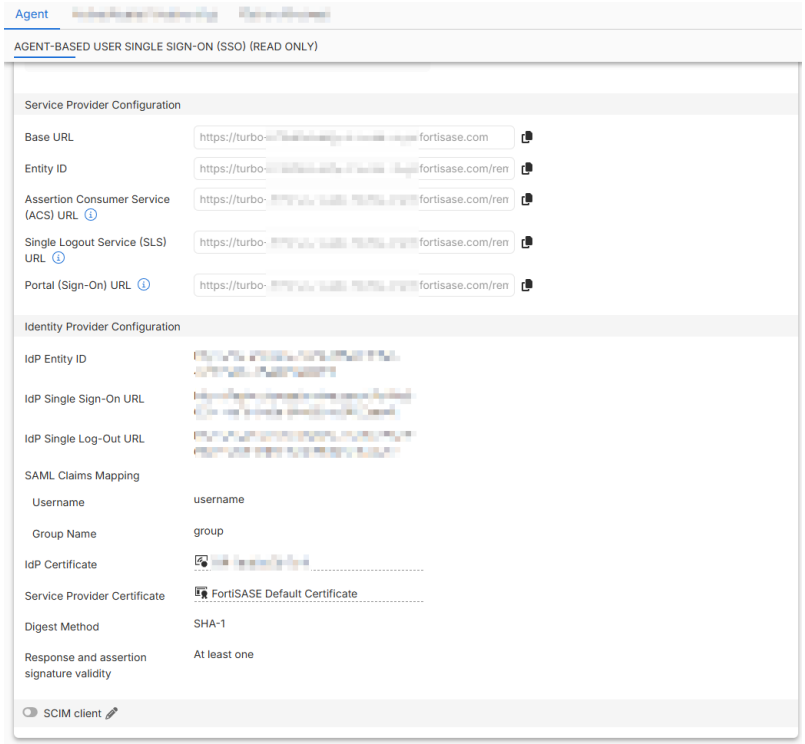
b. Click *OK*.



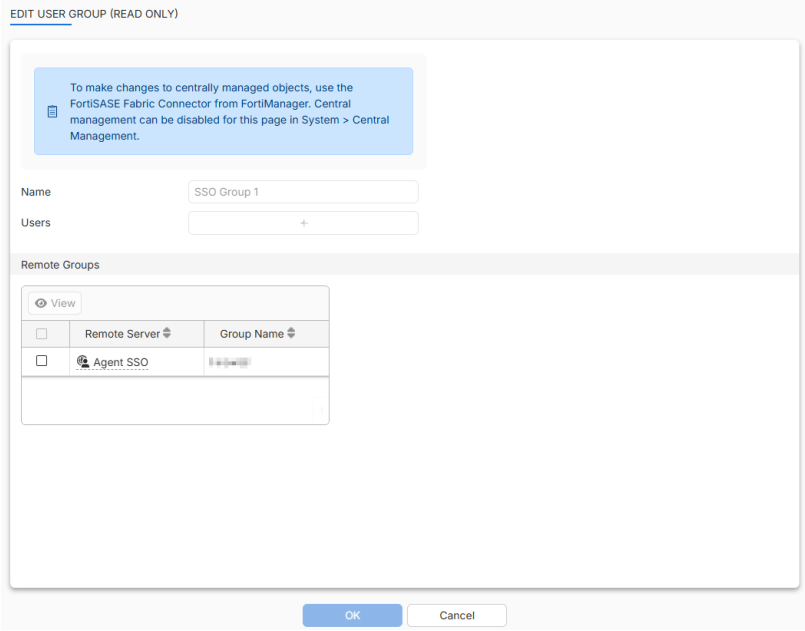
9. In the *custom* policy package, click *Installation Targets*. See Configuring installation targets on page 631.
10. Click *Install Wizard* and install the policy package and device settings. See Installing policy package and device settings with the Install Wizard on page 631.
11. In FortiSASE, confirm the desired configuration settings have been synchronized as desired:
    a. Go to *System* > *Certificates* and observe the SAML IdP remote certificate has been imported:



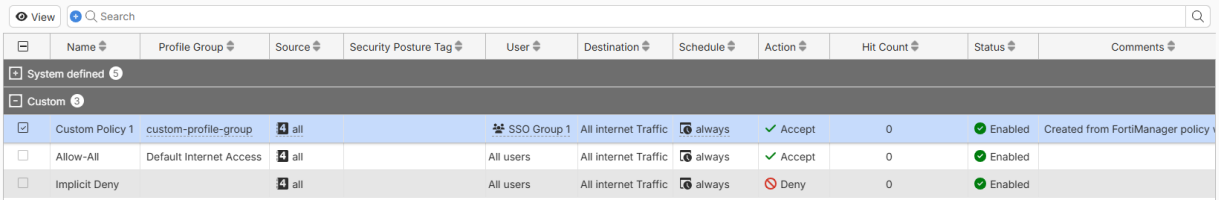
    b. Go to *Access & authentication* > *Authentication Sources* > *SSO* > *Agent* and observe the Agent-based User SSO page has been populated including selecting the IdP remote certificate imported previously:



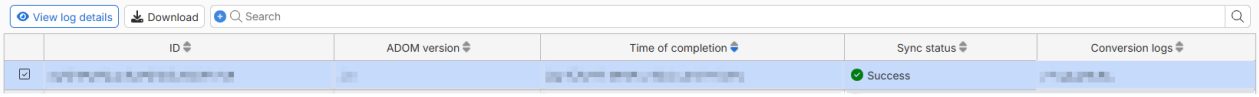
    c. Go to *Access & authentication* > *Access* > *Users* and groups and select the user group *SSO Group 1* with the Remote Group of *Agent SSO* specified with the *Group ID*:



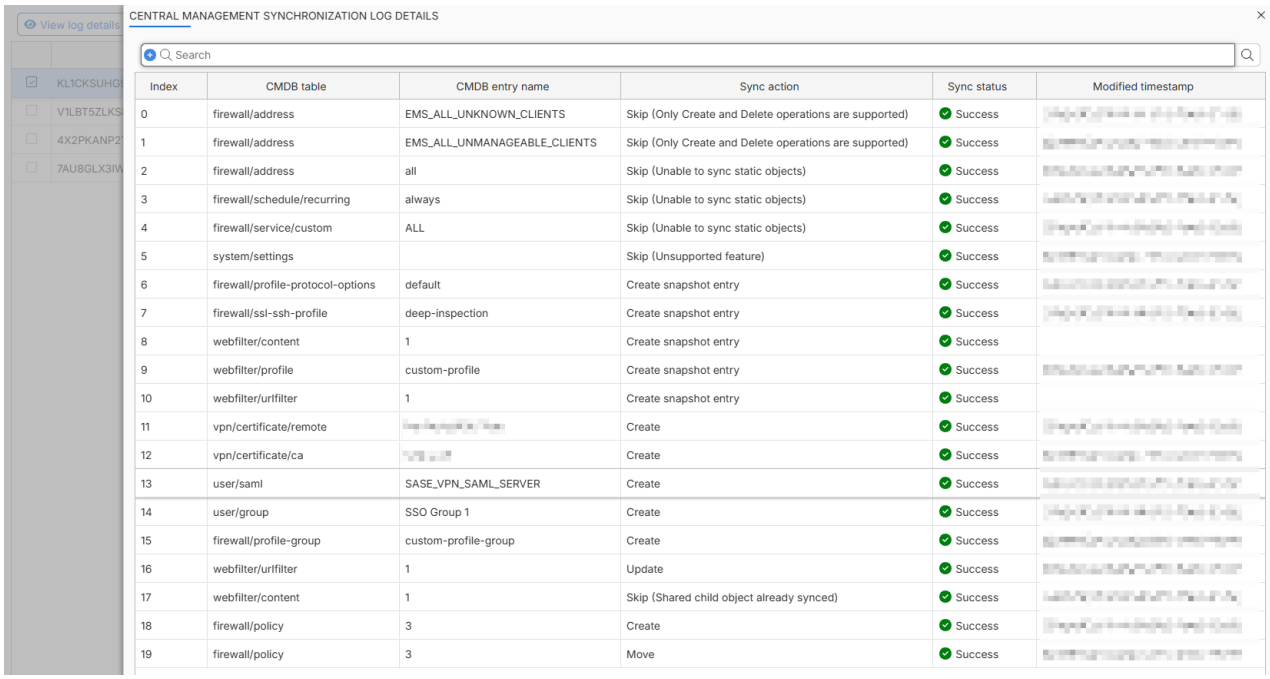
d. Go to *Security* > *Traffic* > *Policies* and observe the newly created policy:



12. Go to *Operations* > *Logs* > *Central management synchronizations* to verify the synchronization status.



13. Click on the log entry and click *View log details* to see desired configuration settings have been synchronized from FortiManager.



Index	CMDB table	CMDB entry name	Sync action	Sync status	Modified timestamp
0	firewall/address	EMS_ALL_UNKNOWN_CLIENTS	Skip (Only Create and Delete operations are supported)	Success	
1	firewall/address	EMS_ALL_UNMANAGEABLE_CLIENTS	Skip (Only Create and Delete operations are supported)	Success	
2	firewall/address	all	Skip (Unable to sync static objects)	Success	
3	firewall/schedule/recurring	always	Skip (Unable to sync static objects)	Success	
4	firewall/service/custom	ALL	Skip (Unable to sync static objects)	Success	
5	system/settings		Skip (Unsupported feature)	Success	
6	firewall/profile-protocol-options	default	Create snapshot entry	Success	
7	firewall/ssl-ssh-profile	deep-inspection	Create snapshot entry	Success	
8	webfilter/content	1	Create snapshot entry	Success	
9	webfilter/profile	custom-profile	Create snapshot entry	Success	
10	webfilter/urlfilter	1	Create snapshot entry	Success	
11	vpn/certificate/remote		Create	Success	
12	vpn/certificate/ca		Create	Success	
13	user/saml	SASE_VPN_SAML_SERVER	Create	Success	
14	user/group	SSO Group 1	Create	Success	
15	firewall/profile-group	custom-profile-group	Create	Success	
16	webfilter/urlfilter	1	Update	Success	
17	webfilter/content	1	Skip (Shared child object already synced)	Success	
18	firewall/policy	3	Create	Success	
19	firewall/policy	3	Move	Success	

Example: Creating a Secure Internet-access proxy policy with Entra ID SSO authentication

After Configuring FortiManager for central management on page 600, you can configure and synchronize policy management settings (firewall policies, firewall proxy policies, firewall schedules, security posture tags) using policy packages in FortiManager.

This example demonstrates how to create a secure internet-access proxy policy with Entra ID SSO authentication using a policy package in FortiManager and synchronize it with a FortiSASE instance. Previously, secure internet access via proxy was known as secure web gateway (SWG).

- Proxy functionality is enabled in the FortiSASE portal directly in the *Network* > *Proxy configuration* page instead of synchronized via FortiManager and the central management feature.
- This example is performed after the Entra ID application has already had its Single Sign-on (SSO) settings configured and the Entra ID SAML IdP certificate has already been downloaded to the administrator's endpoint.

To create a secure internet-access proxy policy with Entra ID SSO authentication:

1. Go to *Policy & Objects* > *User & Authentication* > *Single Sign-On*.
2. Create a new Single Sign-on server by clicking *+Create New*.

> For Proxy User SSO, you must configure the Single Sign-on server with the name *SASE_SWG_SAML_SERVER*.

a. Configure these settings:

Field	Value
Name	*SASE_SWG_SAML_SERVER*
Service Provider Configuration	
Address	URL copied from FortiSASE under *Access & authentication* > *Authentication Sources* > *SSO* > *Agent-based User SSO* > *Base URL*.
Certificate	*Disabled*
Identity Provider Configuration	
Type	*Custom*
Entity ID	URL copied from Entra ID application Single Sign-on *Microsoft Entra Identifier* setting
Assertion Consumer Service URL	URL copied from Entra ID application Single Sign-on *Login* setting
Single Logout Service URL	URL copied from Entra ID application Single Sign-on *Logout* setting
Certificate	Import a new SAML IdP remote certificate by clicking the dropdown list and clicking *+*: **1.** Configure these settings: **2.** Click *OK*. **3.** Select the newly imported SAML IdP remote certificate.
Additional SAML Attributes	
AD FS Claim	*Disabled*
Attribute Used to Identify Users	*username*
Attribute Used to Identify Groups	*group* See Configuring FortiSASE with Microsoft Entra ID SSO: SAML configuration fields on page 515.
Revision	

Field	Value
Certification Name	<Name of certificate>
Import Remote Certificate	Click *Upload*, then *Browse* and look for the SAML IdP remote certificate on your endpoint.
Change Note	<Change note>

Field	Value
Change Note	<Change note>

b. Click *OK*.

3. Go to *Policy & Objects* > *User & Authentication* > *User Groups*.
4. Create a new SSO user group using the SSO server by clicking *+Create New*.
   a. Configure these settings:

Field	Value
Name	*SSO Group 1*
Type	*Firewall*
Remote Authentication Servers	1. Click *+Create New*: **a.** For *Remote Server*, select *SASE_SWG_SAML_SERVER*. **b.** For *Group Name*, select either *Any* or *Specify* if a Group ID from Entra ID is required to specify the group to match.

   b. Click *OK*.
5. Go to *Policy & Objects* > *Policy Packages*.
6. Create a new policy package by clicking *Policy Package* > *New*:
   a. Configure these settings:

Field	Value
Name	*custom*
Central NAT	*Disabled*
NGFW Mode	*Profile-based*
Policy Offload Level	*Disable*
In Folder	<Empty>

   b. Click *OK*.
7. Click the custom policy package, click *Proxy Policy* and then click *+Create New* > *+ Create New*.
8. In the *Create New Firewall Policy* dialog:

a. Configure these settings:

Field	Value
Name	*Custom Policy 1*
Proxy	*Explicit Web*
Outgoing interface	*SASE_public_zone*
Source	**1.** Click *+*. **a.** In the *Address* tab, select *all*. **b.** In the *User* tab, select the newly created SSO group *SSO Group 1*. **2.** Click *Close*.
Negate Source	*Disabled*
Security Posture Tag	*<Empty>*
Destination	*all*
Negate Destination	*Disabled*
Service	*webproxy*
Schedule	*always*
Action	*Accept*
Firewall/Network Options	
Protocol Options	*default*
Web Proxy Forwarding Server	<Blank>
Outgoing source IP	*Proxy Default*
Disclaimer Options > Display Disclaimer	*Disable*
Security Profiles > Security Profiles Status	*Enabled*
Security Profiles > Profile Type	*Use Security Profile Group*
Profile Group	**1.** Click *+Create*. **2.** Configure a new profile group: • *Name*: custom-profile-group • *Web File Profile*: custom-profile • *SSL/SSH inspection*: deep-inspection • *Protocol Options*: default **3.** Add a *Change Note*. **4.** Click *OK*.
Log Allowed Traffic	*All Sessions*

Field	Value
Enable this policy	*Enabled*
Change Note	<Change Note>

b. Click *OK*.

9. In the *custom* policy package, click *Installation Targets*. See Configuring installation targets on page 631.

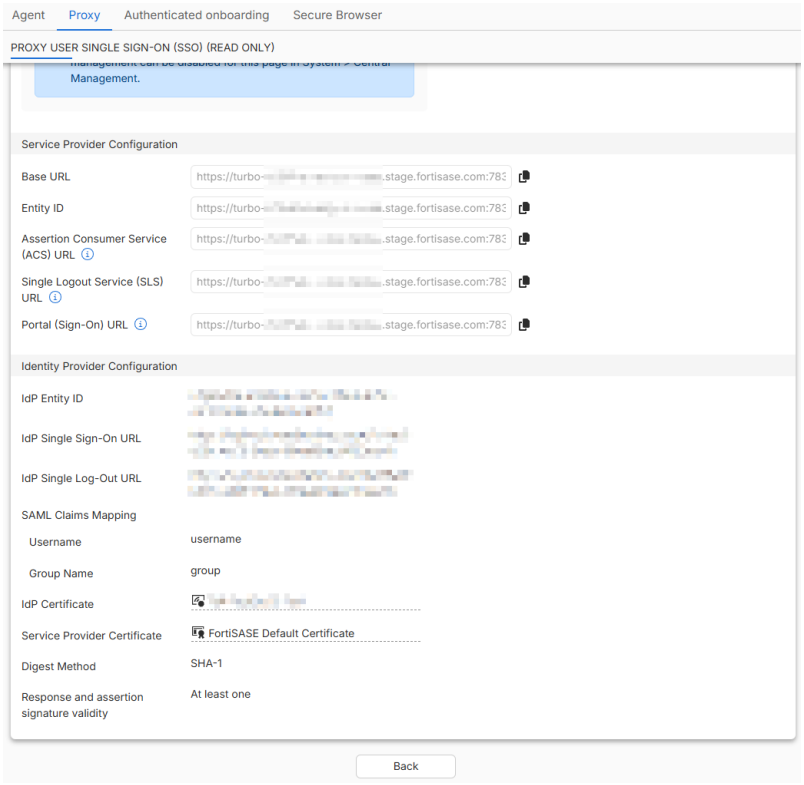
10. Click *Install Wizard* and install the policy package and device settings. See Installing policy package and device settings with the Install Wizard on page 631.

11. In FortiSASE, confirm the desired configuration settings have been synchronized as desired:

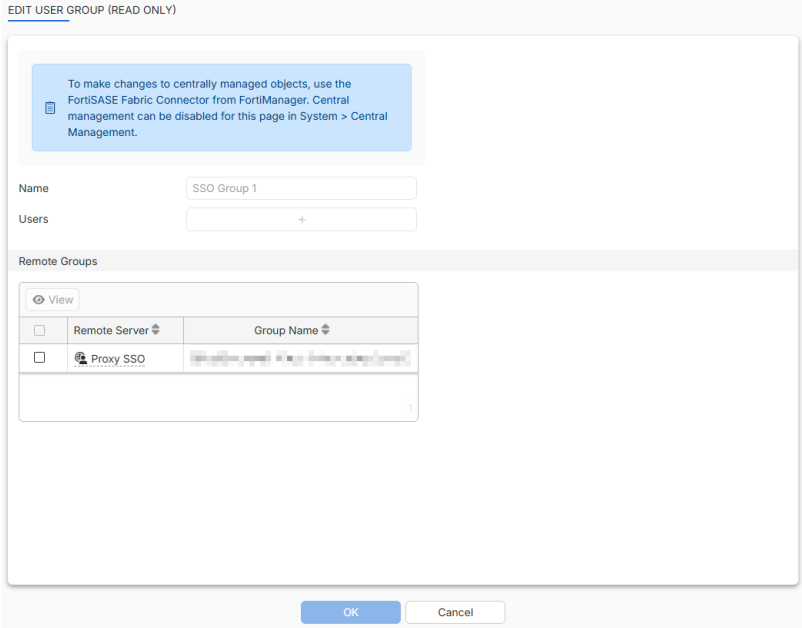
a. Go to *System* > *Certificates* and observe the SAML IdP remote certificate has been imported:



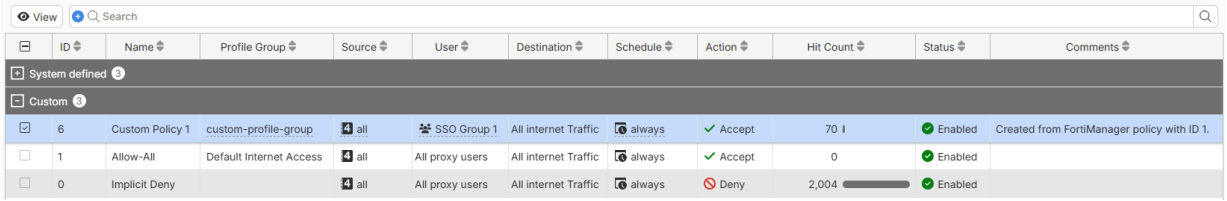
b. Go to *Access & authentication* > *Authentication Sources* > *SSO* > *Proxy* and observe the *Proxy User SSO* page has been populated including selecting the IdP remote certificate imported previously:



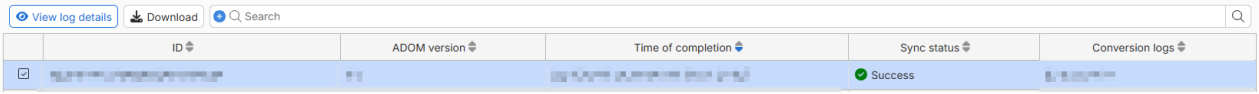
c. Go to *Access & authentication* > *Access* > *Users and groups* and select the user group *SSO Group 1* with the Remote Group of *Proxy SSO* specified with the *Group ID*:



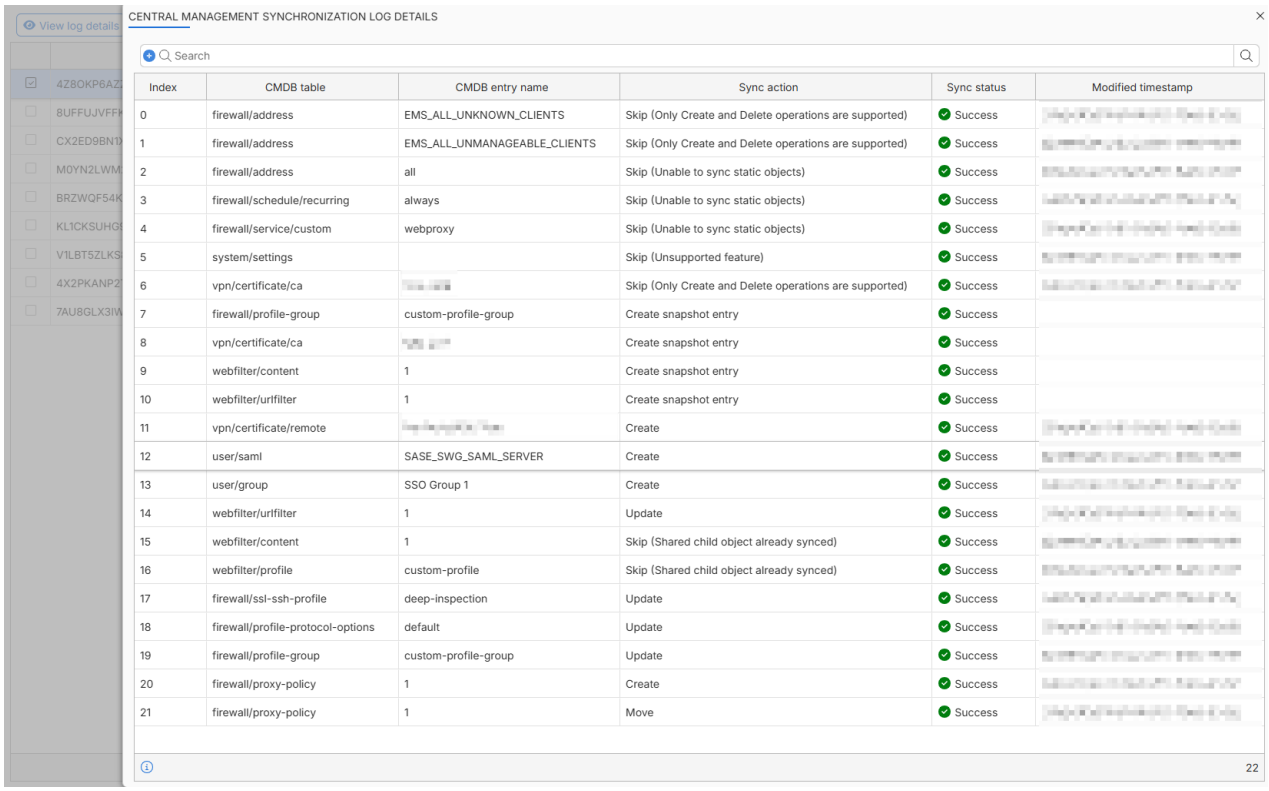
d. Go to *Security* > *Traffic* > *Proxy policies* and observe the newly created policy:



12. Go to *Operations* > *Logs* > *Central management synchronizations* to verify the synchronization status.



13. Click on the log entry and click *View log details* to see desired configuration settings have been synchronized from FortiManager.



Example: Creating a Secure Internet-access policy with one-time schedule

After Configuring FortiManager for central management on page 600, you can configure and synchronize policy management settings (firewall policies, firewall proxy policies, firewall schedules, security posture tags) using policy packages in FortiManager.

This example demonstrates how to create a secure internet-access policy with a one-time schedule using a policy package in FortiManager and synchronize it with a FortiSASE instance.

When a one-time schedule is configured by a FortiManager administrator using the date and time picker fields, respectively, the FortiSASE central management feature considers the dates and times specified in GMT timezone upon synchronization. This example uses these configuration settings.

To avoid timezone ambiguity, a FortiManager administrator can use the *start-utc* and *end-utc* fields in *Advanced Options* instead to input an epoch timestamp instead.

Regardless of the FortiManager configuration settings used, ensure that the GMT timestamps or epoch timestamps are correctly specified to match the desired one-time schedule when applied to the local timezone of your remote users.

To create a secure internet-access policy with one-time schedule:

1. In FortiManager, go to *Policy & Objects* > *Firewall Objects* > *Schedules*.
2. Create a new one-time schedule to take effect 15 minutes from now for a duration of 20 minutes by clicking *+Create New* > *One-Time Schedule*:
   a. Configure these settings:

Field	Value
Name	*One Time Schedule 1*
Start Time	Use date and time picker fields, respectively, to specify the start time. For example, choose a GMT date and time that is 15 minutes in the future.
End Time	Use date and time picker fields, respectively, to specify the end time. For example, choose a GMT date and time that is 35 minutes in the future.
Pre-expiration Event Log	*Disabled*
Number of Days Before	3
Advanced Options	
end-utc	If not using *End Time*, then specify the schedule end date and time, in epoch format.
start-utc	If not using *Start Time*, then specify the schedule start date and time, in epoch format.
Revision	
Change Note	<Change note>

   b. Click *OK*.
3. Go to *Policy & Objects* > *Policy Packages*.
4. Create a new policy package by clicking *Policy Package* > *New*:
   a. Configure these settings:

Field	Value
Name	*custom*
Central NAT	*Disabled*
NGFW Mode	*Profile-based*
Policy Offload Level	*Disable*
In Folder	<Empty>

   b. Click *OK*.
5. Click the custom policy package, click *Firewall Policy* and then click *+Create New* > *+ Create New*. For this example, the default policy package is used.
6. In the *Create New Firewall Policy* dialog:

a. Configure these settings:

Field	Value
Name	*SIA-Policy-1*
Type	*Standard*
Incoming interface	*SASE_ingress_zone*
Outgoing interface	*SASE_public_zone*
Source	Click *+* and in the *Address* tab, select *all*.
Negate Source	*Disabled*
Security Posture Tag	<Empty>
Destination	*all*
Negate Destination	*Disabled*
Service	*ALL*
Schedule	**1.** Click *+* and under *ONE-TIME SCHEDULE*, select *One-time Schedule 1*. **2.** Click *Close*.
Action	*Accept*
Inspection Mode	*Proxy-based*
Security Profiles > Security Profiles Status	*Enabled*
Security Profiles > Profile Type	*Use Security Profile Group*
Profile Group	**1.** Click *+Create*. **2.** Configure a new profile group: • *Name*: custom-profile-group • *Web File Profile*: custom-profile • *SSL/SSH inspection*: deep-inspection • *Protocol Options*: default **3.** Add a *Change Note*. **4.** Click *OK*.
Log Allowed Traffic	*All Sessions*
Enable this policy	*Enabled*

b. Add a *Change Note* then click *OK*.

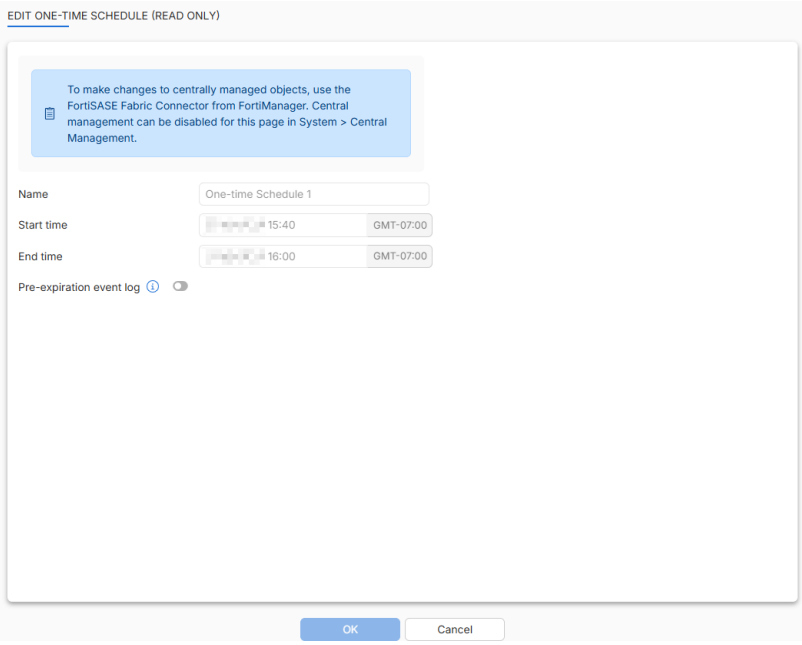
7. In the *custom* policy package, click *Installation Targets*. See Configuring installation targets on page 631.

8. Click *Install Wizard* and install the policy package and device settings. See Installing policy package and device settings with the Install Wizard on page 631.

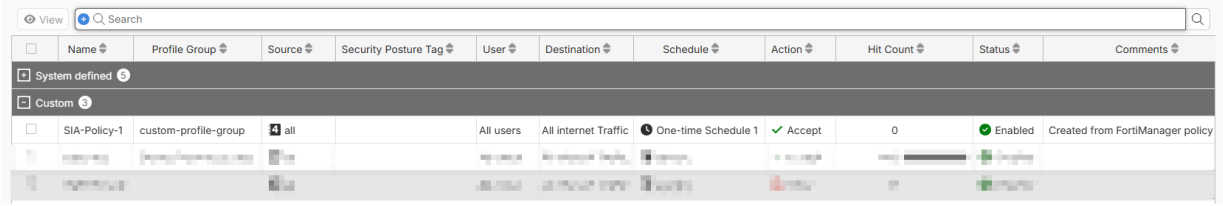
9. In FortiSASE, confirm the desired configuration settings have been synchronized as desired:

a. Go to *Security* > *Resources* > *Schedules* > *One-time schedules*, select *One-Time Schedule 1* and click *View*:

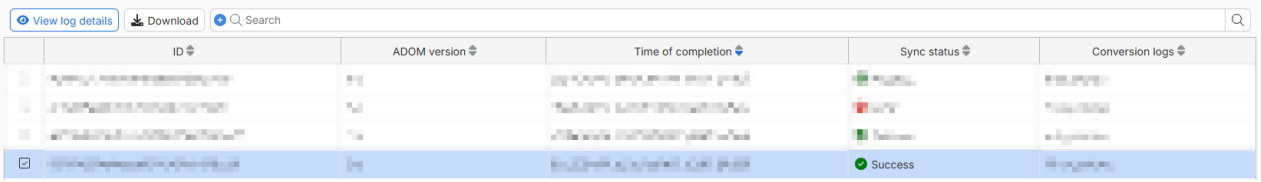
- Observe the specified one-time schedule has been synchronized with the local timezone displayed relative to GMT.
- In the following screenshot, GMT-07:00 corresponds to PDT which is the local timezone of the remote users used in this example:



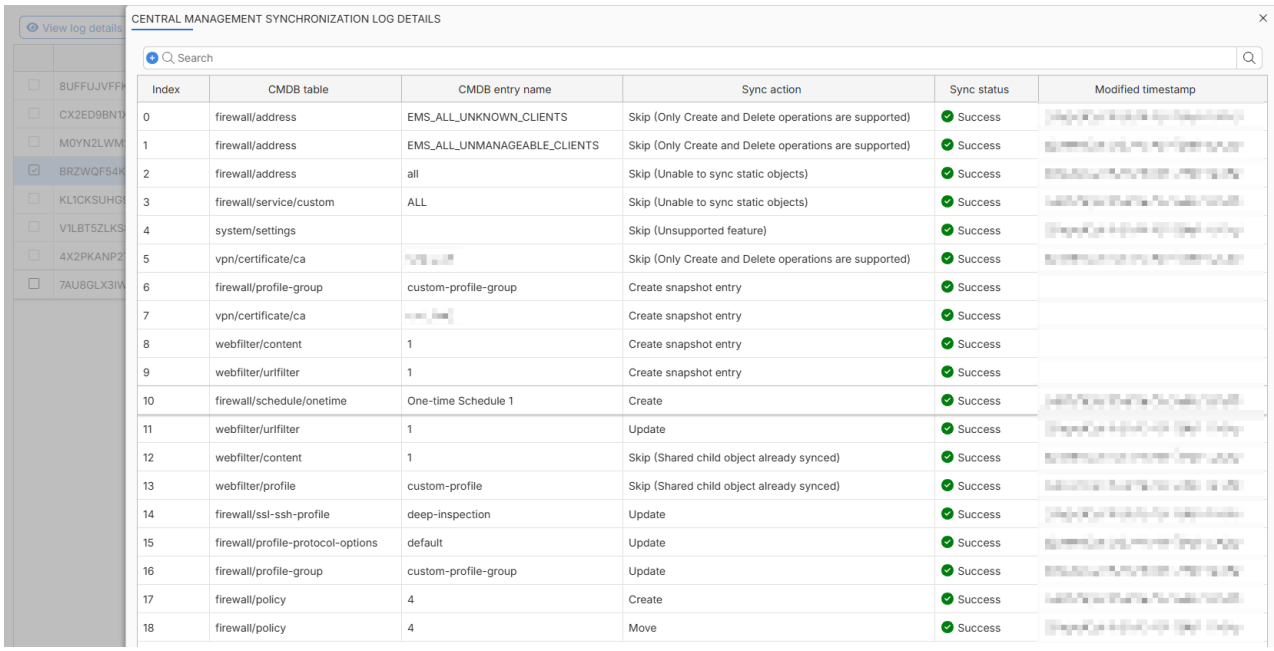
b. Go to *Security* > *Traffic* > *Policies* and observe the newly created policy with one-time schedule specified:



10. Go to *Operations* > *Logs* > *Central management synchronizations* to verify the synchronization status.



11. Click on the log entry and click *View log details* to see desired configuration settings have been synchronized from FortiManager.



Configuring security profiles in FortiManager

In FortiManager, in *Edit FortiSASE Connector*, you can specify an existing security profile group or create a new security profile group.

Within a security profile group, you can configure security profiles including a custom SSL inspection profile through *Policy & Objects > Security Profiles* and some settings through *Policy & Objects > Advanced > CLI Configurations*. This section provides some examples of configuring security profiles in FortiManager.

To display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

The following topics are covered:

- Creating and applying a new CASB profile to Web Filter profile on page 654
- Configuring custom CA certificates for SSL Inspection profile on page 661
- Configuring DLP dictionaries, sensors, and profiles on page 665
- Configuring and applying Video Filter on page 672
- Configuring and applying an IPS profile on page 677
- Configuring and applying an Application Control profile on page 680
- Configuring custom Web Filter categories on page 683
- Configuring external feeds with Web Filter and DNS Filter profiles on page 688
- Configuring and applying a File Filter to block password-protected files on page 702
- Configuring and applying deep/certificate inspection and performance optimization settings on page 706
- Configuring and applying a Web Filter profile on page 707

Creating and applying a new CASB profile to Web Filter profile

When a Web Filter profile with Inline-CASB web-proxy profile is configured, FortiSASE intercepts HTTP headers and can modify them for outgoing traffic. By customizing HTTP headers for FortiSASE outgoing traffic destined for SaaS applications, the Web Filter with Inline-CASB can control SaaS application behaviour. See Customizing inline-CASB headers on page 362.

This example demonstrates how to create a new Inline-CASB web-proxy profile under CLI Configurations and apply it to a Web Filter profile. In this example, we create the `sec-Restrict-Tenant-Access-Policy` HTML header set to `restrict-msa` that was used in Configuring inline-CASB header for Office 365 example on page 367.



This example demonstrates the steps required to configure only one of the HTML headers used for controlling permissions for Microsoft Office 365 to allow corporate domains and deny personal accounts.

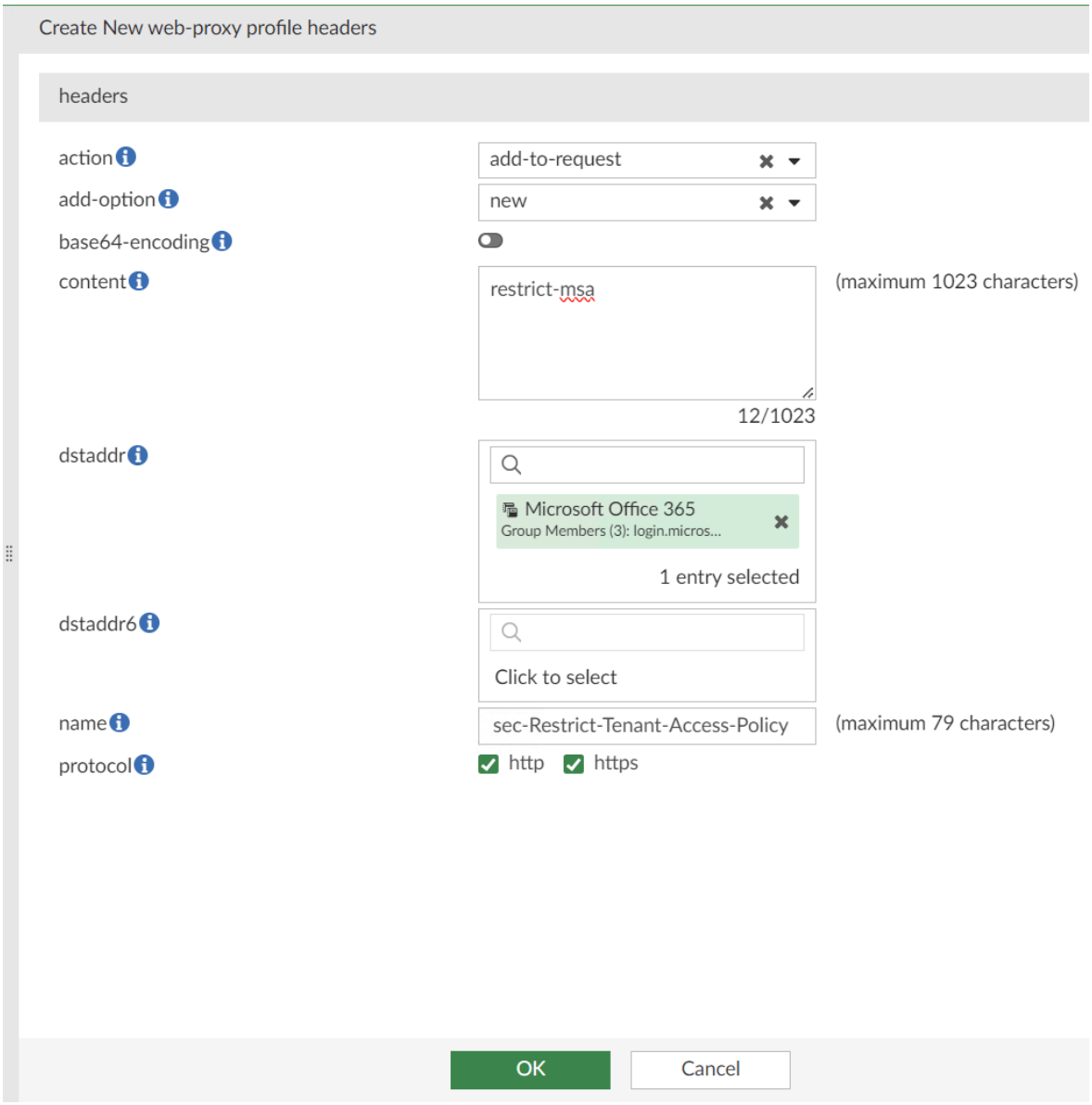
Additional HTML headers must be configured in FortiManager using the steps below to ensure Microsoft Office 365 tenant restrictions are applied to outgoing remote user traffic. For the Office 365 example above, you must also configure the following HTML headers:

- `Restrict-Access-Context`
- `Restrict-Access-To-Tenants`

To create and apply a new CASB profile to Web Filter profile:

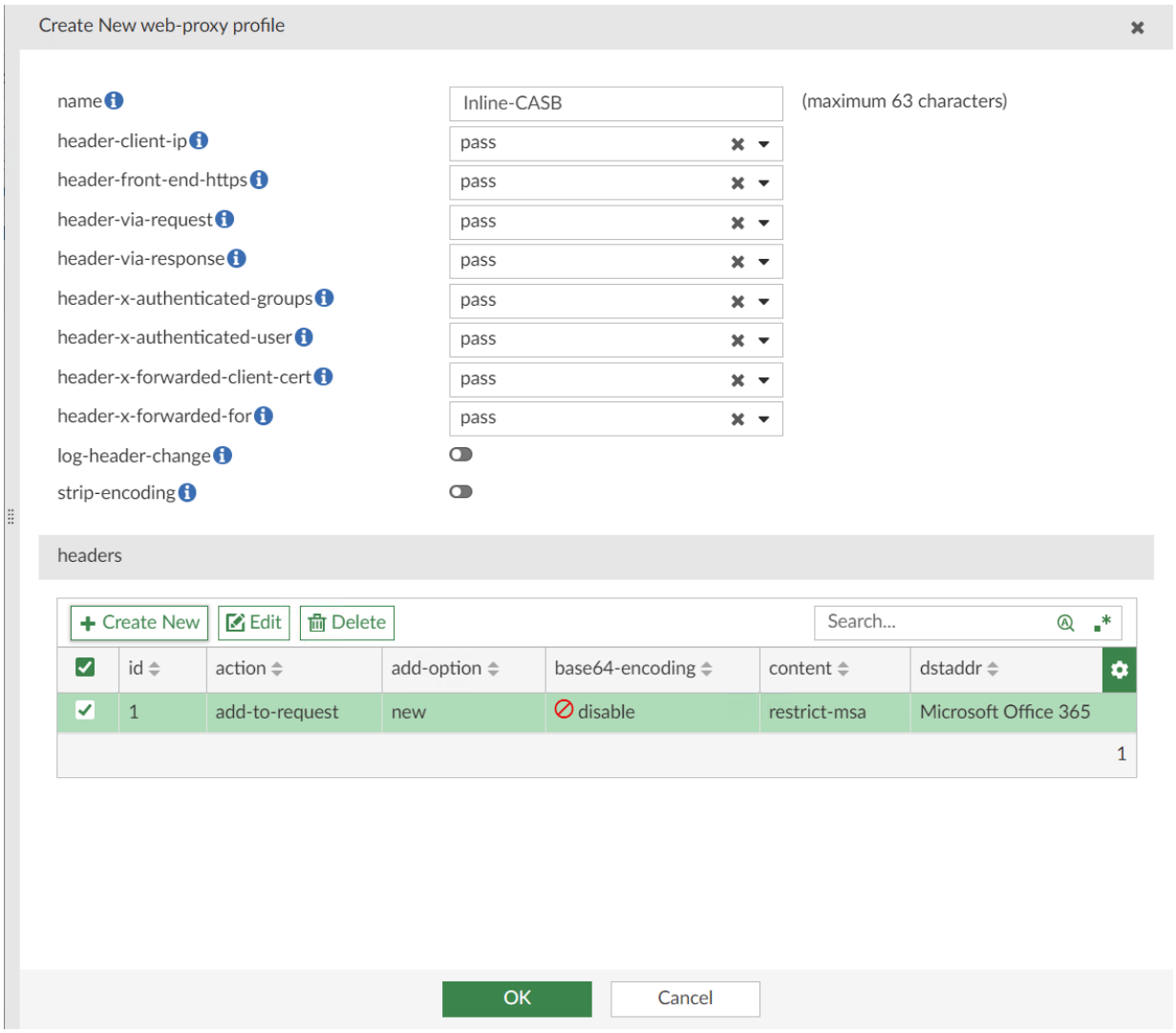
1. Go to *Policy & Objects* > *Advanced* > *CLI Configurations*.
   a. Enter *web-proxy* in the search bar to discover results matching that keyword.
   b. Expand the *web-proxy* result in the tree menu, and select the *profile* menu item.
   c. In *web-proxy* profile, click *+Create New*.
   d. In *Create New web-proxy profile*, in the *name* field, enter *Inline-CASB*.
   e. In headers, click *+Create New*.
      i. In *Create New web-proxy profile headers*, configure these settings and keep all other default settings:

Option	Value
action	add-to-request
content	restrict-msa
dstaddr	Microsoft Office 365
name	sec-Restrict-Tenant-Access-Policy


Create New web-proxy profile headers
headers
action
add-to-request
add-option
new
base64-encoding
content
restrict-msa
(maximum 1023 characters)
12/1023
dstaddr
Microsoft Office 365
Group Members (3): login.micros...
1 entry selected
dstaddr6
Click to select
name
sec-Restrict-Tenant-Access-Policy
(maximum 79 characters)
protocol
http
https
OK
Cancel

ii. Click *OK*.

f. Click *OK*.



2. Go to *Policy & Objects* > *Security Profiles* > *Web Filter*.

a. Click *+Create New*.

b. In *Create New Web Filter*:

i. In the *Name* field, enter *custom-profile*.

ii. For *Feature Set*, select *Proxy-based*.

c. In *Static URL Filter* enable *Web URL Filter*. In *Select an URL Filter*, click the dropdown and click *+* to create a new URL filter.

d. In *Create New Web URL Filter*, configure the following:

i. In the *Name* field, enter *custom-url-filter*.

ii. In *Web URL Filter Entry*, click *+Create New*.

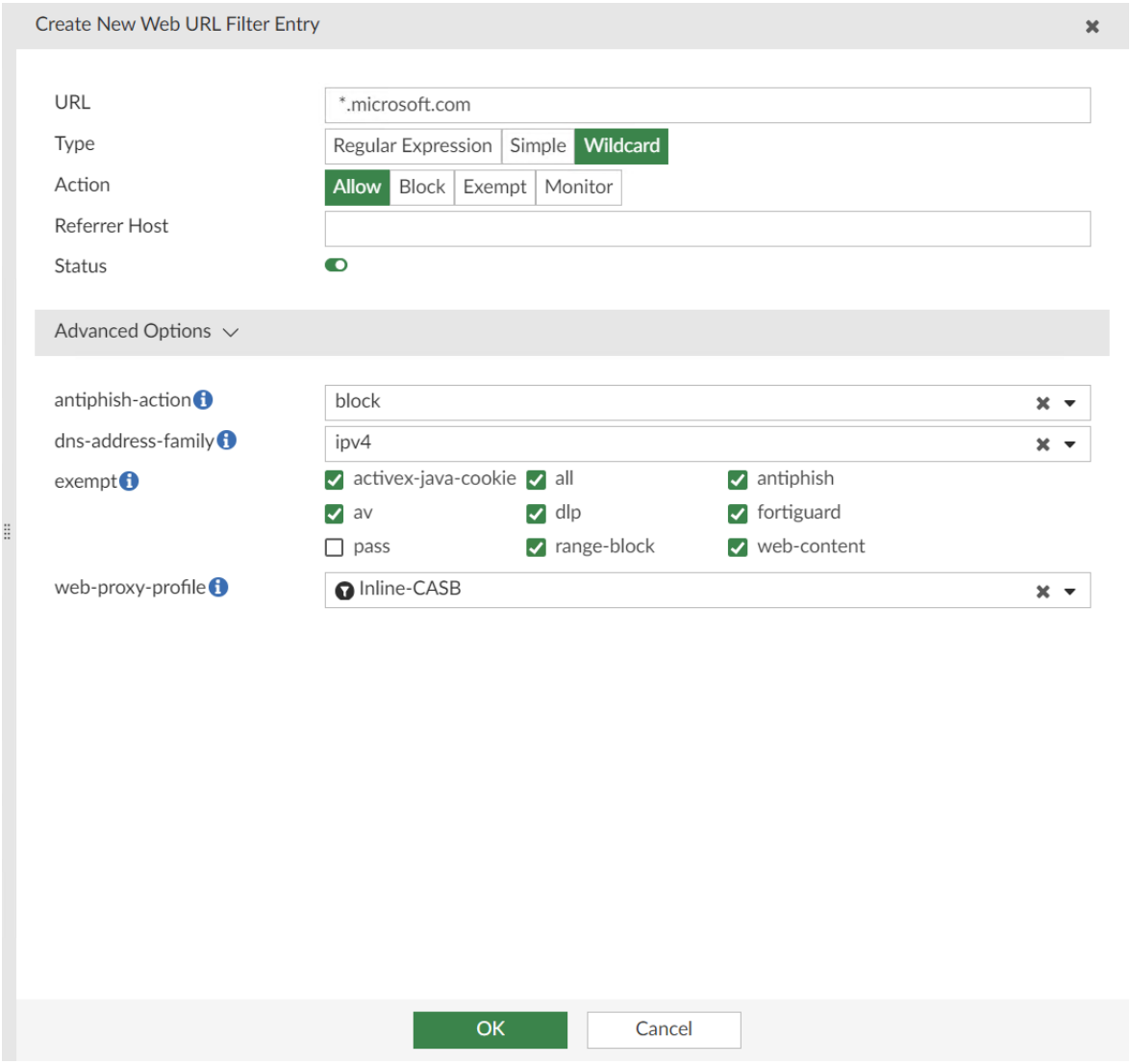
e. In *Create New Web URL Filter Entry*, configure the following:

i. In the *URL* field, enter **.microsoft.com*.

ii. In the *Type* field, select *Wildcard*.

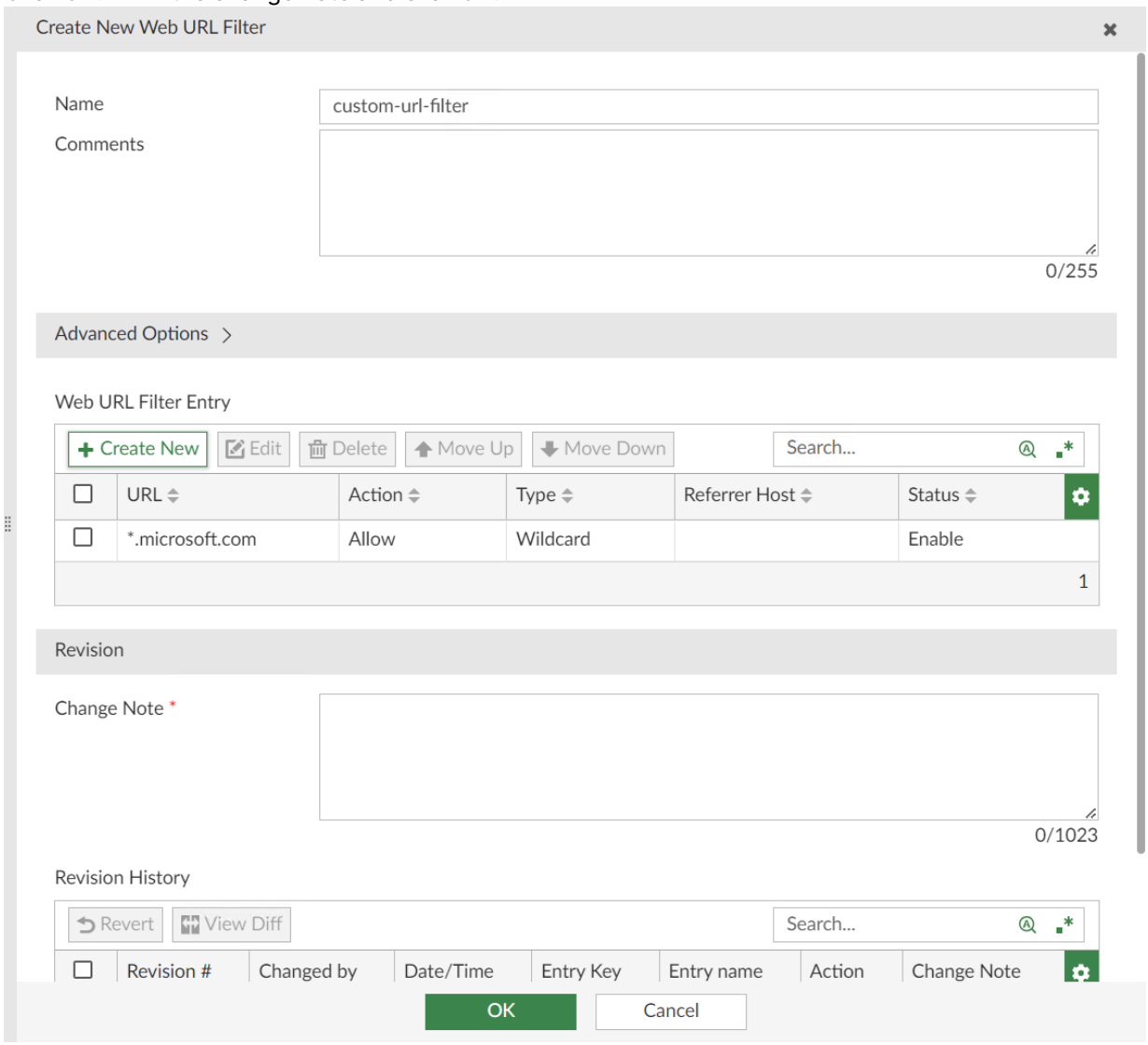
iii. In the *Action* field, select *Allow*.

iv. Expand the *Advanced Options* and in *web-proxy-profile* select *Inline-CASB*.

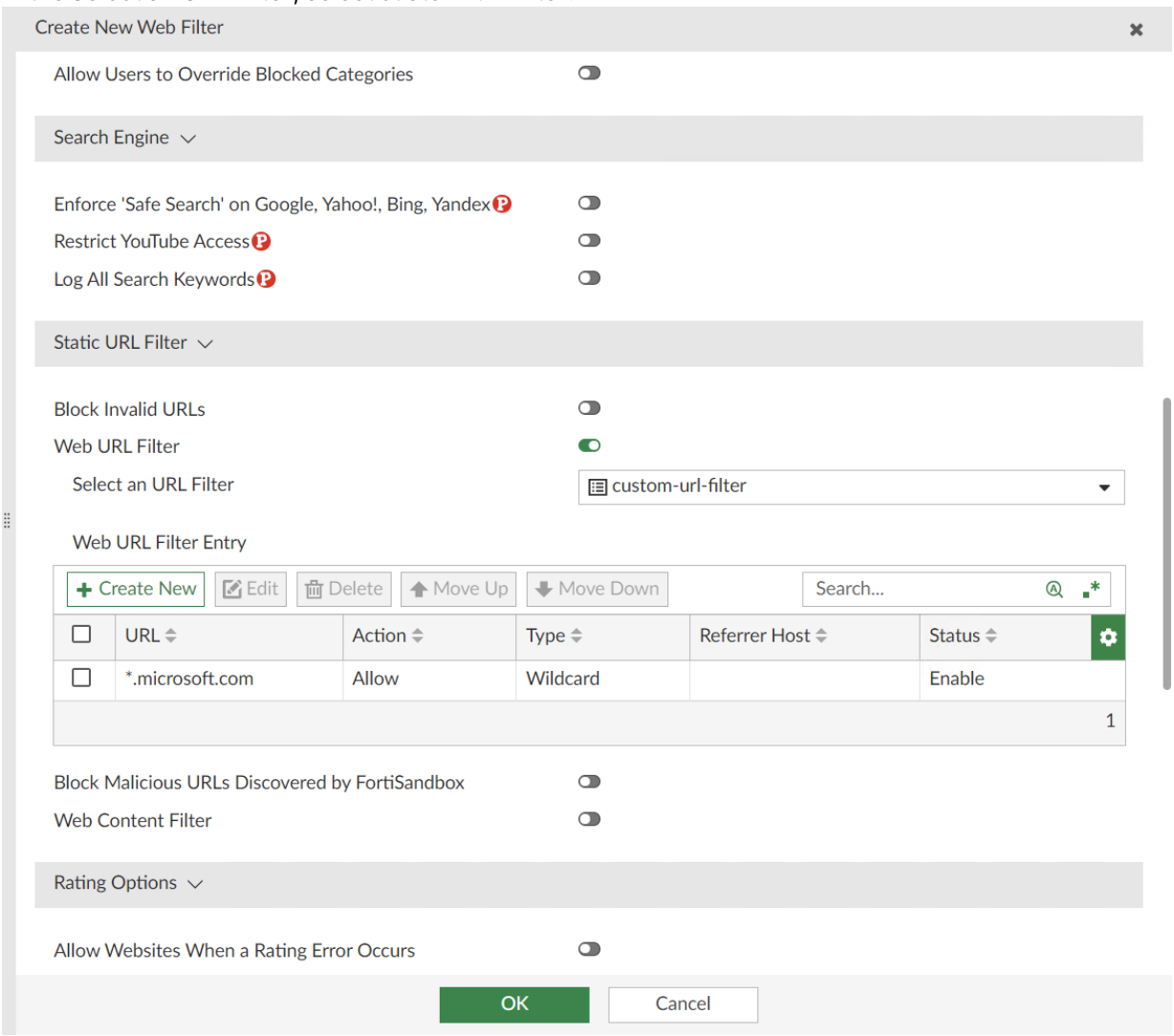


v. Click *OK*.

f. Click *OK*. Fill in the change note and click *OK*.



g. In the *Select an URL Filter*, select *custom-url-filter*.



h. Click *OK*. Fill in the change note and click *OK*.

3. Go to *Policy & Objects > Advanced > CLI Configurations*.

a. Enter *profile-group* in the search bar to discover results matching that keyword.

b. Expand the *firewall* result in the tree menu, and select the *profile-group* menu item.

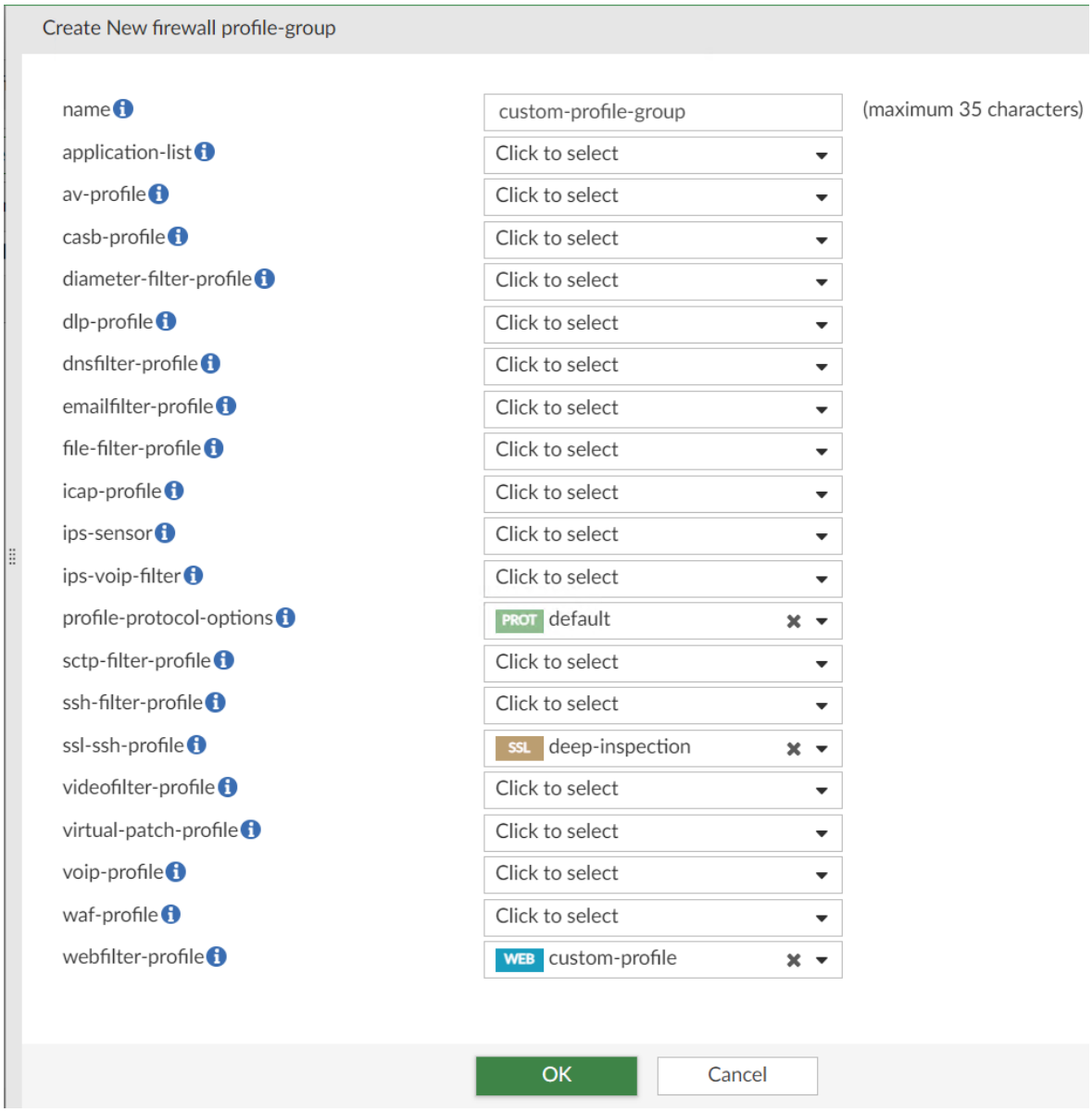
c. In *firewall profile-group*, click *+Create New*.

i. In the *name* field, enter *custom-profile-group*.

ii. For *profile-protocol-options*, select *default*.

iii. For *ssl-ssh-profile*, select *deep-inspection*.

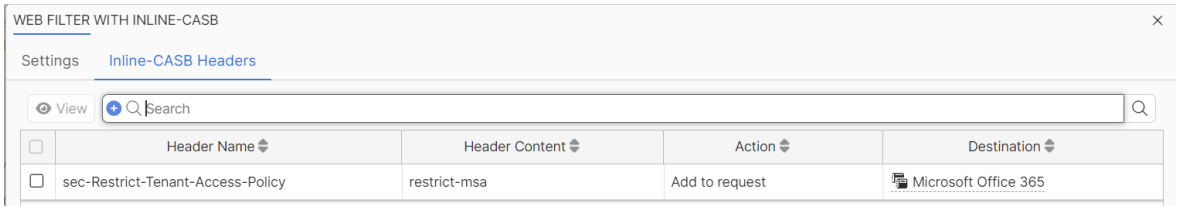
iv. For *webfilter-profile*, select *custom-profile*.



d. Click *OK*.

4. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the *custom-profile-group* Security Profile Group from FortiManager to FortiSASE.
5. In FortiSASE verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *Traffic* > *Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In *Web Filter With Inline-CASB*, click *View*.

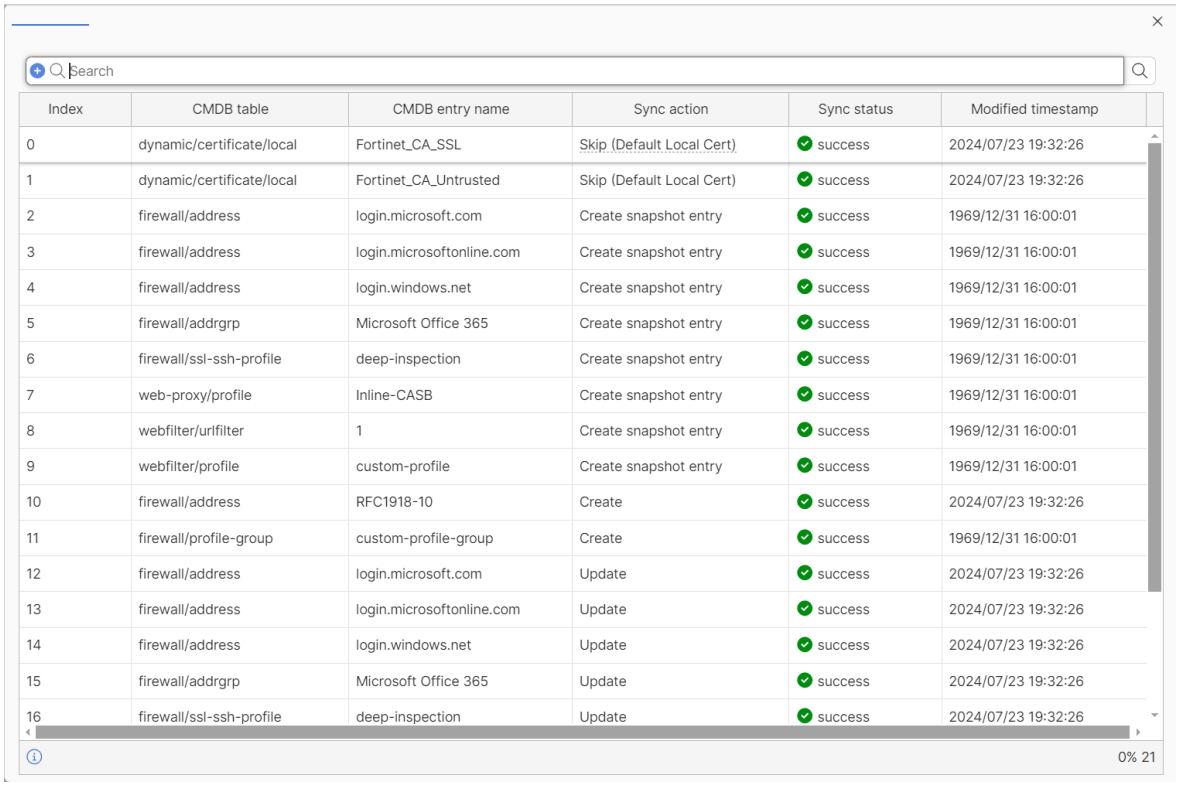
iii. In *Inline-CASB Headers*, confirm the custom header has been added as desired.



b. Go to *Operations > Logs > Central management synchronizations* and do the following:

i. Select the most recent log entry and click *View log details*.

ii. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



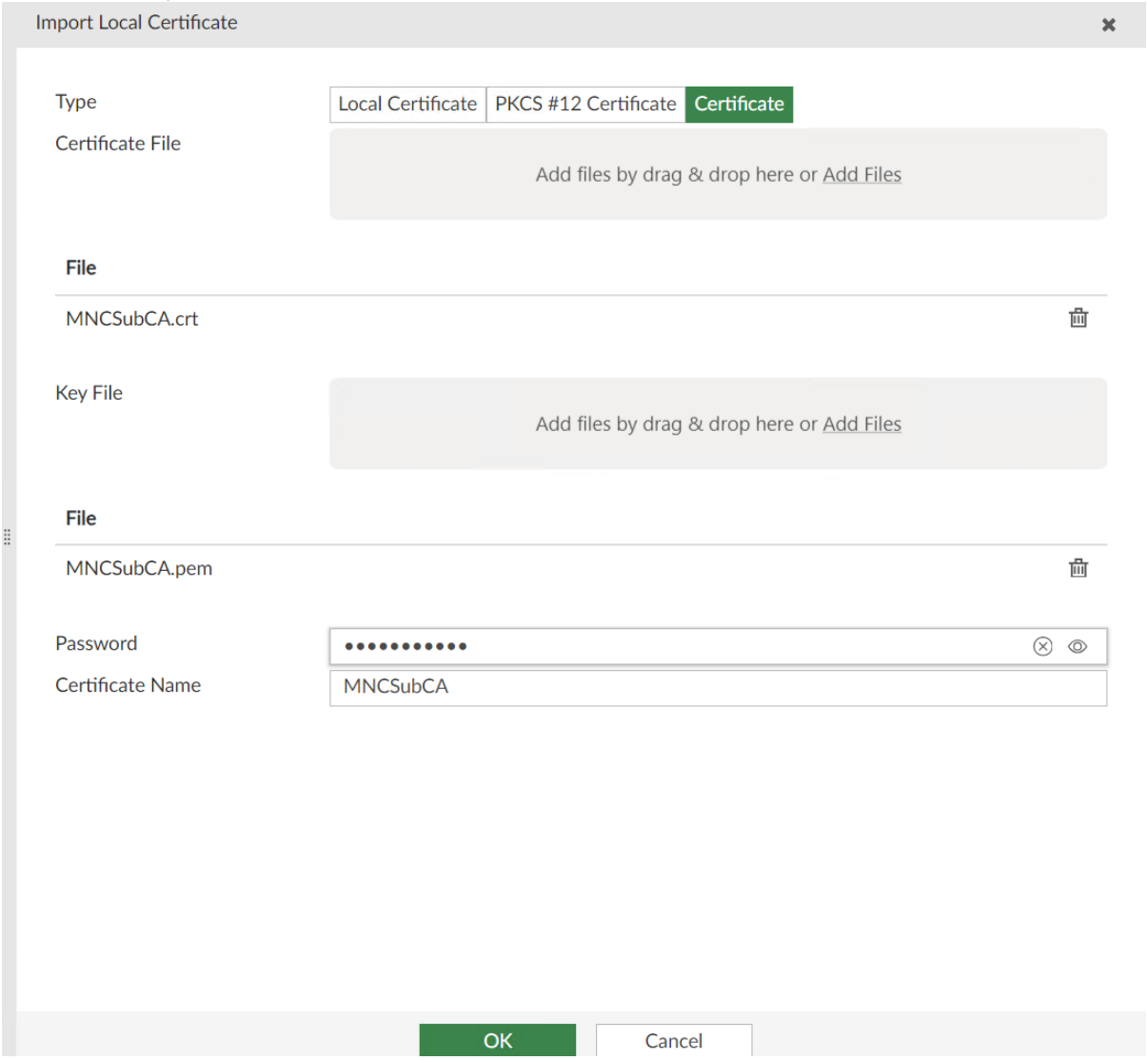
Configuring custom CA certificates for SSL Inspection profile

The following example demonstrates how to import a custom CA certificate to be used with a custom SSL inspection profile. The custom SSL inspection profile is used within a profile group and can be synchronized from FortiManager to FortiSASE.

To display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

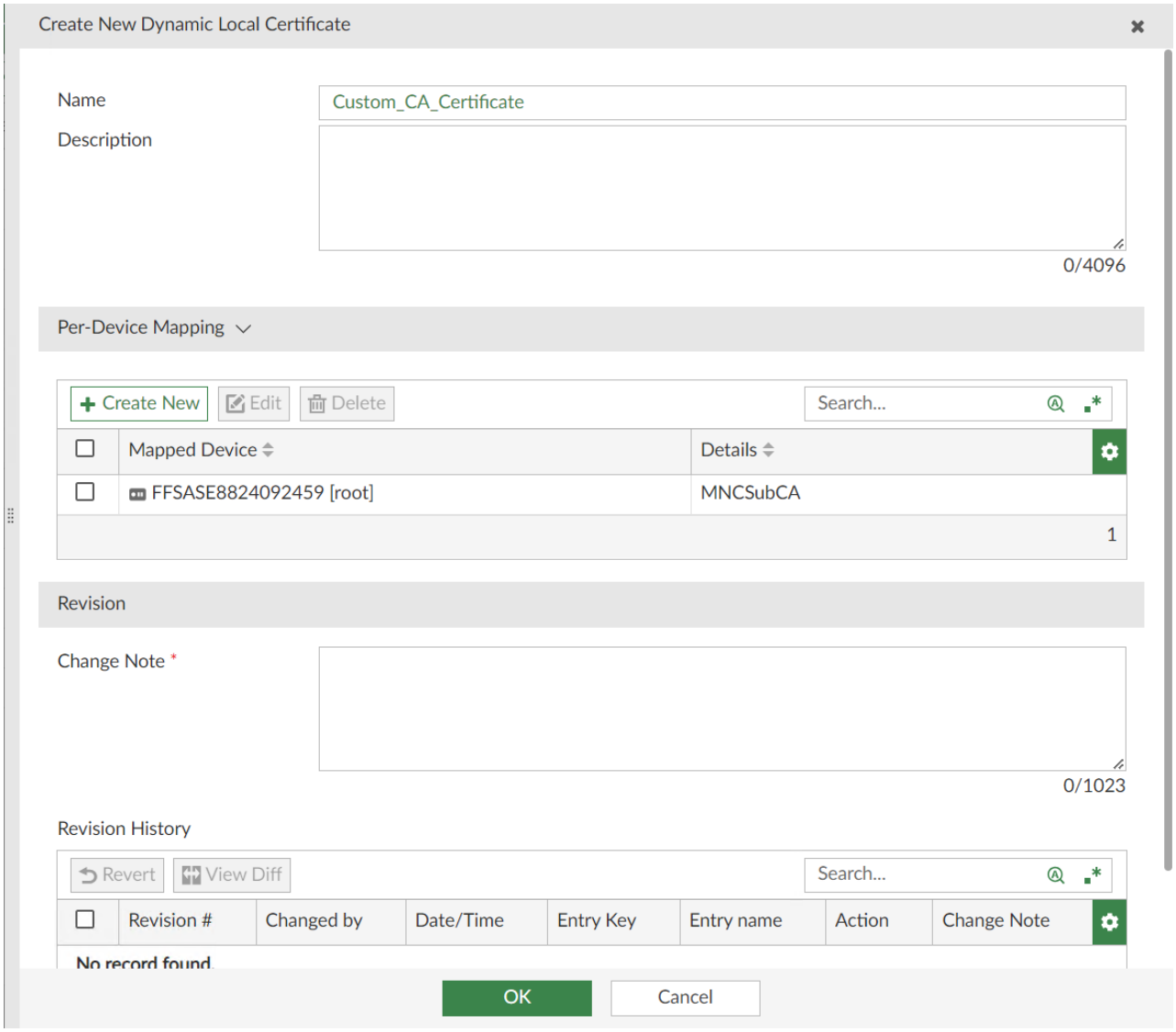
To configure custom certificates for SSL Inspection Profile:

1. Go to *Policy & Objects* > *Advanced* > *CLI Configurations*.
2. Click on *Tools* > *Feature Visibility*.
   a. In *Feature Visibility*, in *Advanced* enable *Dynamic Local Certificate*.
   b. Click *OK*.
3. While still in *Policy & Objects* > *Advanced*, click on *Dynamic Local Certificate*.
4. Click *+Create New*.
5. In *Create New Dynamic Local Certificate*, configure the following:
   a. In *Name* enter *Custom_CA_Certificate*.
   b. In *Per-Device Mapping*, click *+Create New*.
6. In *Per-Device Mapping*, configure the following:
   a. For the *Mapped Device* select the FortiSASE device.
   b. For *Local Certificate* select a previously imported certificate. Otherwise, for *Import Certificate* click *Import*, select a certificate on your local computer to import and once imported, select it from the *Local Certificate* dropdown.



c. Click *OK*.

7. Click *OK*. Fill in the change note and click *OK*.

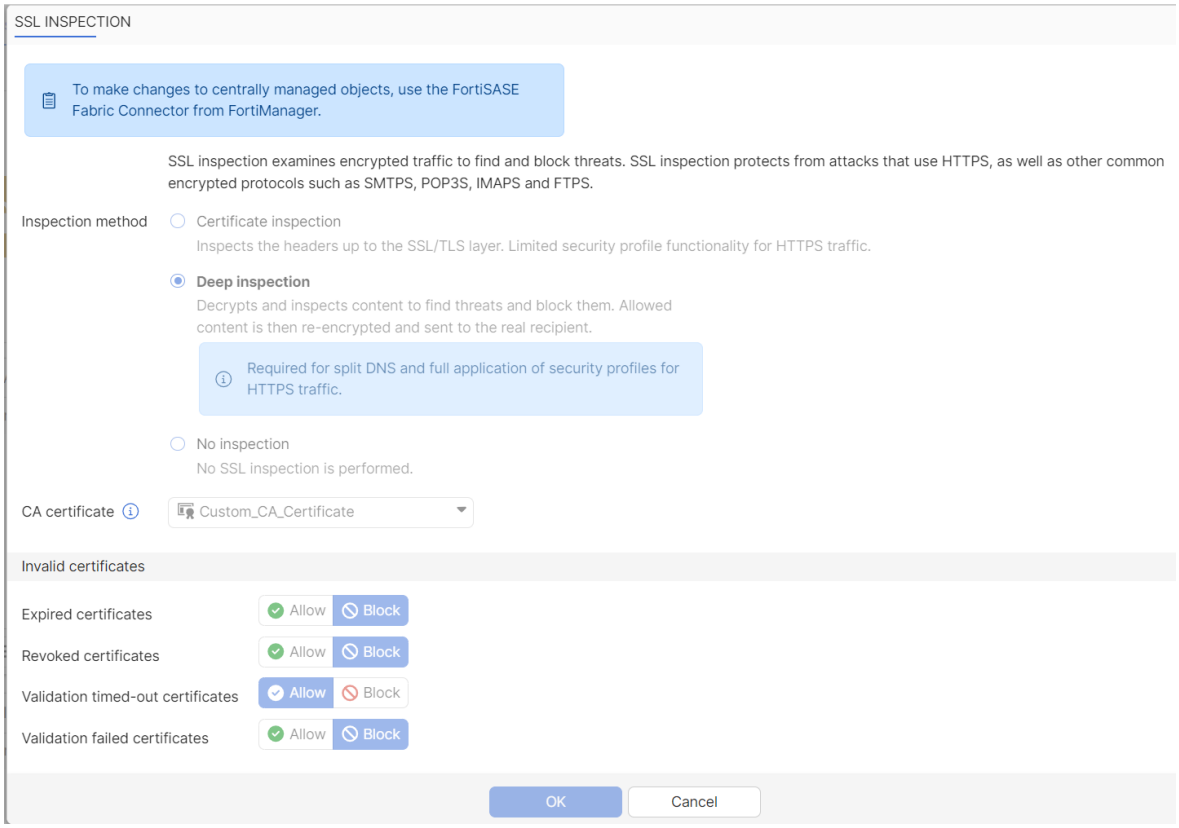


Disabling the FortiSASE connector effectively deletes the FortiSASE device. Therefore, mapping certificates to the FortiSASE device in FortiManager must be done each time whenever the administrator disables the FortiSASE connector and re-enables it.

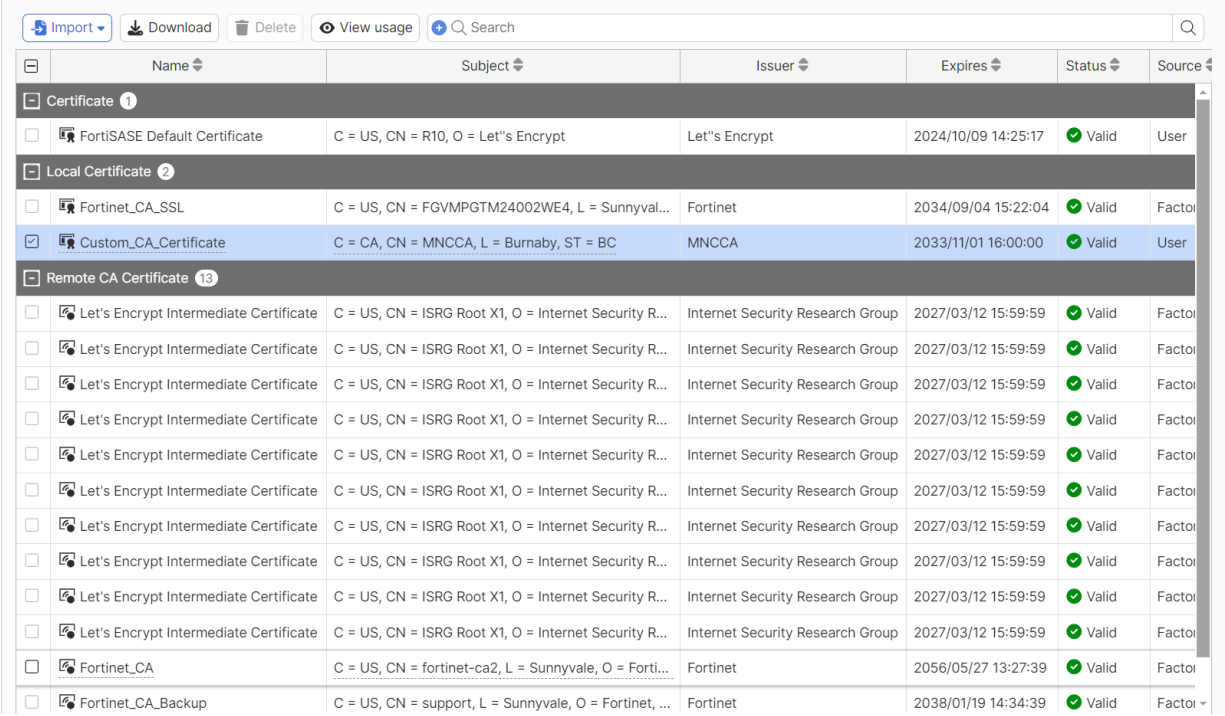
8. Go to *Policy & Objects > Security Profiles*.
   a. Click on *SSL/SSH Inspection* and edit *custom-deep-inspection*.
   b. For *CA Certificate* in the dropdown select *Custom_CA_Certificate*.
   c. Click *OK*. Fill in the change note and click *OK*.
9. Go to *Policy & Objects > Advanced > CLI Configurations*.
   a. Enter *profile-group* in the search bar to discover results matching that keyword.
   b. Expand the *firewall* result in the tree menu, and select the *profile-group* menu item.

c. In *firewall profile-group*, either edit an existing profile-group or click *+Create New*.
   i. In the *name* field, enter *custom-profile-group*.
   ii. For *profile-protocol-options*, select *default*.
   iii. For *ssl-ssh-profile*, select *custom-deep-inspection*.
d. Click *OK*.

10. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the *custom-profile-group* Security Profile Group from FortiManager to FortiSASE.
11. In FortiSASE verify the configuration has been synchronized from FortiManager.
    a. Go to *Security > Traffic > Security profiles* and do the following:
       i. For *Profile Group*, select *custom-profile-group*.
       ii. Click *View SSL inspection configuration*.
       iii. Observe the *Inspection Method* is *Deep inspection* and *CA certificate* is *Custom_CA_Certificate*.



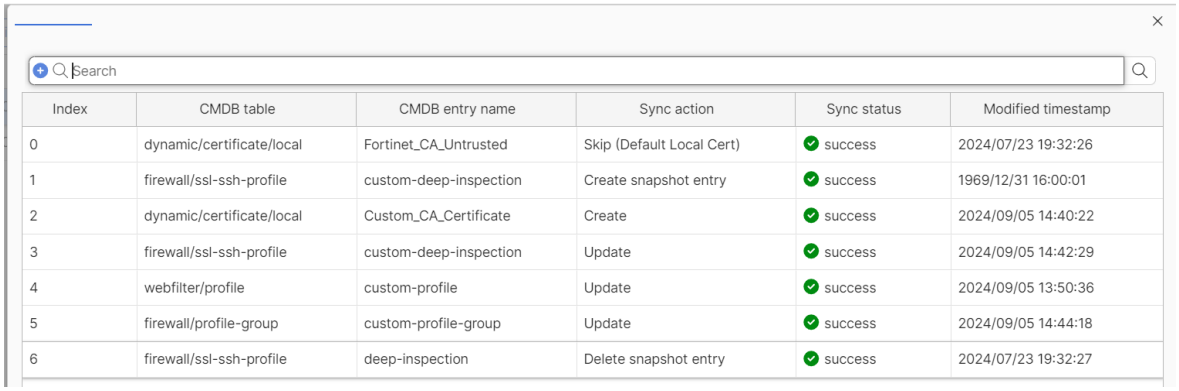
    b. Go to *System > Certificates* and confirm the *Custom_CA_Certificate* is indeed the custom CA certificate that was imported in FortiManager.



c. Go to *Operations > Logs > Central management synchronizations* and do the following:

i. Select the most recent log entry and click *View log details*.

ii. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



Configuring DLP dictionaries, sensors, and profiles

The following example demonstrates how to configure dictionary entries, a dictionary, a sensor, and a DLP profile using these DLP-related objects in FortiManager. The DLP profile is used within a profile group and can be synchronized from FortiManager to FortiSASE.

In this example, we create the DLP dictionary entries, dictionary, sensor, and DLP profile configured in Blocking access to LLM applications using keywords and FQDN example on page 336.

- This example differs in the order of configuring DLP settings compared to the order of configuring these settings in FortiSASE.

- In FortiManager, we can configure a dictionary and a sensor that are independent of a DLP profile. Therefore, a dictionary and a sensor are defined first and then both objects are specified in the DLP profile.

To display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

To configure DLP dictionaries, sensors, and profiles:

1. Go to *Policy & Objects > Security Profiles > Data Loss Prevention* and create a new dictionary by clicking *+Create New > Dictionary*.
   a. In the *Name* field, enter *custom-dictionary*.
   b. In *Dictionary Entries*, configure the following:
      i. For *Logical Relationship*, select *All*.
      ii. Create these dictionary entries for the keywords *programming* and *tips* by clicking *+Create New*, configuring the values below, and clicking *OK*.

Option	Value
Type	keyword
Pattern	programming
Ignore Case	Enabled
Repeats	Disabled
Status	Enabled

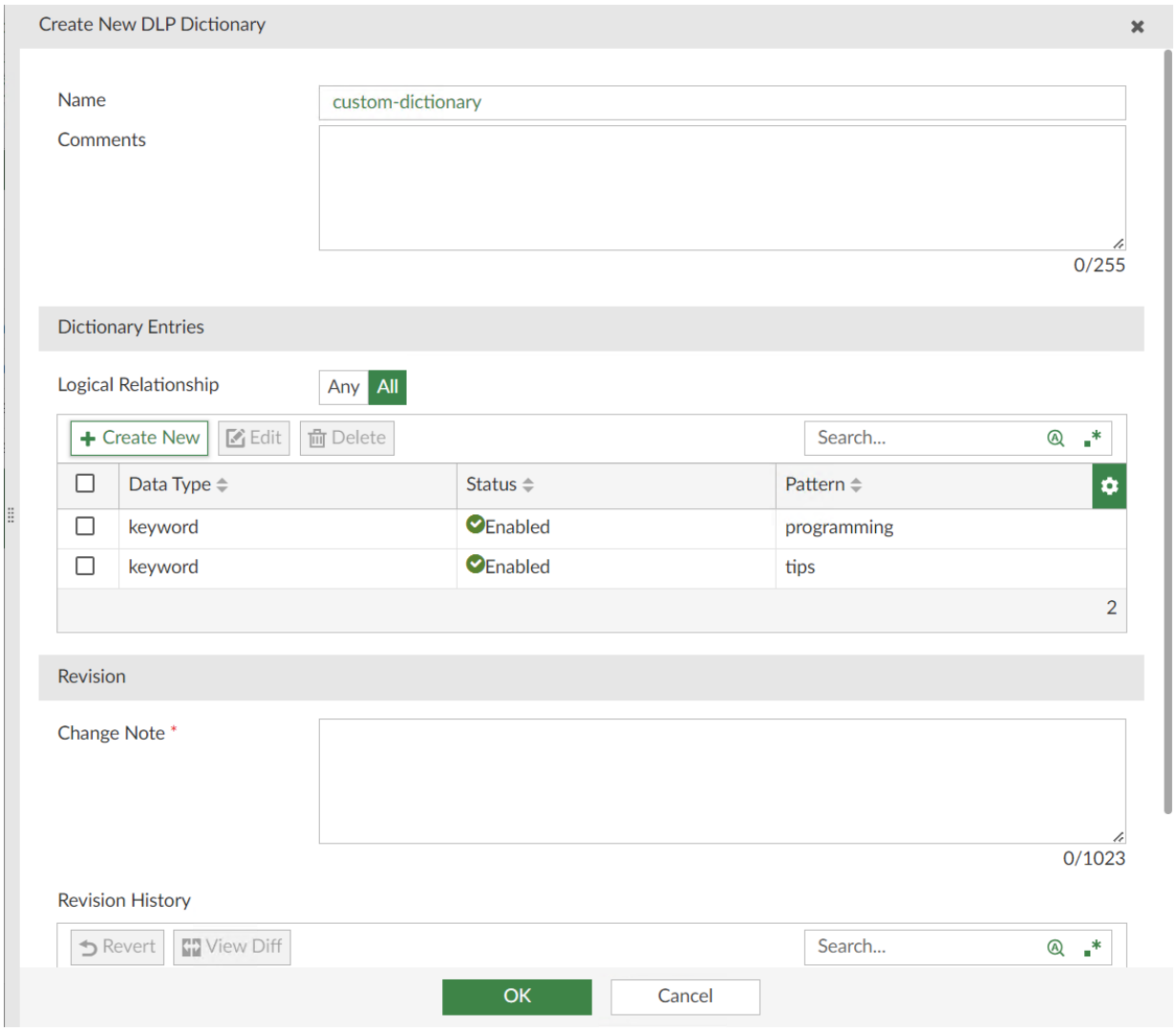
Option	Value
Type	keyword
Pattern	tips
Ignore Case	Enabled
Repeats	Disabled
Status	Enabled

Currently, FortiSASE only supports the following DLP data types:

- *credit-card*
- *hex*
- *keyword*
- *regex*
- *ssn-us*

Therefore, only these data types should be selected when defining dictionary entries.

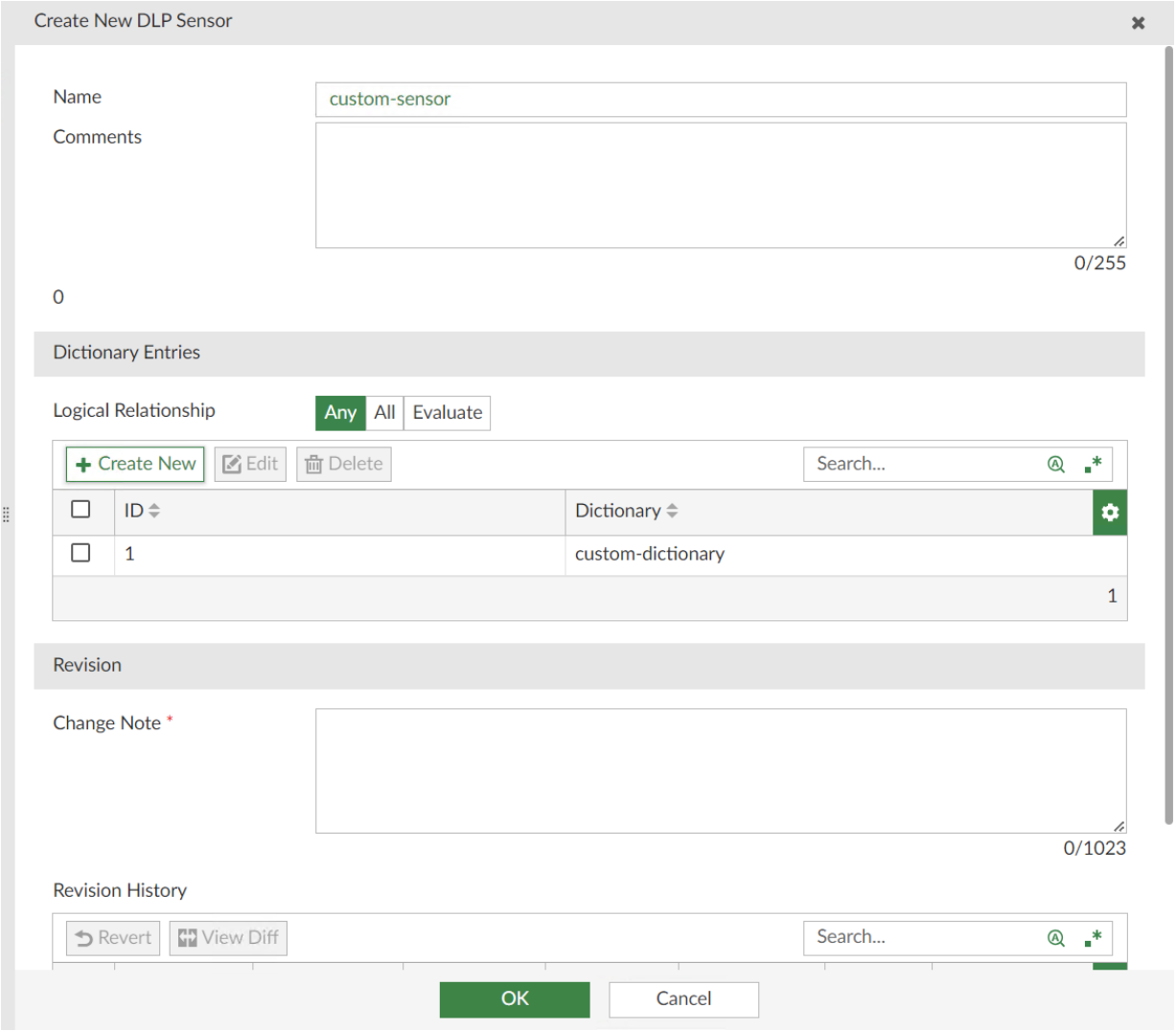
c. Click *OK*. Fill in the change note and click *OK*.



2. While still in *Policy & Objects > Security Profiles > Data Loss Prevention* and create a new sensor by clicking *+Create New > Sensor*.
   a. In the *Name* field, enter *custom-sensor*.
   b. In *Dictionary Entries*, configure the following:
      i. For *Logical Relationship*, select *Any* (this is the default).
      ii. Click on *+Create New*, configure the following settings, and click *OK*:

Option	Value
ID	< Numeric ID automatically filled >
Dictionary	Select DLP Dictionary > custom-dictionary
Count	1
Status	Enabled

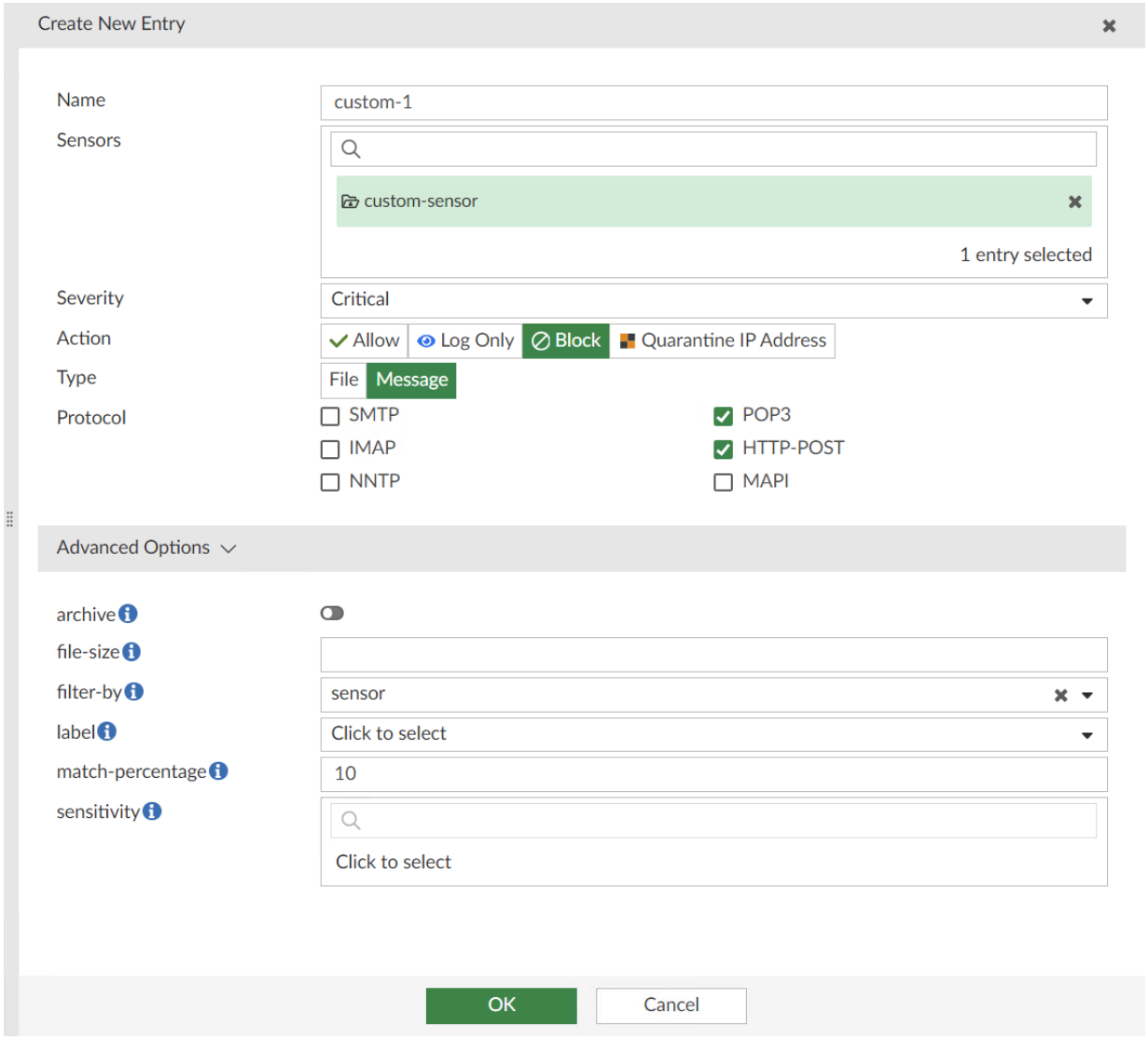
c. Click *OK*. Fill in the change note and click *OK*.



3. While still in *Policy & Objects > Security Profiles > Data Loss Prevention*, create a new profile by clicking *+Create New > Profile*.
   a. In the *Name* field, enter *custom-profile*.
   b. For *Feature Set*, select *Proxy-Based*.
   c. In *Rules*, create a new rule by clicking on *+Create New*.

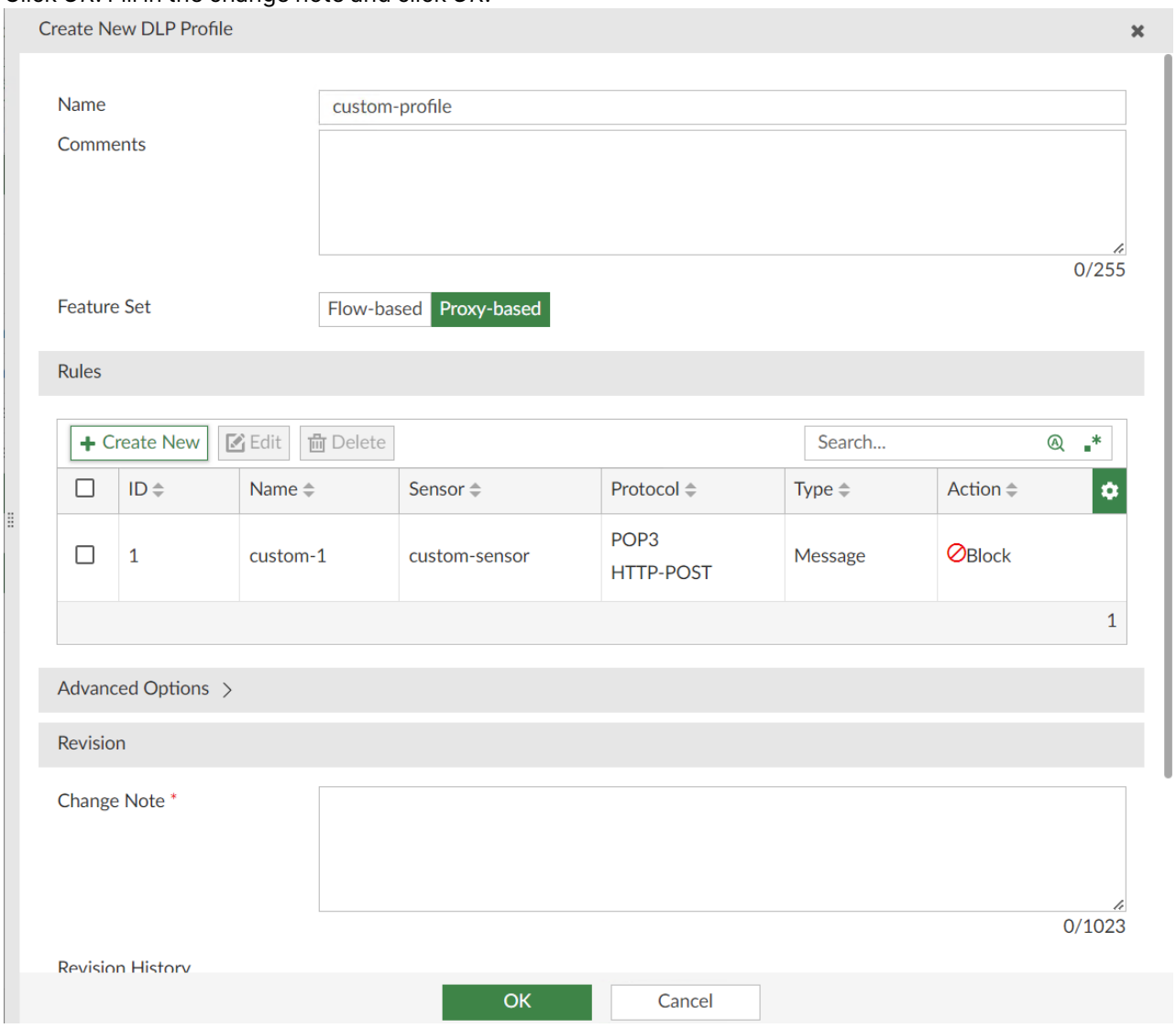
Option	Value
Name	custom-1
Sensors	Select DLP Sensor > custom-sensor
Severity	Critical
Action	Block
Type	Message

Option	Value
Protocol	POP3
HTTP-POST	
Advanced Options	
filter-by	sensor



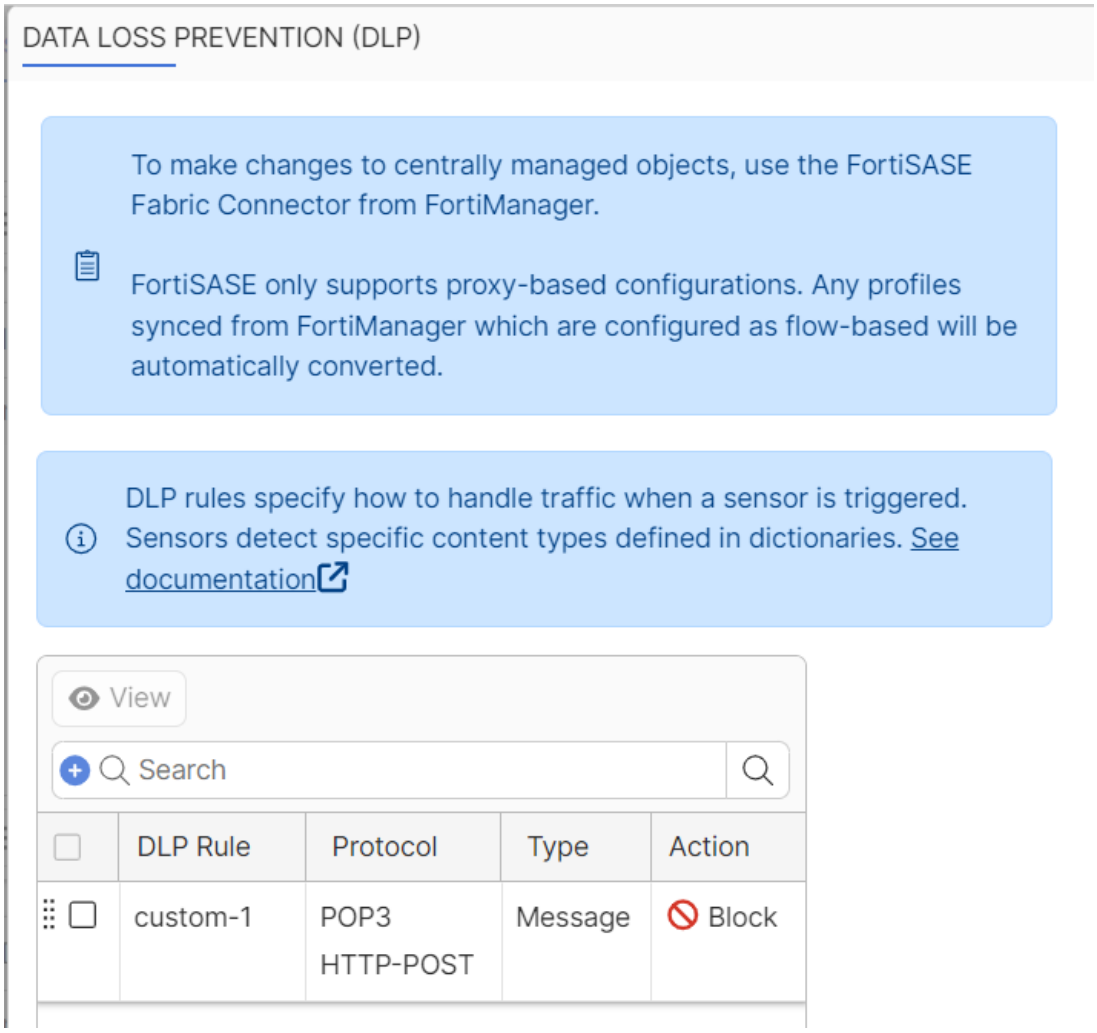
d. Click *OK*.

4. Click *OK*. Fill in the change note and click *OK*.



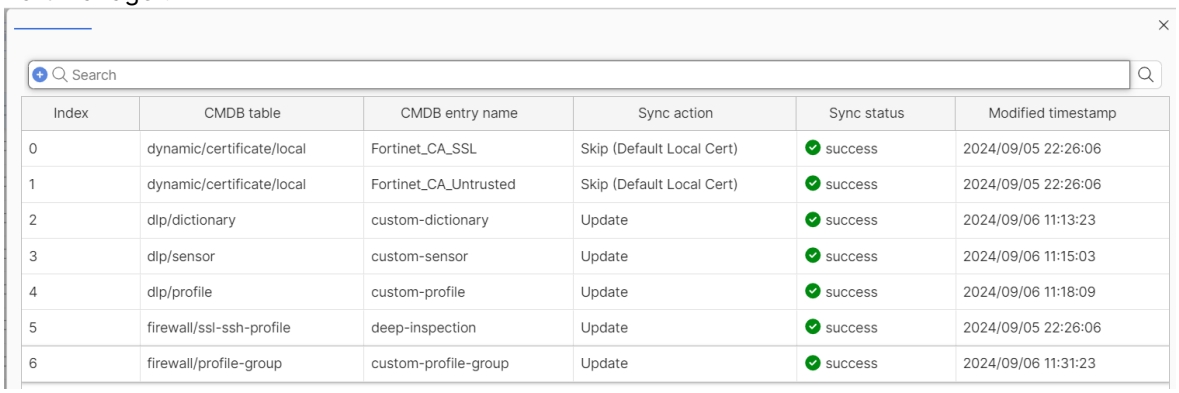
5. Go to *Policy & Objects > Advanced > CLI Configurations*.
   a. Enter *profile-group* in the search bar to discover results matching that keyword.
   b. Expand the *firewall* result in the tree menu, and select the *profile-group* menu item.
   c. In *firewall profile-group*, either edit an existing profile-group or click *+Create New*.
      i. In the *name* field, enter *custom-profile-group*.
      ii. For *dlp-profile*, select *custom-profile*.
      iii. For *profile-protocol-options*, select *default*.
      iv. For *ssl-ssh-profile*, select *custom-deep-inspection*.
   d. Click *OK*.
6. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the *custom-profile-group* Security Profile Group from FortiManager to FortiSASE.

7. In FortiSASE verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *Traffic* > *Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In the *Data Loss Prevention (DLP)* widget, click *View*.
      iii. Observe the *DLP Rule* of *custom-1* has been configured.



   b. Go to *Operations* > *Logs* > *Central management synchronizations* and do the following:
      i. Select the most recent log entry and click *View log details*.

ii. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



Configuring and applying Video Filter

The video filter feature allows you to allow, monitor, or block YouTube videos based on FortiGuard categories. It also provides the flexibility to override the actions configured for a FortiGuard category on a per-channel basis using their channel IDs.

Video filter requires enabling SSL deep inspection inside the profile group. See Certificate and deep inspection modes on page 315. It also requires a Google API key to access the YouTube Data API. To generate an API key, see YouTube Data API Overview.

The following example demonstrates configuring video filter using FortiManager. In this configuration, the video filter is set to:

- Block YouTube videos categorized as News under FortiGuard categories.
- Monitor YouTube videos for all other FortiGuard categories.
- Allow videos from YouTube channel named CNN by using its channel ID.

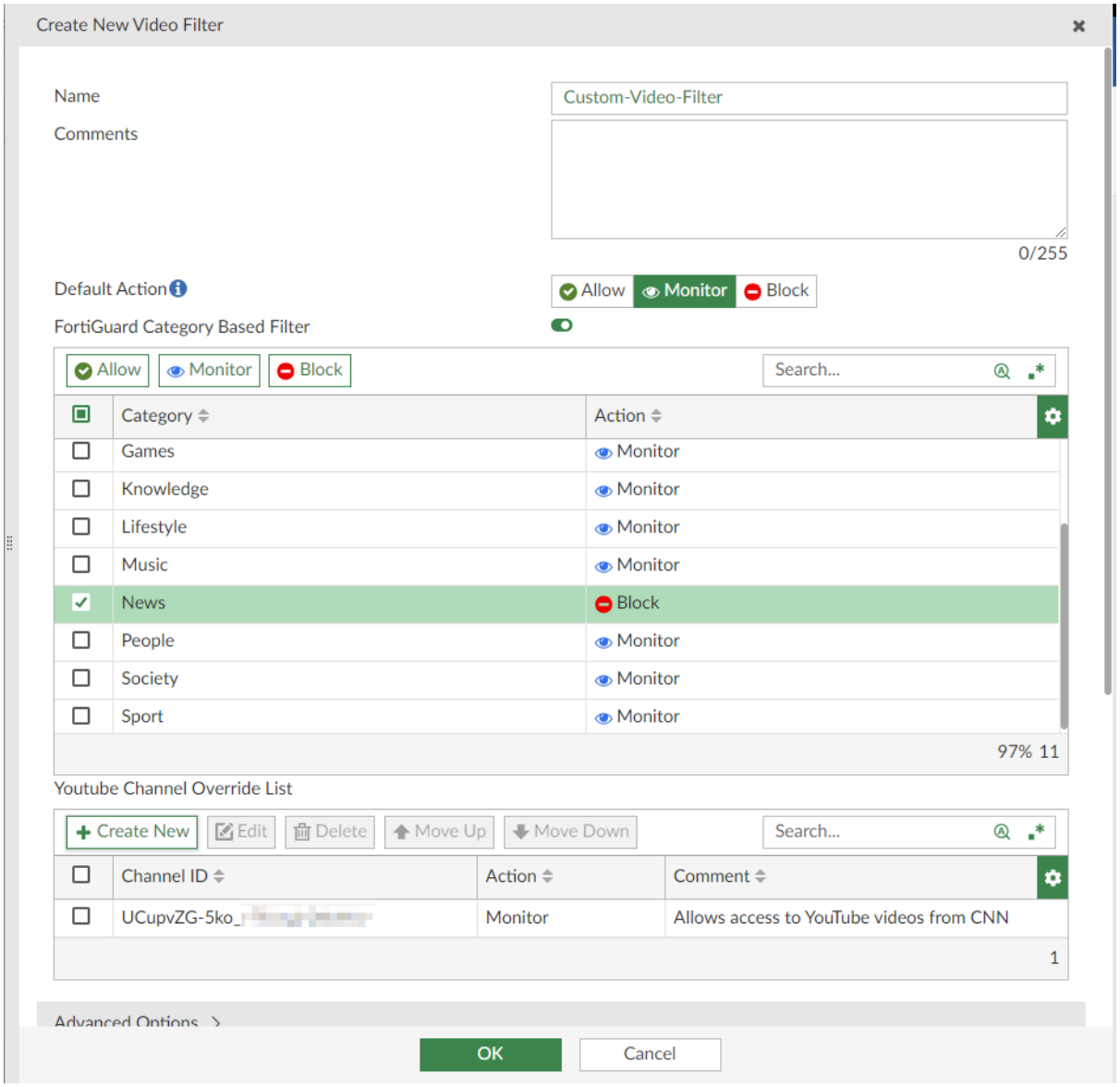
To display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

To create and apply a new Video Filter:

1. Create a new Video Filter:
   a. Go to *Policy & Objects > Security Profiles > Video Filter* and create a new video filter by clicking *Create New*.
   b. In the *Name* field, enter Custom-Video-Filter.
   c. Set *Default Action* for the FortiGuard categories to *Monitor*.
   d. Enable the toggle for *FortiGuard Category Based Filter*.
   e. From the *Category* list, select *News* and set it to *Block*.

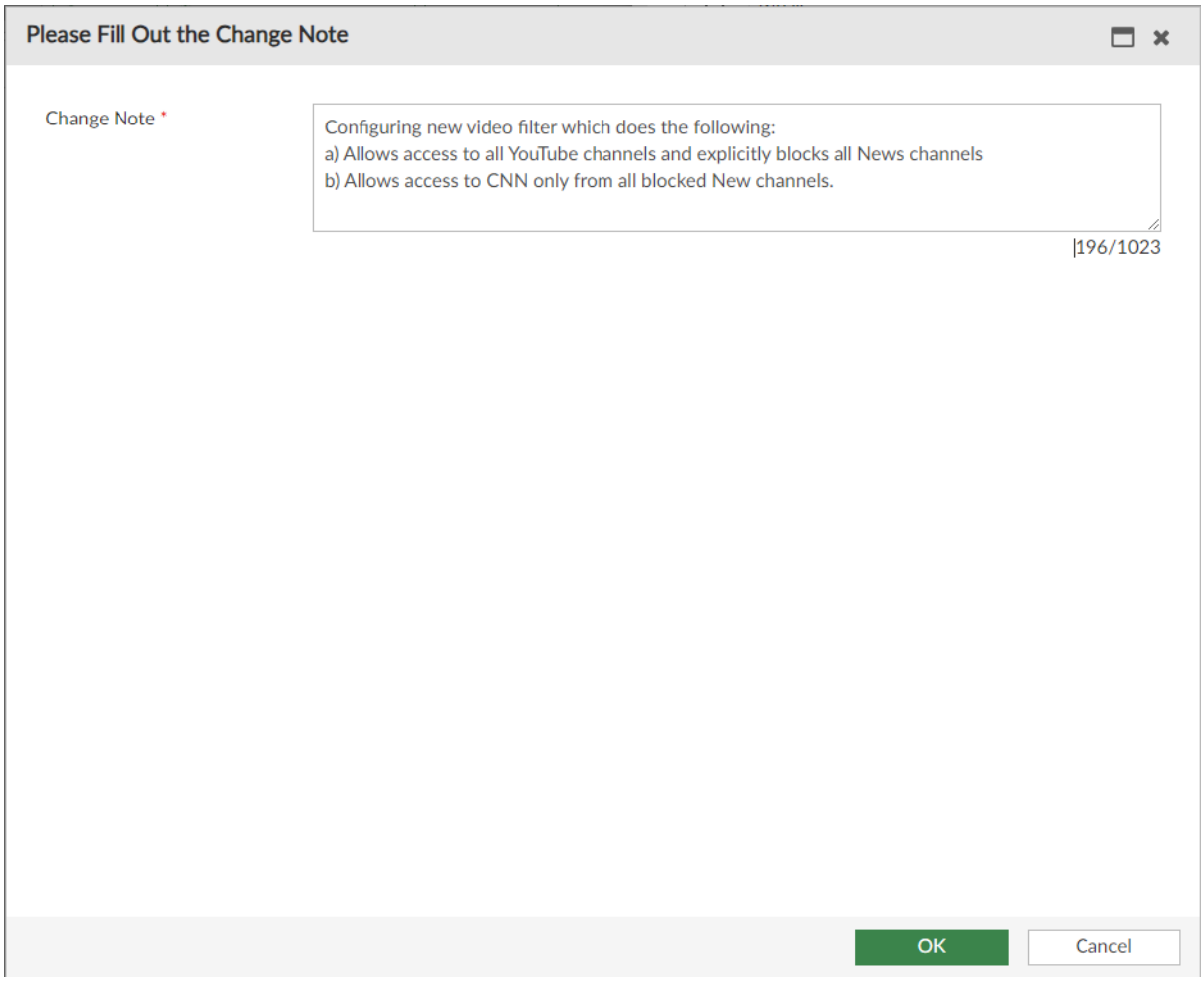
f. In *Youtube Channel Override List*, click *Create New*, enter the following in the slide-in, and click *OK*:

Option	Value
Channel ID	UCupvZG-5ko_...
Comments	Allows access to YouTube videos from CNN
Action	Monitor

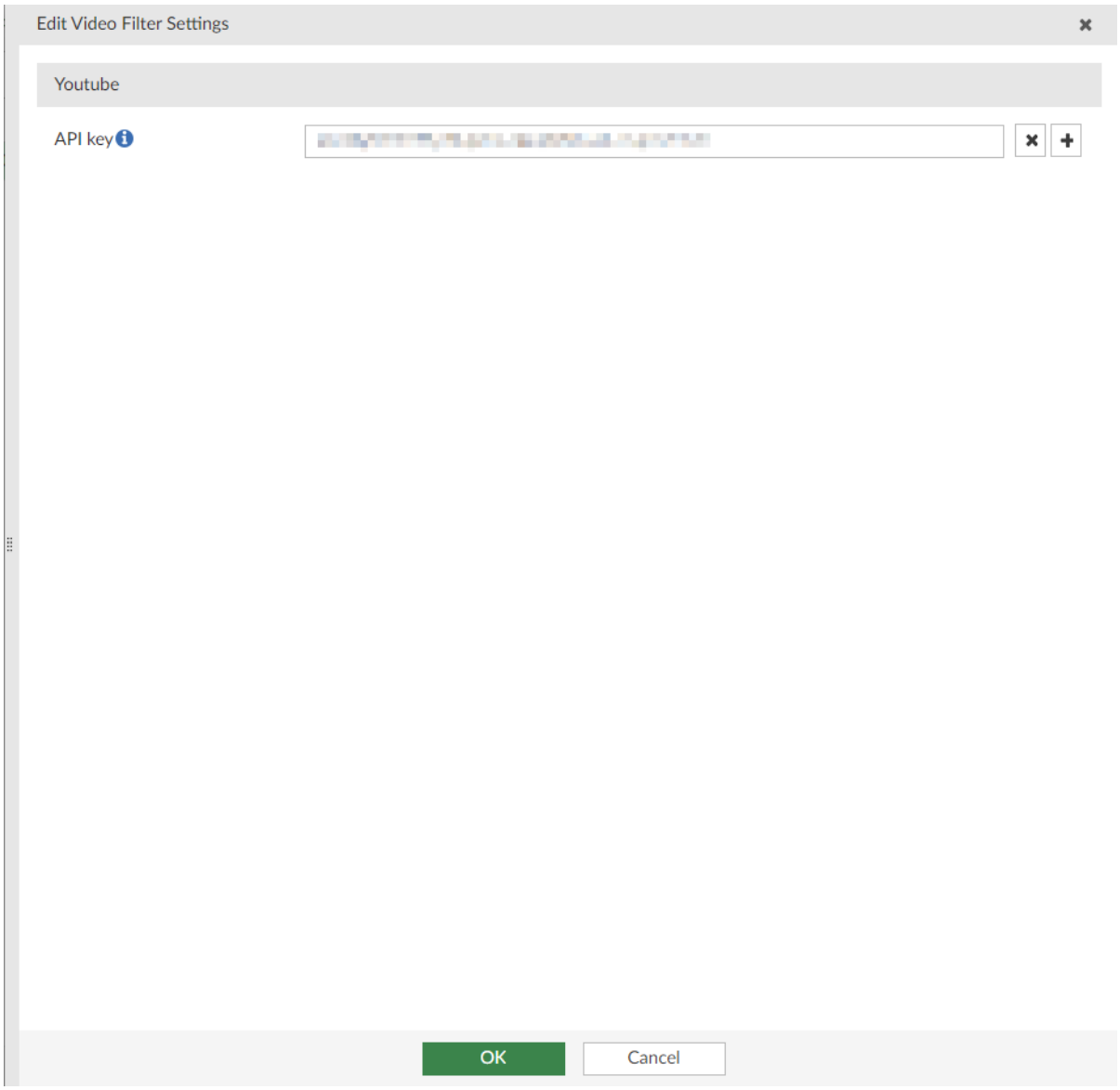


g. Click *OK*.

h. Enter a suitable description in *Change Note* and click *OK*.

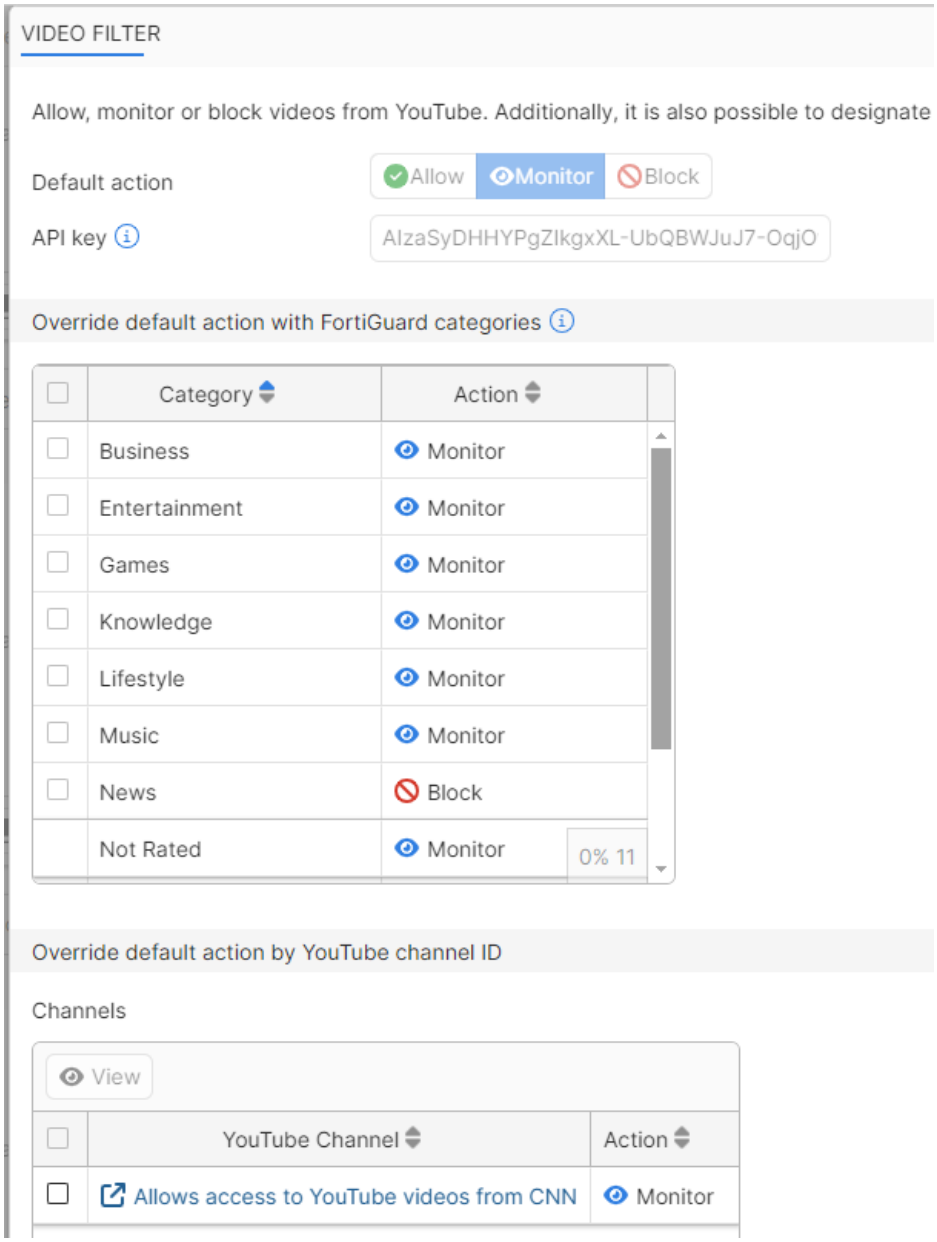


2. Go to *Policy & Object* > *Security Profiles* > *Video Filter*. Click *Custom-Video-Filter*, select *Edit Video Filter Settings*, enter the *API key* to access YouTube data, and click *OK*.

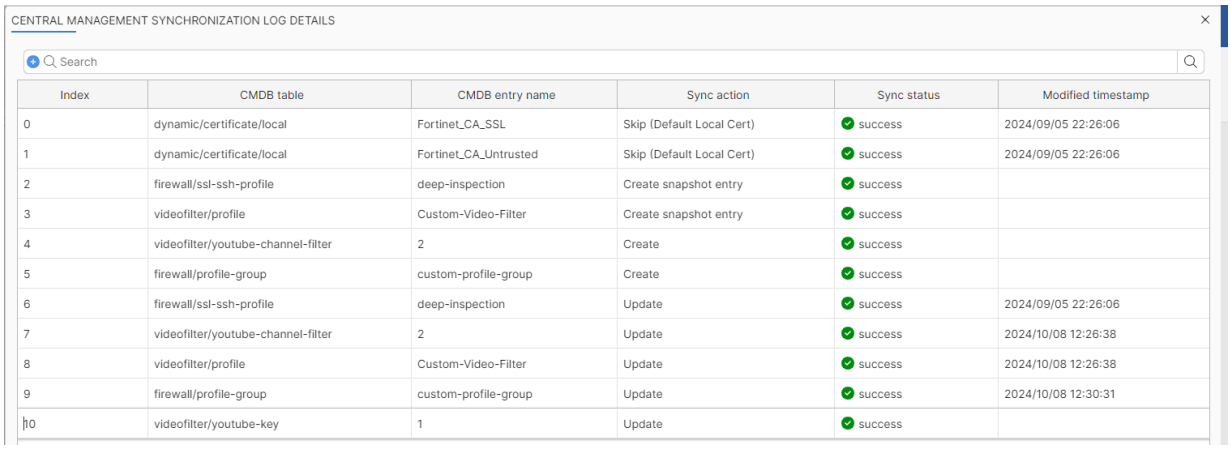


3. Apply Video Filter:
   a. Go to *Policy & Objects* > *Advanced* > *CLI Configurations*.
   b. Enter profile-group in the search bar to discover results matching that keyword.
   c. Expand the *firewall* result in the tree menu, and select the *profile-group* menu item.
   d. In *firewall profile-group*, edit an existing profile-group or click *Create New*.
   e. In the *name* field, enter custom-profile-group.
   f. For *videofilter-profile*, select *Custom-Video-Filter*.
   g. For *profile-protocol-options*, select *default*.
   h. For *ssl-ssh-profile*, select *deep-inspection*.
   i. Click *OK*.
4. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605to synchronize the custom-profile-group Security Profile Group from FortiManager to FortiSASE.
5. In FortiSASE, verify the configuration has been synchronized from FortiManager:

6. Go to *Security* > *Traffic* > *Security profiles* and do the following:
   a. For *Profile Group*, select *custom-profile-group*.
   b. In the *Video Filter* widget, click *View*.
   c. Observe the required configuration is synchronized to FortiSASE.



7. Go to *Operations* > *Logs* > *Central management synchronizations* and do the following:
   a. Select the most recent log entry and click *View log details*.
   b. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



Index	CMDB table	CMDB entry name	Sync action	Sync status	Modified timestamp
0	dynamic/certificate/local	Fortinet_CA_SSL	Skip (Default Local Cert)	success	2024/09/05 22:26:06
1	dynamic/certificate/local	Fortinet_CA_Untrusted	Skip (Default Local Cert)	success	2024/09/05 22:26:06
2	firewall/ssl-ssh-profile	deep-inspection	Create snapshot entry	success	
3	videofilter/profile	Custom-Video-Filter	Create snapshot entry	success	
4	videofilter/youtube-channel-filter	2	Create	success	
5	firewall/profile-group	custom-profile-group	Create	success	
6	firewall/ssl-ssh-profile	deep-inspection	Update	success	2024/09/05 22:26:06
7	videofilter/youtube-channel-filter	2	Update	success	2024/10/08 12:26:38
8	videofilter/profile	Custom-Video-Filter	Update	success	2024/10/08 12:26:38
9	firewall/profile-group	custom-profile-group	Update	success	2024/10/08 12:30:31
10	videofilter/youtube-key	1	Update	success	

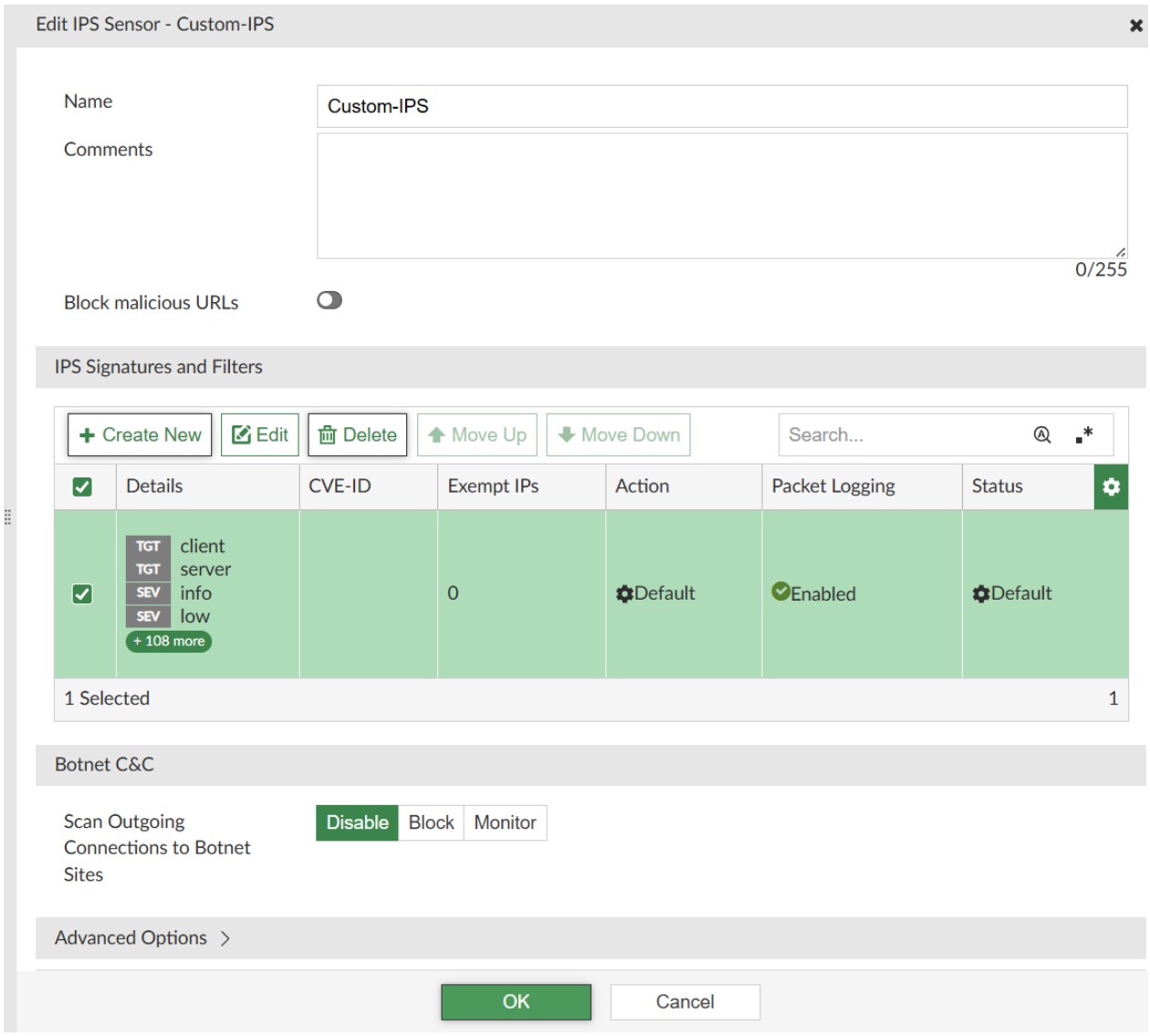
Configuring and applying an IPS profile

The following example demonstrates how to configure an intrusion prevention system (IPS) profile in FortiManager. The IPS profile is used within a profile group and can be synchronized from FortiManager to FortiSASE

> In FortiManager, to display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page, such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

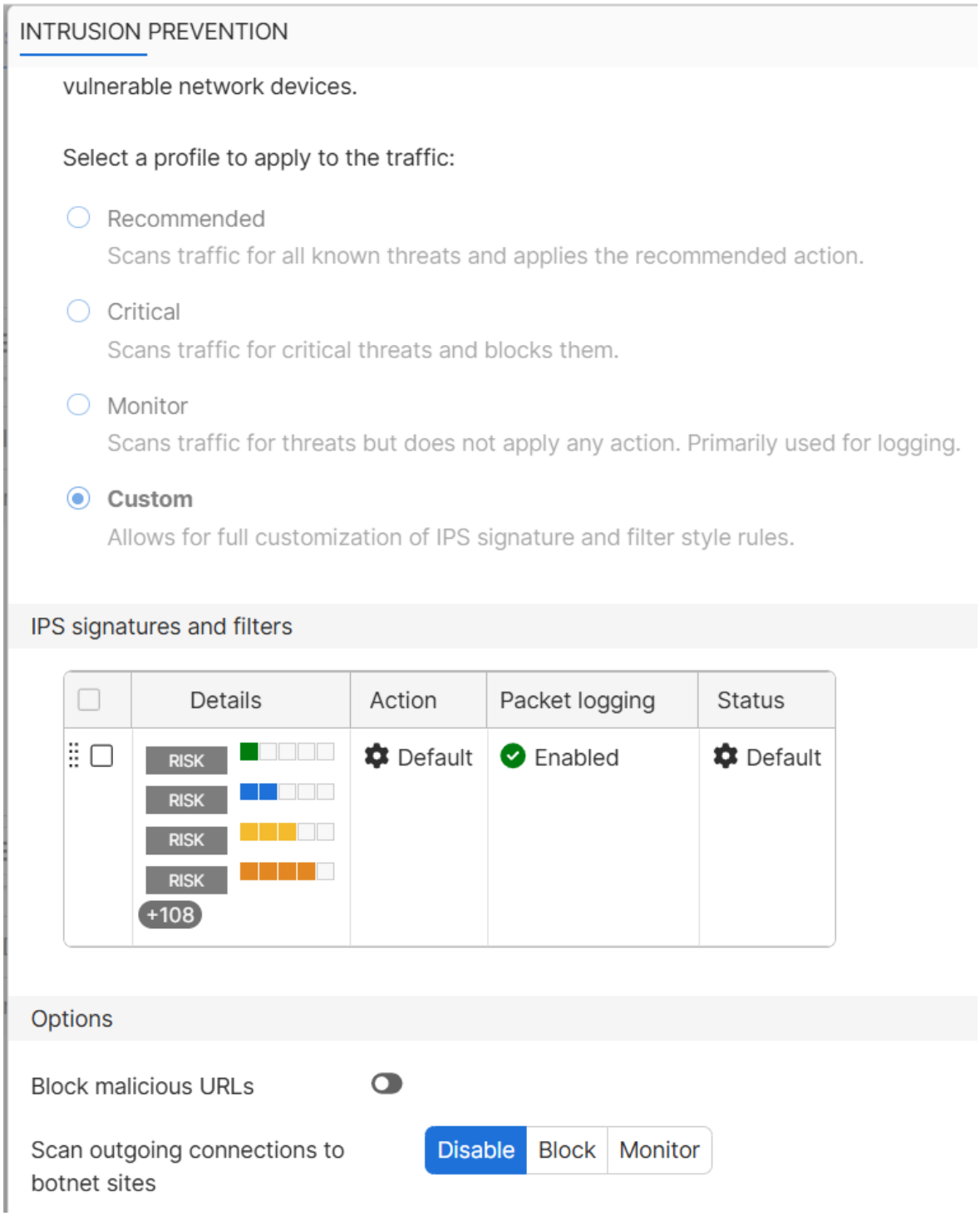
To create and apply a new IPS profile:

1. Create a new Intrusion Prevention Profile:
   a. Go to *Policy & Objects > Security Profiles > Intrusion Prevention* and create a new IPS profile by clicking *Create New*.
   b. In the *Name* field, enter Custom-IPS.
   c. In *IPS Signatures and Filters*, create a new *IPS Signatures and Filters* entry:
      i. Click *Create New*.
      ii. For *Type*, select *Filter*.
      iii. For *Action*, select *Default*.
      iv. For *Packet logging*, select *Enable*.
      v. For *Status*, select *Default*.
      vi. For *Filter*, click the dropdown, select all filter entries by clicking the select all icon on the bottom-left of the dropdown list, and click *OK*.
      vii. Click *OK*.
2. Observe the following settings before saving them. Enter a suitable description in *Change Note* and click *OK*.

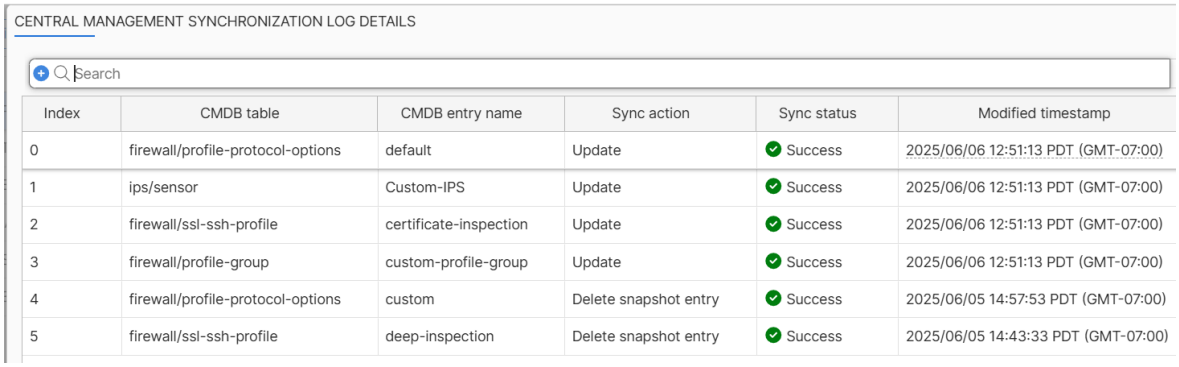


3. Apply Intrusion Prevention profile by going to *Policy & Objects* > *Security Profiles* > *Profile Group*:
   a. Click *Create New*.
   b. In the *Name* field, enter custom-profile-group.
   c. For *IPS Profile*, select *Custom-IPS*.
   d. For *SSL/SSH Inspection*, select *certificate-inspection*.
   e. For *Protocol Options*, select *default*.
   f. Click *OK*. Fill in the change note and click *OK*.
4. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the custom-profile-group Security Profile Group from FortiManager to FortiSASE.
5. In FortiSASE, verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *Traffic* > *Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In the *Intrusion Prevention* widget, click *View*.

iii. Observe the required configuration is synchronized to FortiSASE.



b. Go to *Operations* > *Logs* > *Central Management Synchronizations* and do the following:
   i. Select the most recent log entry and click *View log details*.
   ii. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.


CENTRAL MANAGEMENT SYNCHRONIZATION LOG DETAILS

Search

Index	CMDB table	CMDB entry name	Sync action	Sync status	Modified timestamp
0	firewall/profile-protocol-options	default	Update	Success	2025/06/06 12:51:13 PDT (GMT-07:00)
1	ips/sensor	Custom-IPS	Update	Success	2025/06/06 12:51:13 PDT (GMT-07:00)
2	firewall/ssl-ssh-profile	certificate-inspection	Update	Success	2025/06/06 12:51:13 PDT (GMT-07:00)
3	firewall/profile-group	custom-profile-group	Update	Success	2025/06/06 12:51:13 PDT (GMT-07:00)
4	firewall/profile-protocol-options	custom	Delete snapshot entry	Success	2025/06/05 14:57:53 PDT (GMT-07:00)
5	firewall/ssl-ssh-profile	deep-inspection	Delete snapshot entry	Success	2025/06/05 14:43:33 PDT (GMT-07:00)

Configuring and applying an Application Control profile

The following example demonstrates how to configure an application sensor in the Application Control profile in FortiManager. The Application Control profile is used within a profile group and can be synchronized from FortiManager to FortiSASE.

This example configures the following options:

- Application overrides to block YouTube applications as configured in Application Control With Inline-CASB on page 376.
- Application overrides to block applications considered critical risk by the FortiGuard Application Control Service as configured in Application Control With Inline-CASB on page 376.
- Protocol enforcement options as configured in Network protocol enforcement on page 380 and Blocking applications detected on non-default ports on page 381.

In FortiManager, to display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page, such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

To create and apply a new Application Control profile:

1. Create a new Application Control Profile:
   a. Go to *Policy & Objects > Security Profiles > Application Control* and create a new application control profile by clicking *Create New*.
   b. In the *Name* field, enter *Custom-AppCtrl-Profile*.
   c. In *Application and Filter Overrides*, create a new application override for blocking YouTube:
      i. Click *Create New*.
      ii. For *Type*, select *Application*.
      iii. For *Action*, select *Block*.
      iv. In *Application*, click *Add*. Enter *YouTube* in the top-right *Search* field and then click on the top-left selection box to select the application names. Click *Use Selected Signatures*.
      v. Click *OK*.
   d. In *Application and Filter Overrides*, create a new filter override for blocking critical risk applications as classified by the FortiGuard Application Control Service:

i. Click *Create New*.
ii. For *Type*, select *Filter*.
iii. For *Action*, select *Block*.
iv. In *Filter*, click *Edit*.
    i. Click *+Add Filter*.
    ii. Select *Risk*.
    iii. Select *Critical*.
    iv. Click *Apply*.
    v. Click *Use Filters*.
v. Click *OK*.

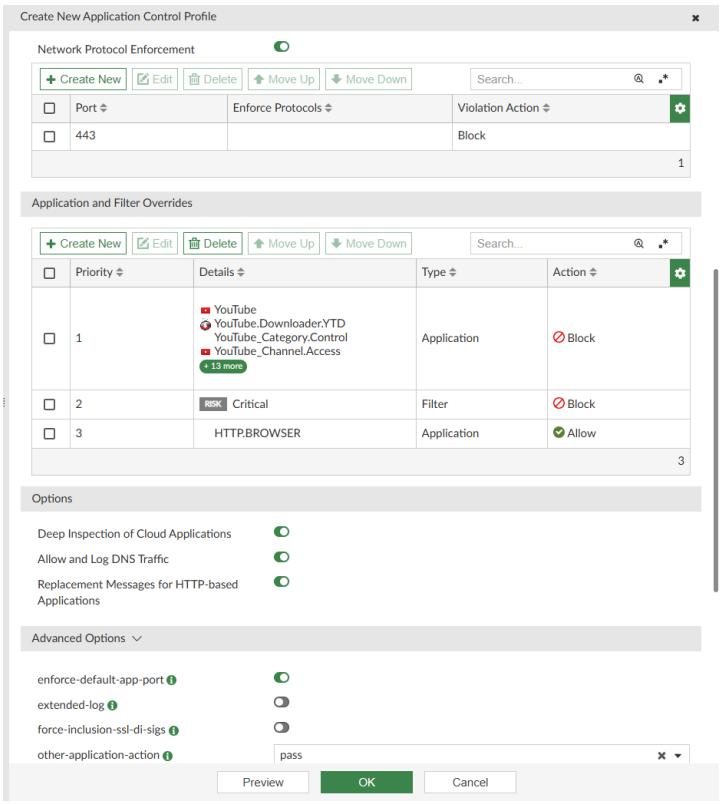
e. Enable *Network Protocol Enforcement*.
i. Click *Create New*.
ii. Configure these settings:

Field	Value
Port	Port number for the network service. For example, enter *443*.
Enforce protocols	Select one or more protocols to enforce from a list of common network protocols. For example, select *HTTPS*.
Violation action	Action to take for protocols which are not allowed under the selected port. For example, select *Block*.

iii. Click *OK*.

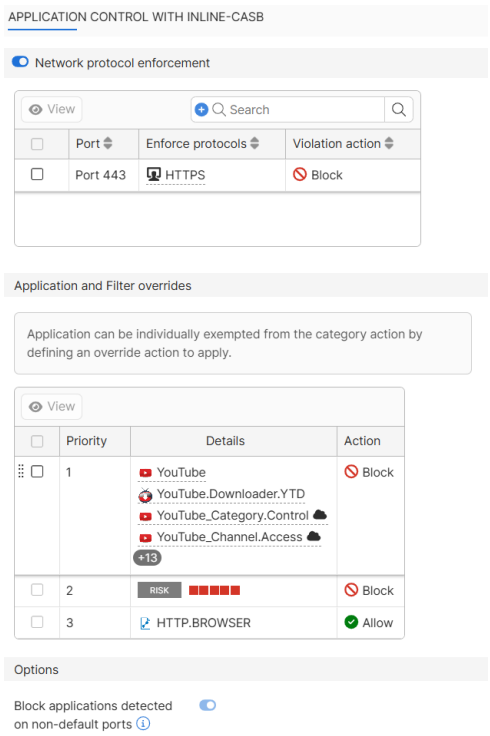
f. In *Application and Filter Overrides*, create a new application override for allowing HTTP browser traffic:
i. Click *Create New*.
ii. For *Type*, select *Application*.
iii. For *Action*, select *Allow*.
iv. In *Application*, click *Add*. Enter *HTTP.BROWSER* in the top-right *Search* field and then click on the selection box to the left of *HTTP.BROWSER*.
v. Click *Use Selected Signatures*.
vi. Click *OK*.

g. Collapse *Advanced Options*.
h. Enable *enforce-default-app-port*. This option enables default application port enforcement for allowed applications, namely, applications configured with either the *Allow* or *Monitor* action. It is used with the override for HTTP browser traffic.
i. Observe the following settings before saving them:

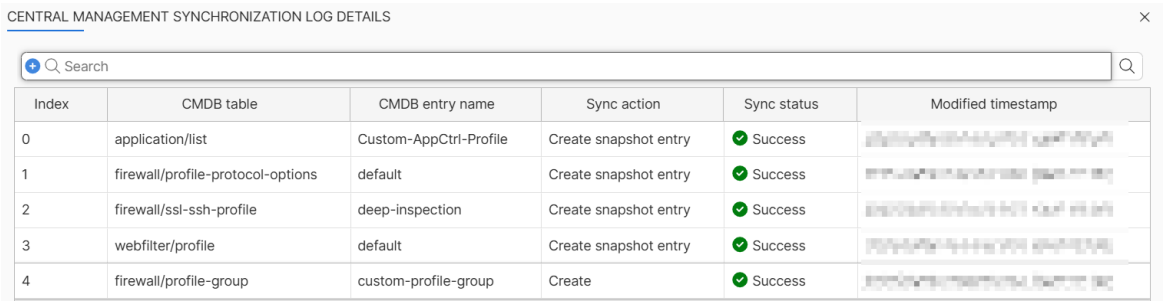


j. Enter a suitable description in *Change Note* and click *OK*.

2. Apply Application Control profile:
   a. Go to *Policy & Objects* > *Security Profiles* > *Profile Group*.
   b. Click *Create New*.
   c. In the *Name* field, enter *custom-profile-group*.
   d. For *Web Filter Profile*, select *default*.
   e. For *Application Control*, select *Custom-AppCtrl-Profile*.
   f. For *SSL/SSH Inspection*, select *deep-inspection*.
   g. For *Protocol Options*, select *default*.
   h. Fill in the *Change Note*.
   i. Click *OK*.
3. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the *custom-profile-group* Security Profile Group from FortiManager to FortiSASE.
4. In FortiSASE, verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *Traffic* > *Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In the *Application Control With Inline-CASB* widget, click *View*.
      iii. Observe the required configuration is synchronized to FortiSASE.



5. Go to *Operations* > *Logs* > *Central management synchronizations* and do the following:
   a. Select the most recent log entry and click *View log details*.
   b. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



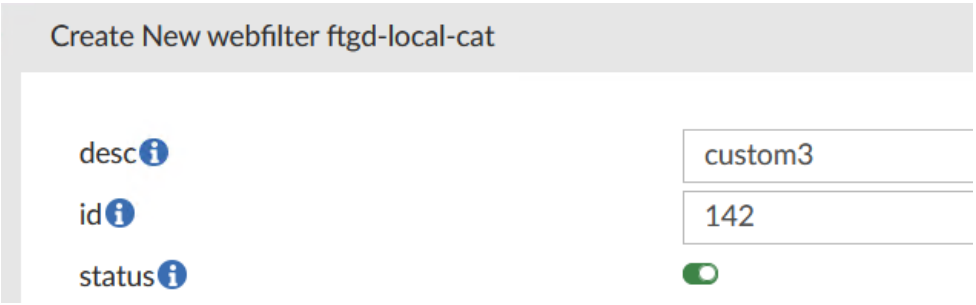
Configuring custom Web Filter categories

FortiSASE supports synchronization of empty custom web filter categories from FortiManager followed by configuration of these categories from FortiSASE.

To configure custom web filter categories:

1. In FortiManager, go to *Policy & Objects* > *Advanced* > *CLI Configurations*. Create a custom category:
   a. Enter ftgd-local-cat in the search bar to discover results matching that keyword.
   b. Select the *ftgd-local-cat* menu item.
   c. In *webfilter ftgd-local-cat*, click *Create New*.

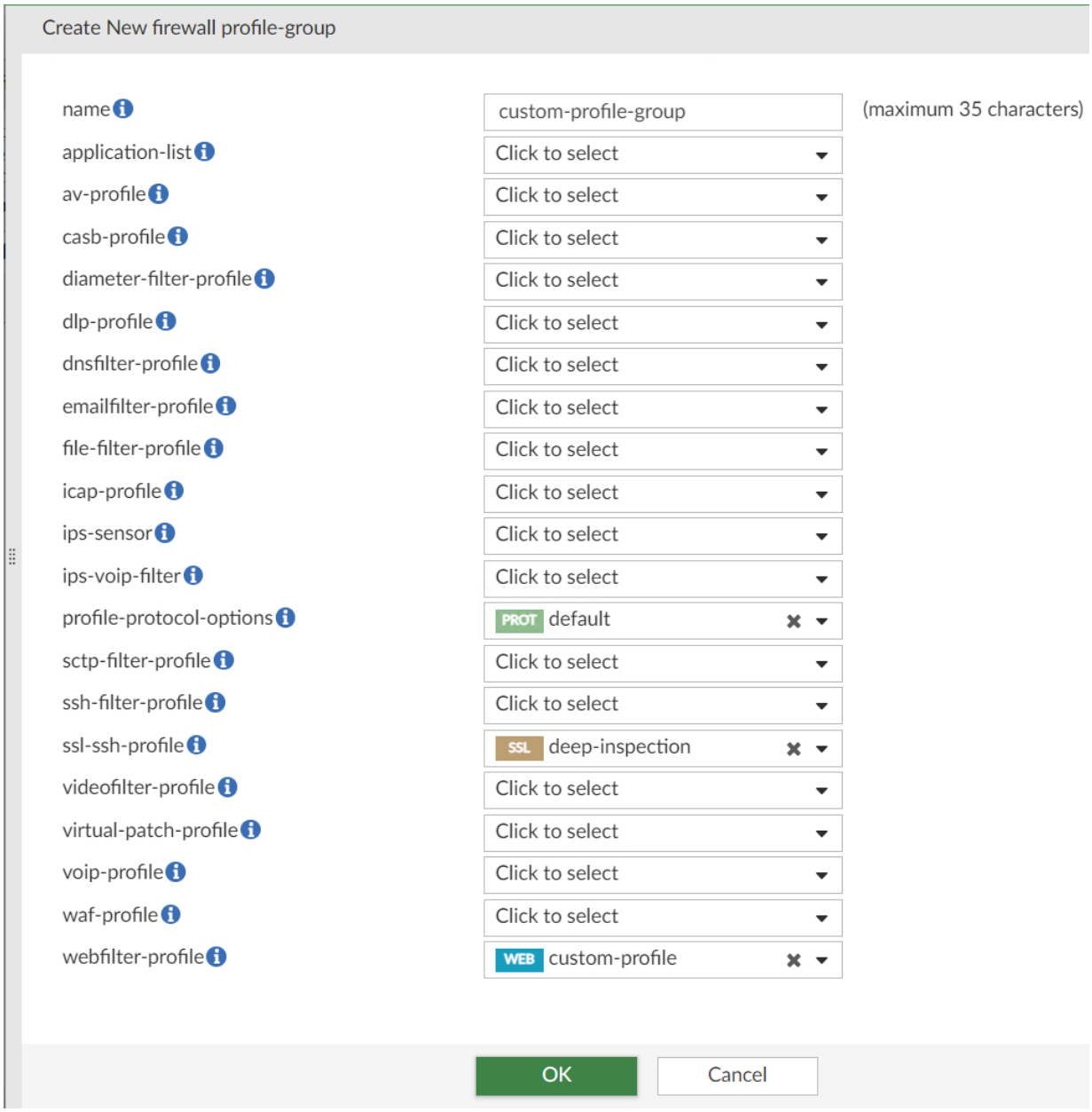
d. In *Create New webfilter ftgd-local-cat*, in the *desc* field, enter custom3. In the *id*, field enter 142.



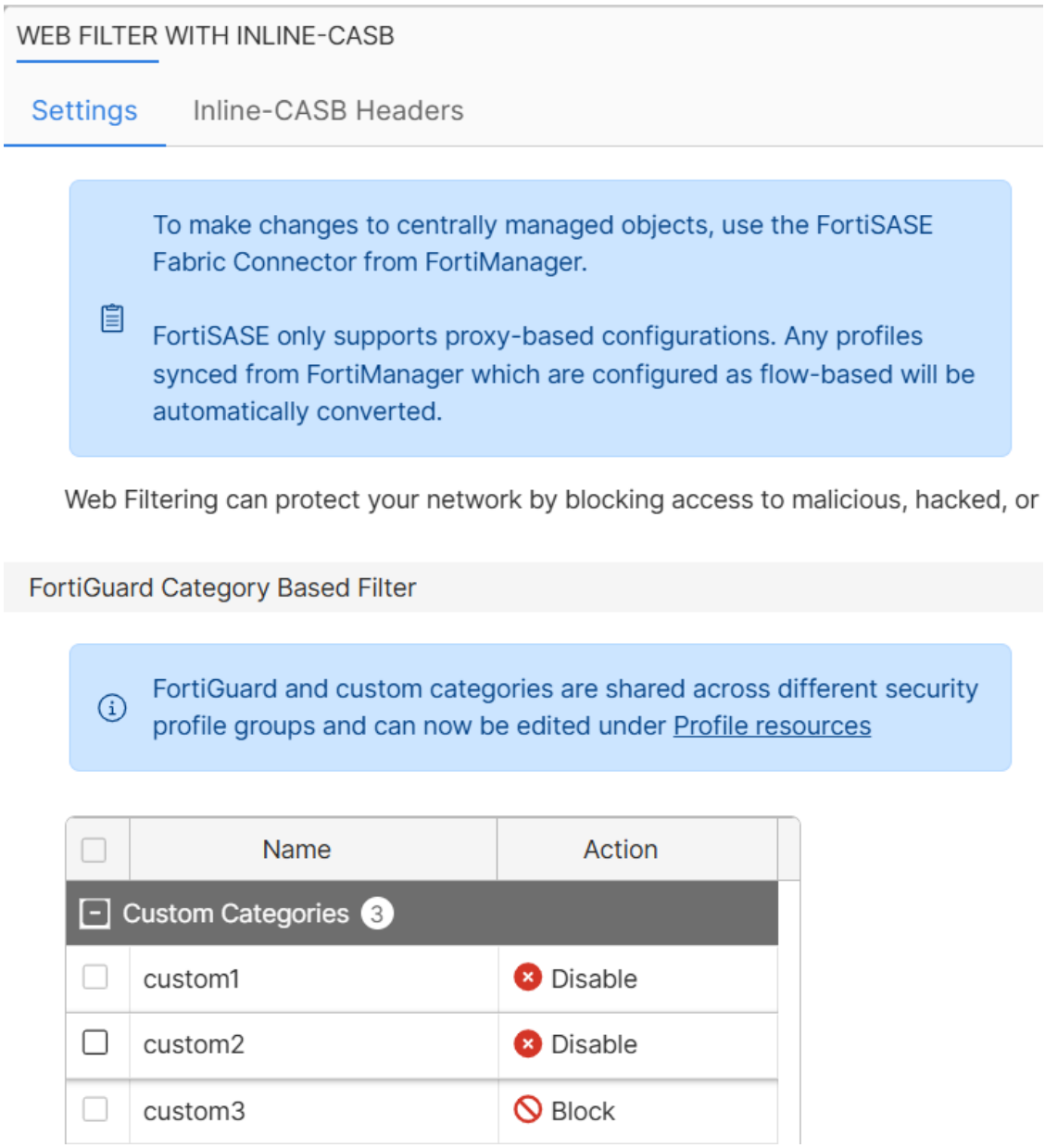
e. Click *OK*.

2. Create a Web Filter:
   a. Go to *Policy & Objects* > *Security Profiles* > *Web Filter*.
   b. Click *Create New*.
   c. In *Create New Web Filter*, in the *Name* field, enter custom-profile.
   d. For *Feature Set*, select *Proxy-based*.
   e. Enable *FortiGuard Category Based Filter*.
   f. Under *Local Categories*, select *custom3* and click *Block*.
   g. Click *OK*. Fill in the change note and click *OK*.
3. Create a firewall profile group:
   a. Go to *Policy & Objects* > *Advanced* > *CLI Configurations*.
   b. Enter profile-group in the search bar to discover results matching that keyword.
   c. Expand the *firewall* result in the tree menu, and select the *profile-group* menu item.
   d. In *firewall profile-group*, click *Create New*.
   e. In the *name* field, enter custom-profile-group.
   f. For *profile-protocol-options*, select *default*.
   g. For *ssl-ssh-profile*, select *deep-inspection*.
   h. For *webfilter-profile*, select *custom-profile*.

i. Click *OK*.



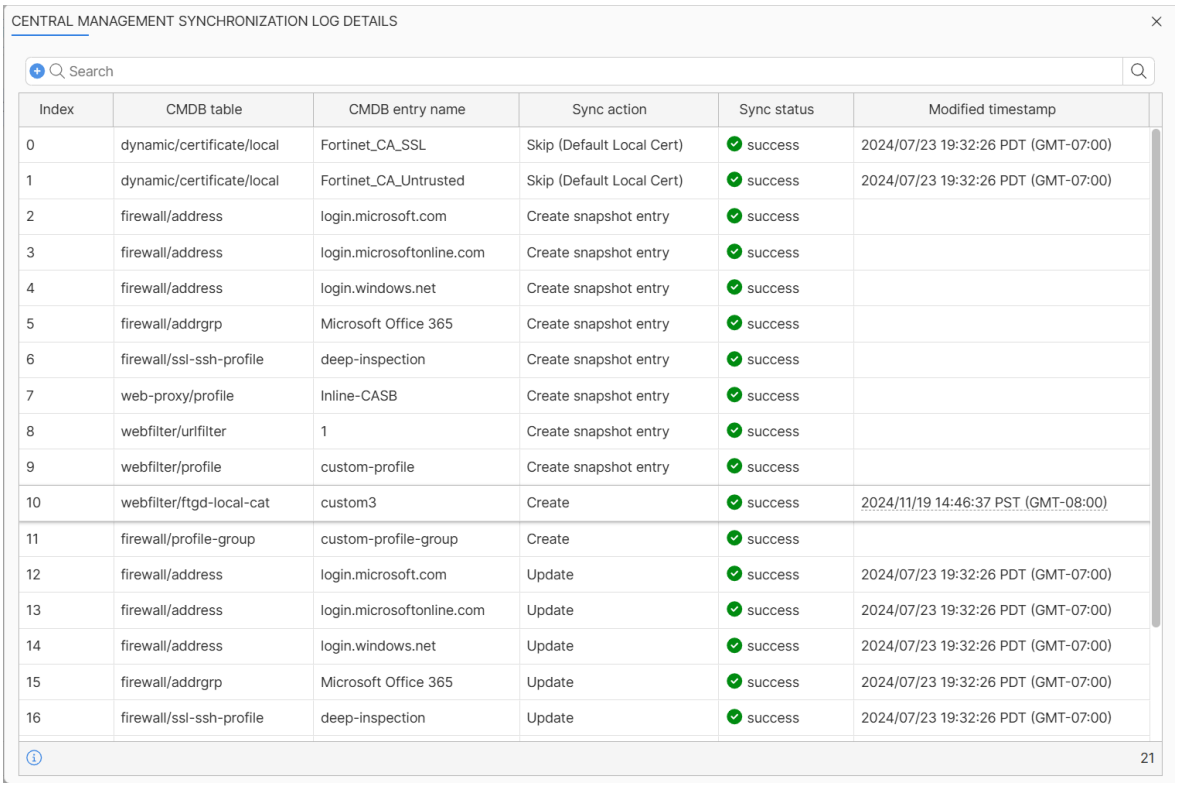
4. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the *custom-profile-group* security profile group from FortiManager to FortiSASE.
5. In FortiSASE, verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *Traffic* > *Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In *Web Filter With Inline-CASB*, click *View*.
      iii. In *FortiGuard Category Based Filter*, confirm the newly created custom3 custom category is set to *Block*.



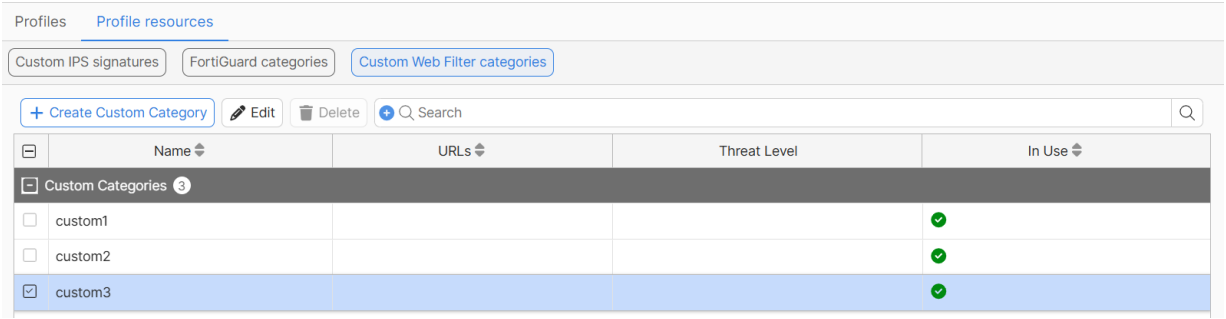
b. Go to *Operations* > *Logs* > *Central management synchronizations* and do the following:

i. Select the most recent log entry and click *View log details*.

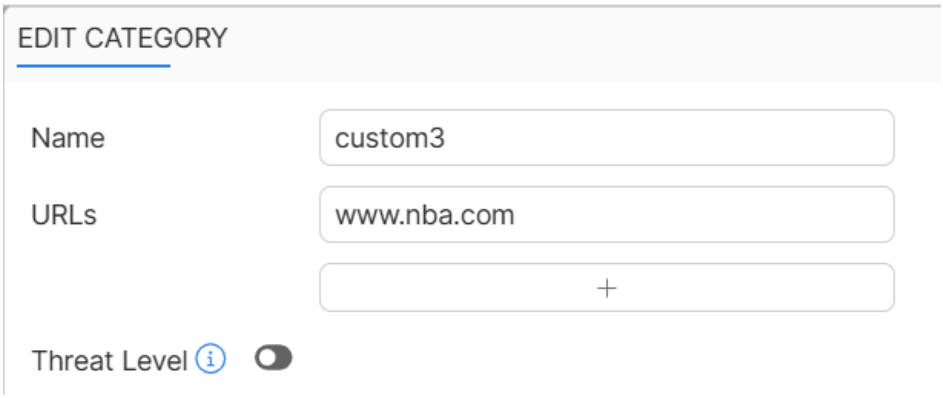
ii. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



6. Note that custom category custom3 is still empty at this point. Therefore, you will need to add web sites to custom3:
   a. Go to *Security* > *Traffic* > *Security profiles*.
   b. At the top of the page, click the *Profile resources* tab and click the *Custom Web Filter categories* subtab.
   c. In *Custom Categories*, select the *custom3* category and click *Edit*.

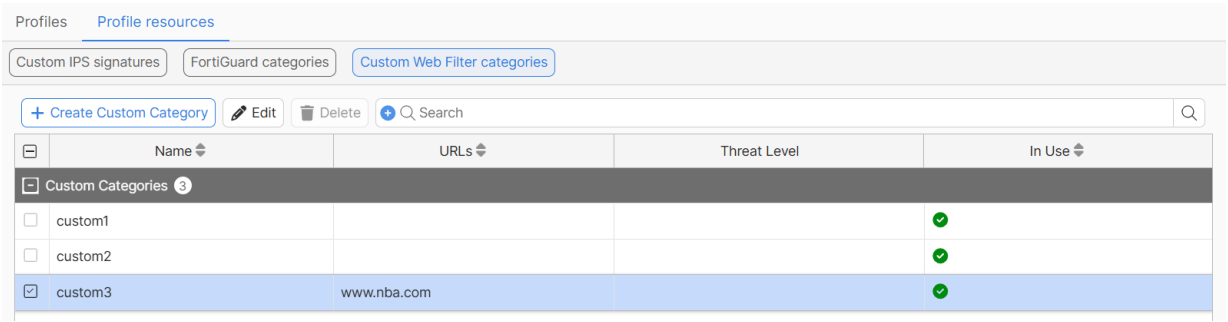


d. Add URLs by clicking + and entering the URLs without a protocol. For example, enter www.nba.com.



e. Click *OK*.

f. Observe the URLs added for the custom3 category.



Configuring external feeds with Web Filter and DNS Filter profiles

FortiSASE supports synchronization of external feeds referenced in Web Filter and DNS Filter profiles.

This example covers the following use cases:

- Configuring an FQDN feed referenced in a Web Filter
- Configuring a domains feed referenced in a DNS Filter
- Configuring an external hosts feed referenced in a DNS Filter

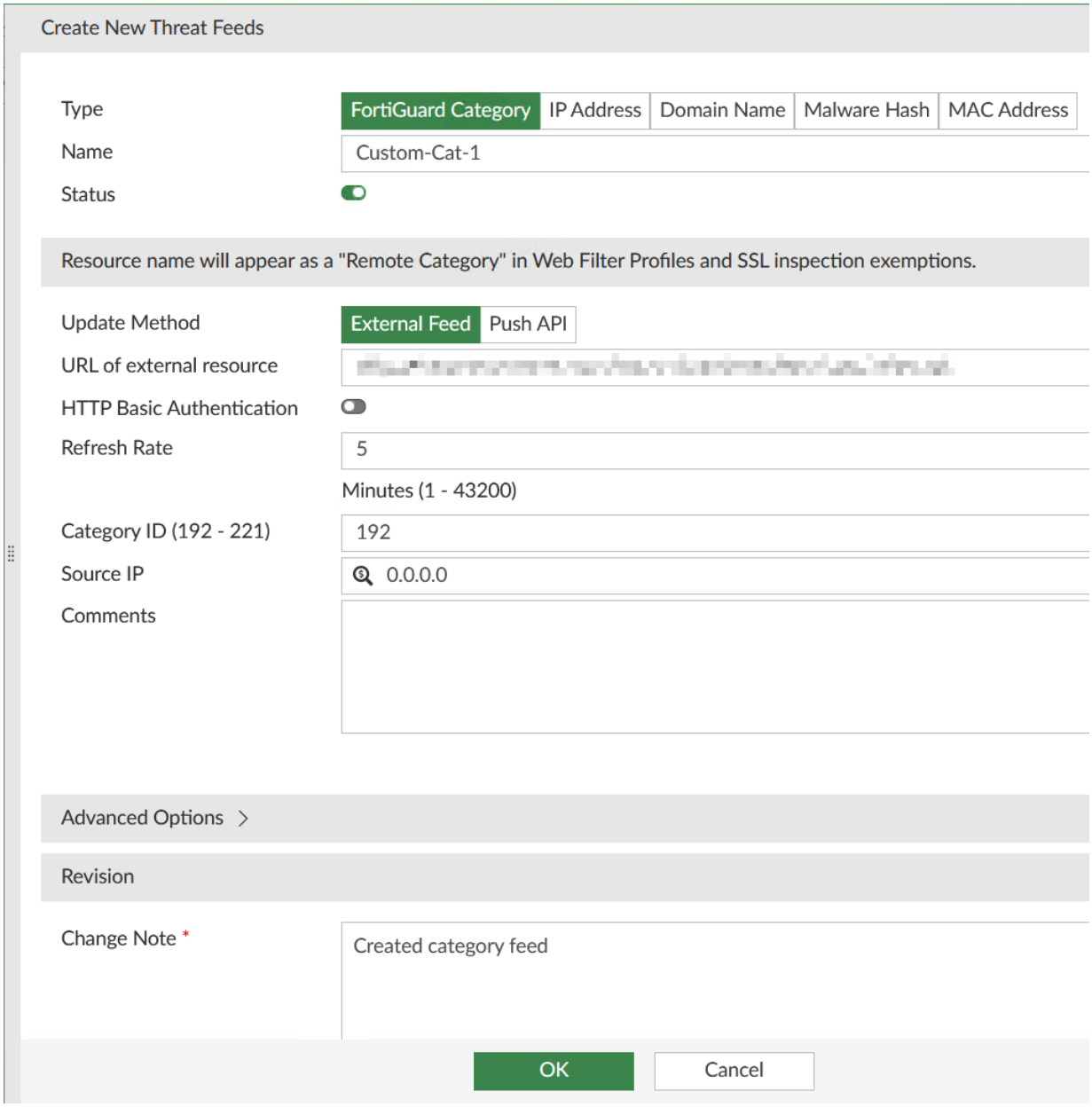
To configure an FQDN feed referenced in a Web Filter:

1. Go to *Policy & Objects* > *Security Fabric* > *Threat Feeds*.
   a. Click *Create New*.
   b. In *Create New Threat Feeds*, configure these settings and keep all other default settings:

Option	Value
Type	*FortiGuard Category*
Name	Custom-Cat-1
URL of external resource	<URL of external feed>
Category ID	192

Option	Value
Change Note	Created category feed

c. Click *OK*.



2. Go to *Policy & Objects* > *Security Profiles* > *Web Filter*.

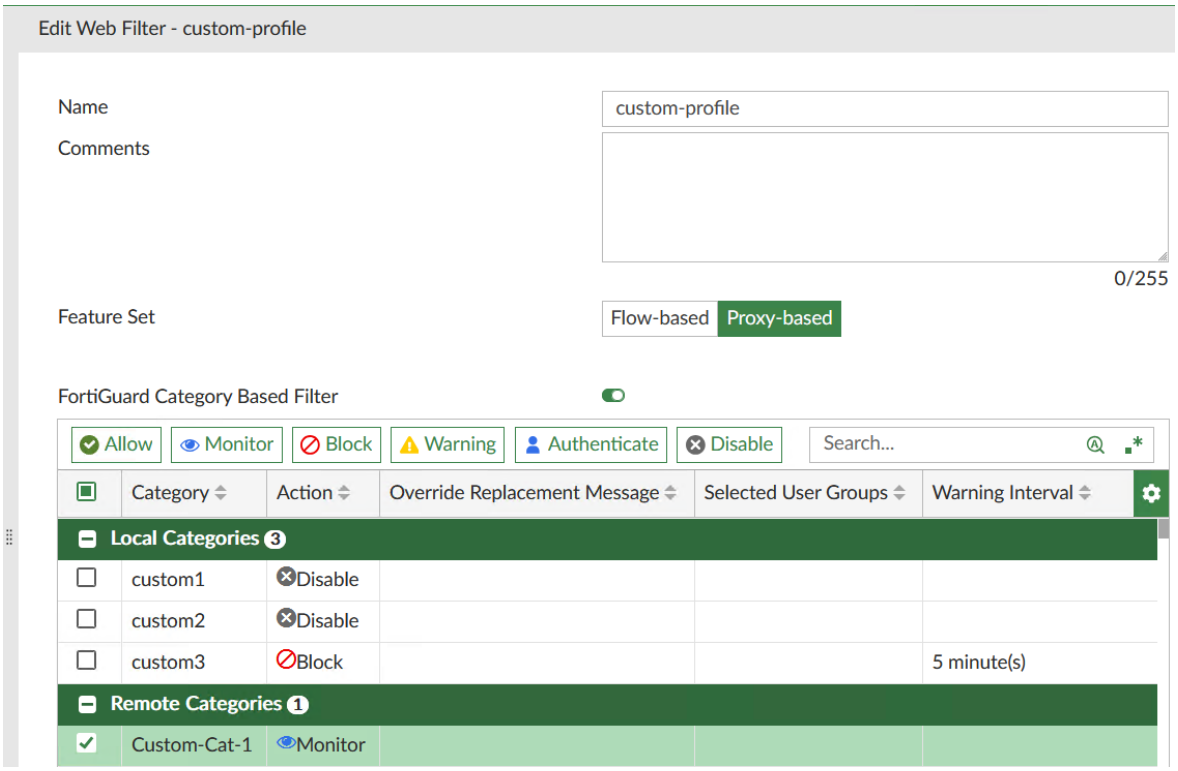
a. Click *Create New*.

b. In *Create New Web Filter*, configure the following:

i. In the *Name* field, enter custom-profile.

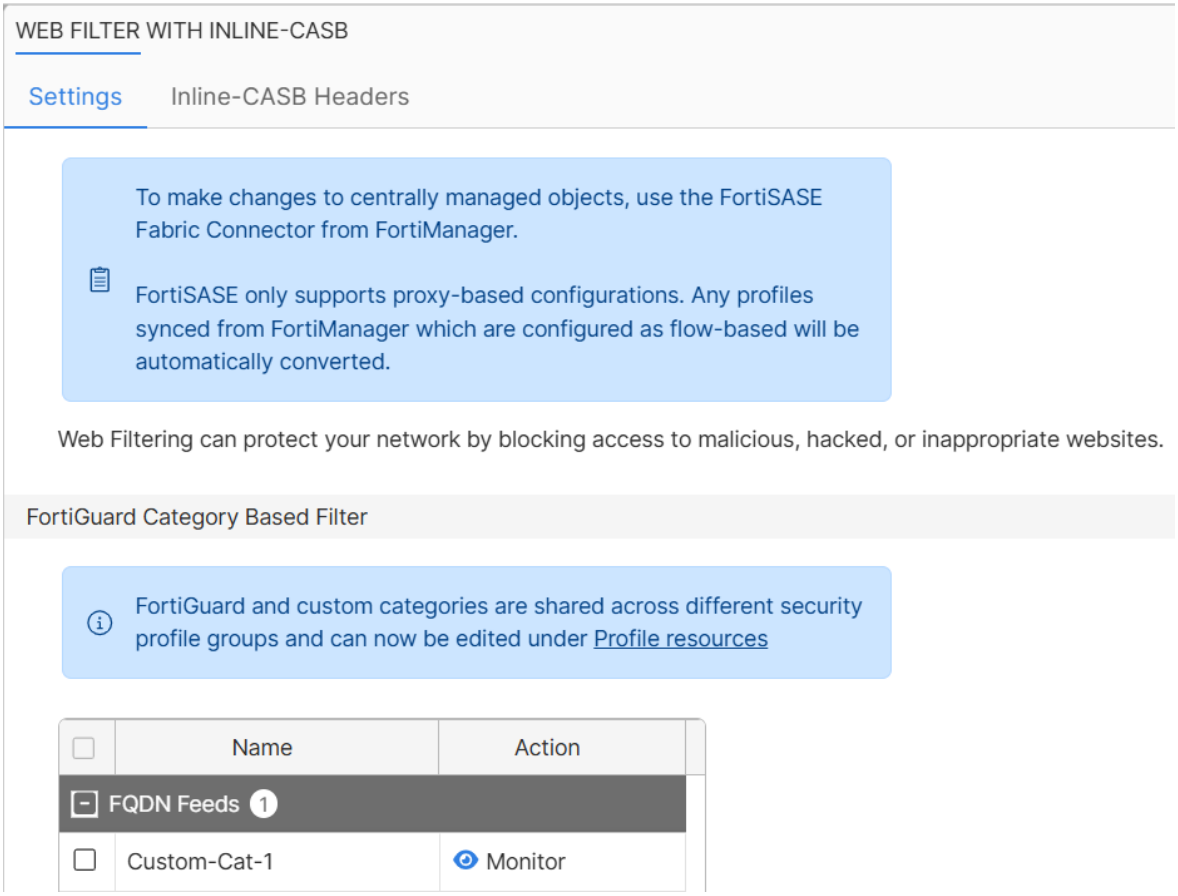
ii. For *Feature Set*, select *Proxy-based*.

iii. In *FortiGuard Category Based Filter*, under *Remote Categories* right-click the custom category corresponding to the external feed, Custom-Cat-1, and change the action from *Disable* to *Monitor*.



iv. Click *OK*. Fill in the change note and click *OK*.

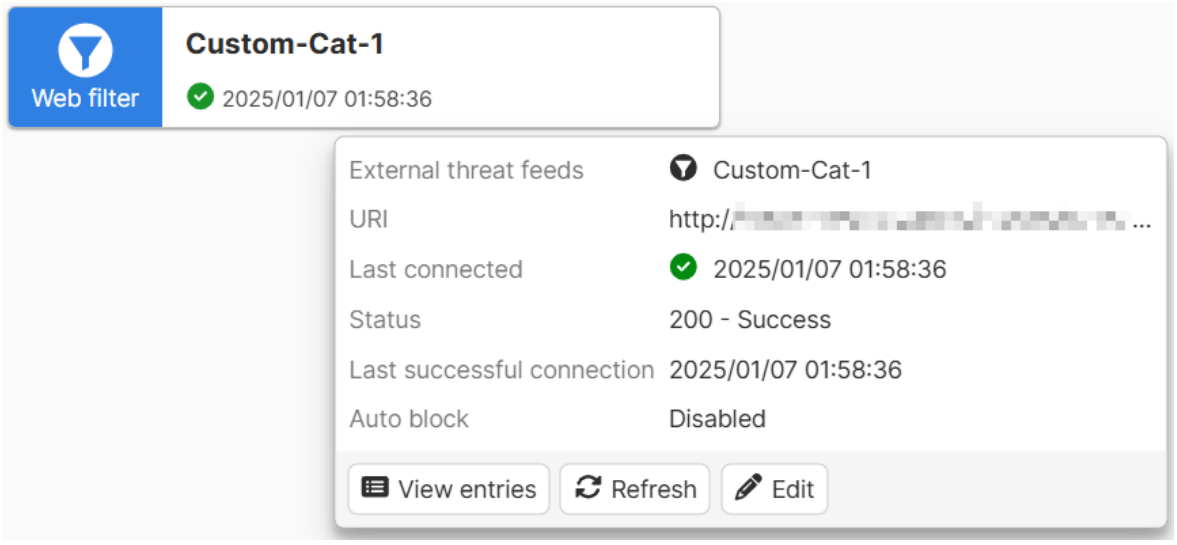
3. Go to *Policy & Objects* > *Security Profiles* > *Profile Group*.
   a. Click *Create New*.
   b. In the *Name* field, enter custom-profile-group.
   c. For *Web Filter Profile*, select *custom-profile*.
   d. For *SSL/SSH Inspection*, select *deep-inspection*.
   e. For *Protocol Options*, select *default*.
   f. Click *OK*. Fill in the change note and click *OK*.
4. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the custom-profile-group Security Profile Group from FortiManager to FortiSASE.
5. In FortiSASE verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *Traffic* > *Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In *Web Filter With Inline-CASB*, click *View*.
      iii. In the *Settings* tab, in *FortiGuard Category Based Filter* under *FQDN Feeds* observe *Custom-Cat-1* is configured with an action of *Monitor*.



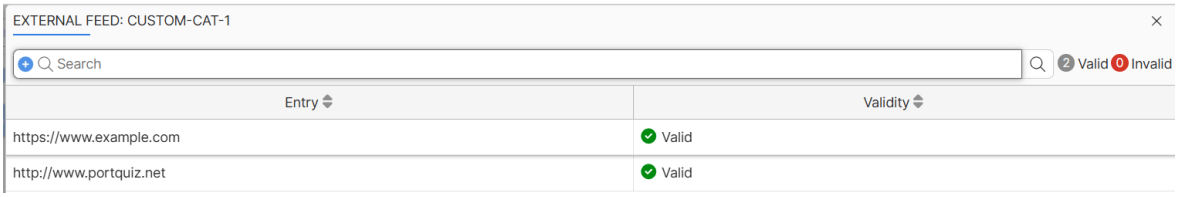
b. Go to *Security* > *External feeds*:

i. Observe the card for the *Custom-Cat-1* external feed.

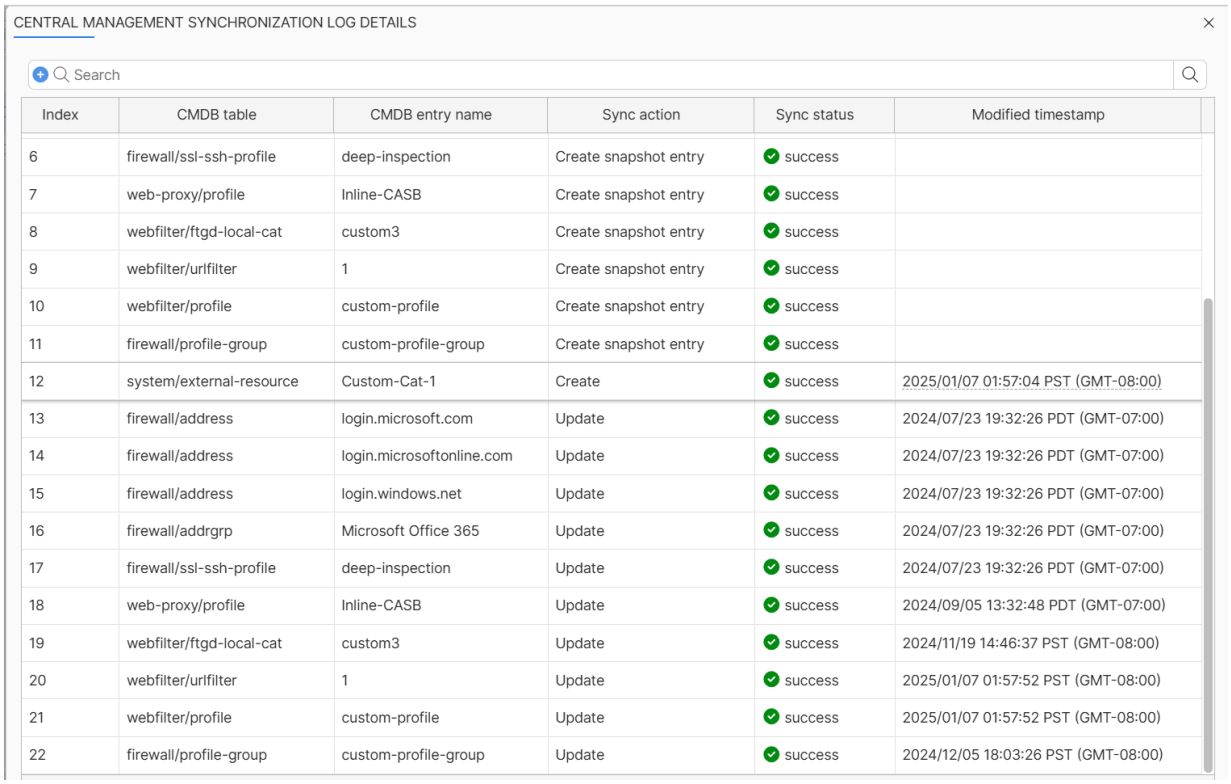
ii. Hover over the card to view details.



iii. Click on *View entries* to view the FQDNs included in the external feed.



6. Go to *Operations > Logs > Central management synchronizations* and do the following:
   a. Select the most recent log entry and click *View log details*.
   b. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



Index	CMDB table	CMDB entry name	Sync action	Sync status	Modified timestamp
6	firewall/ssl-ssh-profile	deep-inspection	Create snapshot entry	success	
7	web-proxy/profile	Inline-CASB	Create snapshot entry	success	
8	webfilter/ftgd-local-cat	custom3	Create snapshot entry	success	
9	webfilter/urlfilter	1	Create snapshot entry	success	
10	webfilter/profile	custom-profile	Create snapshot entry	success	
11	firewall/profile-group	custom-profile-group	Create snapshot entry	success	
12	system/external-resource	Custom-Cat-1	Create	success	2025/01/07 01:57:04 PST (GMT-08:00)
13	firewall/address	login.microsoft.com	Update	success	2024/07/23 19:32:26 PDT (GMT-07:00)
14	firewall/address	login.microsoftonline.com	Update	success	2024/07/23 19:32:26 PDT (GMT-07:00)
15	firewall/address	login.windows.net	Update	success	2024/07/23 19:32:26 PDT (GMT-07:00)
16	firewall/addrgrp	Microsoft Office 365	Update	success	2024/07/23 19:32:26 PDT (GMT-07:00)
17	firewall/ssl-ssh-profile	deep-inspection	Update	success	2024/07/23 19:32:26 PDT (GMT-07:00)
18	web-proxy/profile	Inline-CASB	Update	success	2024/09/05 13:32:48 PDT (GMT-07:00)
19	webfilter/ftgd-local-cat	custom3	Update	success	2024/11/19 14:46:37 PST (GMT-08:00)
20	webfilter/urlfilter	1	Update	success	2025/01/07 01:57:52 PST (GMT-08:00)
21	webfilter/profile	custom-profile	Update	success	2025/01/07 01:57:52 PST (GMT-08:00)
22	firewall/profile-group	custom-profile-group	Update	success	2024/12/05 18:03:26 PST (GMT-08:00)

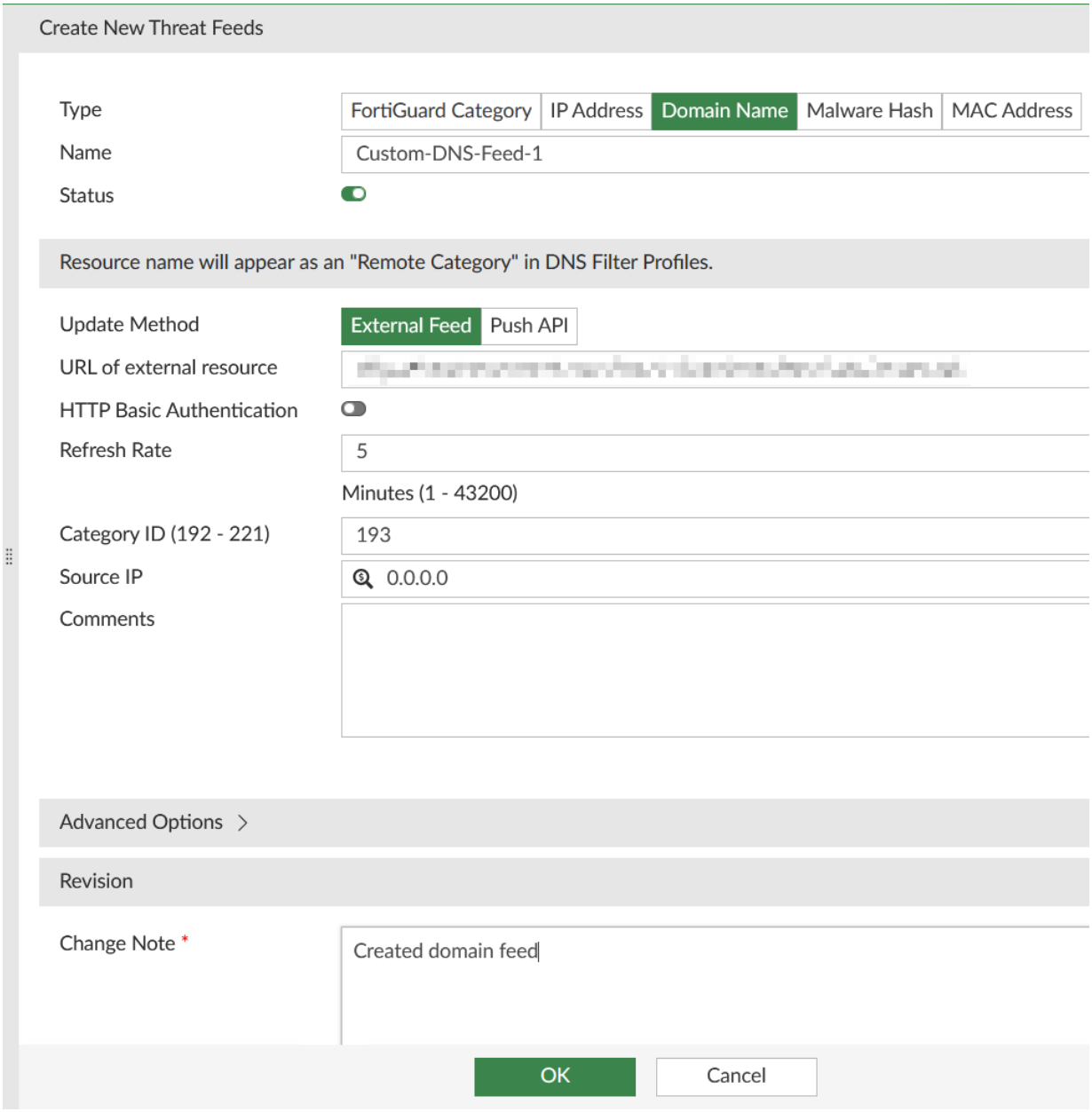
To configure a domains feed referenced in a DNS Filter:

1. Go to *Policy & Objects > Security Fabric > Threat Feeds*.
   a. Click *Create New*.
   b. In *Create New Threat Feeds*, configure these settings and keep all other default settings:

Option	Value
Type	*Domain Name*
Name	Custom-DNS-Feed-1
URL of external resource	<URL of external feed>
Category ID	193

Option	Value
Change Note	Created domain feed

c. Click *OK*.



2. Go to *Policy & Objects > Security Profiles > DNS Filter*.

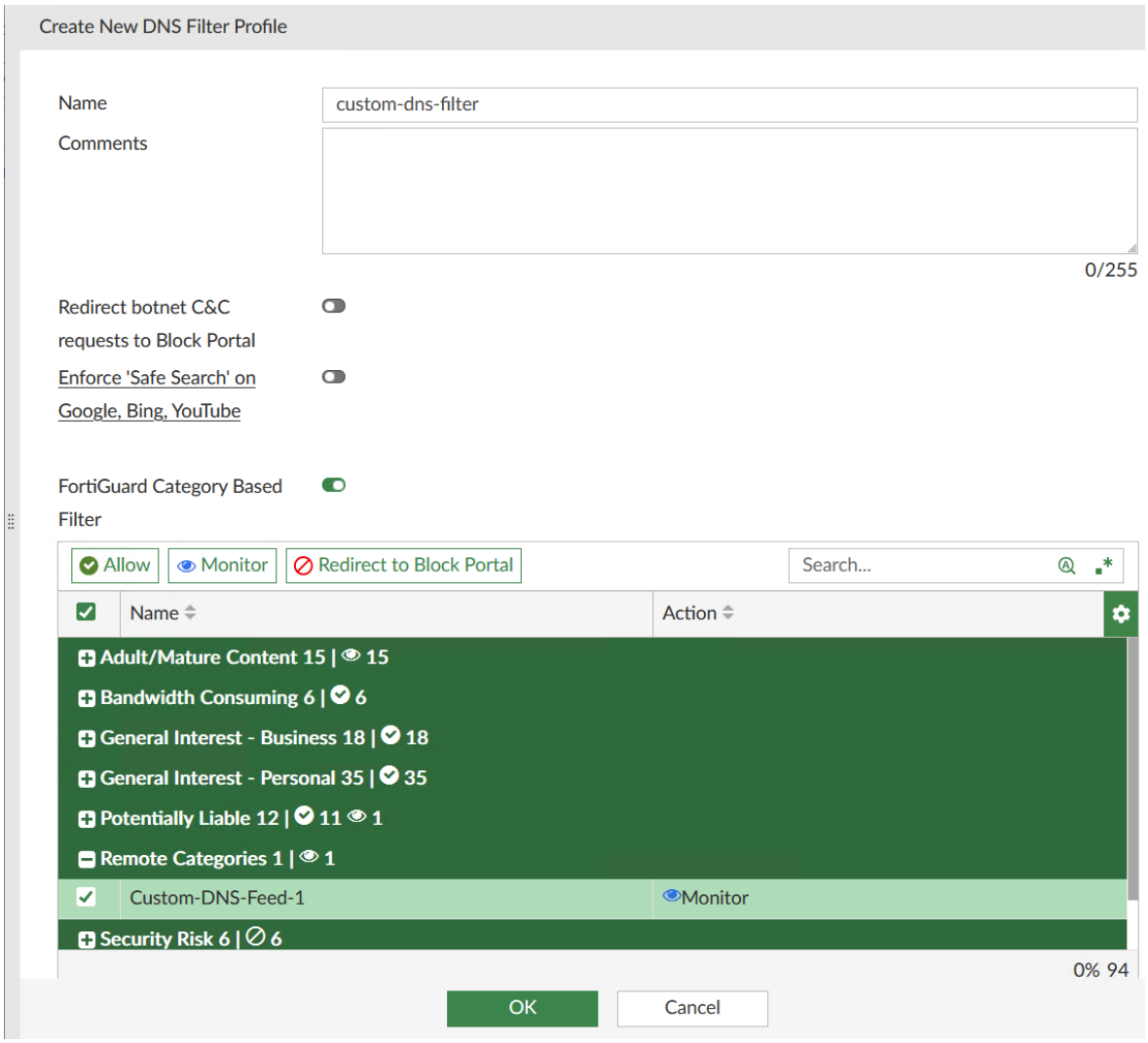
a. Click *Create New*.

b. In *Create New DNS Filter Profile*, configure the following:

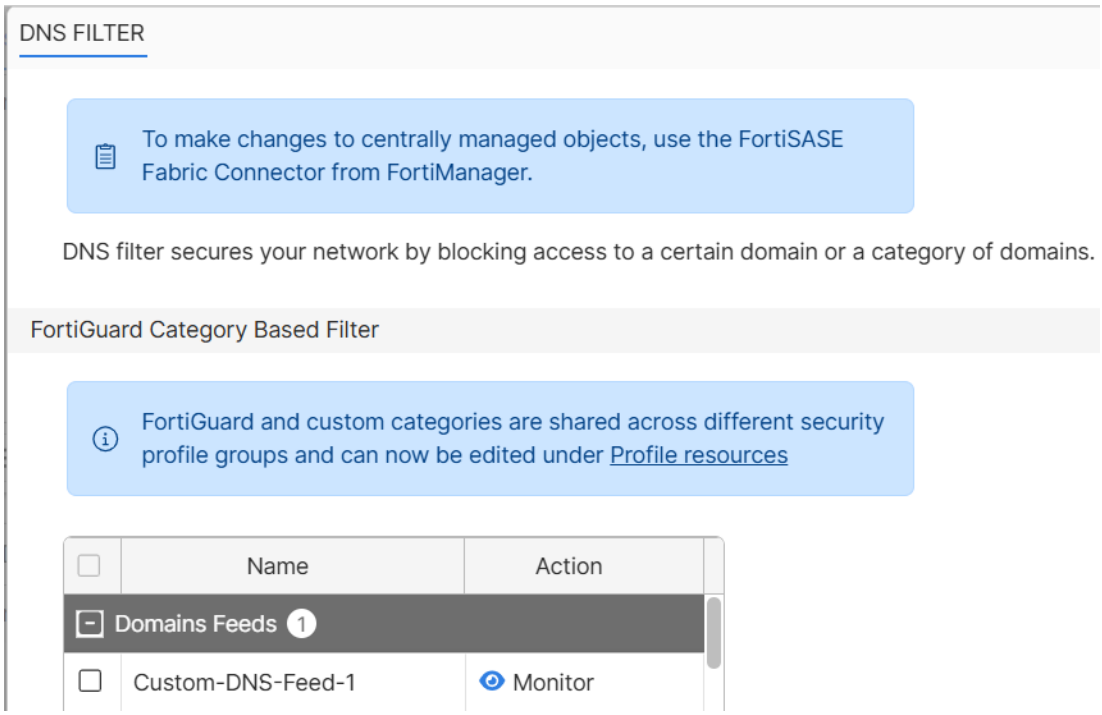
i. In the *Name* field, enter custom-dns-filter.

ii. In *FortiGuard Category Based Filter*, under *Remote Categories* right-click the custom category corresponding to the external feed, Custom-Cat-1, and change the action from *Allow* to *Monitor*.

iii. Click *OK*. Fill in the change note and click *OK*.



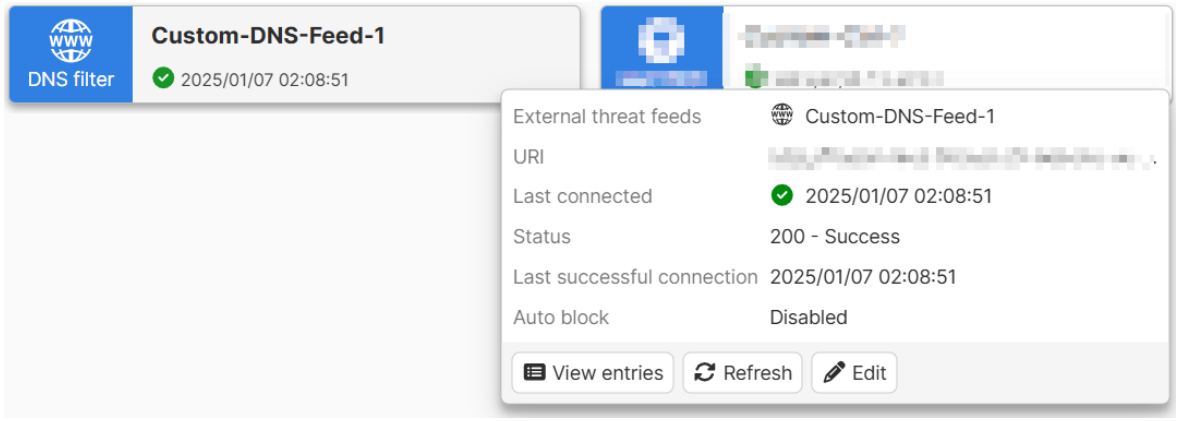
3. Go to *Policy & Objects* > *Security Profiles* > *Profile Group*.
   a. Click *Create New*.
   b. In the *Name* field, enter custom-profile-group.
   c. For *DNS Filter*, select *custom-dns-filter*.
   d. For *SSL/SSH Inspection*, select *deep-inspection*.
   e. For *Protocol Options*, select *default*.
   f. Click *OK*. Fill in the change note and click *OK*.
4. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the custom-profile-group Security Profile Group from FortiManager to FortiSASE.
5. In FortiSASE verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *Traffic* > *Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In *DNS Filter*, click *View*.
      iii. In *FortiGuard Category Based Filter* under *Domain Feeds* observe *Custom-DNS-Feed-1* is configured with an action of *Monitor*.



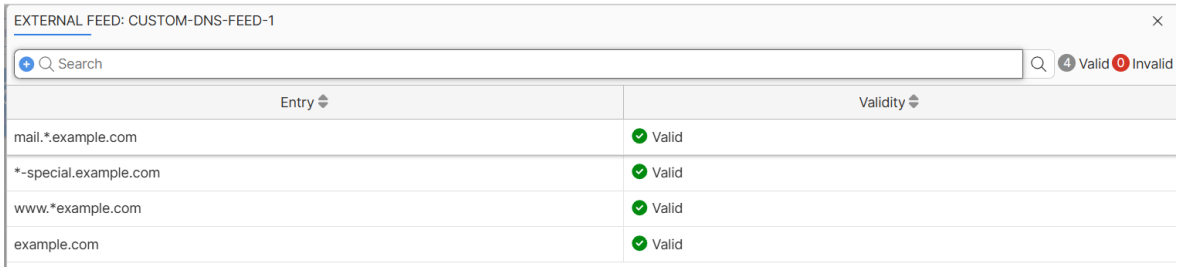
b. Go to *Security* > *External feeds*:

i. Observe the card for the *Custom-DNS-Feed-1* external feed.

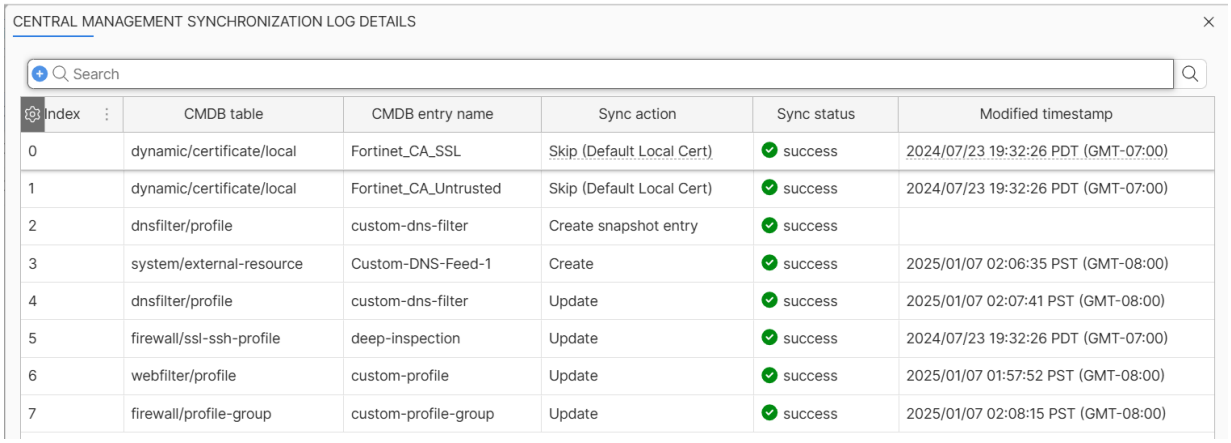
ii. Hover over the card to view details.



iii. Click on *View entries* to view the domains included in the external feed.



6. Go to *Operations* > *Logs* > *Central management synchronizations* and do the following:
   a. Select the most recent log entry and click *View log details*.
   b. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.

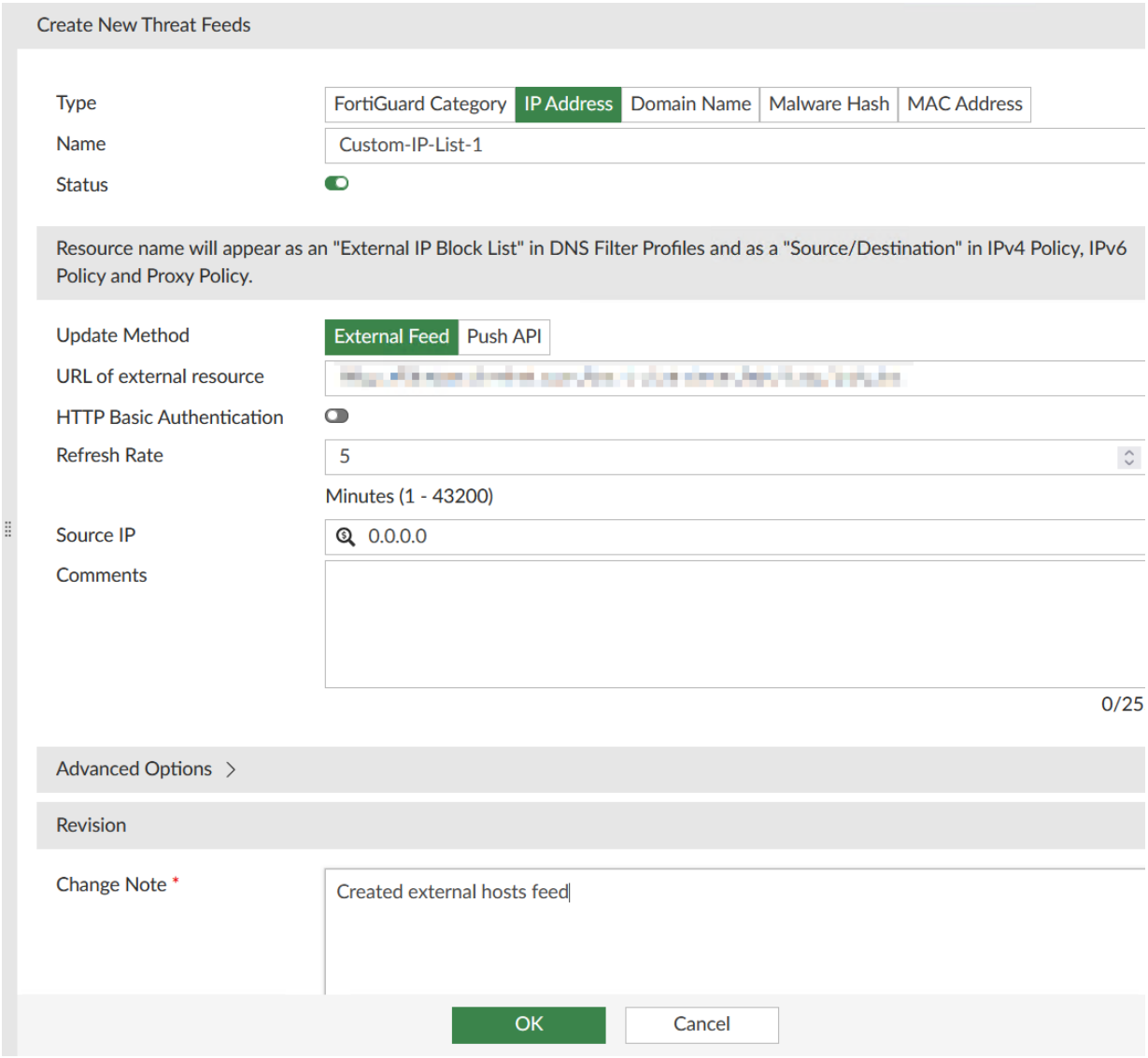


To configure an external hosts feed referenced in a DNS Filter:

1. Go to *Policy & Objects* > *Security Fabric* > *Threat Feeds*.
   a. Click *Create New*.
   b. In *Create New Threat Feeds*, configure these settings and keep all other default settings:

Option	Value
Type	*IP Address*
Name	Custom-IP-List-1
URL of external resource	<URL of external feed>
Category ID	193
Change Note	Created external hosts feed

c. Click *OK*.



2. Go to *Policy & Objects* > *Security Profiles* > *DNS Filter*.

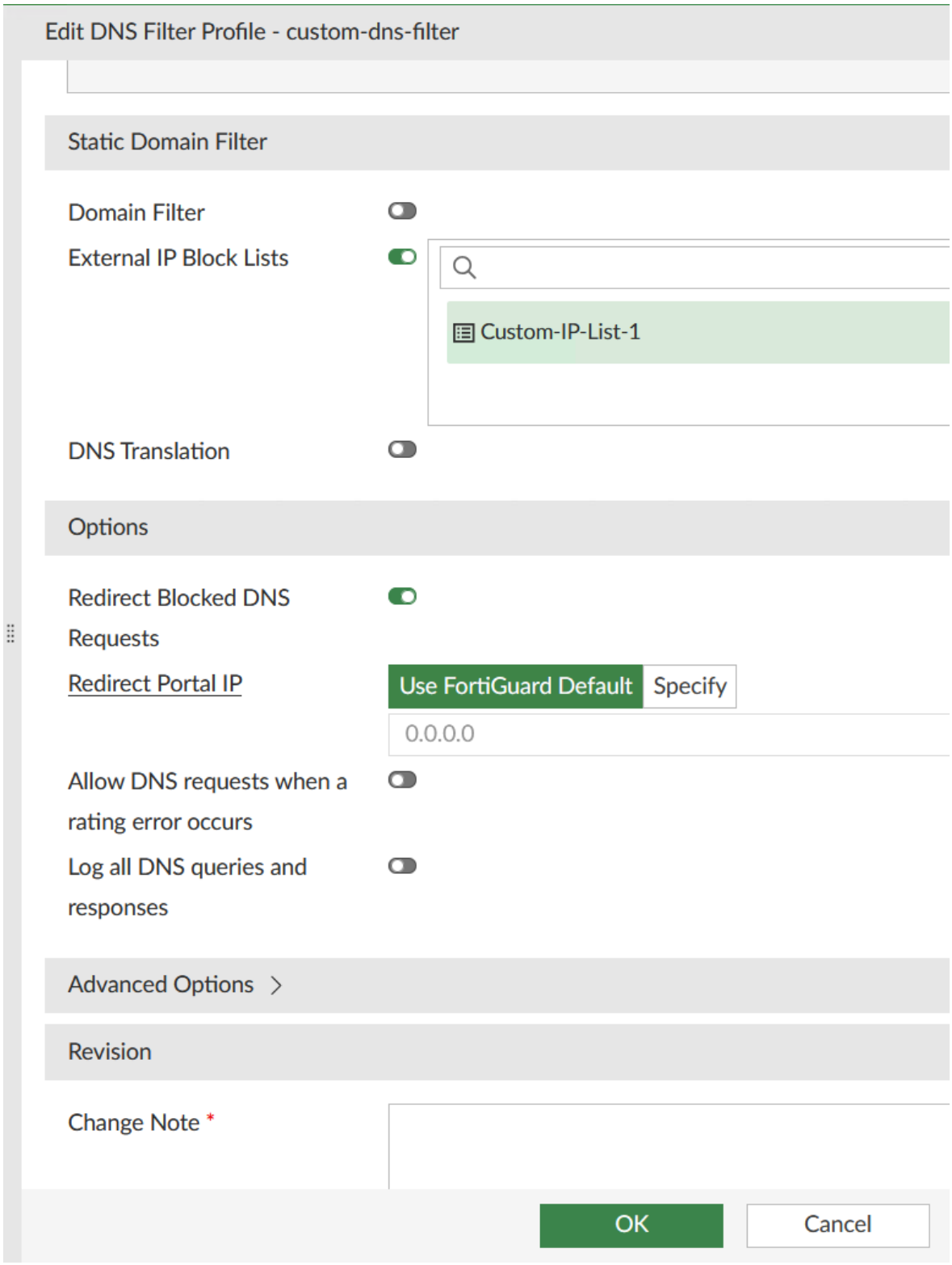
a. Click *Create New*.

b. In *Create New DNS Filter Profile*, configure the following:

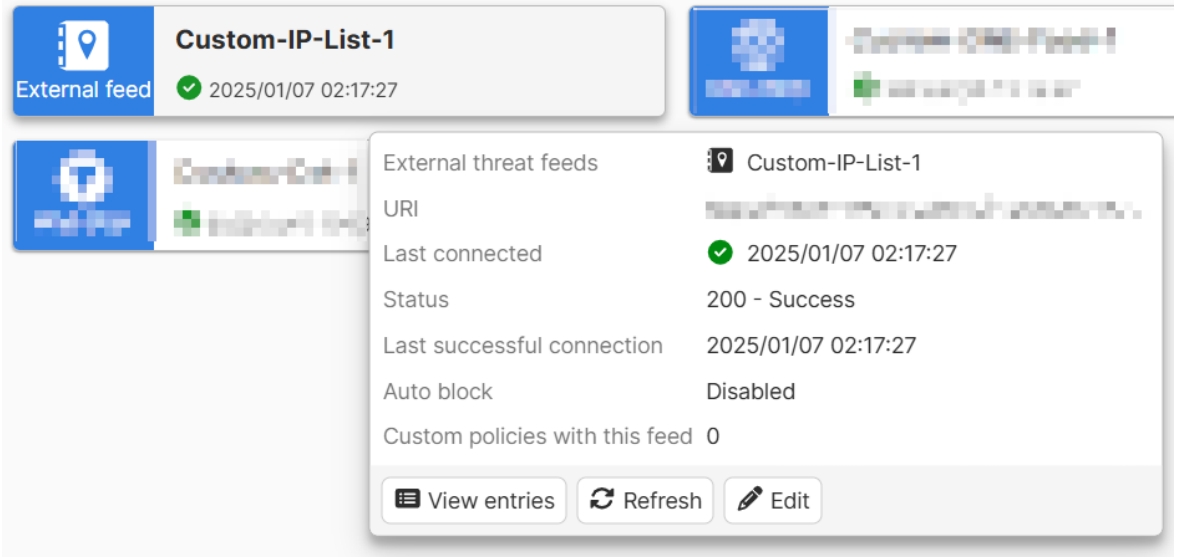
i. In the *Name* field, enter custom-dns-filter.

ii. In *Static Domain Filter*, enable *External IP Block Lists* and select the custom category corresponding to the external feed, *Custom-IP-List-1*.

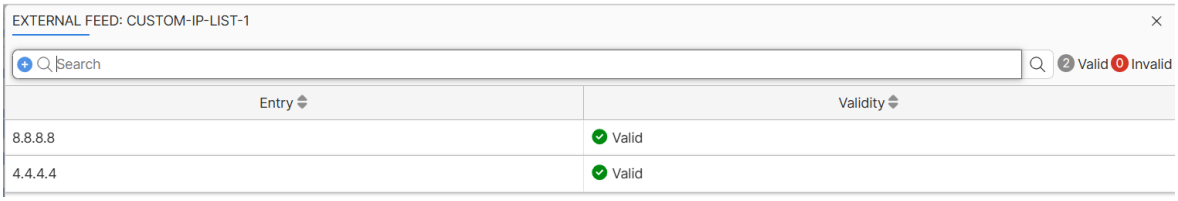
iii. Click *OK*. Fill in the change note and click *OK*.



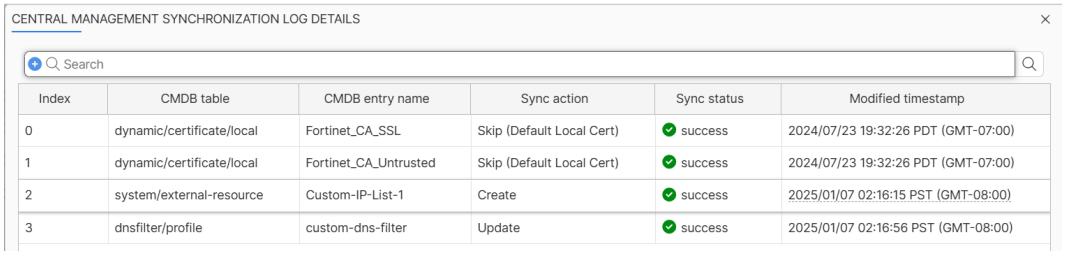
3. Go to *Policy & Objects* > *Security Profiles* > *Profile Group*.
   a. Click *Create New*.
   b. In the *Name* field, enter custom-profile-group.
   c. For *DNS Filter*, select *custom-dns-filter*.
   d. For *SSL/SSH Inspection*, select *deep-inspection*.
   e. For *Protocol Options*, select *default*.
   f. Click *OK*. Fill in the change note and click *OK*.
4. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the custom-profile-group Security Profile Group from FortiManager to FortiSASE.
5. In FortiSASE verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *External feeds*:
      i. Observe the card for the *Custom-IP-List-1* external feed.
      ii. Hover over the card to view details.



      iii. Click on *View entries* to view the domains included in the external feed.

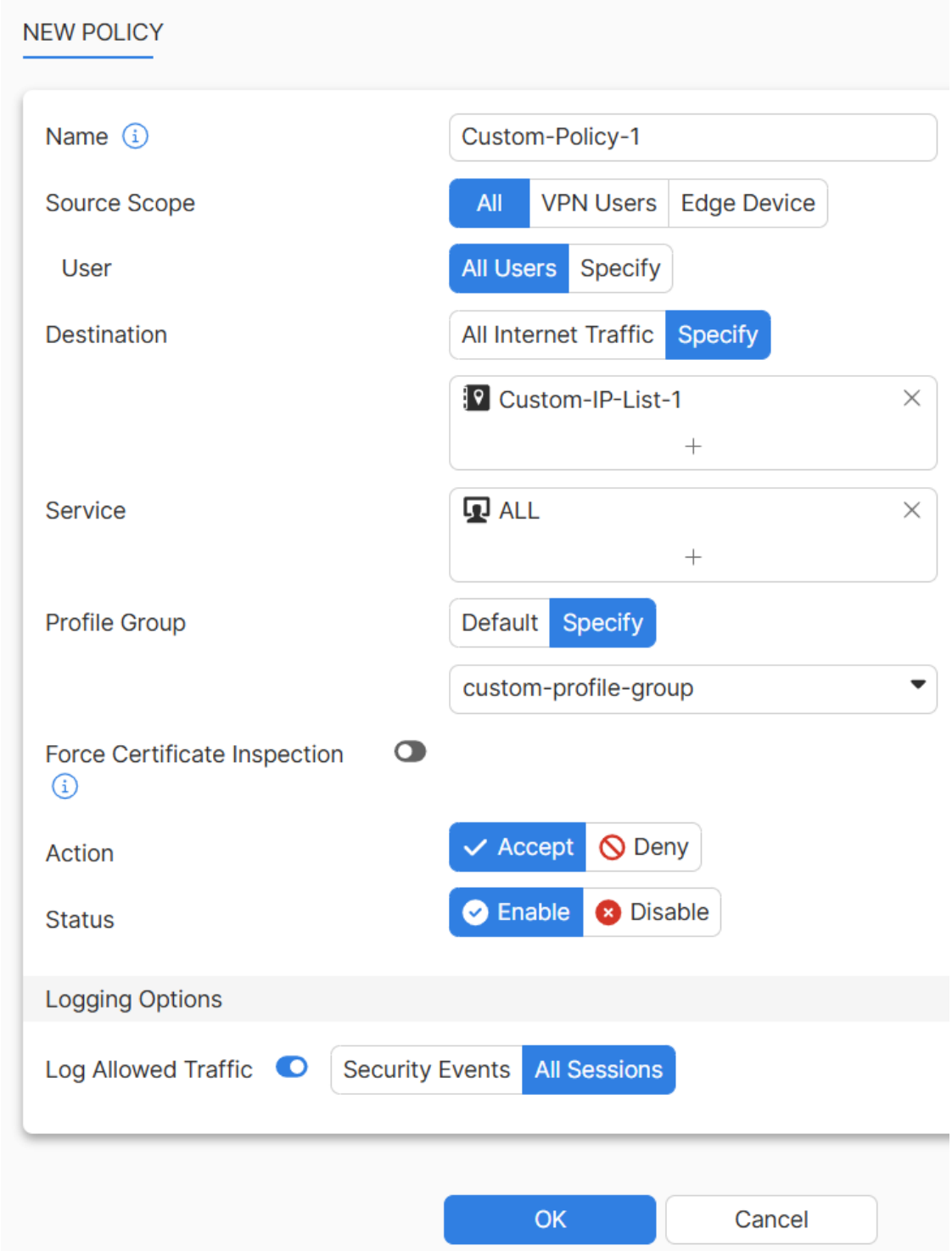


6. Go to *Operations* > *Logs* > *Central management synchronizations* and do the following:
   a. Select the most recent log entry and click *View log details*.
   b. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



7. Apply the external hosts feed synchronized from FortiManager to an Internet Access agent policy in FortiSASE:
   a. Go to *Security* > *Traffic* > *Policies*.
   b. Click *Create*.

c. In the *New Policy* page, configure the policy according to your requirements.



d. For the *Destination* field, click *Specify* and select the external hosts feed, namely, *Custom-IP-List-1*.

e. Click *OK*.

Considerations

- To display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.
- Only external feeds defined and then associated with Web Filter or DNS Filter profiles are synchronized.
- If an external feed requires HTTP basic authentication, the username and password configured in FortiManager are not synchronized. After synchronizing the external feed referenced to a Web Filter or DNS Filter profile, you must edit the external feed in FortiSASE and configure the username and password used for HTTP basic authentication.
- A maximum of 21 DNS Filter Domains and Web Filter FQDNs are supported by using the available category ID range of 201 - 221 inclusive. External hosts feeds are not included in the maximum feeds count. The following error message is observed in FortiManager if attempting to configure beyond the 21 maximum feeds:

```
system/external-resource - Failed to assign category ID for external threat feed. FortiSASE only
      supports a maximum of 21 Domain and Web Filter feeds.
```

Configuring and applying a File Filter to block password-protected files

The following example demonstrates how to configure a file filter profile to block password-protected files in FortiManager. The File Filter profile is used within a profile group and can be synchronized from FortiManager to FortiSASE.

> In FortiManager, to display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page, such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

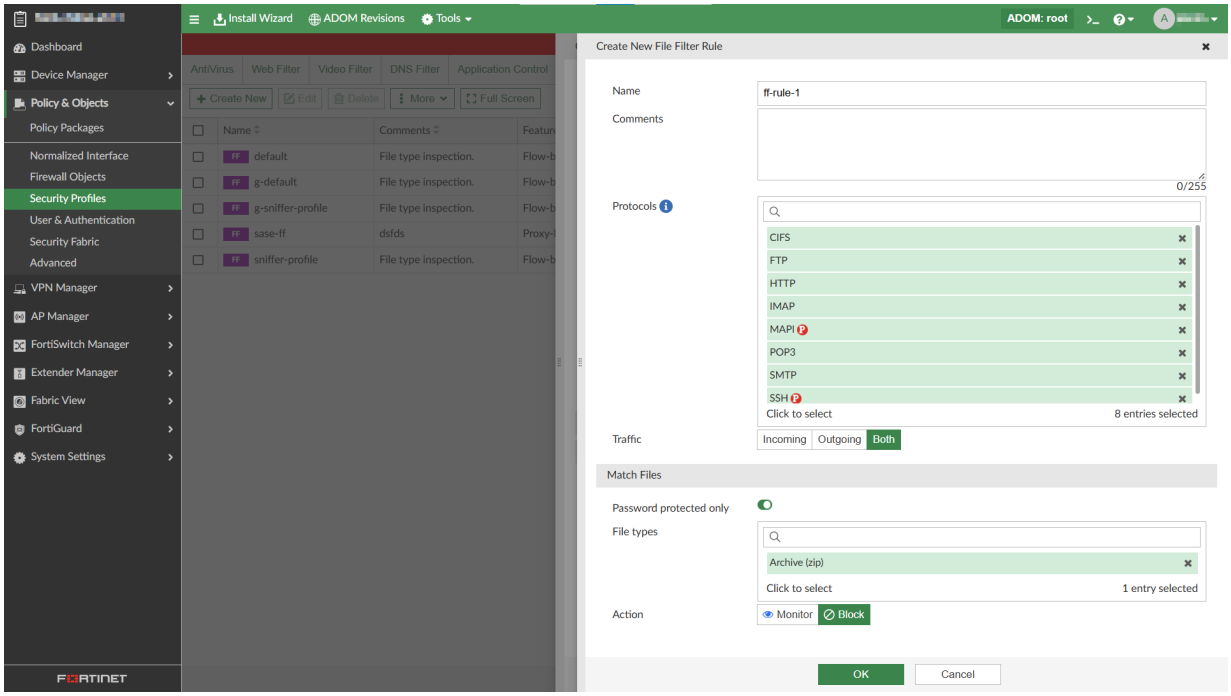
To create and apply a new File Filter profile:

1. Create a new File Filter Profile:
   a. Go to *Policy & Objects > Security Profiles > File Filter* and create a new file filter profile by clicking *Create New*.
   b. In the *Name* field, enter custom-ff-profile.
   c. In the *Feature set* field, select *Proxy-based*.
   d. In *Rules*, create a new rule for blocking password-protected ZIP files:
      i. Click *Create New*.
      ii. For *Name* field, enter ff-rule-1
      iii. For *Protocols*, all protocols are selected, by default.
      iv. In *Match Files*, configure these settings:

Field	Value	Example
Password protected only	Enable or disable inspection of password-protected file types.	Enabled

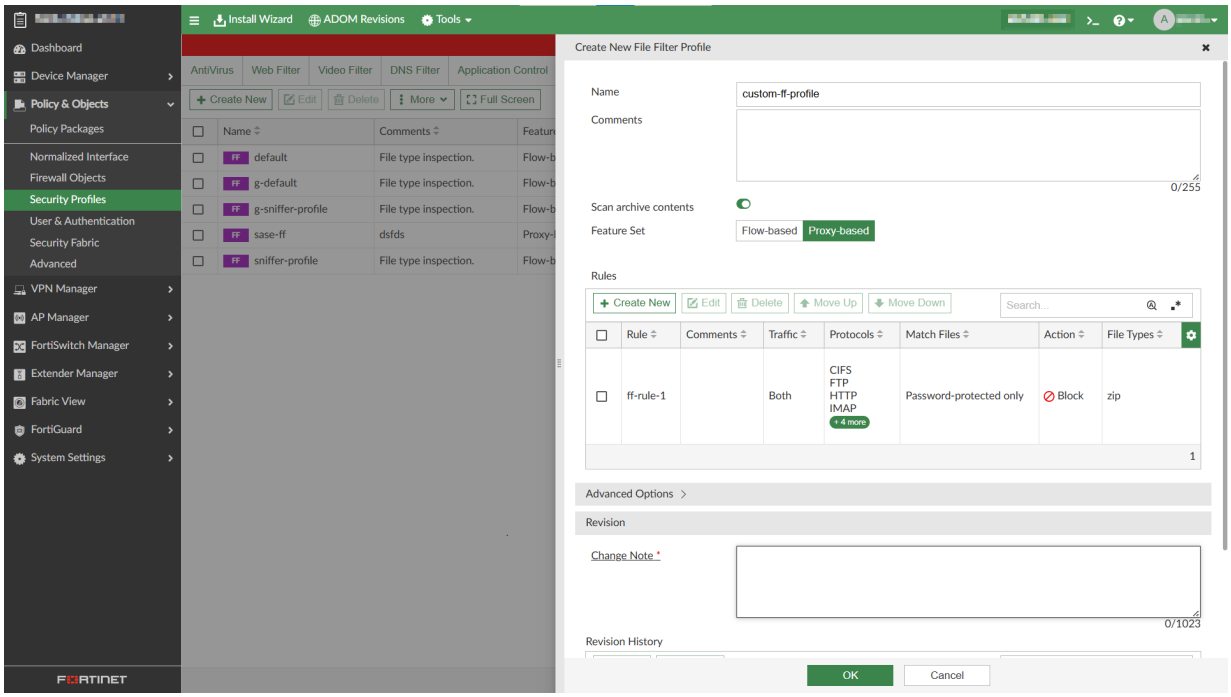
Field	Value	Example
File types	Select one or more file types to inspect.	*Archive (zip)*
Action	Action to take for file types matched. Select *Monitor* or *Block*.	*Block*

e. Observe the following settings before saving them:



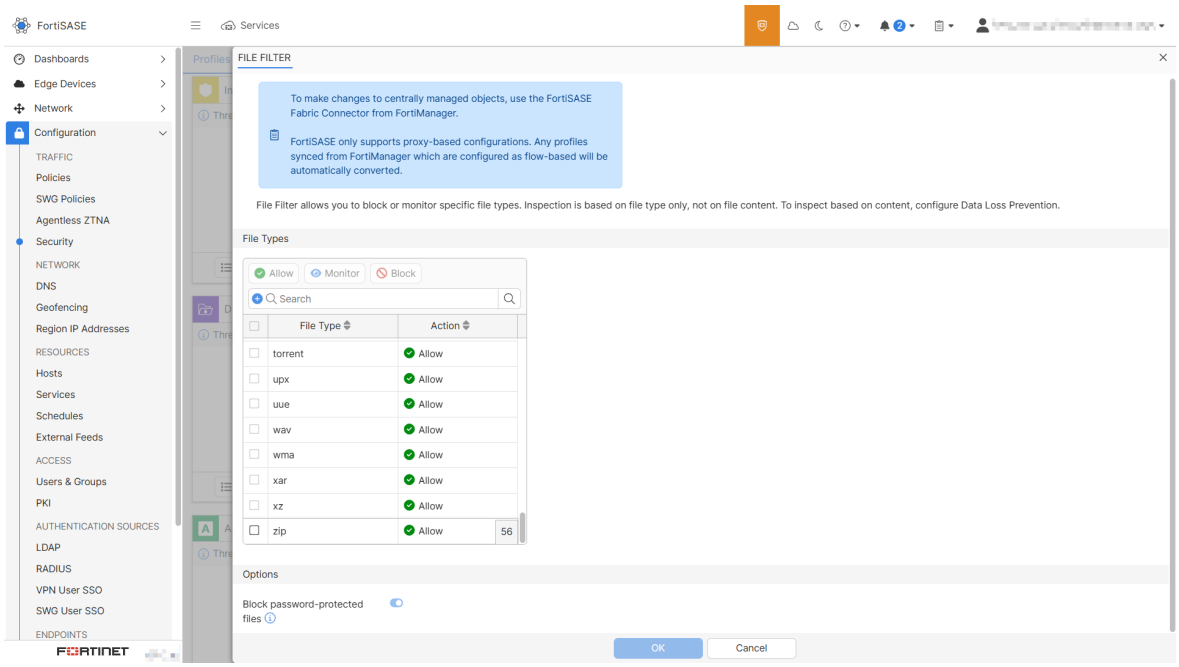
f. Click *OK*.

g. Observe the following settings before saving them:



h. Enter a suitable description in *Change Note* and click *OK*.

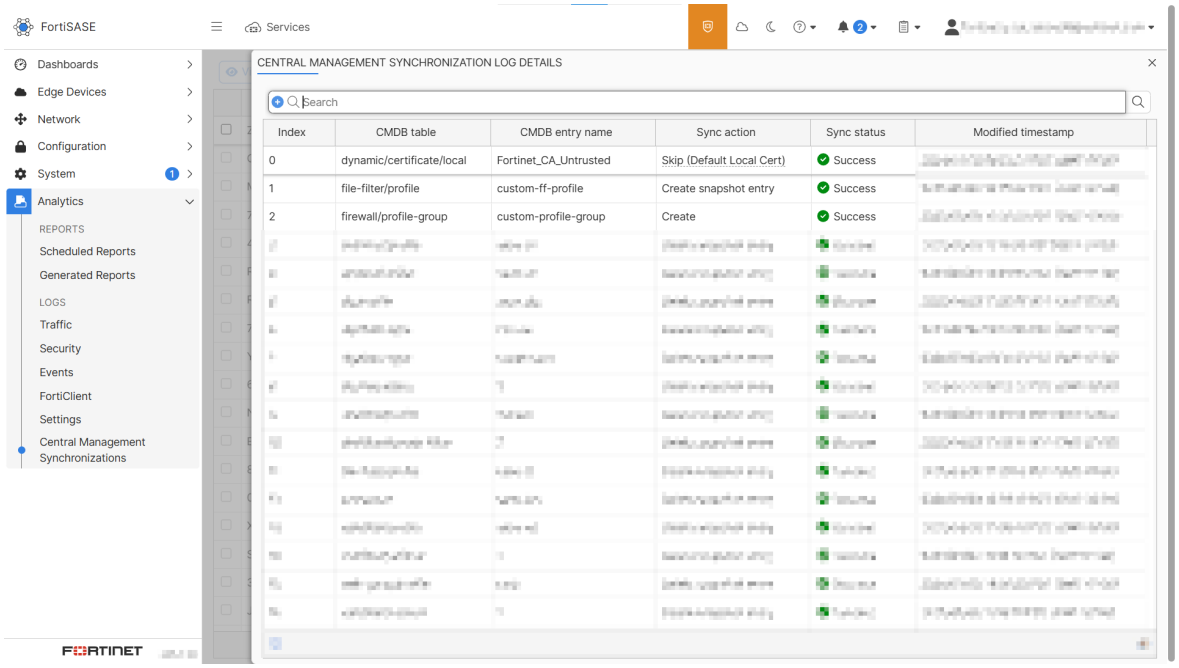
2. Apply the File Filter profile:
   a. Go to *Policy & Objects* > *Security Profiles* > *Profile Group*.
   b. Edit an existing profile group or click *Create New*.
   c. In the *name* field, enter custom-profile-group.
   d. For *File Filter Profile*, select *custom-ff-profile*.
   e. For *SSL/SSH Inspection*, select *deep-inspection*.
   f. For *Protocol Options*, select *default*.
   g. Enter a suitable description in *Change Note* and click *OK*.
3. Repeat the steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the custom-profile-group security profile group from FortiManager to FortiSASE.
4. In FortiSASE, verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *Traffic* > *Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In the *File Filter* widget, click *View*.
      iii. Observe the *Block password-protected files* configuration is synchronized to FortiSASE. When File Filter configuration is synchronized using central management, the *File Types* table only reflects the status of files that are not password-protected.



b. Go to *Operations* > *Logs* > *Central management synchronizations* and do the following:

i. Select the most recent log entry and click *View log details*.

ii. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



Configuring and applying deep/certificate inspection and performance optimization settings

The following example demonstrates how to configure a custom protocol options profile in FortiManager to block oversized compressed and uncompressed files larger than 20 and 30 MB, respectively, and to bypass sessions when FortiSASE detects an unknown content type. The protocol options profile is used within a profile group and can be synchronized from FortiManager to FortiSASE.

In FortiManager, to display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page, such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

To create and apply deep/certificate inspection and performance optimization settings:

1. In FortiManager, go to *Policy & Objects > Advanced > CLI Configurations*. Create a custom category:
   a. Enter protocol in the search bar to discover results matching that keyword.
   b. Select the *profile-protocol-options* menu item.
   c. In *firewall profile-protocol-options*, click *Create New*.
   d. In the *Name* field, enter *custom*.
   e. In the *HTTP* section, enter these settings:
      i. *options*: select *oversize*.
      ii. *oversize-limit*: 20 (modify value in MB as required between 10-64 MB)
      iii. *ports*: 80
      iv. *uncompressed-oversize-limit*: 30 (modify value in MB as required between 10-64 MB)
      v. *unknown-content-encoding*: bypass
      vi. *Change note*: < Enter a suitable note here >.
   f. Click *OK*.
2. Go to *Policy & Objects > Security Profiles > Profile Group*.
   a. Click *Create New*.
   b. In the *Name* field, enter custom-profile-group.
   c. For *SSL/SSH Inspection*, select *certificate-inspection*.
   d. For *Protocol Options*, select *custom*.
   e. Click *OK*. Fill in the change note and click *OK*.
3. Repeat the steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the custom-profile-group security profile Ggroup from FortiManager to FortiSASE.
4. In FortiSASE verify the configuration has been synchronized from FortiManager:
   a. Go to *Security > Traffic > Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In the *Profiles* tab, select *View security profile group settings*. Observe these settings have been synchronized correctly:

Field	Value
Inspection method	*Certificate inspection*
Handling unknown content types	*Allow*
Handling oversized files	*Block*
Oversized, uncompressed files are larger than	30
Oversized, compressed files are larger than	20

b. Go to *Operations > Logs > Central management synchronizations* and do the following:
  i. Select the most recent log entry and click *View log details*.
  ii. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.

Configuring and applying a Web Filter profile

The following example demonstrates how to configure a web filter profile in FortiManager. The Web Filter profile is used within a profile group and can be synchronized from FortiManager to FortiSASE.

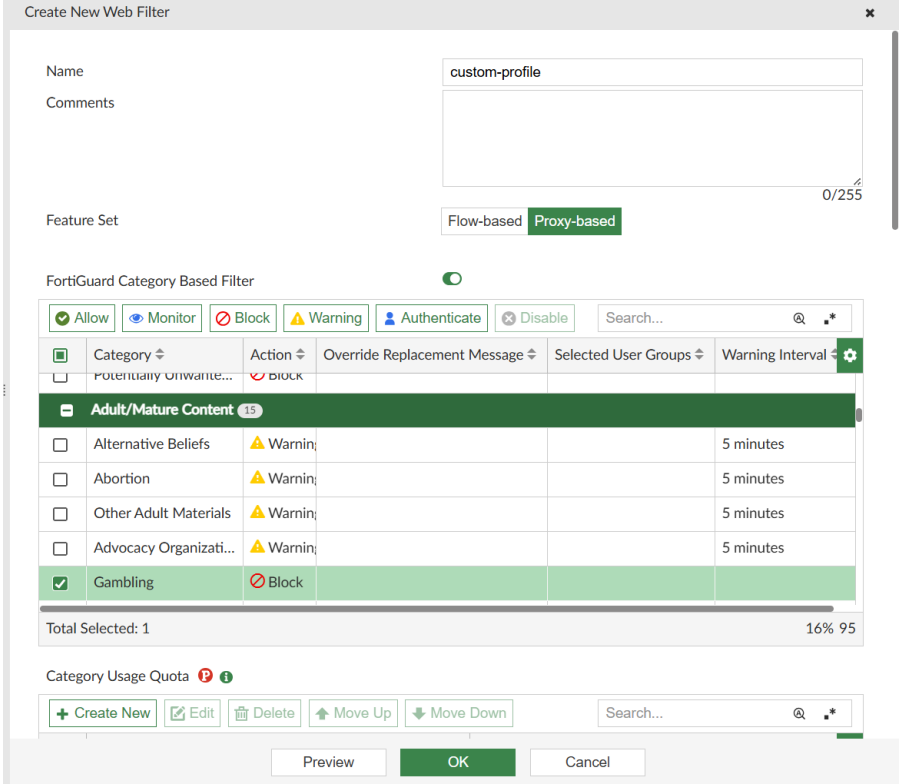
This example configures the following options:

- All supported web filter options. See Web Filter.
- Restricting web usage using FortiGuard URL categories and URL filter on page 356
- Restricting web usage using content filter on page 358

In FortiManager, to display some security profiles or advanced CLI configurations, from within any *Policy & Objects* page, such as *Policy & Objects > Security Profiles* or *Policy & Objects > Advanced*, you must click *Tools > Feature Visibility* and ensure the desired security features are enabled. See Feature visibility.

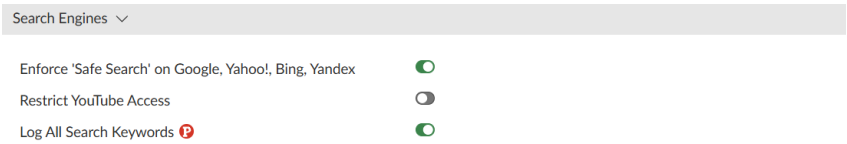
To create and apply a new Web Filter profile:

1. Create a Web Filter:
   a. Go to *Policy & Objects > Security Profiles > Web Filter*.
   b. Click *Create New*.
   c. In *Create New Web Filter*, in the *Name* field, enter `custom-profile`.
   d. For *Feature Set*, select *Proxy-based*.
   e. Enable *FortiGuard Category Based Filter*. Under *Adult/Mature Content*, set *Gambling* to *Block*.



f. Under *Search Engines*, enable these options:

- *Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex*
- *Log All Search Keywords*



g. Under *Static URL Filter*, enable these options:

- *Block invalid URLs*
- *URL Filter*
- *Web Content Filter*

h. Under *Select an URL filter*, click *+* to create a URL filter with entries and once created select it:

i. In the *Name* field, enter `url-filter-1`.

ii. Under *Web URL Filter Entry*, click *+Create New*, and configure the entry for **.fortinet.com* as a *Wildcard* type with *Block* action with *Status* enabled.

iii. Click *OK*.

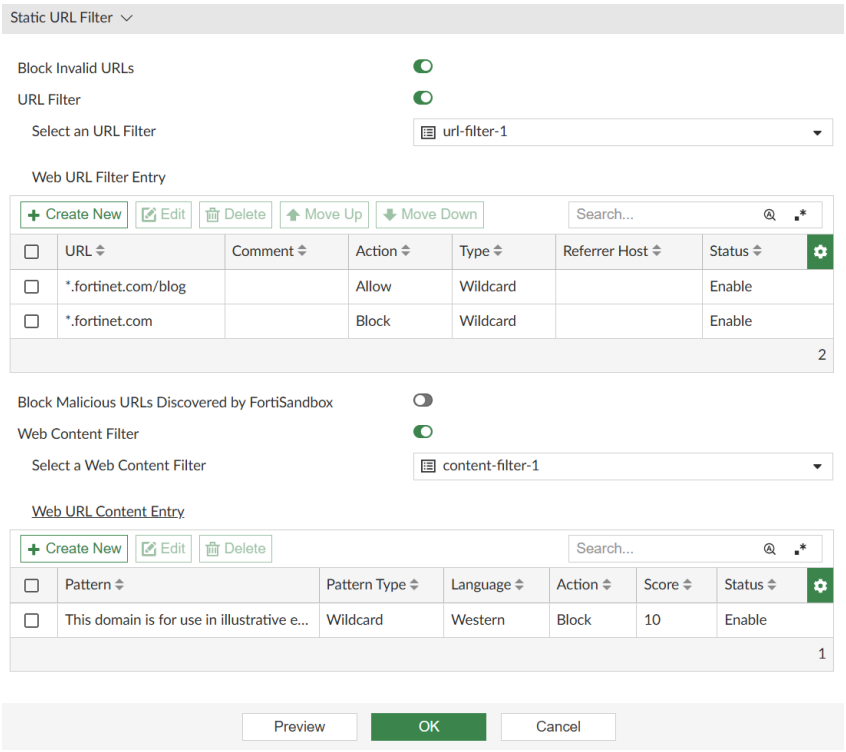
iv. Under *Web URL Filter Entry*, click *+Create New*, and configure the entry for **.fortinet.com/blog* as a *Wildcard* type with *Accept* action with *Status* enabled.

v. Click *OK*.

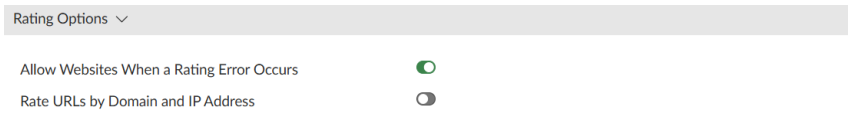
vi. Select the entry for *.fortinet.com/blog* and click *Move Up* to move this entry higher in matching priority than *.fortinet.com*.

vii. Fill in the *Change Note* and click *OK*.

i. Under *Select a Web Content Filter*, click *+* to create a web content filter with an entry and once created select it:
   i. In the *Name* field, enter `content-filter-1`.
   ii. Under *Web URL Content Entry*, click *+Create New*.
   iii. Click *+Create New*.
   iv. Set *Pattern Type* as *Wildcard*.
   v. Configure the pattern *This domain is for use in illustrative examples in documents.* with *Block* action and *Status* set as *Enable*.
   vi. Click *OK*.
   vii. Fill in the change note and click *OK*.



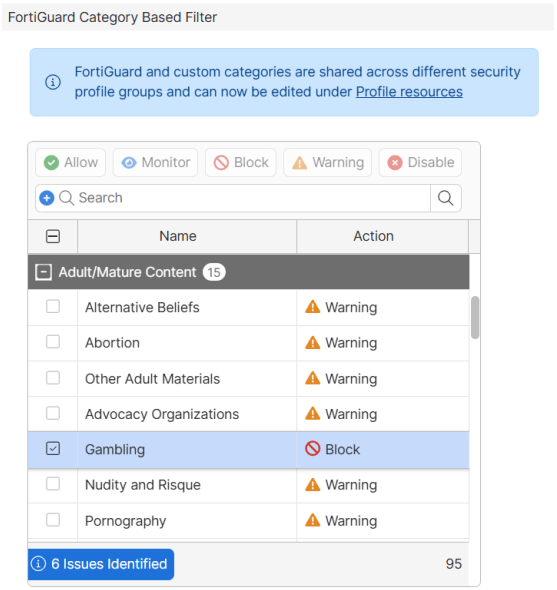
j. Under *Rating Options* enable *Allow Websites When a Rating Error Occurs*.

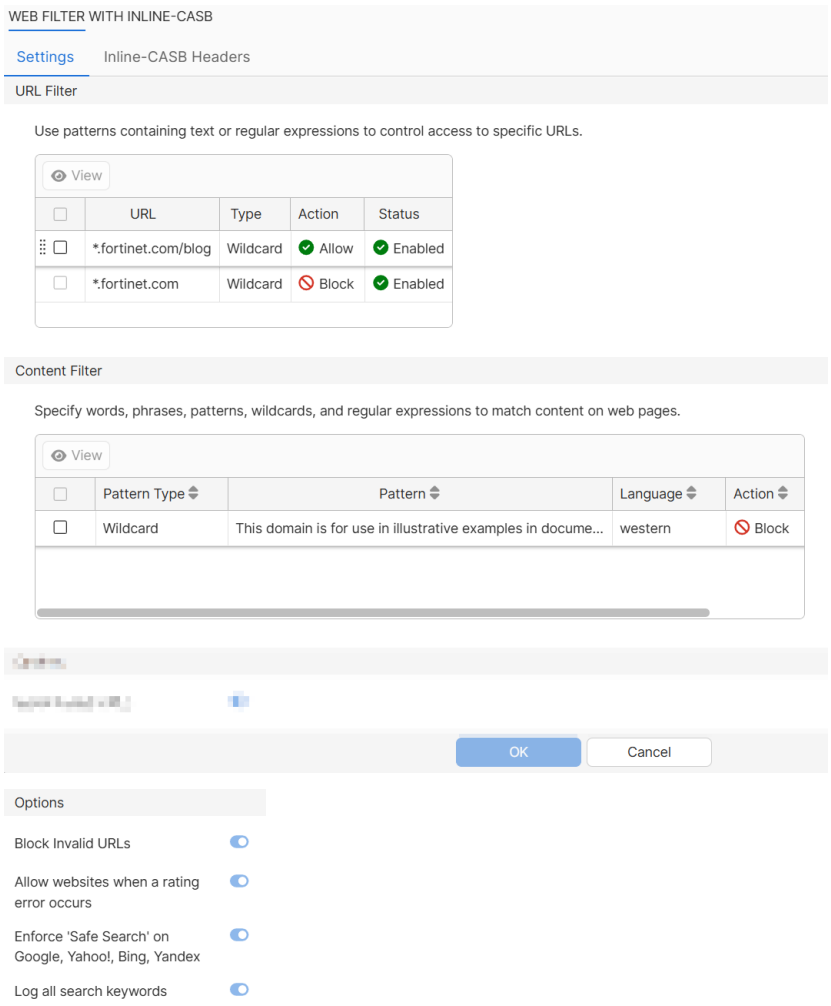


k. Fill in the *Change Note* and click *OK*.

2. Create a firewall profile group:
   a. Go to *Policy & Objects* > *Security Profiles* > *Profile Group*.
   b. Click *Create New*.
   c. In the *Name* field, enter `custom-profile-group`.
   d. For *Web Filter Profile*, select *custom-profile*.
   e. For *SSL/SSH Inspection*, select *deep-inspection*.
   f. For *Protocol Options*, select *default*.
   g. Fill in the *Change Note* and click *OK*.

3. Repeat steps in Configuring settings using Device Manager in FortiManager on page 605 to synchronize the custom-profile-group security profile group from FortiManager to FortiSASE.
4. In FortiSASE, verify the configuration has been synchronized from FortiManager:
   a. Go to *Security* > *Traffic* > *Security profiles* and do the following:
      i. For *Profile Group*, select *custom-profile-group*.
      ii. In *Web Filter With Inline-CASB*, click *View*.
      iii. Confirm the complete Web Filter configuration from FortiManager has been synchronized in FortiSASE.

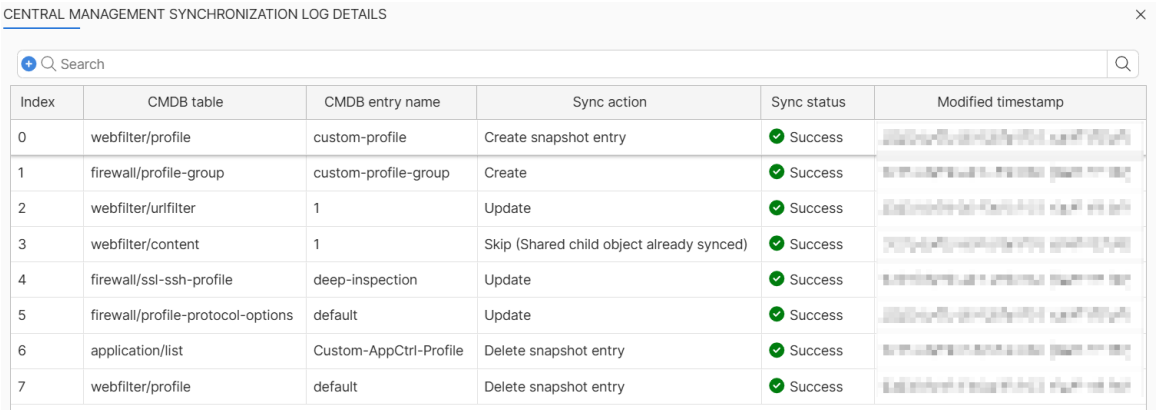




b. Go to *Operations* > *Logs* > *Central management synchronizations* and do the following:

i. Select the most recent log entry and click *View log details*.

ii. Confirm in the log details the desired configuration settings have been synchronized from FortiManager.



Central management for MSSP tenants

For MSSPs, FortiSASE supports central management for synchronizing multiple tenants' FortiSASE instances (MSSP tenants) from a single FortiManager instance or from multiple FortiManager instances.

- Currently, each ADOM in FortiManager supports synchronizing configuration with a single FortiSASE instance.
- A FortiManager key, if configured, allows a FortiManager appliance registered under a FortiCare account belonging to a parent Organization Unit (OU) to manage the FortiSASE tenant.
- The FortiManager key can be revoked to only allow connections from FortiManager appliances registered to the current FortiCare account and disable connections from parent OU FortiManagers.
- The FortiManager key will be strictly matched and must match in both FortiManager and FortiSASE connector settings. If a key is revoked on the FortiSASE tenant, then the key must also be removed on the FortiManager intending to manage the tenant.

Central management is still a select availability feature that requires a Fortinet Support ticket to enable it on new and existing instances.

Prerequisites and considerations

Prerequisites

- FortiManager must be adequately licensed for the number of ADOMs, and hence the number of FortiSASE tenants in an MSSP scenario (MSSP tenants), to be synchronized via central management. See FortiManager Ordering Guide.
- FortiManager must be configured with the ADOM feature enabled. See Enabling and disabling the ADOM feature.
- The FortiCloud Organization portal and FortiCloud IAM portal have already been configured to support the FortiSASE MSSP portal. See Configuration workflow on page 771.
  - If a FortiManager is deployed in the Root organizational unit (OU), then FortiSASE instances in child OUs can be synchronized.
  - If a FortiManager is deployed in a sub-OU, then only FortiSASE instances in the same sub-OU or in child OUs of the sub-OU can be synchronized.
- A valid subscription has already been purchased and applied to each FortiSASE tenant.

Considerations

- Regenerating the API key will immediately revoke access for any API consumers using the current key.
- The *New FortiManager* key field in the *Regenerate FortiManager Key* pane is the only place the FortiManager key will be provided. Keep this information secure. The FortiManager ADOM bearing this key will be granted Central Management permissions assigned to this account.

The following topics are covered:

- Enabling central management for an MSSP tenant on page 713
- Configuring FortiManager for central management of an MSSP tenant on page 714

Enabling central management for an MSSP tenant

Ensure you are aware of central management for MSSP tenants Prerequisites and considerations on page 712.

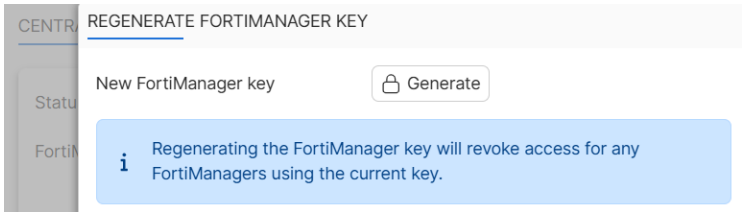
This topic covers how to enable central management on FortiSASE for an MSSP tenant by generating a FortiManager key to grant the associated FortiManager permission to establish a central management connection to FortiSASE.

In addition, this topic covers how to revoke a FortiManager key, which is done for these reasons:

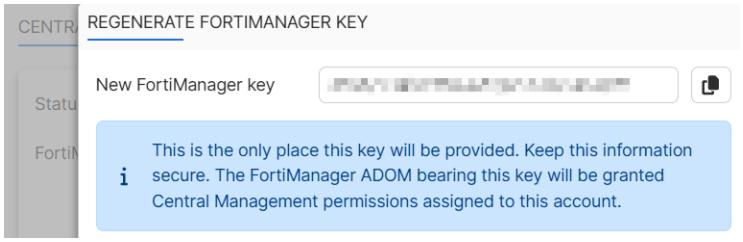
- To limit permission to establish central management connections to a FortiSASE MSSP tenant to FortiManager devices in the same FortiCloud OU account as the FortiSASE MSSP tenant.
- To disconnect central management connections from FortiManager devices belonging to parent OU accounts.

To enable central management on FortiSASE for an MSSP tenant:

1. Log into the MSSP tenant via the MSSP portal. See Managing a tenant's instance on page 783.
2. Once in the tenant, enable central management. See Enabling central management on page 598.
3. Once central management has been enabled in the tenant, click *Regenerate* next to *FortiManager Key*.
4. In the *Regenerate FortiManager Key* pane, click *Generate* next to *New FortiManager key*.



   Regenerating the API key will revoke access for any FortiManagers using the current key.
5. After generating a new FortiManager key, the key appears in the text field to the right of *New FortiManager key*. Click the copy button to the right of the text field to copy the new FortiManager key to the clipboard.

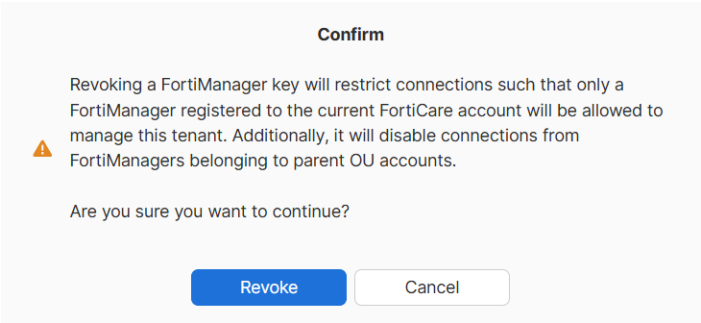


   This is the only place this key will be provided. Keep this information secure. The FortiManager ADOM bearing this key will be granted Central Management permissions assigned to this account.
6. Click *Close*.
7. Click *OK* to update central management settings for the MSSP tenant.

To revoke a FortiManager key in an MSSP tenant:

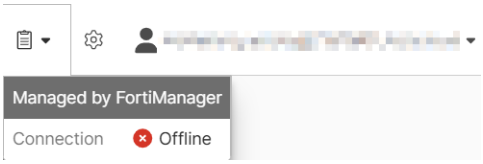
1. Log into the MSSP tenant via the MSSP portal. See Managing a tenant's instance on page 783.
2. Go to *System* > *Central Management*.

3. Click on the *Revoke* button next to the *FortiManager Key* field.
4. Review the warning prompt and click *Revoke*.

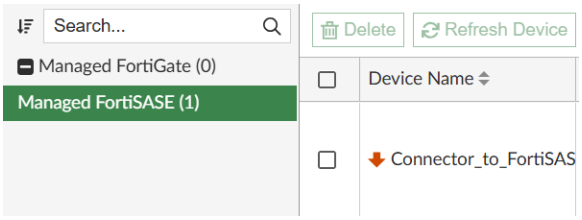


Observe a message *Successfully revoked FortiManager key* appear in the top-right.

5. Click *OK*.
6. In FortiSASE, observe any parent OU FortiManager connections to the MSSP tenant get disconnected after the steps above are completed.



7. In the parent OU FortiManager, in the associated ADOM, go to *Device Manager* > *Device & Groups* and observe the FortiSASE connector has the disconnected status.



Configuring FortiManager for central management of an MSSP tenant

Ensure you are aware of central management for MSSP tenants Prerequisites and considerations on page 712.

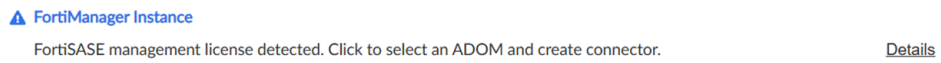
Currently, each ADOM in FortiManager supports synchronizing configuration with a single FortiSASE instance.

This example demonstrates how to configure a FortiManager for central management of a single FortiSASE tenant in an MSSP scenario. These steps can then be repeated to configure a FortiManager for central management of multiple FortiSASE tenants in an MSSP scenario, provided that unique FortiManager keys are obtained from each tenant per steps in Enabling central management for an MSSP tenant on page 713.

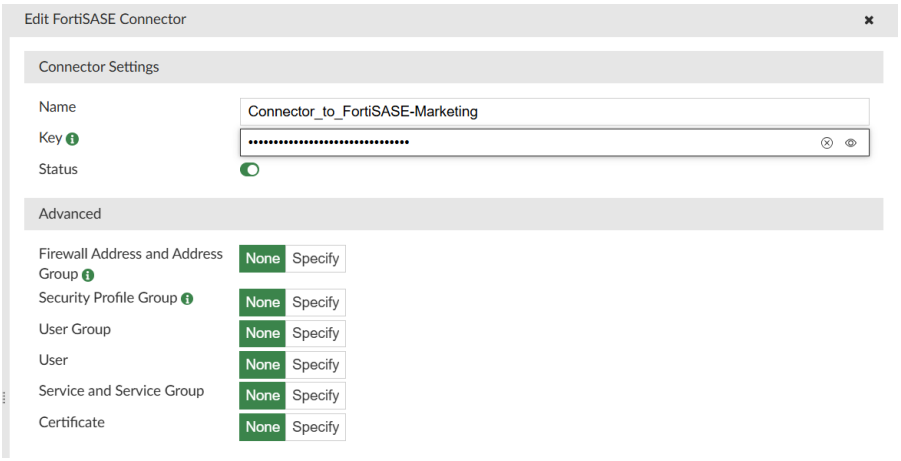
These steps can similarly be applied to a single FortiManager performing central management for a single FortiSASE tenant in an MSSP scenario, that is, for a scenario where a unique FortiManager manages a unique FortiSASE tenant.

To configure FortiManager for central management of an MSSP tenant:

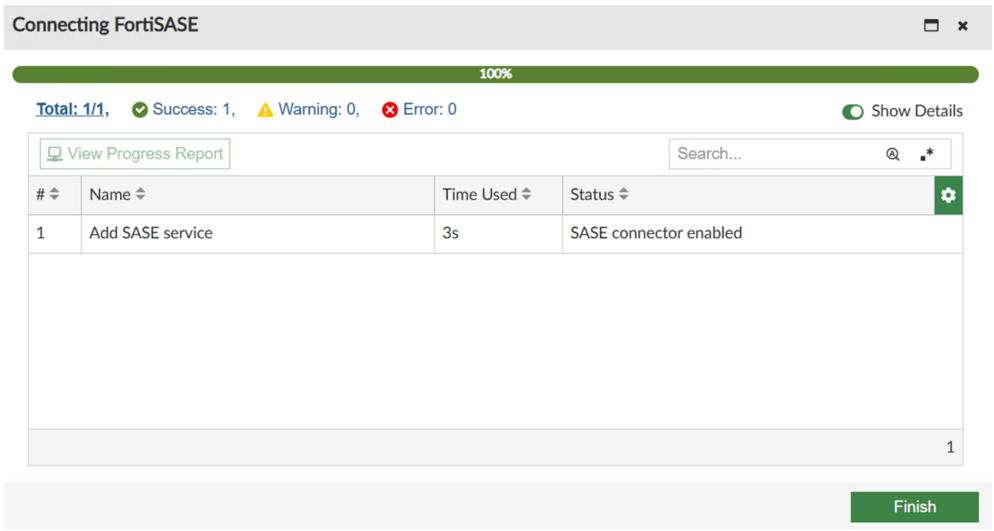
1. When a FortiSASE subscription is registered to the same FortiCloud account as your FortiManager, you receive a notification in the header. Click the notification.



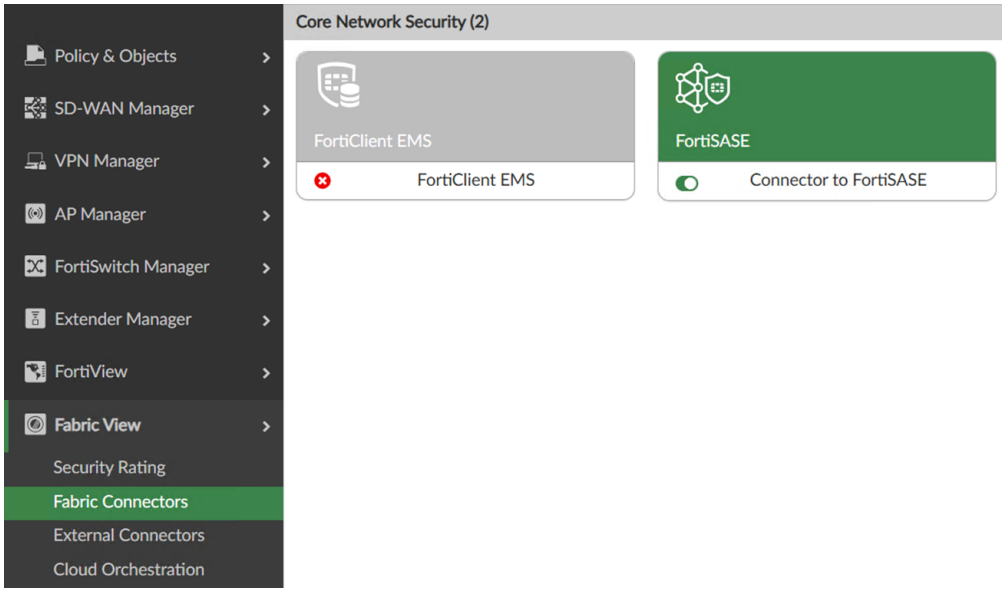
2. Administrative domains (ADOM) enable administrators to manage only devices that they are assigned, based on the ADOMs to which they have access. In the dialog, select the ADOM corresponding to a FortiSASE tenant used in an MSSP scenario (MSSP tenant). Alternatively, create a new ADOM. See Creating ADOMs.
3. After selecting the ADOM version, the *Edit FortiSASE Connector* dialog appears with *Status* set to enabled.
   a. Each FortiSASE Connector name must be unique on a FortiManager device. Therefore, create a unique FortiSASE Connector name.
      - For instance, you can append the name of the ADOM to the end of the connector name, such as *Connector_to_FortiSASE-<ADOM>*.
      - In the example screenshot below, since the ADOM is named *Marketing*, the FortiSASE Connector is named *Connector_to_FortiSASE-Marketing*.
   b. In the *Key* field, copy and paste the FortiManager key copied from the FortiSASE MSSP tenant's portal.
      - This is the key step that grants this FortiManager ADOM Central Management permission to connect to the assigned to the corresponding FortiSASE tenant.
      - For FortiSASE authentication, you can get this key from the FortiSASE portal if you have not done so already. See Enabling central management for an MSSP tenant on page 713.
   c. Under *Advanced*, you can define objects. You can leave all object types set to *None* and click *OK*.



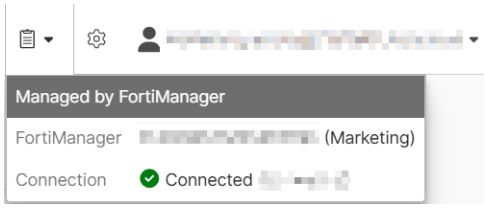
4. The *Connecting FortiSASE* dialog appears with the item *Add SASE service*.
   The progress bar should proceed to completed with the *Status* displaying *SASE connector enabled*.



5. In *Fabric View* > *Fabric Connectors*, observe that the FortiSASE Connector is enabled.



6. In the FortiSASE header for the MSSP tenant, observe the connection status to FortiManager with the associated FortiManager ADOM displayed.



7. FortiManager can now be used to synchronize supported configuration settings with the FortiSASE tenant used in an MSSP scenario. See the following topics for details:
   - Configuring settings using Device Manager in FortiManager on page 605
   - Configuring settings using policy packages in FortiManager on page 612
   - Configuring security profiles in FortiManager on page 653

Snapshot

Currently, only the Factory reset feature is available on this page. See Factory reset on page 717.

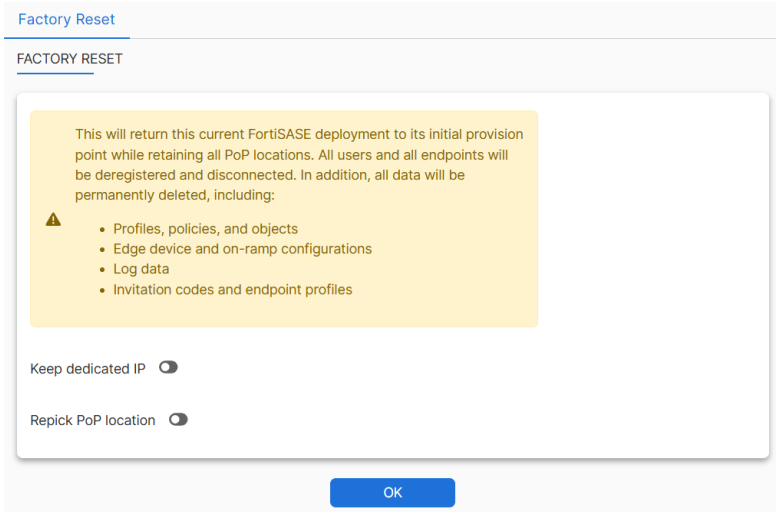
Factory reset

When the Prerequisites on page 719 below are met, FortiSASE supports performing a factory reset on a FortiSASE instance that returns it to its initial provision point, disconnect all users, and deregister all endpoints.

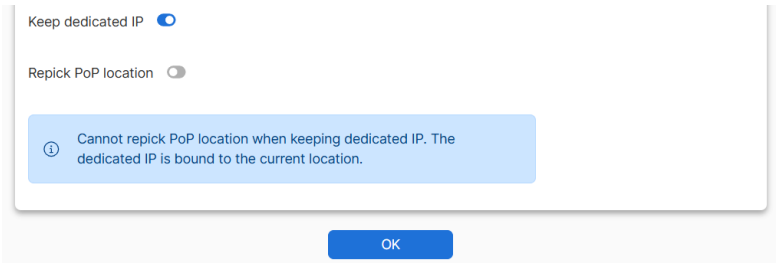
> ⚠ After running a factory reset on a FortiSASE instance, **all data will be permanently deleted**, including:
> - Profiles, policies, and objects
> - Edge and On-ramp device configurations
> - Log data
> - Invitation codes and endpoint profiles

To perform a factory reset on a supported instance:

1. Go to *System* > *Snapshot* > *Factory Reset*.



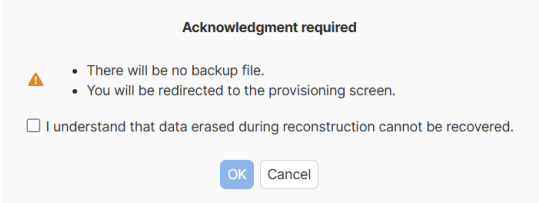
   a. Ensure you review the banner text carefully.
   b. Review the following options (you can only choose one option and they cannot be used together):
      - *Keep dedicated IP*: When enabled, after the factory reset, the instance will keep the current dedicated IP addresses already assigned to its security PoPs.
        - When enabled, an inline message appears indicating that you cannot repick PoP location when keeping dedicated IP.



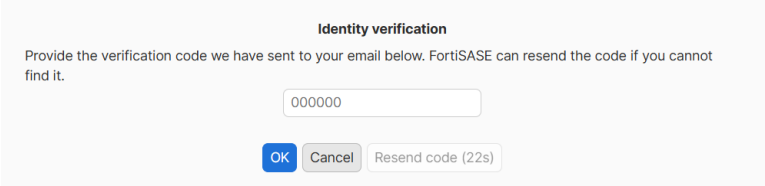
- The FortiSASE domain name already assigned to its security PoPs remains the same regardless of the *Keep dedicated IP* state.

- *Repick PoP location*: When enabled, after the factory reset, the instance will prompt the administrator to select new security PoPs. This option cannot be enabled when *Keep dedicated IP* is enabled.

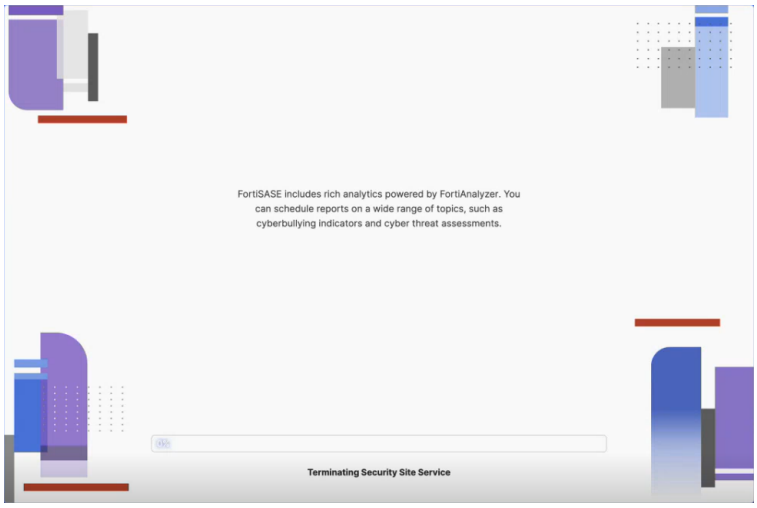
2. Click *OK*.
3. In the *Acknowledgment required* prompt, carefully review the points listed, namely:
   - There will be no backup file.
   - You will be redirected to the provisioning screen.
4. Select the checkbox next to *I understand data erased from factory reset cannot be recovered*.



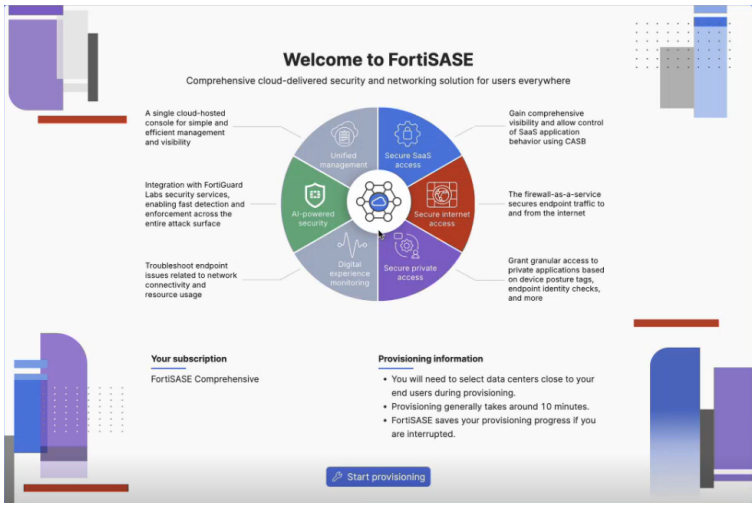
5. Click *OK*. You cannot click *OK* unless you first select the checkbox.
6. The *Identity verification* prompt appears. An email with the one-time passcode (OTP) is sent to the email address for the primary FortiCloud account for the instance. Click *Resend* if you have not received the code via email.



7. Enter the OTP received via email in the code field and click *OK*.
8. FortiSASE will display *Terminating Security Site Service*. This process will take a few minutes.



9. After terminating the security site service, FortiSASE will then redirect you to the provisioning screen. Click *Start provisioning* to start the provisioning process.



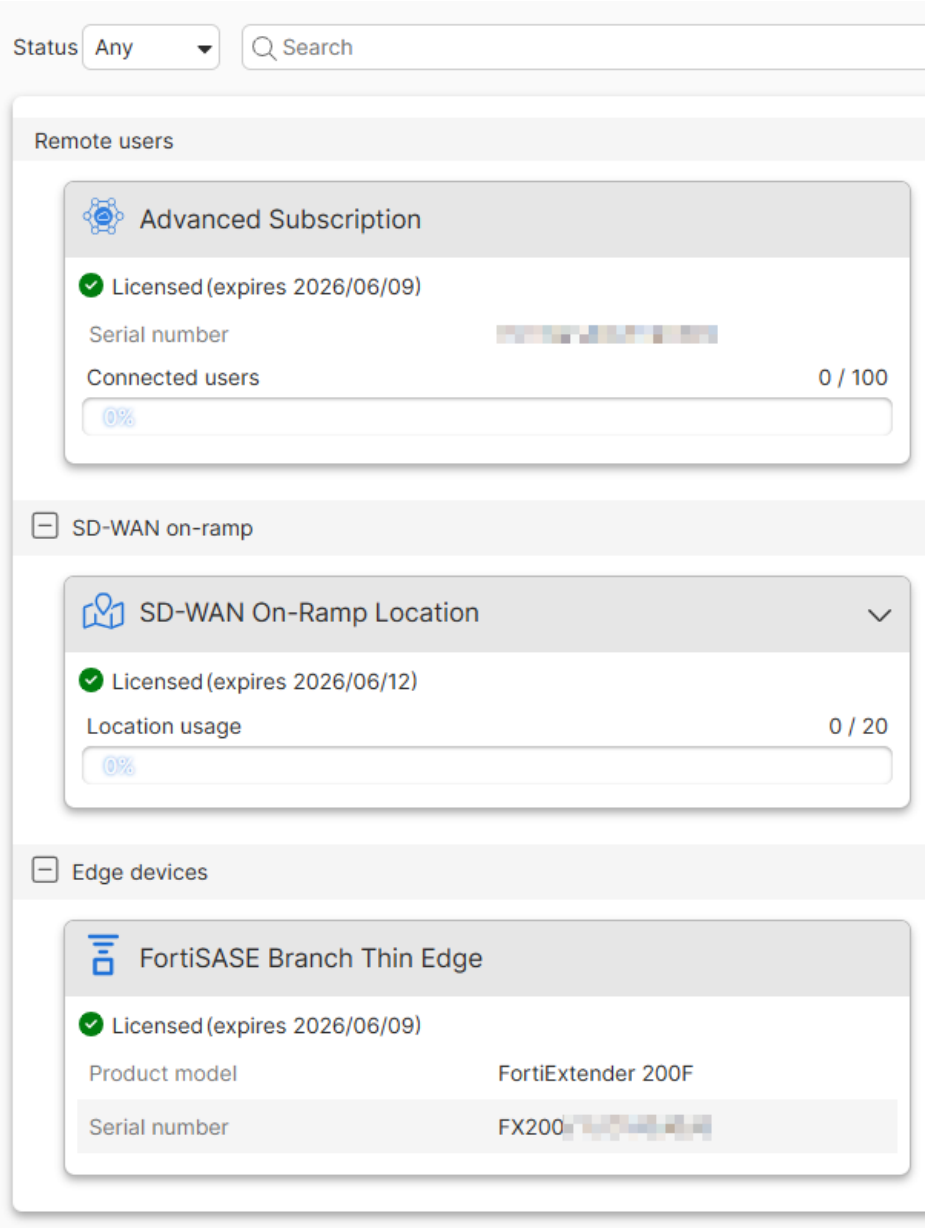
10. If *Repick PoP location* was enabled, then you will be prompted to select the security PoPs for the instance, like what is done when deploying a new instance.
11. If your web browser is in the foreground, you may need to refresh, minimize then restore the browser window, or click on *Start provisioning* to display provisioning process updates.

Prerequisites

- This feature is enabled by default on FortiSASE instances with the Not-for-Resale (NFR) and Advanced NFR subscriptions applied.
- For FortiSASE instances with other licenses, this is a select availability feature that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE Feature instance, create a new ticket with FortiCare Support.
- This feature is available only when logged into the FortiSASE portal with the principal FortiCloud account, where an OTP code is sent via email. This feature is not available from IAM accounts.

Subscription overview

FortiSASE supports various subscription types to support different use cases. Therefore, you may have multiple subscriptions applied to your FortiSASE instance, with individual expiry dates. You can view information regarding your subscriptions, such as expiry, status, and usage, in *System > License overview*. You can use the *Status* dropdown list and search bar at the top to filter for the desired subscription.

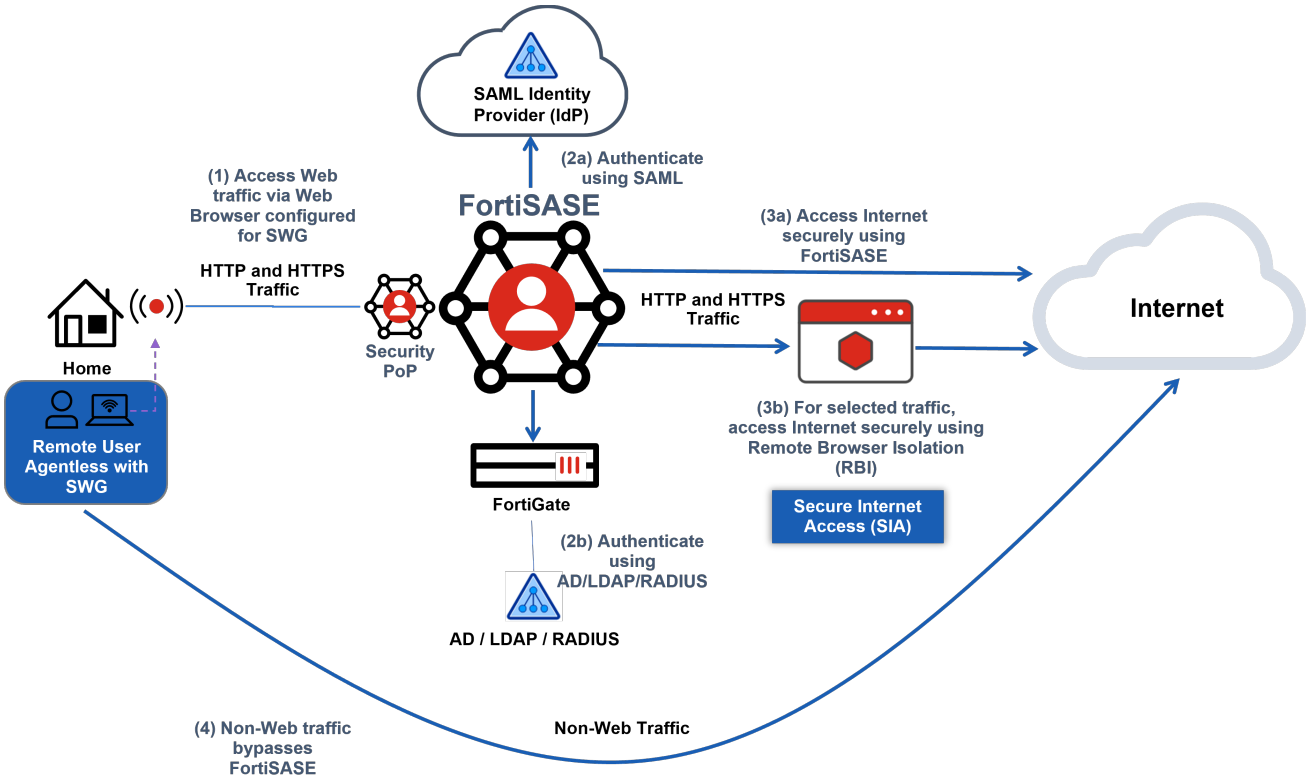


RBI

Remote browser isolation (RBI) is a select availability feature that is disabled by default for all instances where it is not already enabled. The recommended alternative to RBI functionality is the Secure Browser extension. See Secure Browser on page 415.

To mitigate web-based threats for end users proxying traffic through FortiSASE, you can enable remote browser isolation (RBI) to isolate browser sessions of certain websites or categories in an isolated environment, which renders content safely in a remote container.

FortiSASE supports RBI for proxy users.



Prerequisites

The following requirements must be met for the feature to be available in the GUI:

- RBI requires a FortiSASE instance with an Advanced or Comprehensive remote users FortiSASE subscription. See Licensing on page 722.
- The FortiSASE deployment is deployed in a Fortinet security PoP only. See Global data centers.
- Proxy is enabled under *Network* > *Proxy configuration*. See Proxy configuration on page 285.

Considerations

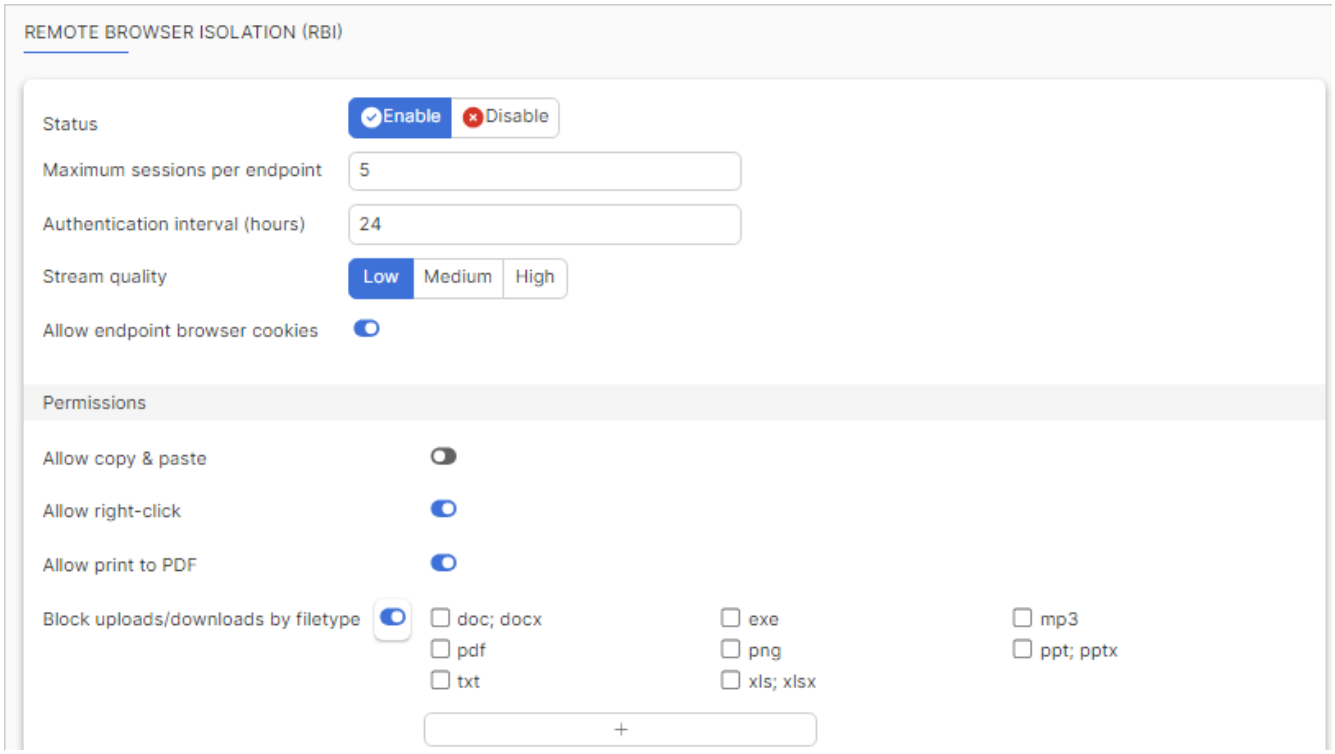
- Each instance is entitled to a maximum isolation data per month as listed in RBI. When the limit is exceeded, traffic configured to be isolated will be blocked for all users.
- When configuring RBI with SWG SSO, ensure the security profile group used for the "CSP_REPORT" proxy policy is using certificate inspection instead of deep inspection.

Licensing

The FortiSASE instance must have an Advanced or Comprehensive remote users subscription applied to it. For limitations, see RBI.

Configuration options

When you enable RBI, the following configuration options are available:



Maximum sessions per endpoint	Maximum number of concurrent RBI sessions allowed for each user. Default is 5. Valid range is 1-5.
Authentication interval (hours)	Interval (in hours) after which users will be prompted to re-authenticate for any isolated traffic and web requests.

Stream Quality	Quality of streamed videos. Higher quality means more bandwidth usage.
Allow endpoint browser cookie	Specifies whether to allow users to store cookies from isolated browser sessions.
Allow copy & paste	Specifies whether to allow client users to copy and paste content from isolated sessions to the clipboard using the keyboard or right-click menu. To enable copying content from isolated sessions using the right-click menu, the *Allow right-click* option must be enabled.
Allow right-click	Specifies whether to allow end users to right click on mouse to display a menu.
Allow print to PDF	Specifies whether to allow end users to print the isolated session pages into a PDF file.
Block uploads/downloads by filetype	Enable to select the file types to block from uploading and downloading. • *doc; docx* • *exe* • *mp3* • *pdf* • *png* • *ppt; pptx* • *txt* • *xls; xlsx* You can also add more file types by clicking the *Add* button.

See Example: Configuring RBI with proxy on page 723 for an end-to-end example of configuring FortiSASE to isolate all traffic to specific types of websites from proxy users.

Example: Configuring RBI with proxy

Each instance is entitled to a maximum isolation data per month as listed in RBI. When the limit is exceeded, traffic configured to be isolated will be blocked for all users.

You can configures FortiSASE to isolate traffic to specific types of websites from all or specific proxy users by following these steps:

1. Configure proxy users and user groups
2. Enable RBI and configure isolation behavior
3. Configure a proxy policy to define isolation scope
4. Configure the proxy settings of each proxy endpoint
5. Verify the isolation

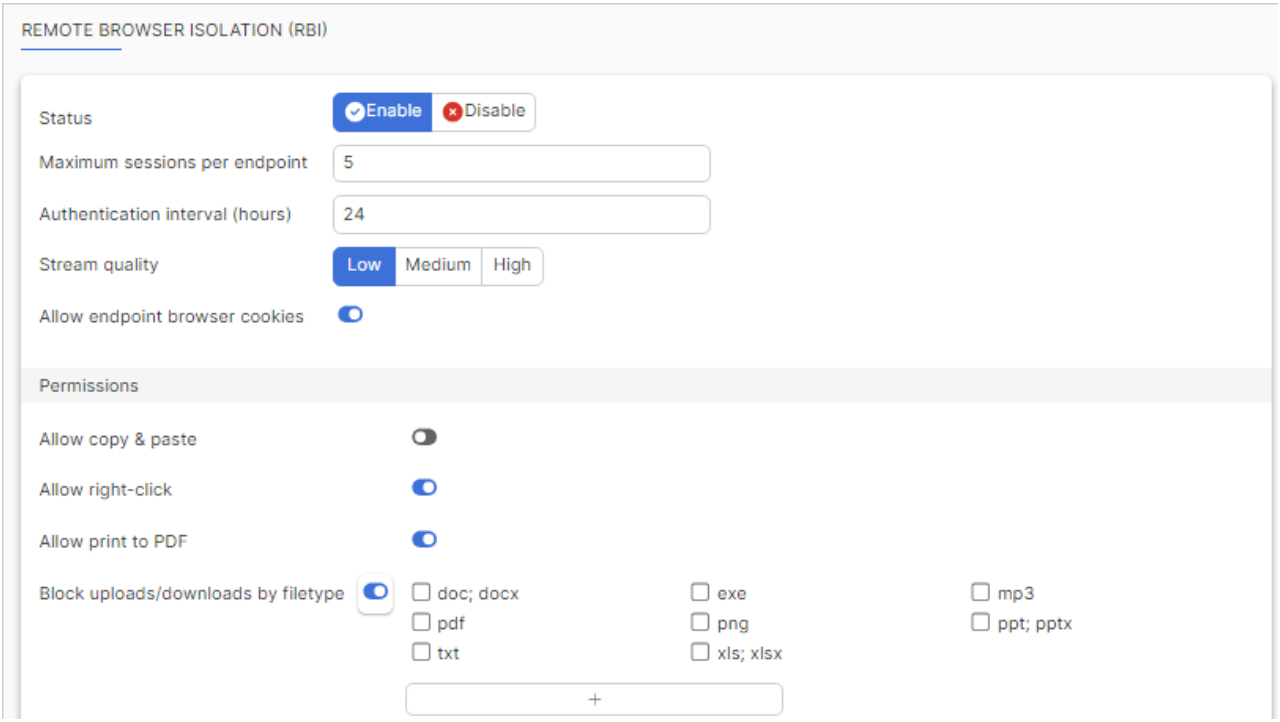
To configure proxy users and user groups:

Follow one of the procedures below, depending on your authentication source:

- **(Recommended)** Configuring FortiSASE with Entra ID SSO in proxy agentless mode on page 526
  - When configuring RBI with SWG SSO, ensure the security profile group used for the "CSP_REPORT" proxy policy is using certificate inspection instead of deep inspection.
- Configuring FortiSASE with an LDAP server for remote user authentication in proxy agentless mode on page 508
- Configuring FortiSASE with a RADIUS server for remote user authentication on page 512
- Users and groups on page 502

To enable RBI and define the isolation behavior:

1. Ensure that proxy is enabled under *Network* > *Proxy configuration*.
2. Go to *System* > *Remote Browser Isolation* and toggle *Enable* to on.
   If the menu is unavailable, ensure that you have the proper subscription and security PoP access for the feature. See Subscriptions on page 786 and Global data centers.
3. Configure the options to define the isolation behavior based on your needs. See Configuration options on page 722.
   This example uses the following configuration:



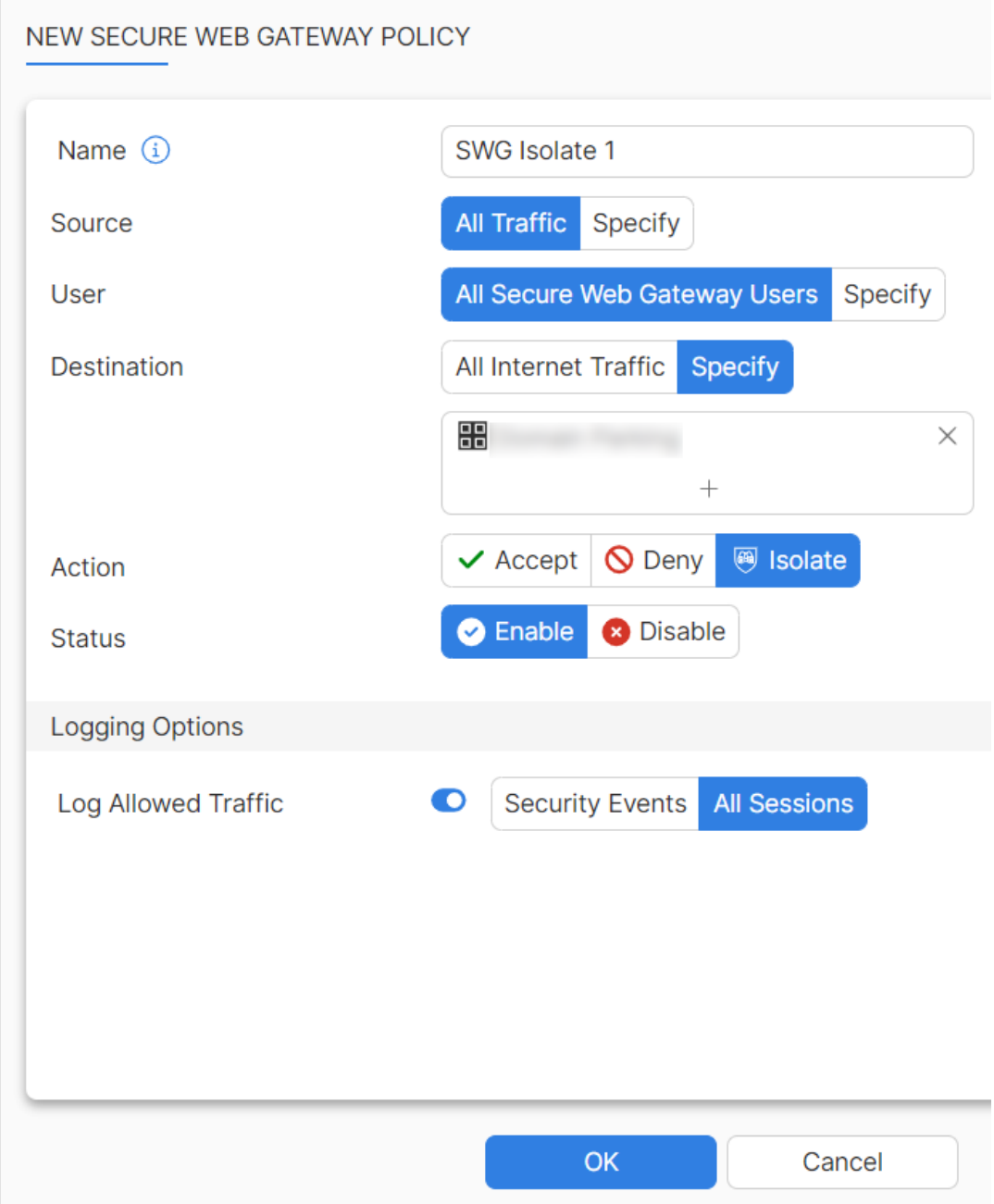
4. Click *OK*.

To configure a proxy policy to define the isolation scope:

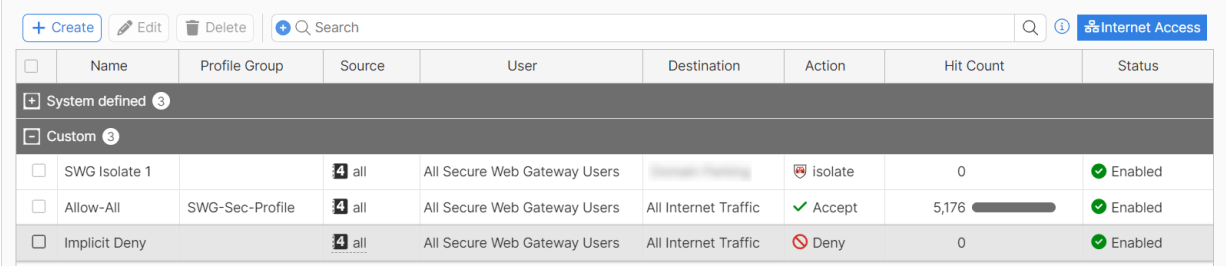
1. Go to *Security* > *Traffic* > *Proxy policies* and click *Create*.
2. For *Name*, enter *Proxy Isolate 1*.
3. For *Source*, select *All Traffic* or specify the specific traffic type to isolate.

4. For *User*, select *All Proxy Users* or specify the specific users to isolate traffic for.
5. In the *Destination* field, click *Specify*.
6. Click the *Add* icon under *Destination*.
7. Select from the following categories of websites to isolate traffic for.
   - Unrated
   - Newly Observed Domain
   - Newly Registered Domain
   - Malicious Websites
8. In the *Action* field, select *Isolate* to run all sessions to the specified categories of websites in an isolated environment.
9. In the *Status* field, select *Enable*.

10. Configure logging options as needed.



11. Click *OK*.
12. In the proxy policy list, drag the *Proxy Isolate 1* policy row and place it in a desired location. Ensure it is above the *Allow-All* policy as FortiSASE performs policy match from top down.

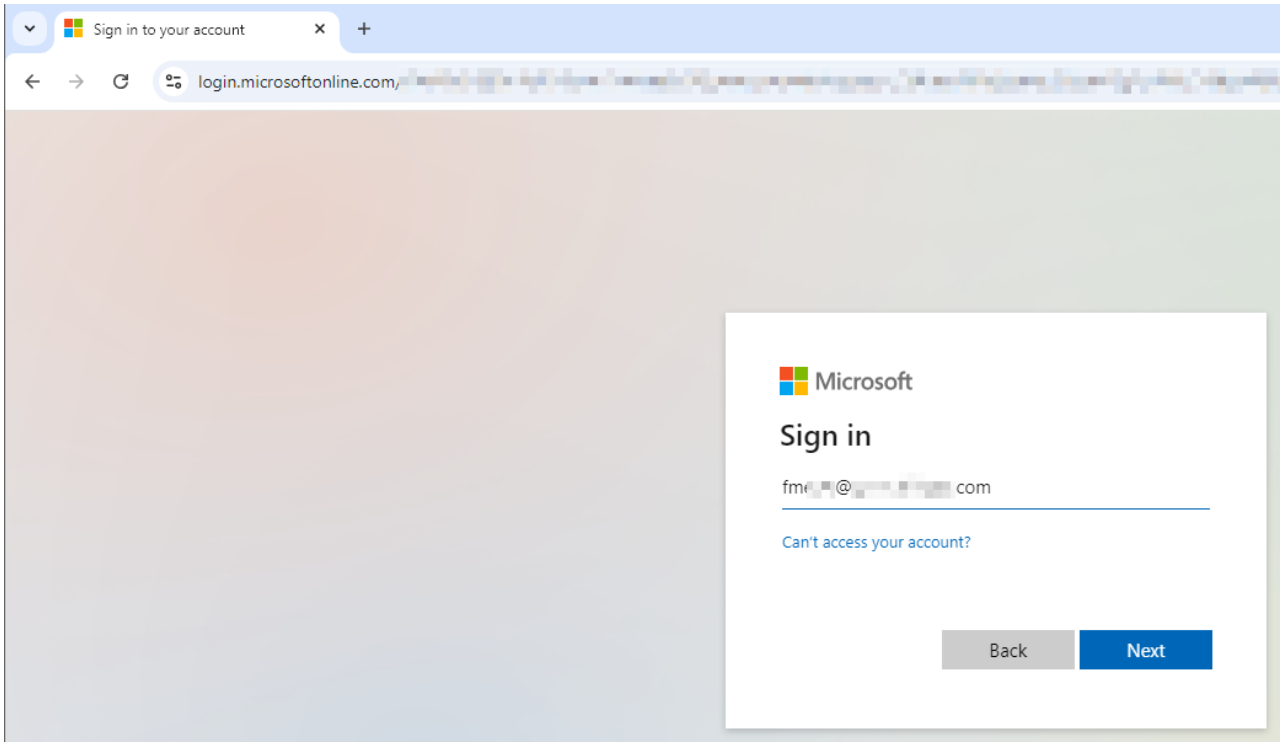


To onboard your proxy users to FortiSASE remote browser isolation:

1. Go to *Network* > *Proxy configuration*.
2. Copy the URL in the *Hosted PAC File* field and click *Download Proxy Certificates* on the right pane.
3. Distribute the *Hosted PAC File* URL and certificate to all your proxy users.
4. Ask the proxy users to install the certificate on their endpoints to avoid untrusted certificate errors. See Installing a certificate for deep inspection mode on page 317.
5. Ask the proxy users to configure the proxy settings on their endpoints using the *Hosted PAC File* URL. The proxy can be configured at the OS level or in a browser. Configuring proxy settings at the OS level applies them to all installed browsers. See Proxy configuration on page 744.

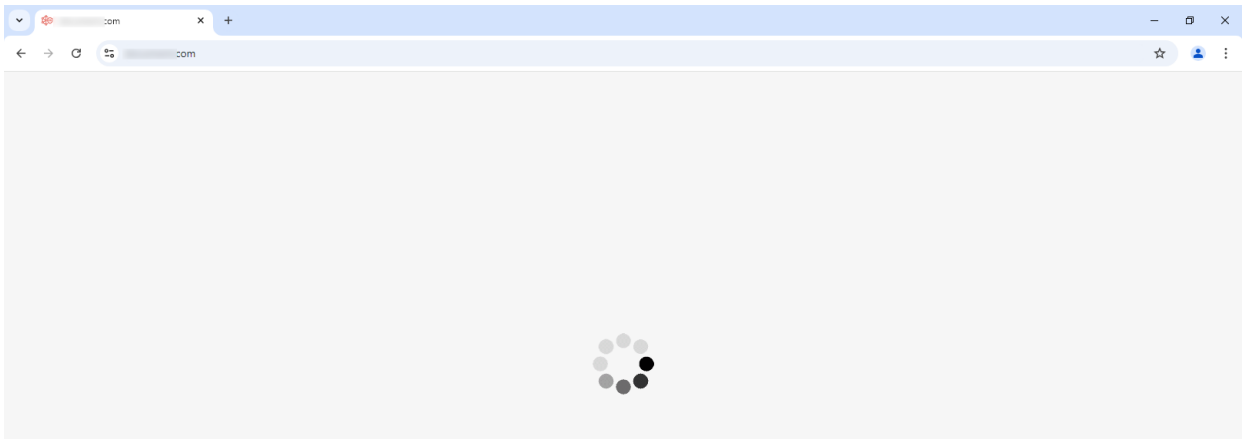
To verify RBI functionality for a proxy user:

1. On the proxy user's endpoint, start a browser session. In this example, the recommended method of using SSO authentication with Microsoft Entra ID as the SAML IdP was configured for proxy. Therefore, the browser is redirected to the SAML IdP for authentication.

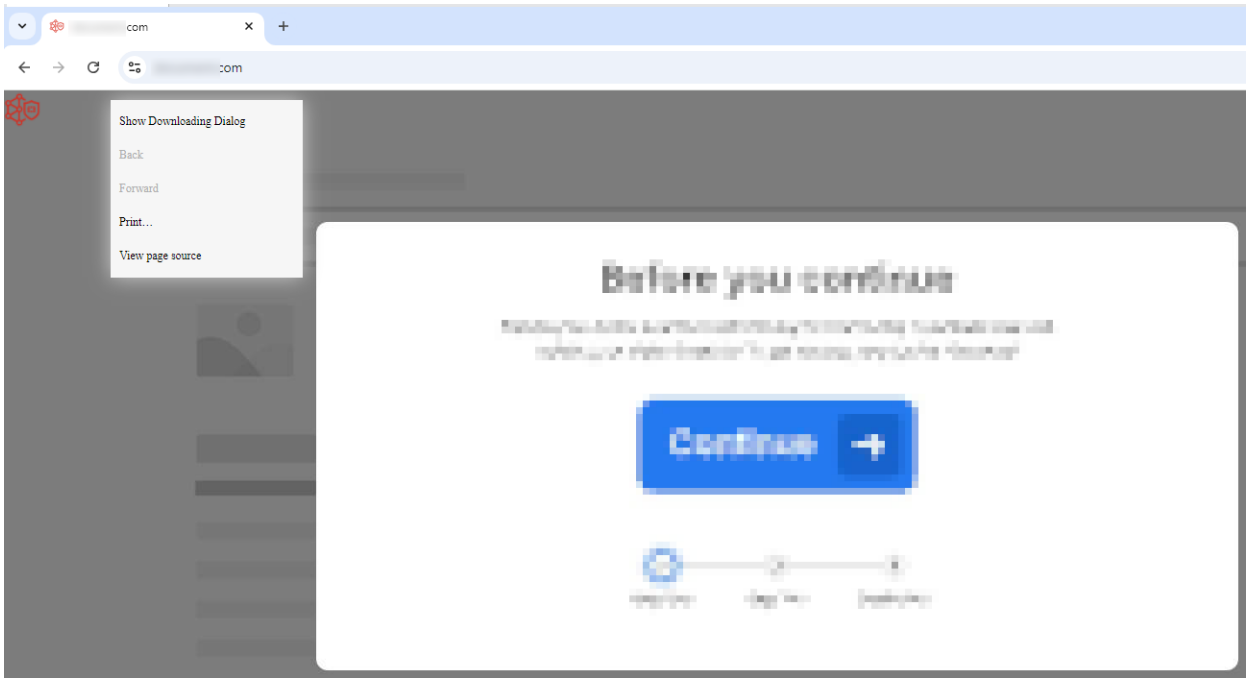


2. Enter the proxy SSO user credentials and open a website of the configured isolate category in the browser. The FortiSASE RBI feature analyzes the connection, matches the session with the proxy Isolate 1 policy, and

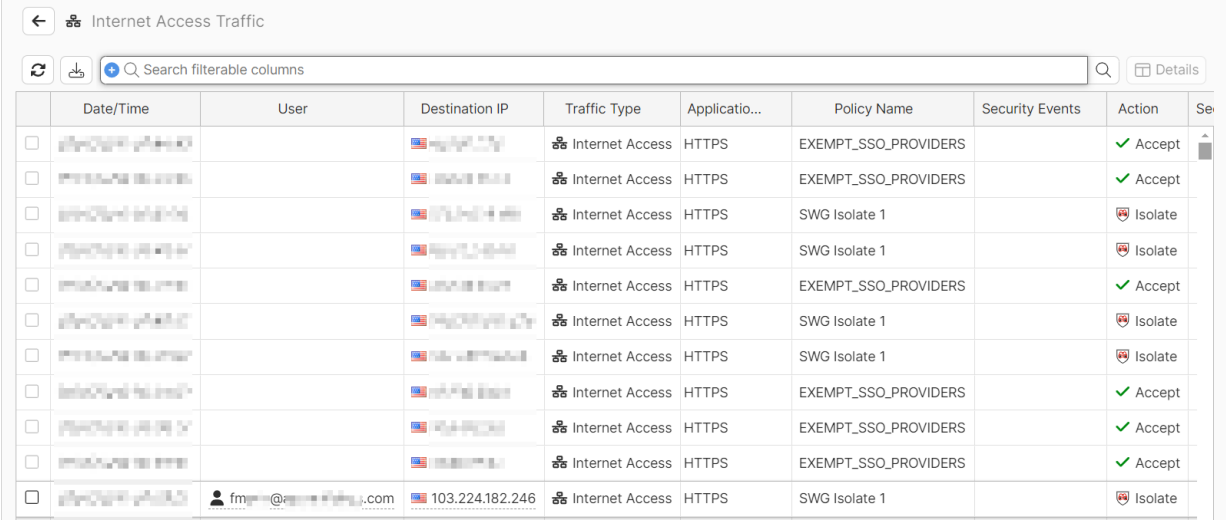
isolates the traffic. When the RBI feature is loading the website, the FortiSASE icon appears in the browser tab and a circular progress bar becomes active.



Once the RBI feature has finished loaded the website, the FortiSASE icon at the top-left corner is displayed on the page. Also, a replaced right-click menu becomes available if the *Allow right-click* option was enabled in the configuration as shown previously.



3. To confirm proxy sessions have been isolated, in the FortiSASE portal GUI go to *Operations* > *Logs* > *Traffic* > *Internet Access Traffic*.
4. Locate the log entry corresponding to the SSO authenticated web browsing activity to the website, which is categorized by FortiGuard as part of the configured isolate category.
5. For this log entry, observe the proxy Isolate 1 policy has been matched and FortiSASE has taken the Action of Isolate, which indicates RBI functionality has been applied to this traffic.


Internet Access Traffic
Search filterable columns
Details
Date/Time
User
Destination IP
Traffic Type
Applicatio...
Policy Name
Security Events
Action
Internet Access HTTPS EXEMPT_SSO_PROVIDERS Accept
Internet Access HTTPS EXEMPT_SSO_PROVIDERS Accept
Internet Access HTTPS SWG Isolate 1 Isolate
Internet Access HTTPS SWG Isolate 1 Isolate
Internet Access HTTPS EXEMPT_SSO_PROVIDERS Accept
Internet Access HTTPS SWG Isolate 1 Isolate
Internet Access HTTPS SWG Isolate 1 Isolate
Internet Access HTTPS EXEMPT_SSO_PROVIDERS Accept
Internet Access HTTPS EXEMPT_SSO_PROVIDERS Accept
Internet Access HTTPS EXEMPT_SSO_PROVIDERS Accept
fm @ .com 103.224.182.246 Internet Access HTTPS SWG Isolate 1 Isolate

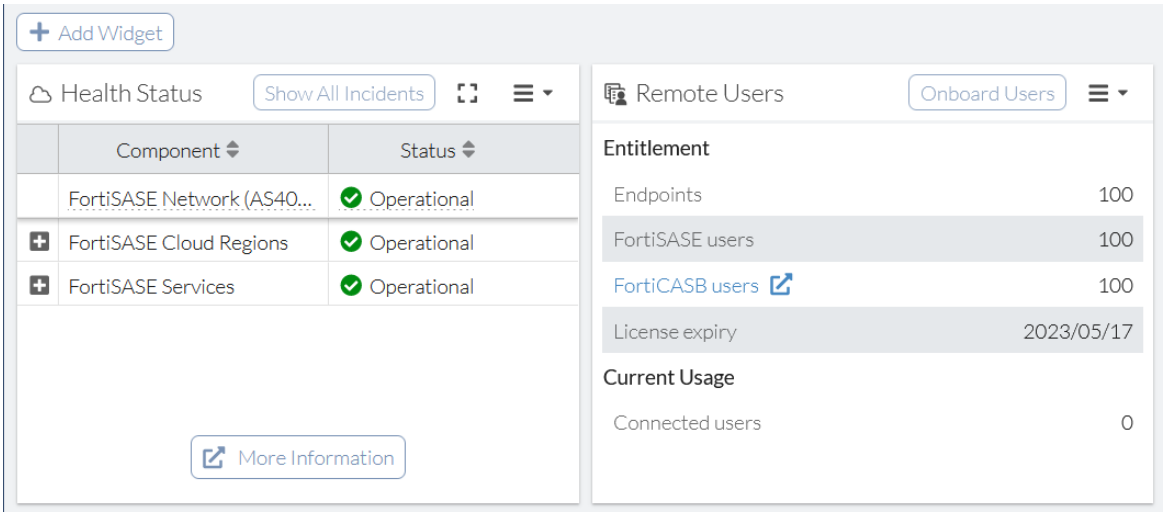
Client onboarding

Clients using managed endpoints connect using tunnels. You can onboard them using the *Onboard Users* slide-in.

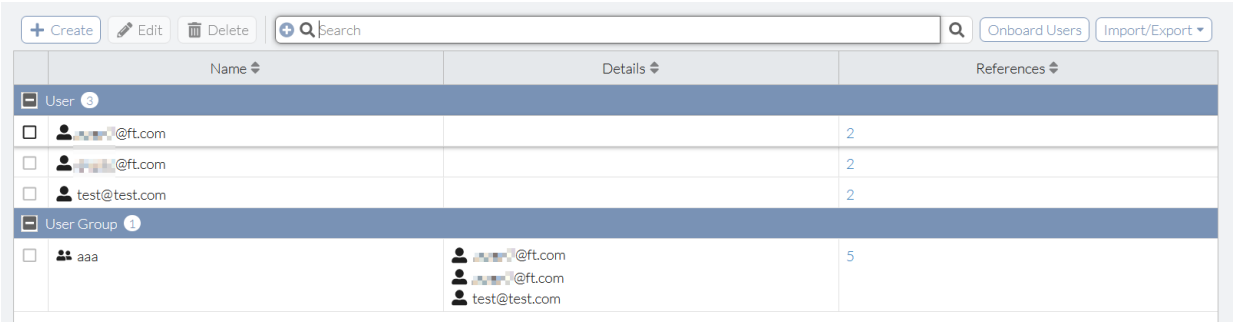
To access the Onboard Users slide-in:

You can access the *Onboard Users* page by doing one of the following:

- Go to *Monitoring* > *Dashboards* > *Status* and under the *Remote users* widget, click *Onboard Users*. If this widget does not exist, add a new *Remote users* widget as Adding a custom dashboard on page 59 describes.



- Go to *Access & authentication* > *Access* > *Users and groups* and click *Onboard Users* at the top right of the page.



When you click the *Onboard Users* button, the *Onboard Users* slide-in page appears. The page consists of the following sections:

- Managed Endpoint Users. See Managed endpoint client onboarding on page 731.
- Proxy. See Proxy client onboarding on page 737.

Managed endpoint client onboarding

Onboard Users > *Agent* includes features to support onboarding managed endpoint clients.

Feature	Description
Delivery	Method for obtaining the FortiClient installer: • *Download installer*: download the installer directly from the FortiSASE portal. The remaining features in this table appear when you select this method. • *Send link to installer*: send invitation email to selected users containing links to FortiClient installers for all major operating systems (OS). When you select this method, the *Invite Users* option appears. • *Invite Users*: click + to add a blank field where you can enter a managed endpoint user's email address to onboard to FortiSASE. Click + as many times as desired to enter multiple email addresses. When you complete entering managed endpoint users' email addresses, click *Send*.
OS	Use the *OS* dropdown to select the installer for the major OS that you want to download. MacOS and Windows installers are preconfigured with your FortiSASE invitation code.
FortiClient Version	Recommended FortiClient version for FortiSASE users.
Download preconfigured Installer	After selecting MacOS or Windows as the OS, clicking *Download preconfigure Installer* downloads the preconfigured installer for the selected OS to your local machine.
Download installer	After selecting Android or iOS as the OS, clicking *Download installer* downloads publicly available installers that do not come preconfigured with your FortiSASE invitation code. Clicking *Download installer* for a supported OS goes to a download page where you can select and download the installer to your local machine.

Prerequisites and considerations

Prerequisites

- Support for custom invitation codes is a select availability feature in FortiSASE that is not enabled by default on new instances and requires that the instance has been provisioned with Feature version support. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.
  - With custom invitation codes enabled, default and custom invitation codes are no longer displayed in the *Onboard Users* dialog. Instead, you can display invitation codes by going to *Endpoint management* > *Endpoint profiles* and clicking on the *Invitation codes* tab.
  - For existing instances running the Mature release, the invitation code will still be displayed in the *Onboard Users* dialog.
- Starting in 25.2.a, default and custom invitation codes are no longer displayed in the *Onboard Users* dialog. Instead, you can display invitation codes by going to *Endpoint management* > *Endpoint profiles* and clicking on the *Invitation codes* tab.

- The preconfigured FortiClient installers for MacOS and Windows platforms are preconfigured with the *Default* invitation code.
- When using a custom invitation code, administrators must assign the invitation code using endpoint CLI commands and the `-r` or `--register` flag with enterprise mobility management or mobile device management software.
  - FortiClient (Windows) CLI commands
  - FortiClient (macOS) CLI commands
- For an example of assigning an invitation code for iOS endpoints using Intune, see Enterprise mobility management on page 752.
- Refer to the documentation for your enterprise mobility management or mobile device management software for details on running the above endpoint CLI commands in endpoint deployment scripts.

Considerations

- For new instances created in FortiSASE Feature 25.4.b or later, the MSI version of the FortiClient installer is not available.
- For instances with the Standard, Advanced or Comprehensive remote user subscription and Windows endpoints, the MSI version of the FortiClient installer does not install the Digital Experience Monitoring (DEM) agent on the endpoint. You must use the executable version of the FortiClient installer to install the DEM agent on Windows endpoints.
- Microsoft Defender marks preconfigured FortiClient installers for your FortiSASE instance as coming from an unknown publisher. To request signing a preconfigured installer using your own CA certificate or using the Fortinet CA certificate, open a FortiCare Support ticket.
- For any endpoint installer downloaded, you can proceed to provision your endpoints by doing one of the following:
  - Using a mobile device management (MDM) software suite using the installer
  - Distributing the installer to end users and having them install it on their endpoints
- When using *Download Installer*, whether you decide to provision your endpoints using this installer and an MDM, or distribute this installer to end users, end users must still input the invitation code that you provide for your FortiSASE instance.
- Managed endpoints can be authenticated via SAML SSO when they connect to FortiSASE Management service using an Invitation code ensuring only authenticated users and endpoints can register, thus enhancing security during managed endpoint client onboarding. For more information, see Authenticated onboarding on page 43.
- For FortiClient (macOS) endpoint management connections to be successfully established with FortiSASE Endpoint Management Service, in FortiSASE you must create a policy with deep inspection disabled for Fortinet infrastructure destinations (Fortinet-FortiSASE, Fortinet-FortiCloud, Fortinet-FortiClient.EMS, and Fortinet-FortiSandbox.Cloud) to exempt this traffic.

Allowlisting FortiClient (Windows) processes

The following table identifies the processes in Task Manager that FortiClient (Windows) uses to send outgoing traffic. You will need to allowlist this end traffic for any third-party application firewalls such as Microsoft Defender.

All processes will access UDP/TCP port 53 when they have outgoing traffic for DNS queries.

Name	Purpose	Server	Protocol/Port
ipsec.exe	Remote Access for IPsec VPN	turbo-<tenant>.edge.prod.fortisase.com	UDP 4500 for IPsec over UDP TCP 443 for IPsec over TCP TCP 443 for public IP query
AzureToken.exe	Entra ID Token information verification	login.microsoftonline.com	TCP 443
fcaptmon.exe	Sandbox Detection	aptctrl1.fortinet.com	TCP 443 when querying FortiSASE FortiSandbox server address. Server sends a list of Sandbox server addresses to FortiClient. There are no fixed IP addresses, FQDNs, or ports for these servers. However, the returned port is usually 514.
		Standalone FortiSandbox	TCP 514 for standalone FortiSandbox.
		sfctwf.fortinet.net	TCP 8888 for cloud-based malware protection to safeguard endpoints against high-risk file types from untrusted sources.
FCDBLog.exe	FortiClient log uploading to FortiAnalyzer	FortiSASE analytics and logging services	TCP 514

Name	Purpose	Server	Protocol/Port
FortiESNAC.exe	FortiClient Telemetry	forticlient-emsproxy.forticloud.com	TCP 10443 for installer downloads
		forticlient.forticloud.com forticlient-dispatch.forticloud.com fct-*-8013.forticlient-emsproxy.forticloud.com	TCP 443 for FortiSASE Endpoint Management Service
		LDAP server	TCP 389 for LDAP queries
FortiGuardAgent.exe	Web Filter service	fctguard.fortinet.net fctusguard.fortinet.net fcteuguard.fortinet.net	TCP 443
FortiSSLVPNdaemon.exe	Remote Access for SSL VPN	turbo-<tenant>.edge.prod.fortisase.com	TCP 80 for captive portal detection TCP 443 for SSL VPN tunnel UDP 443 for SSL VPN tunnel using DTLS
FortiSSLVPNsys.exe	SSLVPN authentication	turbo-<tenant>.edge.prod.fortisase.com	TCP 443
FortiTcs.exe	ZTNA service	FortiGate ZTNA application gateway	TCP or UDP, configured according to security posture tagging (ZTNA) rules
FortiVPN.exe	Schedules, controls, and monitors VPN connections	turbo-<tenant>.edge.prod.fortisase.com	ICMP
fortivrs.exe	Use FortiPAM for privilege access management	FortiPAM server	UDP 9191 WebSocket (WS) over TCP 7115 for FortiPAM Extension
FortiWF.exe	Used by Web Filter to access FortiGuard rating server	fgd1.fortigate.com usfgd1.fortigate.com	UDP 8888

Name	Purpose	Server	Protocol/Port
FSSOMA.exe	User authentication via Single sign on mobility agent	FortiAuthenticator	TCP 8001
submitv.exe	Used by antivirus (AV) and FortiClient to submit samples to FortiGuard via SMTP	fortinetvirussubmit.com	TCP 25
update_task.exe	Communication with FortiGuard servers for signature updates	forticlient.fortinet.net myforticlient.fortinet.net usforticlient.fortinet.net	TCP 80
		fctupdate.fortinet.net fctusupdate.fortinet.net fcteuupdate.fortinet.net	TCP 443
vcm2.exe	FortiClient Vulnerability Scan Engine for auto-patch and Windows updates	Microsoft Windows update servers	TCP 443 and TCP 80
FortiAuth.exe	SAML authentication	SAML Identity Provider (IdP) server	TCP 443

Allowlisting FortiClient (MacOS) processes

The following table identifies the processes in Task Manager that FortiClient (MacOS) uses to send outgoing traffic. You will need to allowlist this endpoint traffic for any third-party application firewalls.

Name	Purpose	Server	Protocol and Port
FortiTray	FortiClient System Tray Controller	turbo-<tenant>.edge.prod.fortisase.com	TCP 443
epctrl	FortiClient endpoint control daemon	forticlient-emsproxy.forticloud.com forticlient.forticloud.com	TCP 443
FortiGuardAgent	Web Filter	fctguard.fortinet.net	TCP 443

Name	Purpose	Server	Protocol and Port
		fctusguard.fortinet.net fcteuguard.fortinet.net	
ssoavgent_launchdaemon	FSSO daemon	Windows Active Directory Server	TCP 443
fct_tunnel_ctl	IPsec VPN Service	turbo-<tenant>.edge.prod.fortisase.com	UDP 4500 for IPsec over UDP TCP 443 for IPsec over TCP
fct_tunnel_ctl2	IPsec VPN Service	turbo-<tenant>.edge.prod.fortisase.com	UDP 4500 for IPsec over UDP TCP 443 for IPsec over TCP
com.fortinet.forticlient.macos.vpn.nwextension	SSL VPN Service	turbo-<tenant>.edge.prod.fortisase.com	TCP 443 for SSL VPN tunnel UDP 443 for SSL VPN tunnel using DTLS
fctupdate	FortiClient update tool	fctupdate.fortinet.net fctusupdate.fortinet.net fcteuupdate.fortinet.net	TCP 443
fctupgrade	FortiClient upgrade tool	fctupdate.fortinet.net fctusupdate.fortinet.net fcteuupdate.fortinet.net	TCP 443
ztagent	ZTNA Service	FortiGate ZTNA application gateway	TCP 443, configured according to security posture tagging (ZTNA) rules
ztnafw	ZTNA Service	FortiGate ZTNA application gateway	TCP 443 or UDP 53 for DNS

Name	Purpose	Server	Protocol and Port
fortifs	FortiPAM Service	FortiPAM server	UDP 9191
fctdnsd	DNS Service	DNS servers	TCP 443 or UDP 53 for DNS

Proxy client onboarding

PAC file customization

To ensure Proxy/SWG users can properly authenticate using SAML SSO, administrators must not use the `dnsResolve()` function in custom PAC files.

FortiSASE proxy mode involves configuring and hosting a proxy autoconfiguration (PAC) file for respective endpoints to connect to the FortiSASE gateway.

A PAC file is based on JavaScript and contains rules for the proxy client to follow to route traffic to the proxy server or directly to the internet. For FortiSASE proxy users:

- The proxy client is a web browser or another proxy-aware application.
- The proxy server is the FortiSASE proxy.
- Routing traffic to the proxy uses the FortiSASE proxy as a web proxy.
- Routing traffic directly to the internet bypasses the FortiSASE proxy.

Typically, some web applications require traffic to be routed directly to the internet for specific domains which do not support redirection for security reasons or are required for authentication, such as common SAML identity providers, to load correctly. In these cases, you must customize the PAC file with specific IP addresses and hostnames, and then host the custom PAC file on a server that the endpoints can access.

The workflow for customizing a PAC file hosted on the FortiSASE server is as follows:

1. In FortiSASE, go to *Network* > *Proxy configuration* > *Hosted PAC files* and click *Create* to create a new hosted PAC file.
2. In the PAC file editor interface, add a name, edit the contents of the default PAC file, and click *OK* to save it. See Customizing the PAC file on page 739.
3. In *Network* > *Proxy configuration* > *Hosted PAC files*, select the newly created PAC file and click *Download* > *Download directly* to download it directly or click *Download* > *Copy link* to copy the link for the hosted PAC file.

Each FortiSASE instance supports a maximum of 32 hosted PAC files.

Alternatively, the workflow for customizing a preconfigured PAC file downloaded to a computer is as follows:

1. FortiSASE provides a preconfigured PAC file hosted on the FortiSASE server for use. Download the PAC file to a computer for editing. See Downloading the preconfigured PAC file on page 738.
2. Customize the PAC file in a text editor to exclude certain hosts from being proxied. See Customizing the PAC file on page 739.

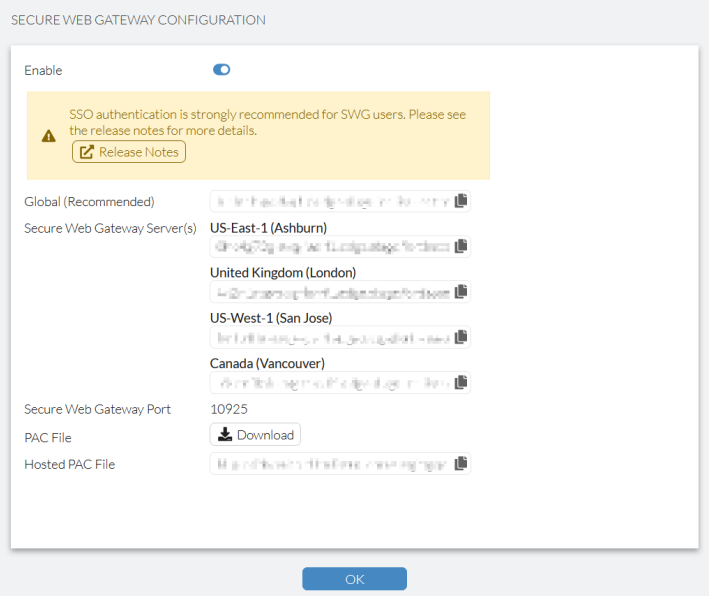
Below is the common workflow for using a customized PAC file:

1. Host the custom PAC file on a server accessible by the endpoints. See Hosting the custom PAC file on page 742.
2. On an endpoint, download and install the proxy certificates provided in the FortiSASE portal. This can be done manually or using a group policy on multiple Windows devices that are part of an Active Directory. See Distribute certificates to Windows devices by using Group Policy.
3. On an endpoint, install and configure the client browser or OS settings to point to the hosted custom PAC file. This can be done manually or using a group policy on multiple Windows devices that are part of an Active Directory. See Distributing PAC file URLs on page 743.

While setting up SSO with AD FS or other custom identity providers (IdP) (except Google, Entra ID, FortiTrustID, or Okta) for agentless users, customizing the PAC file to add IdP URLs to it such that the traffic to IdP URLs is not forwarded to the FortiSASE proxy server and instead goes directly to the internet is mandatory. See Customizing the PAC file on page 739.

Downloading the preconfigured PAC file

The *Network* > *Proxy configuration* page displays the proxy servers, port, and hosted proxy autoconfiguration (PAC) file. You can download the predefined PAC file to customize.



By default, the FortiSASE hosted PAC file contains the global (recommended) URL and the proxy port specific to your instance. This global (recommended) URL automatically directs users to the closest geographical location for all browsers and proxy-aware applications. For example:

```
function FindProxyForURL(url, host) {
    return "PROXY turbo-hqwdvq17.edge.prod.fortisase.com:10925; DIRECT";
}
```

This simple PAC file specifies that the web request should be sent through the proxy server turbo-hqwdvq17.edge.prod.fortisase.com on TCP port 10925 and if the proxy does not respond to this request, the browser sends the web request directly to the internet without using the proxy.

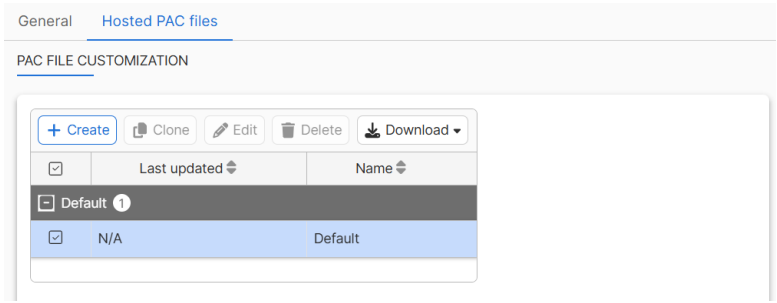
Customizing the PAC file

To ensure Proxy/SWG users can properly authenticate using SAML SSO, administrators must not use the `dnsResolve()` function in custom PAC files.

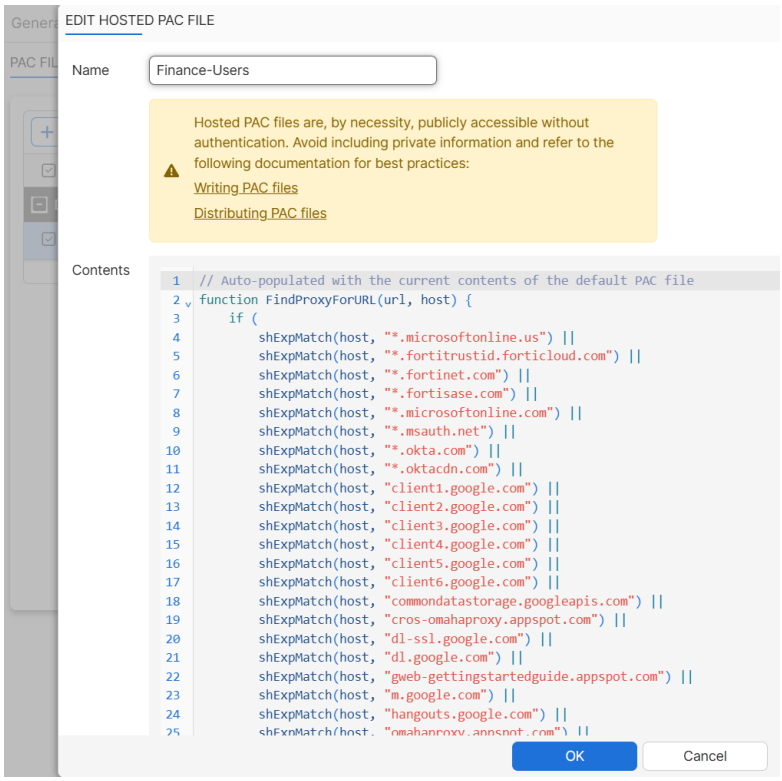
This example customizes the PAC file to exclude common external URLs and networks from being forwarded to the FortiSASE proxy server, which allows specific domains which do not support redirection for security reasons or are required for authentication, such as common SAML identity providers, to load correctly.

Typically, you can simply customize a custom PAC file hosted by FortiSASE directly in the FortiSASE portal as follows:

1. Go *Network* > *Proxy configuration* > *Hosted PAC files*.



2. Either click *Create* to create a new hosted PAC file or select an existing hosted PAC file and click *Edit* to edit it.



3. Edit the contents as needed and click *OK* to save the changes.

Each FortiSASE instance supports a maximum of 32 hosted PAC files.

Alternatively, you can also choose to download and edit the preconfigured PAC file to create a custom PAC file that you will host externally. In this case, you must replace the final `return` statement at the end of the PAC file with the corresponding proxy URL and port listed in your preconfigured PAC file in the previous step Downloading the preconfigured PAC file on page 738.

Below is an example of a FortiSASE-hosted PAC file for an instance using secure explicit proxy, as distinguished by the HTTPS in the `return` value instead of PROXY.

```
function FindProxyForURL(url, host) {
       if (
                shExpMatch(host, "*.microsoftonline.us") ||
                shExpMatch(host, "*.fortitrustid.forticloud.com") ||
                shExpMatch(host, "*.fortinet.com") ||
                shExpMatch(host, "*.fortisase.com") ||
                shExpMatch(host, "*.microsoftonline.com") ||
                shExpMatch(host, "*.msauth.net") ||
                shExpMatch(host, "*.okta.com") ||
                shExpMatch(host, "*.oktacdn.com") ||
                shExpMatch(host, "client1.google.com") ||
                shExpMatch(host, "client2.google.com") ||
                shExpMatch(host, "client3.google.com") ||
                shExpMatch(host, "client4.google.com") ||
                shExpMatch(host, "client5.google.com") ||
                shExpMatch(host, "client6.google.com") ||
                shExpMatch(host, "commondatastorage.googleapis.com") ||
```

```
            shExpMatch(host, "cros-omahaproxy.appspot.com") ||
            shExpMatch(host, "dl-ssl.google.com") ||
            shExpMatch(host, "dl.google.com") ||
            shExpMatch(host, "gweb-gettingstartedguide.appspot.com") ||
            shExpMatch(host, "m.google.com") ||
            shExpMatch(host, "hangouts.google.com") ||
            shExpMatch(host, "omahaproxy.appspot.com") ||
            shExpMatch(host, "pack.google.com") ||
            shExpMatch(host, "safebrowsing-cache.google.com") ||
            shExpMatch(host, "safebrowsing.google.com") ||
            shExpMatch(host, "ssl.gstatic.com") ||
            shExpMatch(host, "storage.googleapis.com") ||
            shExpMatch(host, "tools.google.com") ||
            shExpMatch(host, "www.googleapis.com") ||
            shExpMatch(host, "*.gstatic.com") ||
            shExpMatch(host, "play.google.com") ||
            shExpMatch(host, "mtalk.google.com") ||
            shExpMatch(host, "accounts.google.com") ||
            shExpMatch(host, "aadcdn.msftauthimages.net") ||
            shExpMatch(host, "aadcdn.msftauth.net") ||
            shExpMatch(host, "*.auth.microsoft.com") ||
            shExpMatch(host, "*.lync.com") ||
            shExpMatch(host, "*.mail.protection.outlook.com") ||
            shExpMatch(host, "*.msftidentity.com") ||
            shExpMatch(host, "*.msidentity.com") ||
            shExpMatch(host, "*.mx.microsoft") ||
            shExpMatch(host, "*.officeapps.live.com") ||
            shExpMatch(host, "*.online.office.com") ||
            shExpMatch(host, "*.protection.office.com") ||
            shExpMatch(host, "*.protection.outlook.com") ||
            shExpMatch(host, "*.security.microsoft.com") ||
            shExpMatch(host, "*.sharepoint.com") ||
            shExpMatch(host, "*.teams.cloud.microsoft") ||
            shExpMatch(host, "*.teams.microsoft.com") ||
            shExpMatch(host, "*.teams.live.com") ||
            shExpMatch(host, "*.msauth.net") ||
            shExpMatch(host, "account.activedirectory.windowsazure.com") ||
            shExpMatch(host, "accounts.accesscontrol.windows.net") ||
            shExpMatch(host, "autologon.microsoftazuread-sso.com") ||
            shExpMatch(host, "clientconfig.microsoftonline-p.net") ||
            shExpMatch(host, "compliance.microsoft.com") ||
            shExpMatch(host, "defender.microsoft.com") ||
            shExpMatch(host, "graph.microsoft.com") ||
            shExpMatch(host, "graph.windows.net") ||
            shExpMatch(host, "login.microsoft.com") ||
            shExpMatch(host, "login.microsoftonline-p.com") ||
            shExpMatch(host, "login.windows.net") ||
            shExpMatch(host, "nexus.microsoftonline-p.com") ||
            shExpMatch(host, "office.live.com") ||
            shExpMatch(host, "outlook.cloud.microsoft") ||
            shExpMatch(host, "outlook.office.com") ||
            shExpMatch(host, "outlook.office365.com") ||
```

```
                shExpMatch(host, "protection.office.com") ||
                shExpMatch(host, "purview.microsoft.com") ||
                shExpMatch(host, "security.microsoft.com") ||
                shExpMatch(host, "smtp.office365.com") ||
                shExpMatch(host, "teams.cloud.microsoft") ||
                shExpMatch(host, "teams.live.com") ||
                shExpMatch(host, "aadcdn.msftauthimages.net") ||
                shExpMatch(host, "teams.microsoft.com") ||
                shExpMatch(host, "*teams.live.com") ||
                shExpMatch(host, "*data.microsoft.com") ||
                shExpMatch(host, "*onecdn.static.microsoft.com") ||
                shExpMatch(host, "*cdn.office.net")
        ) {
                return "DIRECT";
        }
        return "HTTPS turbo-hqwdvq17.edge.prod.fortisase.com:9443; DIRECT";
}
```

For example, add new URL to exempt from being proxied, such as “example.com”, go to the end of the `if` statement see the added script in **bold**:

```
function FindProxyForURL(url, host) {
        if (
                shExpMatch(host, "*.microsoftonline.us") ||
                shExpMatch(host, "*.fortitrustid.forticloud.com") ||
                shExpMatch(host, "*.fortinet.com") ||
                shExpMatch(host, "*.fortisase.com") ||
        ...
                shExpMatch(host, "*onecdn.static.microsoft.com") ||
                shExpMatch(host, "*cdn.office.net") ||
                shExpMatch(host, “*.example.com)
        ) {
                return "DIRECT";
        }
...
```

Hosting the custom PAC file

Typically, once you have modified the custom proxy autoconfiguration (PAC) file you will not need to externally host it since you can use the FortiSASE PAC file editor to edit custom PAC files hosted by FortiSASE.

Alternatively, you can host the custom PAC file on a web server (such as Amazon S3) that is externally accessible by your remote users. The web server must be configured to allow .PAC file extensions to be downloaded and specified using the MIME type application/x-ns-proxy-autoconfig.

Whether you use the FortiSASE hosted PAC file or an externally hosted one, the PAC file does not require user authentication to access. However, any user that is pointing to the PAC file will be subject to authentication by FortiSASE when it accesses the internet.

Additional endpoint configuration steps

To complete the workflow for using a custom PAC file, the end user must download and install the proxy certificate on the endpoint and point the endpoint's web browsers to this hosted PAC file.

For details on downloading and installing the proxy certificate on an endpoint, refer to the steps in Certificate installation on page 743.

For details on configuring the endpoint to use the custom hosted PAC file, refer to the steps in Proxy configuration on page 744.

Distributing PAC file URLs

You can obtain PAC file URLs for FortiSASE hosted PAC files as follows:

In FortiSASE, go to *Network* > *Proxy configuration* > *Hosted PAC files*.

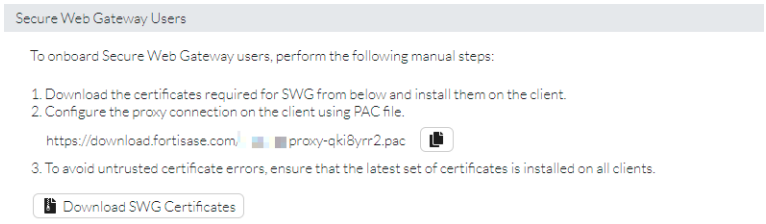
Select the desired PAC file and click *Download* > *Copy link* to copy the link for the hosted PAC file.

Once you have the PAC file URL, you can distribute it using a group policy on multiple Windows devices that are part of an Active Directory. See How to configure proxy server settings in Internet Explorer or by using Group Policy.

Certificate installation

When users connect to FortiSASE in proxy mode, FortiSASE proxies traffic from the client. While being proxied, connections using secure protocols like HTTPS have their certificates replaced and signed by FortiSASE. To avoid seeing warnings and errors, the client must trust the signing certificate authority (CA) and have a valid certificate chain back to the root CA. Therefore, installing FortiSASE's CA certificate on the client's trusted certificate store is important.

You should provide users with the required CA certificate during onboarding. In proxy agentless mode, when you onboard users from the GUI, download the proxy certificates package that appears at the end of the *Onboarding proxy users* instructions. You can also find this on the right side of the *Network* > *Proxy configuration* page.



For instructions demonstrate how to install certificates on various operating systems, see Installing a certificate for deep inspection mode on page 317.

Proxy configuration

To connect to FortiSASE in proxy mode, each endpoint client must configure proxy settings within its network or browser settings to point to FortiSASE's servers. You can configure this individually on the endpoint or, if you are using an enterprise management system, push it out to managed endpoints centrally.

You should provide users one of the following during the user onboarding process:

- URL to the hosted proxy autoconfiguration (PAC) file
- Proxy server addresses and port if users are to configure proxy settings manually.

From the *Network* > *Proxy configuration* page, make note of the following information:

Field	Description
Global (Recommended)	Global FortiSASE server address for your instance.
Proxy server(s)	Lists address of each individual regional FortiSASE server for your instance.
Proxy port	Port that client should connect to in their proxy settings.
PAC File	Static copy of the PAC file, which you can customize and rehost on your server.
Hosted PAC File	Address of the PAC file hosted on the FortiSASE server.

See Proxy configuration on page 285.

Users are expected to have installed the FortiSASE certificate authority certificate on their devices. See Certificate installation on page 743.

Proxy settings on endpoint clients can differ between operating systems (OS) and browsers. While the following examples demonstrate the configuration for the selected OSes, refer to your OS or browser for complete instructions on configuring proxy settings.

- Windows on page 744
- macOS on page 745
- Chrome OS on page 746
- Managed Chromebook on page 748

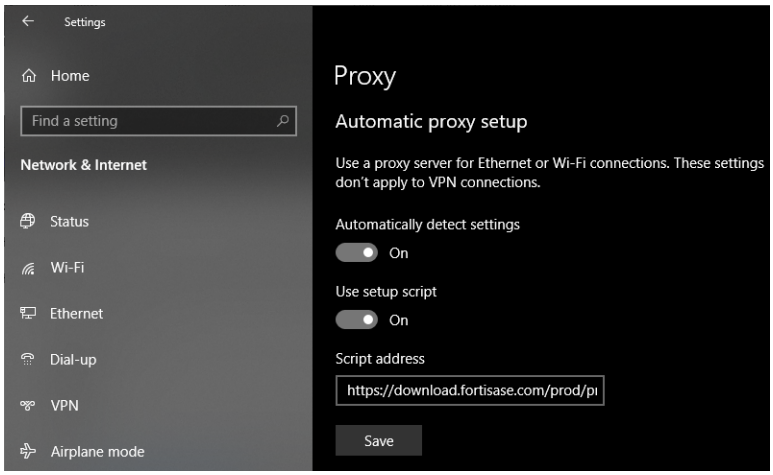
Windows

The end user can configure proxy settings at the operating system (OS) level or in a browser. When you configure proxy settings at the OS level, Windows applies them to all installed browsers. The following gives instructions for configuring proxy settings at the OS level on a Windows 10 device.

To configure Windows 10 to use the FortiSASE proxy server:

1. In Windows, go to *Windows Settings* > *System* > *Proxy Settings*.
2. Enable *Use setup script*.

3. In the *Script address* field, enter the *Hosted PAC File* URL.



4. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

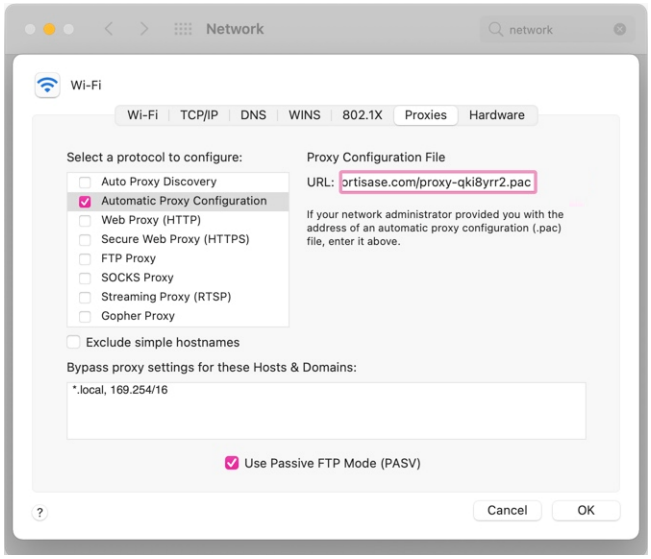
macOS

This example demonstrates manually configuring proxy settings on macOS. See also Change proxy settings in Network preferences on Mac.

To manually configure proxy settings on a macOS endpoint:

1. Go to the *Apple menu* > *System Preferences* > *Network*.
2. In the list, select the Network service. For example, you may select your connected wireless SSID.
3. Click *Advanced*.
4. On the *Proxies* tab, select the protocol to configure. Enable *Automatic Proxy Configuration*, then enter the URL to your hosted PAC file.

5. Click *OK*, then apply to apply the changes.



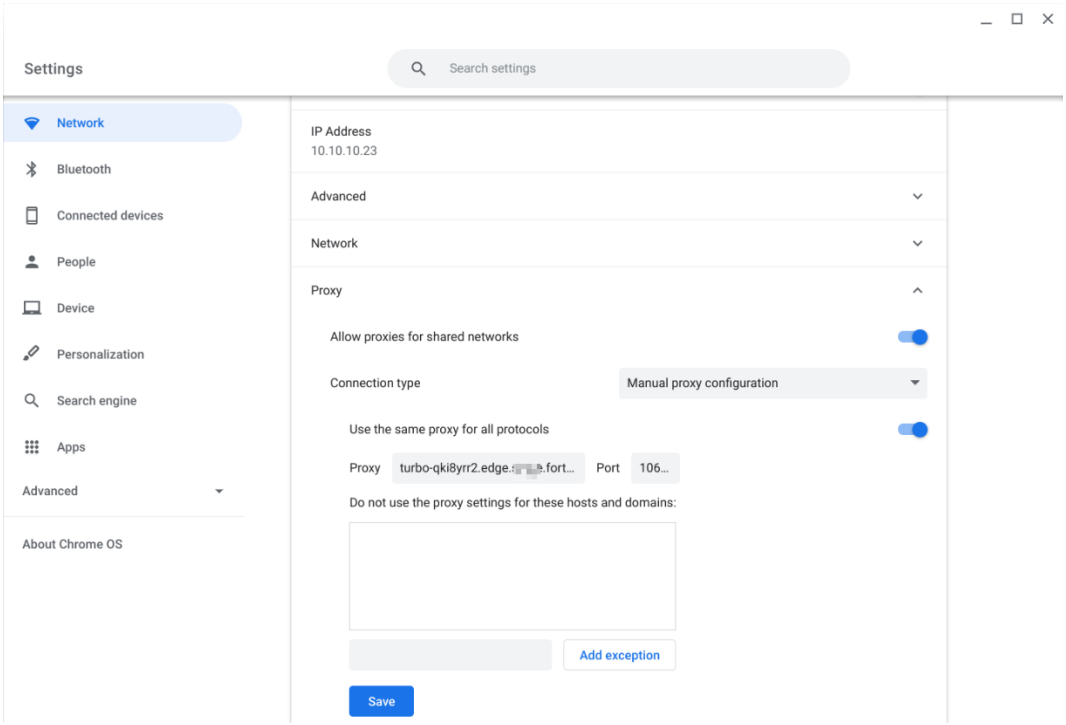
6. The next time that the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE user credentials in the prompt to authenticate.

Chrome OS

To configure proxy as a system-wide setting:

1. Open the Launcher, and search for *Settings*.
2. Click *Network* on the left menu. Then select your Wireless Network SSID and click the right arrow to expand.
3. Scroll to the bottom and expand the proxy settings.
4. For *Connection type*, select one of the following:
   a. Select *Automatic proxy configuration*. This is the recommended method. Point the *Autoconfiguration URL* to the FortiSASE-hosted PAC file.
   b. To configure manual proxy configuration, do the following:
      i. Select *Manual proxy configuration*.
      ii. Enable *Use the same proxy for all protocols*.
      iii. Enter the proxy server address, and the proxy port that your administrator provided. You can select the global proxy or the server closest to you.

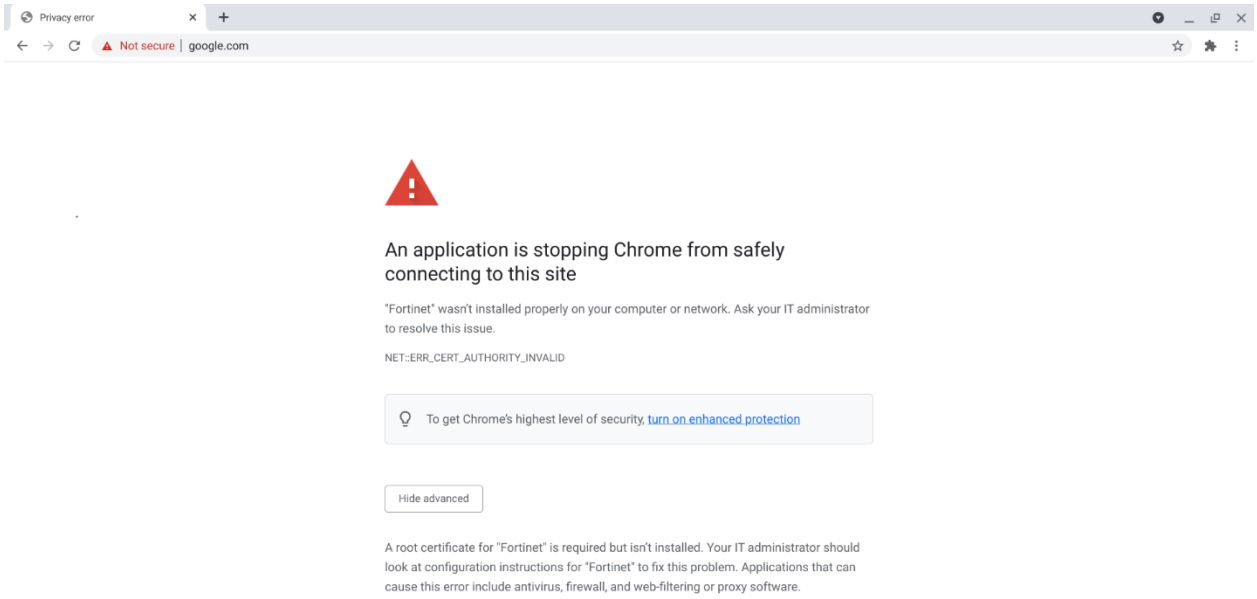
iv. Click *Save*.



If issues arise with some websites using SOCKS, you can work around this by disabling *Use the same proxy for all protocols*. Then only define the proxy server address for HTTP proxy and secure HTTP proxy.

5. On a successful connection, your browser prompts you to authenticate. Enter your user credentials to authenticate to FortiSASFortiSASE and continue browsing the web.

If you receive a warning message from Chrome preventing you to go further, you must disable your proxy settings, and install the FortiSASE certificate authority certificate before reenabling proxy.



Managed Chromebook

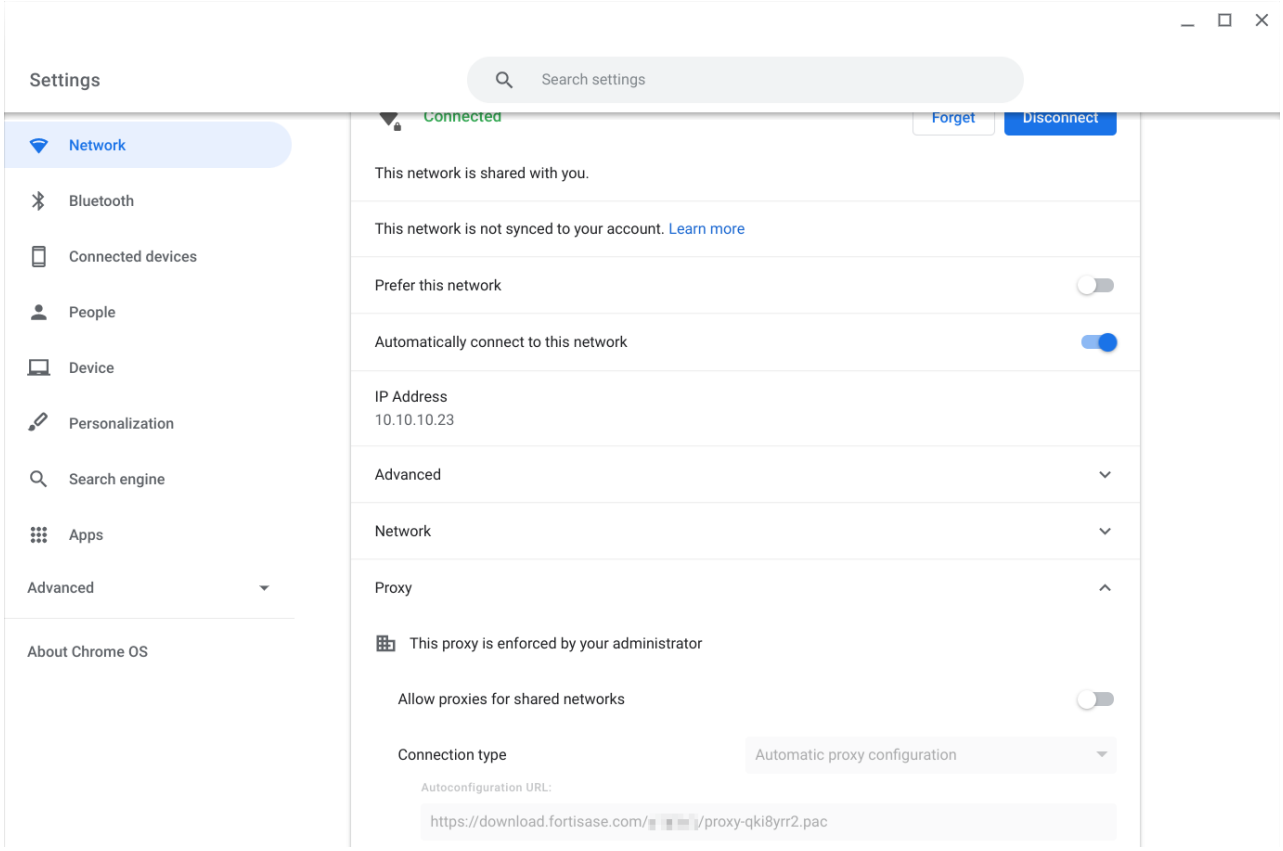
If your organization manages Chromebooks using the Google Admin console, you can centrally configure proxy settings on the Admin console and distribute them to each managed Chromebook.

To configure proxy as a system-wide setting on Google Admin Console:

1. On the Google Admin console, go to *Device* > *Chrome* > *Settings* > *Users & Browsers*..
2. Select the organizational unit in which to apply these settings.
3. Under *User and Browser Settings*, filter for the keyword `Proxy`. The *Network* section appears.
4. For *Proxy mode*, use one of the following options:
   a. Select *Always use the proxy auto-config specified below*. Enter FortiSASE's hosted PAC file address. Save.
   b. Select *Always use the proxy specified below*. Enter the proxy server URL in the format <proxy server address>:<proxy port>. Save.

To verify proxy settings are configured on the managed Chromebook:

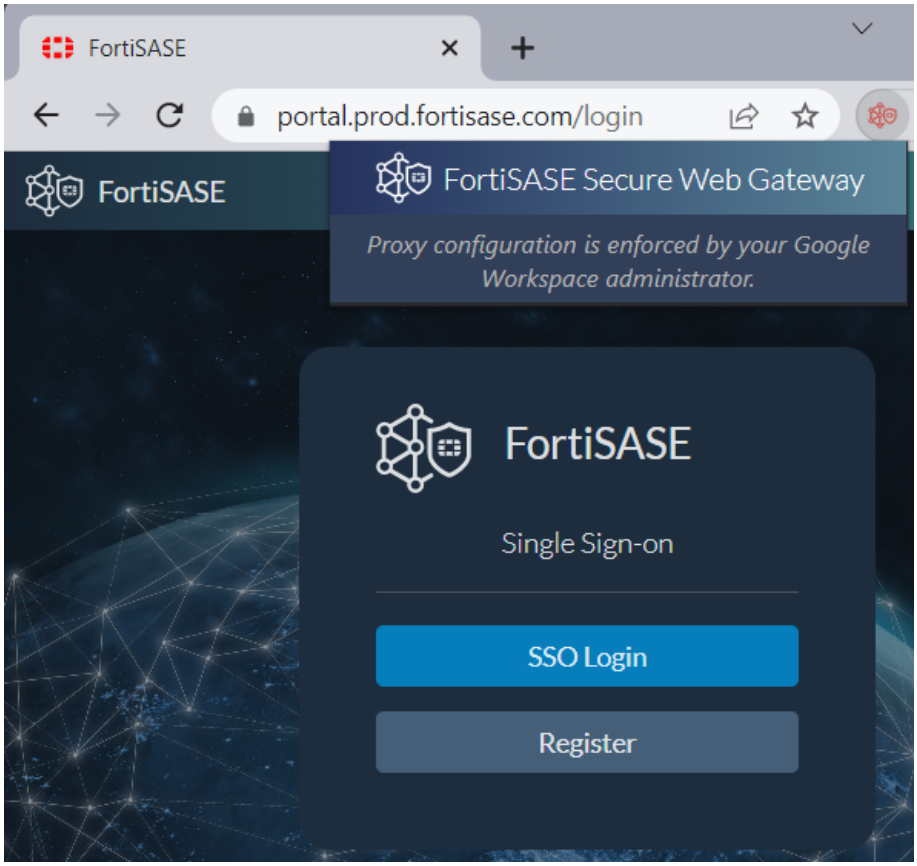
1. Open the Launcher and search for Settings.
2. Click *Network* on the left menu. Then select your Wireless Network SSID and click the right arrow to expand.
3. Scroll to the bottom and expand the proxy settings. The settings pushed from the Google Admin Console appear with an icon and warning that your administrator is enforcing this setting.



Proxy Chrome extension and Chromebook support

FortiSASE supports a Chrome extension that allows enforcing FortiSASE proxy connectivity for selected endpoints with the Chrome browser installed, including Chromebooks, based on the endpoint operating system (OS) and the corresponding extension policy that the Google Workspace administrator configured.

You can download the FortiSASE Secure Web Gateway Chrome extension from the Google Chrome Web store and add it to the Chrome web browser.



This extension relies on the following features being configured in FortiSASE:

- Proxy single sign-on
- Proxy configuration

The extension also requires that the user has already downloaded and installed the proxy certificates to the device certificate store as Certificate installation on page 743 describes. Alternatively, you can use Google Workspace to install certificates on Chromebooks as Add and assign digital certificates for managed devices describes.

Since this extension is not installed in Chrome incognito mode, the administrator should disable incognito mode in Google Workspace.

This extension allows you to configure the following settings on an endpoint through Google workspace:

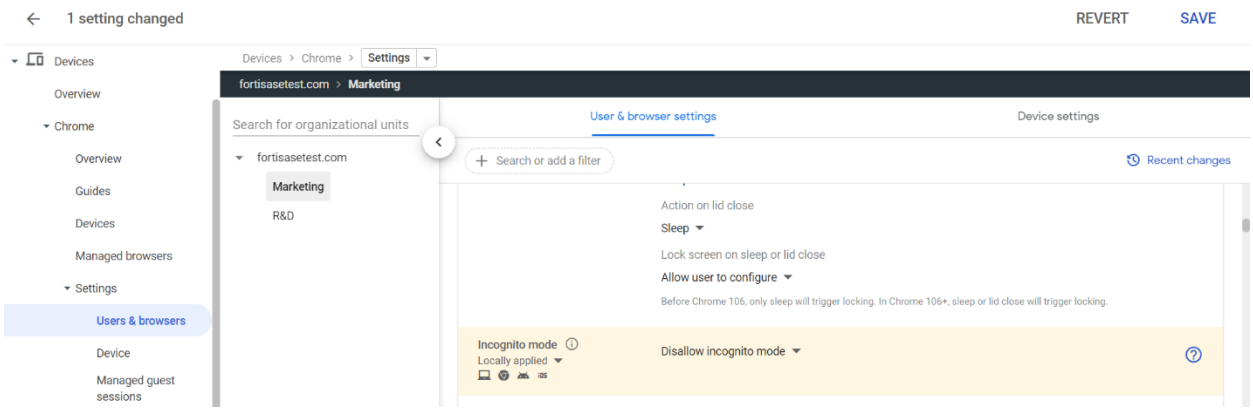
- Default or custom hosted PAC file URL
- User ability to view PAC file URL within the extension

- Configuration of supported platforms (ChromeOS, Linux, macOS, and Windows) where proxy is enforced

To disable incognito mode in Google Workspace:

Since this extension is not installed in incognito mode, proxy policies are not enforced when using incognito mode. The Google Workspace administrator must disallow incognito mode to ensure that proxy is always enforced on the Chromebook and other devices with managed Chrome browsers.

1. Go to *Devices* > *Chrome* > *Settings* > *Users & browsers*.
2. Select the desired organizational unit (OU).
3. Scroll to *Security* > *Incognito mode*.
4. From the dropdown menu, select *Disallow incognito mode*.
5. Click *Save*.



To configure the extension policy for FortiSASE proxy Chrome extension:

You can apply the FortiSASE proxy extension to one or more user OUs within Google Workspace. All users assigned within an OU that the FortiSASE proxy extension is applied to have the extension installed and proxy enforced on their Chromebook and Chrome browser.

1. In the Google Admin console, go to *Devices* > *Chrome* > *Apps & extensions* > *Users & browsers*.
2. Select the desired OU to install and enforce the FortiSASE proxy extension.
3. Add the Chrome extension to the OU by clicking the + button on the bottom right, clicking *Chrome app or extension by ID*, and searching using the ID aecejhdejcnfihadbfidmndehobfdpcc.
4. Select the *FortiSASE Secure Web Gateway extension* to push to Chromebooks and devices with managed Chrome browsers.
5. Configure the policy using the following parameters:

Parameter	Description
`pacFileUrl`	PAC file that the extension will enforce. Configure one of the following: • Default hosted PAC file link from FortiSASE in *Network* > *Proxy configuration*. See Proxy configuration on page 285. • Custom hosted PAC file link from a server accessible to endpoints. See PAC file customization on page 737.
`showProxyInfo`	Possible values: `false` or `true`.

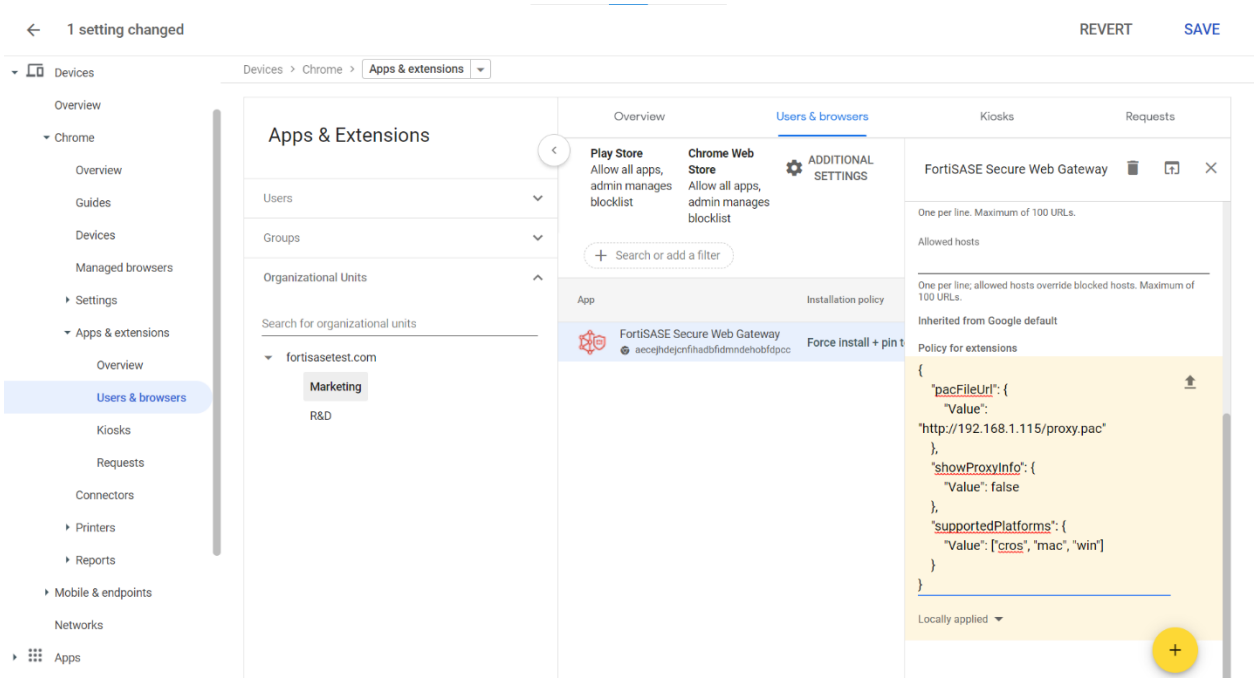
Parameter	Description
	• Setting this to `false` hides the PAC file URL from the extension. • Setting this value to `true` makes the PAC file URL visible to the extension.
`supportedPlatforms`	Possible values include `cros`, `linux`, `mac`, and `win` to specify ChromeOS (Chromebook), Linux, macOS, and Windows, respectively. To exempt a device from proxy enforcement, you can set one of these options: • Remove the device OS from the `supportedPlatforms` array • Set `pacFileUrl` to an empty string • Remove the `pacFileUrl` key-value pair from the policy configuration

6. Click *Save*.

Following is an example extension policy configuration using a custom PAC file hosted on a LAN server with the PAC file URL hidden from extension and the extension applied to ChromeOS, macOS, and Windows devices:

```
{
    "pacFileUrl": {
        "Value": "https://192.168.1.115/proxy.pac"
    },
    "showProxyInfo": {
        "Value": false
    },
    "supportedPlatforms": {
       "Value": ["cros", "mac", "win"]
    }
}
```

The following shows the FortiSASE proxy extension and example extension policy applied to users within the Marketing OU:



To verify the policy has been enforced on the device with the extension installed:

On the Chromebook or device with Chrome browser installed, go to chrome://policy from the Chrome browser to verify the aforementioned example policy has been enforced on the Chromebook or device with managed Chrome browser:

FortiSASE Secure Web Gateway

Policy name	Policy value	Source	Applies to	Level	Status	
pacFileUrl	https://192.168.1.115/proxy.pac	Cloud	Machine	Mandatory	OK, Superseding	Show more
showProxyInfo	false	Cloud	Machine	Mandatory	OK, Superseding	Show more
supportedPlatforms	["cros","mac","win"]	Cloud	Machine	Mandatory	OK, Superseding	Show more

Enterprise mobility management

FortiClient on different platforms supports integration with enterprise mobility management or mobile device management software. You can use this software to onboard endpoints to successfully connect to and be managed by FortiSASE.

Configuring Microsoft Intune integration with FortiClient (iOS)

You can find details for configuring Microsoft Intune integration with FortiClient (iOS) in Configuring Microsoft Intune integration to allow FortiClient (iOS) to connect to EMS.

Configuring the FortiSASE invitation code

Since FortiSASE uses an invitation code instead of a direct IP address or hostname and port, ensure that you configure `invitation_code` in one of the following locations in Intune:

- In the *Create app configuration policy* window on the *Settings* tab
- For an existing configuration policy, click *Properties* and check under *Settings*.

Deploying trusted certificates

When FortiSASE security components are configured to use SSL deep inspection, the certificate authority (CA) certificate is automatically installed on desktop FortiClient endpoints. However, for mobile endpoints such as Apple devices running FortiClient (iOS), you must use enterprise mobility management software to install CA certificates.

You can find details on deploying a trusted root certificate such as the CA certificate configured on FortiSASE for SSL deep inspection in Trusted root certificate profiles for Microsoft Intune.

Deploying FortiClient (macOS) using Intune

The following topics provide information about deploying FortiClient (macOS) using Microsoft Intune mobile device management (MDM). These instructions assume that you have already completed some configuration steps, such as creating an Apple MDM push certificate, enrolling devices to Intune, and creating and assigning members to the desired group. For instructions on these topics, see macOS.

Configuring the configuration profile

When deploying FortiClient (macOS) without Intune configuration profiles, the endpoint displays the following prompts to the user:

- To grant network access to the following extensions:
  - Web Filter
  - VPN
  - Proxy
- To grant full disk access to FortiClient processes
- To grant FortiTray permission to load the following extensions. This occurs if the user has not previously installed FortiClient on the macOS device:
  - com.fortinet.forticlient.macos.webfilter
  - com.fortinet.forticlient.macos.vpn.nwextension
  - com.fortinet.forticlient.macos.proxy

Silently deploying FortiClient (macOS) so that the user does not view these prompts requires an Intune custom configuration profile that allows all prompts. This single custom configuration profile grants the following:

- Full disk access for FortiClient processes:
  - FortiClient
  - fmon2
  - fcaptmon

    - fctservctl2
- Permission for loading system extensions
- Network access for the following:
    - VPN
    - Web Filter
    - Proxy
- Permission for adding zero trust network access (ZTNA) root CA certificate to the keychain

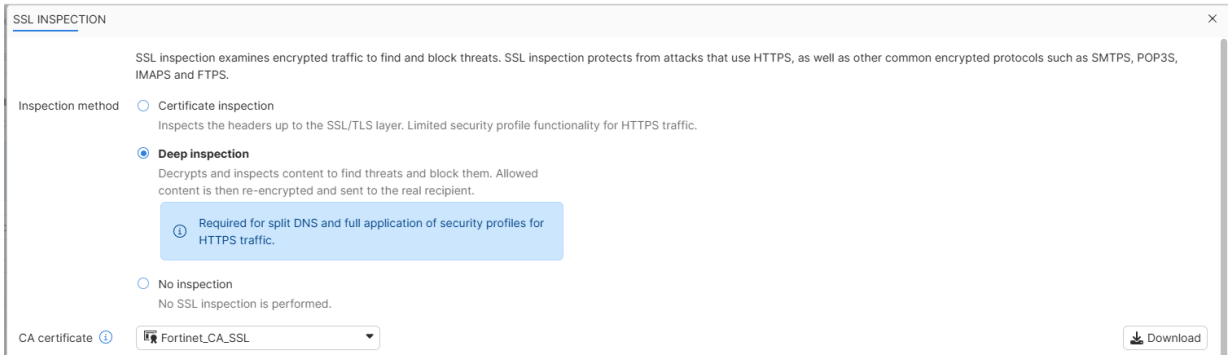
You can silence certificate prompts in one of the following ways:

- Add certificate content to the configuration profile between `<data>` and `</data>` as To grant the permissions: on page 754 describes
- Directly upload the certificate as a trusted certificate in the Intune configuration profiles after changing the extension type

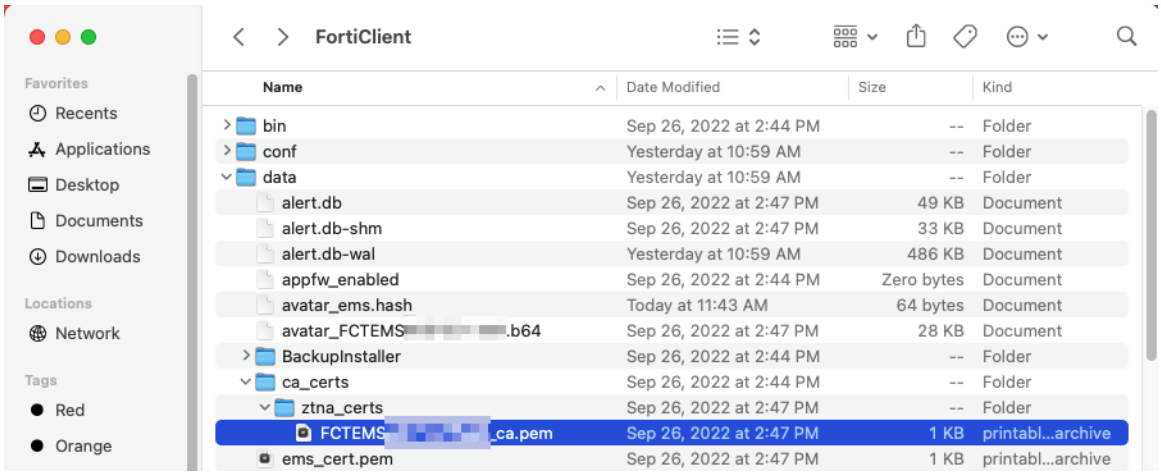
This document provides instructions for the first method. For the second method, see To directly upload the ZTNA certificate as trusted certificate:.

To grant the permissions:

1. Download the FortiClient_Configuration_Profile.Intune.mobileconfig sample configuration profile file:
    a. Go to Fortinet Service & Support > Support > Firmware Download.
    b. From the *Select Product* dropdown list, select *FortiClientMac*.
    c. On the *Download* tab, go to *Mac > v7.00 > 7.2 > 7.2.14*
    d. Download the FortiClient_Configuration_Profile.Intune.mobileconfig sample configuration profile file.
2. Prepare the configuration profile with the FortiSASE root and ZTNA root CA certificates:
    a. To obtain the FortiSASE root certificate, in FortiSASE, go to *Security*.
    b. Click *Configure SSL*.
    c. Beside the *CA certificate* value, click *Download*.



    d. To obtain the ZTNA root CA certificate:
        i. On a macOS endpoint where FortiClient (7.2.0-7.2.4) is connected to FortiSASE, go to `/Library/Application Support/Fortinet/FortiClient/data/ca_certs/ztna_certs`.
        ii. On a macOS endpoint where FortiClient (7.2.5 or later, or 7.4.0 or later) is connected to FortiSASE, go to `/private/etc/Fortinet/FortiClient/data/ca_certs/ztna_certs`.



e. In a text editor, open the FortiSASE root certificate and ZTNA root CA certificate.

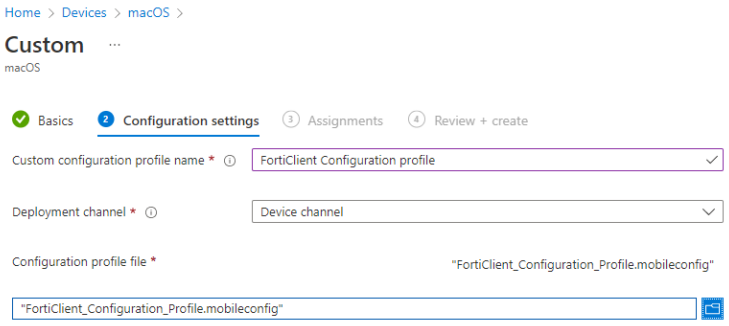
f. Copy the certificates content to an accessible location.

g. Open the FortiClient_Configuration_Profile.Intune.mobileconfig file in a text editor. The file contains two entries for `PayloadCertificateFileName`. You will leave the first entry, for `FortiClient DNS Root.cer`, as-is. You will overwrite the second entry, for `EMS_ZTNA.cer`, with the following content. Copy and paste the following content in to the profile, overwriting the `EMS_ZTNA.cer` entry. Replace `<!-- Add your FortiSASE root certificate here -->` and `<!-- Add your FortiSASE ZTNA certificate here -->` in the sample with the FortiSASE root certificate content and ZTNA root CA certificate, respectively, that you copied in step f:

```
<dict>
	<key>PayloadCertificateFileName</key>
	<string>FortiSASE_Root.cer</string>
	<key>PayloadContent</key>
	<data>
	<!-- Add your FortiSASE root certificate here -->
	</data>
	<key>PayloadDescription</key>
	<string>Adds a CA root certificate</string>
	<key>PayloadDisplayName</key>
	<string>FortiSASE Root Certificate for SSL Decryption</string>
	<key>PayloadIdentifier</key>
	<string>com.apple.security.root.1255DA5E-C9F1-4FBF-9967-4000DDF1DFC5</string>
	<key>PayloadType</key>
	<string>com.apple.security.root</string>
	<key>PayloadUUID</key>
	<string>1255DA5E-C9F1-4FBF-9967-4000DDF1DFC5</string>
	<key>PayloadVersion</key>
	<integer>1</integer>
</dict>
<dict>
	<key>PayloadCertificateFileName</key>
	<string>FortiSASE_ZTNA.cer</string>
	<key>PayloadContent</key>
	<data>
	<!-- Add your FortiSASE ZTNA certificate here -->
	</data>
```

```
        <key>PayloadDescription</key>
        <string>Adds a CA root certificate</string>
        <key>PayloadDisplayName</key>
        <string>FortiSASE ZTNA Certificate</string>
        <key>PayloadIdentifier</key>
        <string>com.apple.security.root.1255DA5E-C9F1-4FBF-9967-4000DDF1DFC6</string>
        <key>PayloadType</key>
        <string>com.apple.security.root</string>
        <key>PayloadUUID</key>
        <string>1255DA5E-C9F1-4FBF-9967-4000DDF1DFC6</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
</dict>
```

3. Sign in to the Microsoft Endpoint Manager Admin Center.
4. Go to *Devices* > *macOS* > *Configuration Profiles* > *Create Profile* > *Profile Type* > *Templates* > *Custom* and click *Create*.
5. Enter the profile name and description as desired, then click *Next*.
6. Under *Configuration settings*, from the *Deployment channel* dropdown list, select *Device channel*.
7. In the *Configuration profile file* field, import the FortiClient_Configuration_Profile.Intune.mobileconfig sample configuration profile file. The text field shows the sample XML configuration in the file. Click *Next*.



8. Assign this profile to the macOS device group by selecting *Add Groups* under *Included Groups*. Click *Next*.
9. Review the summary, then click *Create*. Intune creates the custom profile to grant access to the Web Filter and VPN extensions.

Deploying FortiClient using a shell script

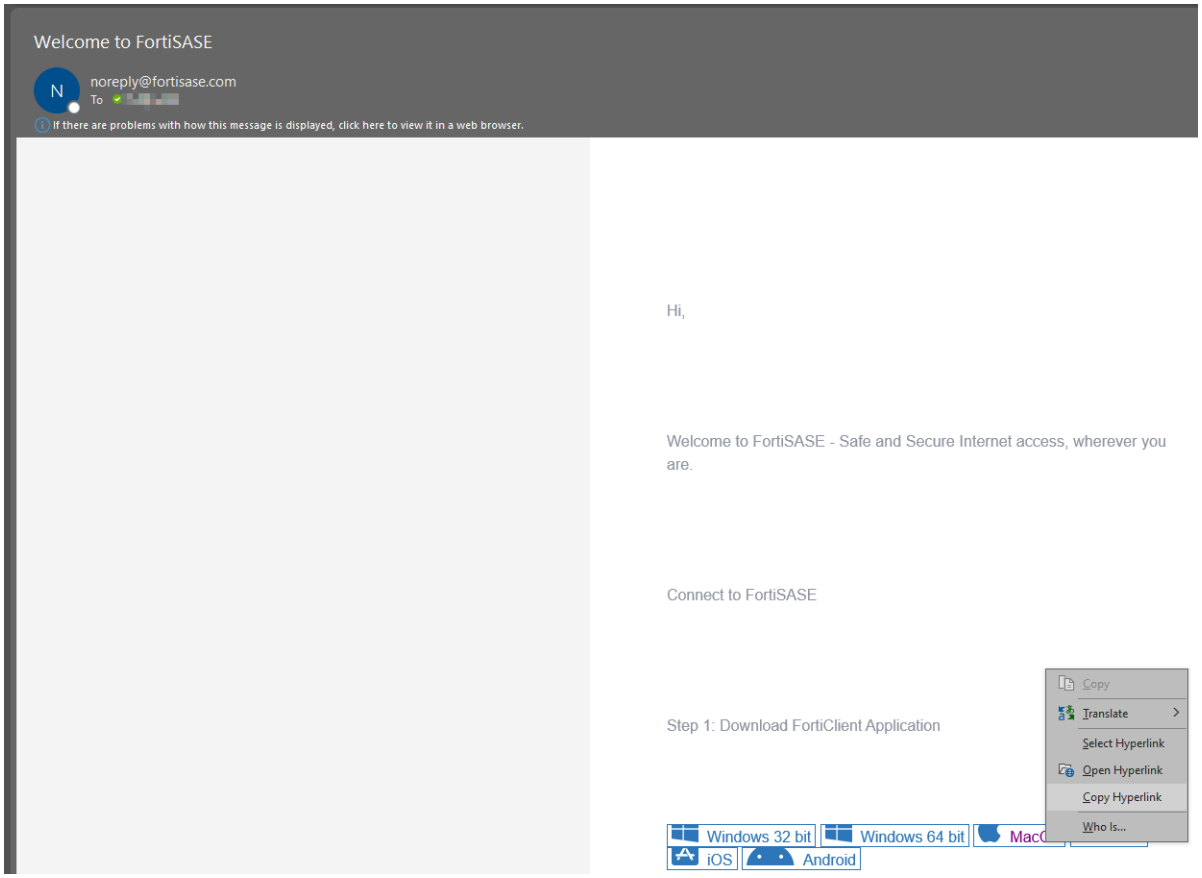
With Intune, you can silently deploy FortiClient to macOS devices that have any user accounts (administrator and non-administrator user accounts) without requiring user interaction. Following this method to deploy FortiClient to macOS devices is recommended, as it is simple and effective. For this procedure, all macOS devices should meet the following prerequisites:

- Running macOS High Sierra (version 10.13) or a later version
- Managed by Intune
- Shell scripts begin with `#!` and are in a valid location, such as `#!/bin/sh` or `#!/usr/bin/env zsh`.
- Command line interpreters for the applicable shells are installed.

After verifying that all macOS devices meet the prerequisites, do the following.

To deploy FortiClient using a shell script:

1. Modify the script file:
   a. On a test macOS device, download the given FortiClient deployment shell script .sh file.
   b. Open a terminal, go to the downloaded script file, and open it.
   c. Modify the `weburl` value to your FortiClient (macOS) installer URL. Obtain the installer URL from the invitation email that FortiSASE sends to end users. Configure an invitation email using the *FortiClient Installer > Send link to users* option in *Onboard Users* configuring only yourself as a recipient. See Managed endpoint client onboarding on page 731. After receiving the invitation email, right-click *MacOS* and select *Copy Hyperlink*.



   Paste the link as the `weburl` value. For example, you may configure your weburl as `weburl="https://example.ems.forticlient.forticloud.com/installers/default/default_fortisase_installer/FortiClient_7.2.6.dmg"`.
   d. Modify the `FortiClient_Installerversion` value in the script file based on your FortiClient installer version. For example, change the value from `FortiClient_Installerversion=<Your FortiClient Installer version>` to `FortiClient_Installerversion=”7060208”` if the FortiClient version is 7.0.6.0208. Enter the version number without periods.
   e. Modify the values `av`, `af`, `sb`, `sra`, `sso`, `vs`, `wf`, `ztna` values as follows. You must modify these values as per the sample below, as you must ensure to only enable FortiClient features that are available when using FortiClient with FortiSASE:

```
av="1"  # Enter 0 when Malware feature is disabled in the FortiClient installer
af="0" # Enter 0 when Application Firewall  feature is disabled in the FortiClient
```

```
installer
sb="0" # Enter 0 when Advanced Persistent Threat (APT) components feature is disabled in
the FortiClient installer
sra="1"        # Enter 0 when Secure Access Architecture Components feature is disabled in the
FortiClient installer
sso="0"        # Enter 0 when Single Sign-On Mobility Agent feature is disabled in the
FortiClient installer
vs="1" # Enter 0 when vulnerability Scan feature is disabled in the FortiClient installer
wf="0" # Enter 0 when Web Filtering feature is disabled in the FortiClient installer
```

   f. If you want the script to uninstall older versions of FortiClient installed on the device, configure `uninstall="1"`. By default, this is disabled.

   g. The shell script mainly performs the following tasks:
   - Check if FortiClient is already installed on the system.
   - Skip the installation process if there is FortiClient installed with same version and features.
   - Continue the installation process if one of the following is true:
     - There is no FortiClient installed or free VPN version installed.
     - FortiClient is installed with a different version and/or different features.
   - Uninstall older versions of FortiClient if there is any.
   - Download the FortiClient deployment package from the EMS server. Therefore, the managed macOS device should be able to access the download link.
   - Install FortiClient on the macOS device.

   If desired, modify the script file based on your requirements.

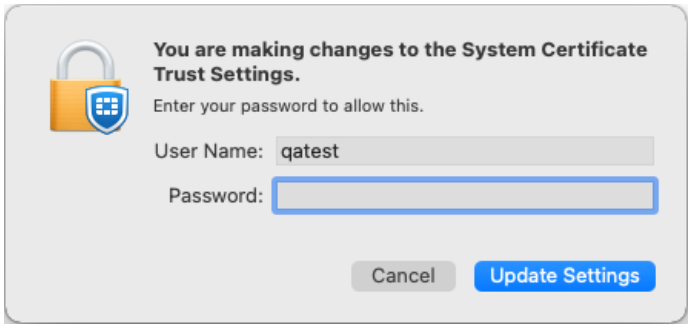
   h. Save the file. The script is now ready to upload to Intune.

2. Log in to the Microsoft Endpoint Manager Admin Center.
3. Go to *Devices > macOS > Shell scripts > Add*.
4. In *Basics*, enter the following:
   a. In the *Name* field, enter the shell script name.
   b. In the *Description* field, enter a description for the shell script. This setting is optional but recommended.
5. Click *Next*. In script settings, enter the following:
   a. In *Upload script*, browse to the shell script. The script file must be less than 200 KB in size.
   b. For *Run script as signed-in user*, select *Yes* to run the script with the user credentials on the device. Select *No* to run the script as the root user. *No* is the default option.
   c. If desired, enable *Hide script notifications on devices*. By default, the device shows a script notification for each script that it runs. On a macOS device, the end user sees a notification from Intune that IT is configuring their computer.
   d. For *Script frequency*, select how often to run the script. To run the script only once, select *Not configured*, the default value.
   e. For *Max number of times to retry if script fails*, select how many times to run the script if it returns a non-zero exit code. A zero exit code means success. To not retry when the script fails, select *Not configured*, the default value.
6. Go to *Assignments > Select groups to include*, and assign the script to the macOS devices group.
7. Review the summary, then click *Add* to save the script.
8. Intune runs the script on all devices and users in the assigned group. Go to *Intune MDM > All services > Devices > macOS > Shell Scripts > Overview* to verify the deployment statistics.

In some cases, Intune may take some time to run the script on the devices. In that case, you can select the device and click *Sync*. If you want to sync on all macOS devices, click *Bulk Device Actions*, select the desired OS, then click *Sync*.This synchronizes the latest configuration changes to the endpoint. After running the script, Intune takes some time to update the device and user statuses.

Note the following:

- Manually uninstalling FortiClient using the FortiClient uninstaller tool removes the VPN virtual adapter and stored zero trust network access (ZTNA) certificates on the endpoint. As a result, reinstalling FortiClient displays the FortiTray VPN and system keychain modification prompts. In this case, push and distribute the MDM configuration profile again before reinstalling FortiClient to fully silence the prompts.
- When connecting to VPN with client certificates, the system prompts the user for keychain access credentials to access and read the stored certificate. The user can decide to allow or deny access. Selecting *Always Allow* silences future prompts when FortiTray accesses the certificate.
- When FortiClient acts as a ZTNA client, the system is expected to display prompts to ask for user credentials to access the ZTNA client certificate stored in the login keychain.
- Revoking the endpoint client certificate from EMS removes the ZTNA client certificate and the MDM preloaded CA certificate from keychain access. Therefore, when removing the revoked CA Certificate, the system prompts for administrator credentials to modify the system keychain.



Deploying FortiClient (macOS) using Jamf Pro

The following topics provide an overview of deploying FortiClient (macOS) for FortiSASE when endpoints are managed by Jamf Pro, building upon the instructions provided in the Jamf Deployment Guide as a starting reference.

FortiSASE already provides a preconfigured FortiClient macOS installer that is unique to each FortiSASE instance.

The goals of these instructions are:

1. To create a macOS installer package (PKG) for FortiClient using Jamf Composer.
2. To deploy required FortiClient files, related scripts, and components and the FortiClient package itself to macOS endpoints using Jamf Pro.

In Jamf Pro, to achieve these goals, the following settings must be configured under *Computers*:

- *Content Management > Configuration Profiles*
- *Content Management > Policies*

Instructions in the Jamf Deployment Guide provide a starting reference and it is strongly recommended for an administrator to become familiar with that guide before using this guide.

This topic covers the following:

- Preliminary steps on page 760
- Configuring a configuration profile on page 761
- Enrolling macOS in Jamf Pro on page 764
- Preparing FortiClient package using Jamf Composer on page 765
- Deploying FortiClient using the package file on page 768

Preliminary steps

This topic covers the following preliminary steps to obtain files that must be used with Jamf Pro:

- Downloading FortiClient from FortiSASE on page 760
- Downloading FortiClient support files from the Fortinet Support site on page 760
- Gathering the FortiSASE certificate required for Jamf Pro on page 761

Downloading FortiClient from FortiSASE

To download FortiClient from FortiSASE:

1. Go to *Dashboards* > *Status*
2. In the *Remote Users* widget, click *Onboard Users*.
3. In the *Onboarding* pane, select *OS* as *MacOS* and *Installer* as *MacOS*.
4. Click *Download preconfigured installer* to download and save the installer to your computer.

   The preconfigured DMG installer includes the Digital Experience Monitor (DEM) agent too. In this example, this file is used for deployment to ensure both FortiClient and DEM agent are installed.

Downloading FortiClient support files from the Fortinet Support site

To download FortiClient support files from the Fortinet Support site:

Instructions in the Jamf Deployment Guide provide a starting reference and it is strongly recommended for an administrator to become familiar with that guide before using this guide. See Configuring a configuration profile.

1. Navigate to https://support.fortinet.com/.
2. Click on *Support* > *Downloads* > *Firmware Downloads*.
3. On the *Firmware Images* page, from the *Select Product* drop down list choose *FortiClient*.
4. Click the *DOWNLOAD* tab and go to the *Mac* folder.
5. Click into the folder for your version of FortiClient, such as *FortiClient /Mac / 7.00* > *7.2.13*.

6. Download *FortiClient_Configuration_Profile.JAMF.mobileconfig* using the *HTTPS* link.

Gathering the FortiSASE certificate required for Jamf Pro

You will need at least one manual installation of FortiClient on a macOS machine. This certificate is found in your computer's root certificate store.

To gather the FortiSASE certificate required for Jamf Pro:

1. On MacOS with FortiClient installed and connected to FortiSASE, open the *Keychain Access* app. Ensure that you select *Open Keychain Access*.
2. In the *Keychain Access* window, go to *System Keychains* > *System*.
3. Locate the ZTNA Certificate shown as *FCTEMS################*.

   The specific serial number should match the *Serial Number* located in the FortiSASE portal under *Dashboards* > *Status* in the *Remote Users* widget.

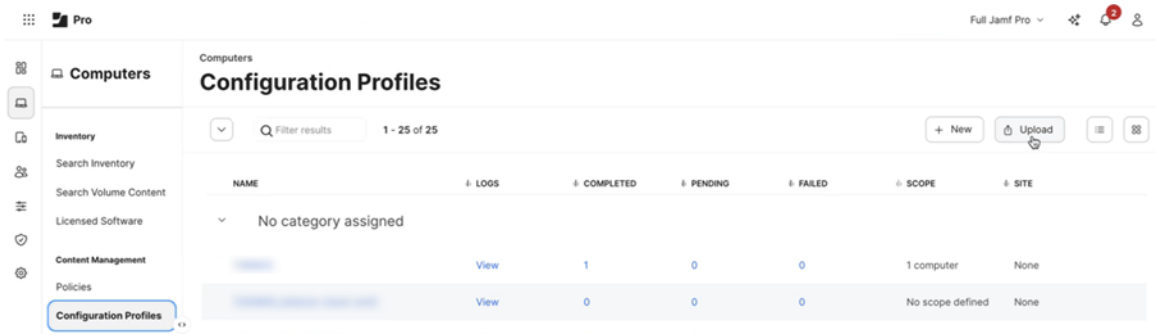
4. Once located, select the certificate file and go to *File* > *Export items*.
5. Save the certificate in the *Certificate* (.cer) format to a workstation that will be administrating Jamf Pro in the next step.

Configuring a configuration profile

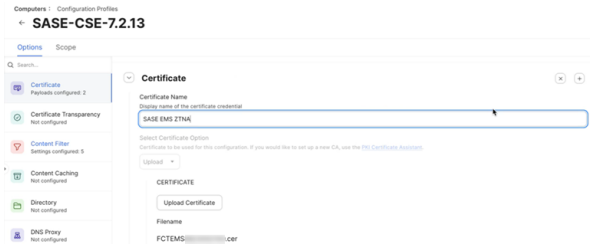
Efficient and silent deployment of FortiClient (macOS) requires a Jamf Pro custom configuration profile that allows all the required prompts.

To configure a configuration profile:

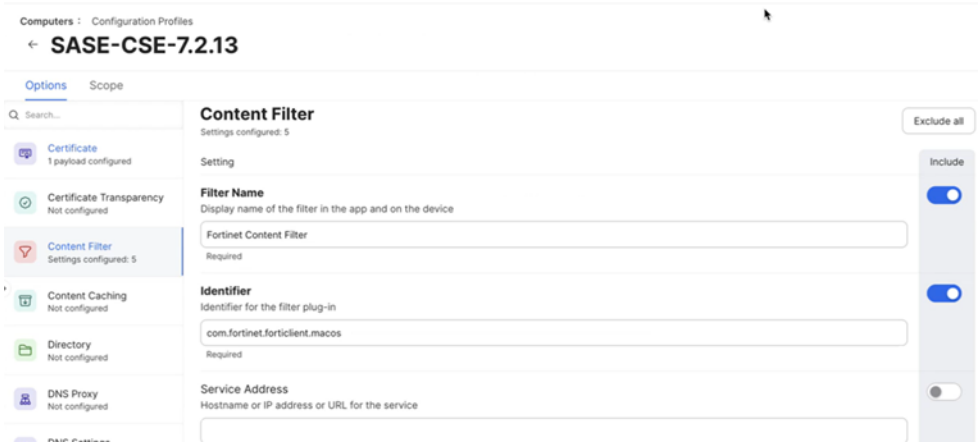
1. In *Computers*, go to *Content Management* > *Configuration Profiles*.
2. Click *Upload* to upload the .mobileconfig file.



3. In *Options* > *General*, provide a display name of your choice.
4. In *Options* > *Certificate*, click *Configure*.
   a. Enter a *Certificate Name*, such as *SASE EMS ZTNA*.
   b. In *Select Certificate Option*, click *Upload*.
   c. To upload your *SASE EMS ZTNA* certificate, click *Upload Certificate*.
   d. Verify that the certificate is uploaded correctly.



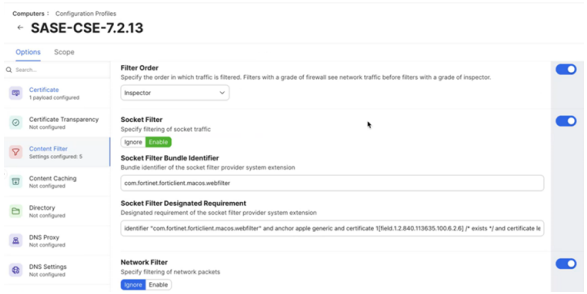
5. In *Options* > *Content Filter*, configure the following settings:
   - *Filter Name*: Fortinet Content Filter
   - *Identifier*: com.fortinet.forticlient.macos
   - *Certificate* (Optional)
   - *Filter Order*: Inspector
   - *Socket Filter*: Enable
   - Enable *Socket filter bundle identifier* and enter: *com.fortinet.forticlient.macos.webfilter*



   - Copy and paste the whole contents from below to *Socket Filter Designated Requirement*:

```
identifier "com.fortinet.forticlient.macos.webfilter" and anchor apple generic and
certificate 1[field.1.2.840.113635.100.6.2.6]
/* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13]
/* exists */ and certificate leaf[subject.OU] = AH4XFXJ7DK
```

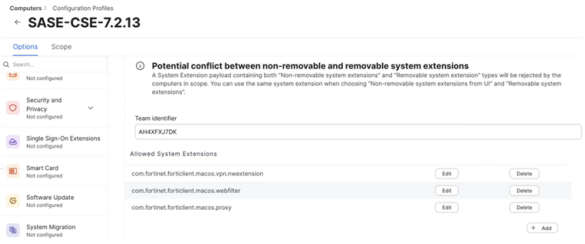
   - *Network filter*: Ignore



> For relevant details about this step, refer to Configuring a configuration profile.

6. In *Options* > *System Extensions*, click *Configure*.

a. Change *System Extension Types* to *Allowed System Extensions* and click *Add*.
b. In *Team Identifier*, enter `AH4XFXJ7DK`.
c. To grant FortiTray permissions to load and grant network access, add the following extensions under *Allowed System Extensions*:
- *com.fortinet.forticlient.macos.webfilter*
- *com.fortinet.forticlient.macos.vpn.nwextension*
- *com.fortinet.forticlient.macos.proxy*



When you import the Jamf mobile configuration file from the Fortinet site, it will only add the first extension on this list. It is mandatory to add the other two extensions manually.

7. (Optional) Go to *Configuration Profiles* > *Options* > *Privacy Preference Policy Control* and validate multiple *App access* identifiers:
- For the first *App access* identifier:
  - *Identifier*: com.fortinet.forticlient.macos.antivirus
  - *Identifier Type*: Bundle ID
  - *Code Requirement*:

```
anchor apple generic and identifier "com.fortinet.forticlient.macos.antivirus" and
(certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1
[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
AH4XFXJ7DK)
```

- For the second *App access* identifier:
  - *Identifier*: com.fortinet.FortiClient
  - *Identifier Type*: Bundle ID
  - *Code Requirement*:

```
identifier "com.fortinet.FortiClient" and anchor apple generic and certificate 1
[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
AH4XFXJ7DK
```

- For the third *App access* identifier:
  - *Identifier*: /Library/Application Support/Fortinet/FortiClient/bin/fcaptmon
  - *Identifier Type*: Path
  - *Code Requirement*:

```
identifier fcaptmon and anchor apple generic and certificate 1
[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
AH4XFXJ7DK
```

- For the fourth *App access* identifier:
  - *Identifier*: /Library/Application Support/Fortinet/FortiClient/bin/fctservctl2
  - *Identifier Type*: Path
  - *Code Requirement*:

```
identifier fctservctl2 and anchor apple generic and certificate 1
[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf
[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
AH4XFXJ7DK
```

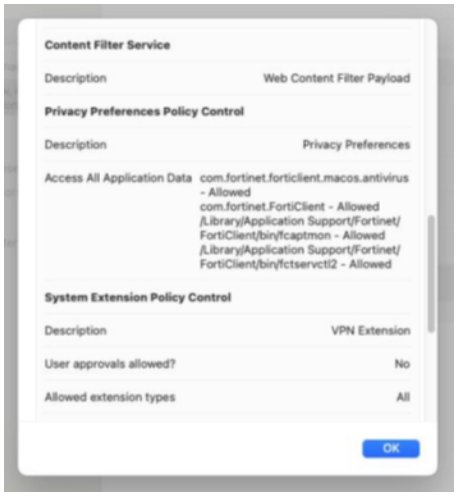
8. Click *Save*.
9. Click *Scope* and under *Targets* > *Specific Computers* > *Your device*, choose *Show in Jamf Pro Dashboard*.
10. Click *Save*.

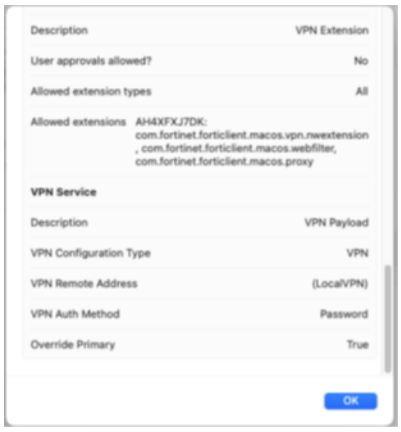
Enrolling macOS in Jamf Pro

Enrollment is the process of adding computers and mobile devices to Jamf Pro. This establishes a connection between the computers and mobile devices and the Jamf Pro server. User-initiated enrollment allows users to initiate the enrollment process on their own by going to an enrollment URL.

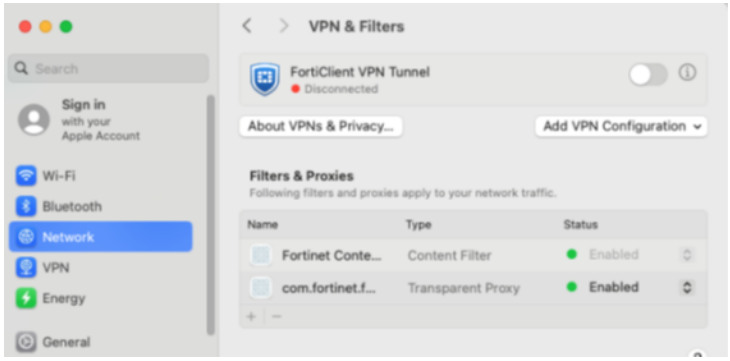
To enroll macOS in Jamf Pro:

1. On your enrolled MacOS end user device, open *Settings* > *Profiles*, review the profile and click *Install*.
2. Observe that profiles are installed on the device. After enrolling, the previously configured profile appears on the endpoint as shown.
   a. *Settings* > *Profiles*





b. *Settings > Network > VPN & Filters*

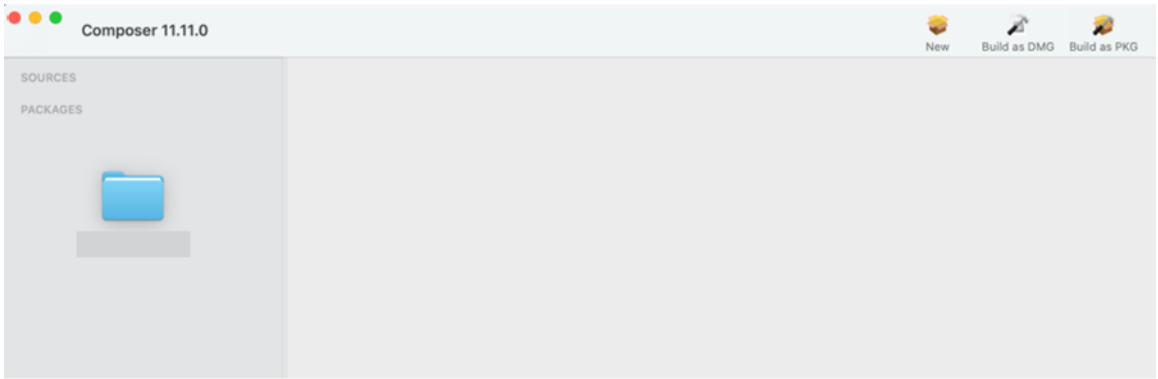


c. *Settings > Login items & Extensions > Network Extension*

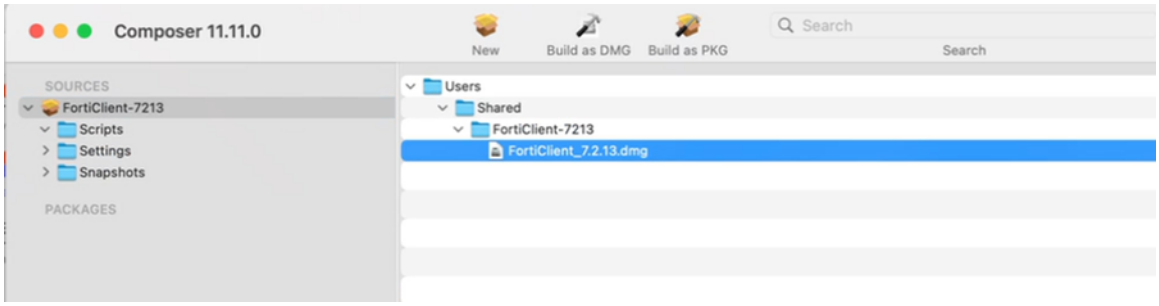
Preparing FortiClient package using Jamf Composer

To prepare the FortiClient package using Jamf Composer:

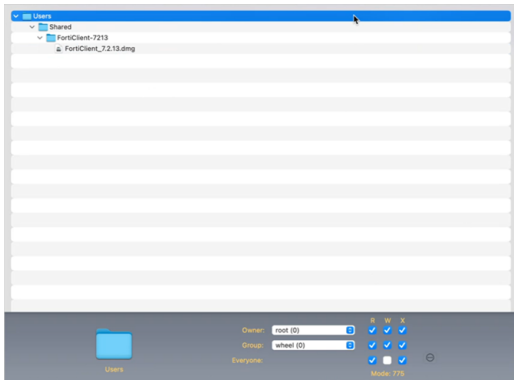
1. Locate the DMG file downloaded from the FortiSASE portal in a previous preliminary step. See Preliminary steps on page 760.
2. Using *Finder*, create a folder structure on macOS. For example, place the DMG file in */User/Shared/FortiClient-7213*.
3. Navigate to the parent directory *FortiClient-7213*.
4. Open Jamf Composer, you will want to drag the *FortiClient-7213* folder from *Finder* to *Sources*.



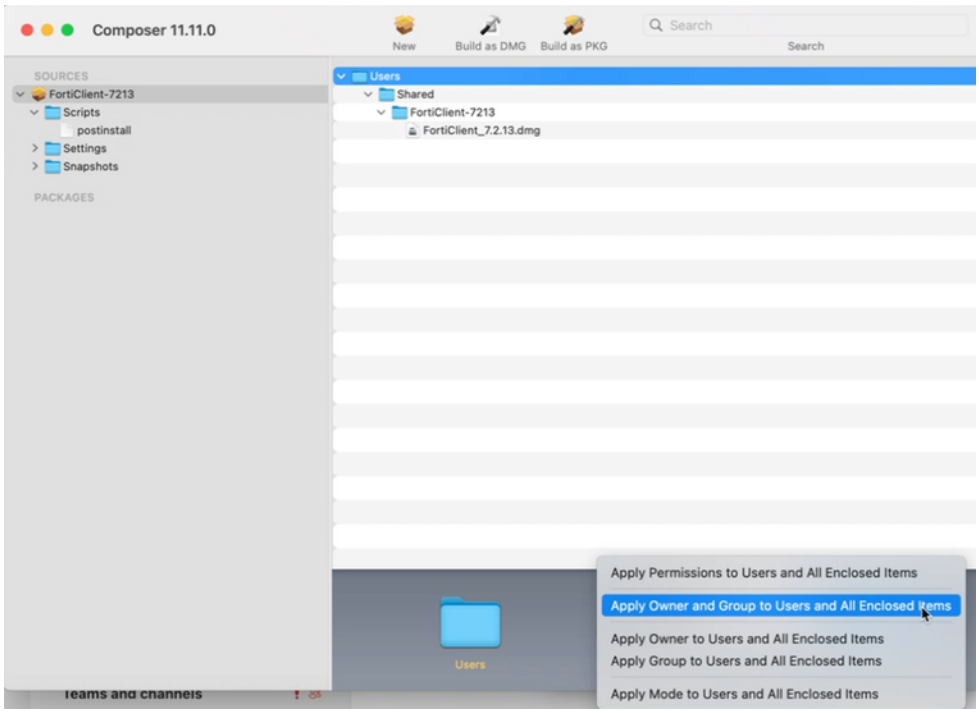
This folder will be visible under *SOURCES* section of Jamf Composer.



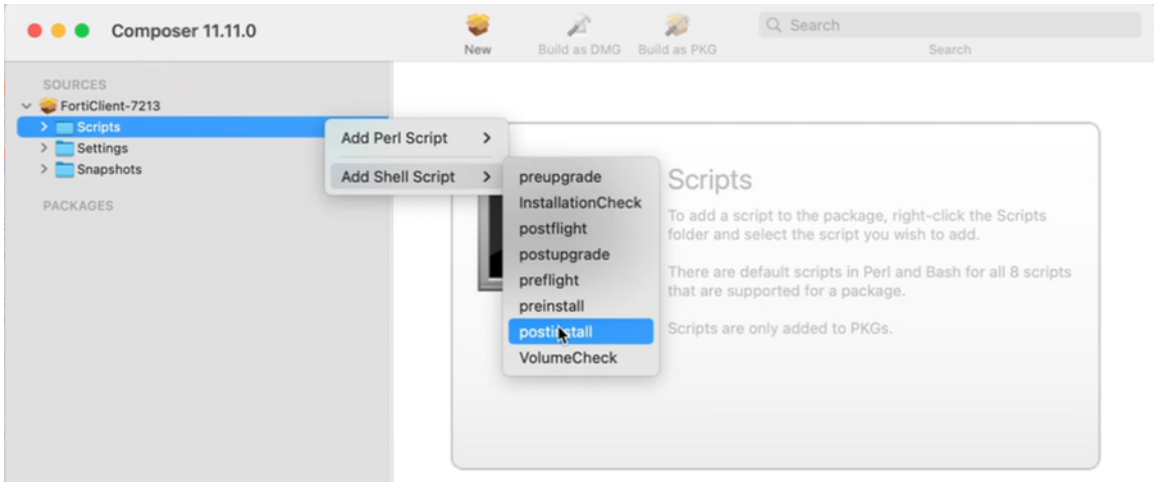
5. Click on the *Users* folder and then use the *Owner* and *Group* dropdown lists to update the *Users* folder permissions to enable Read (*R*), Write (*W*), and Execute (*X*):
   a. Set *Owner* to *root*.
   b. Set *Group* to *wheel*.



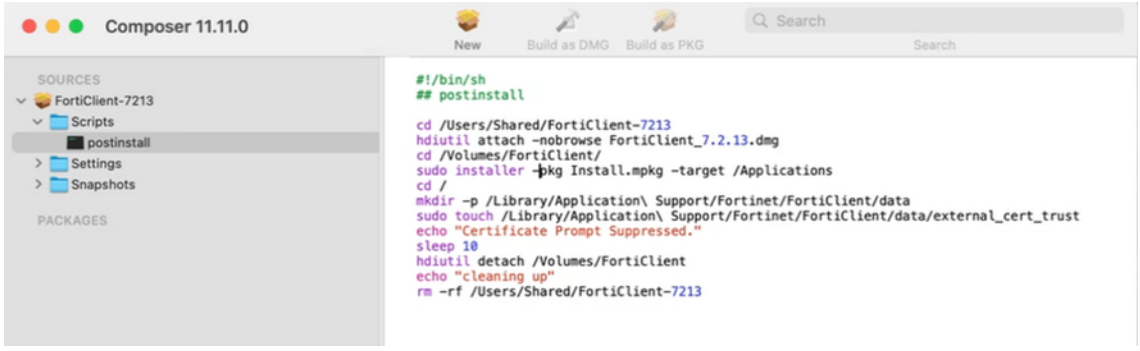
6. On the bottom right corner, click the ellipsis (...) icon to ensure the same permissions are applied to all Enclosed items.



7. On the left pane of Jamf Composer, expand *FortiClient-7213* to reveal additional configuration options including *Scripts*, *Settings*, and *Snapshots*.



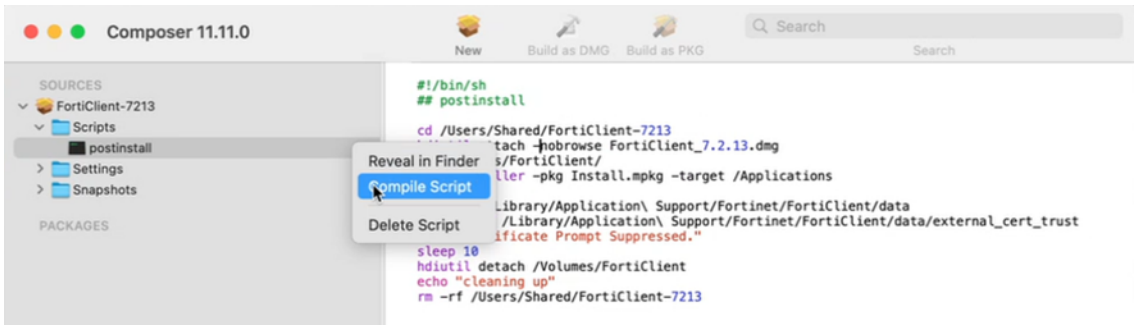
8. Right-click on *Scripts* and select *Add Shell Script > postinstall*. This creates a postinstall script. Click on it to show the default script.



Replace the contents of the default script with the following lines:

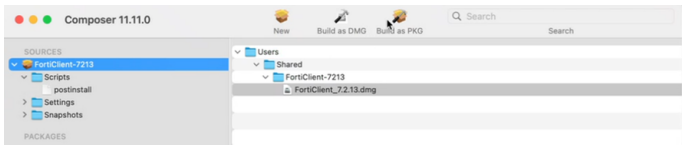
```
#!/bin/sh
cd /Users/Shared/Forti/
hdiutil attach -nobrowse FortiClient_7.2.6.dmg
cd /Volumes/FortiClient/
sudo installer -pkg Install.mpkg –target /Applications
cd /
mkdir -p /Library/Application\ Support/Fortinet/FortiClient/data sudo touch
/Library/Application\ Support/Fortinet/FortiClient/data/external_cert_trust echo"Certificate
Prompt Suppressed."
sleep 10
hdiutil detach /Volumes/FortiClient
echo "cleaning up"
rm -rf /Users/Shared/Forti
```

9. Right-click on *Scripts > postinstall* to reveal the *Compile Script* option.
10. Click *Save* when prompted.



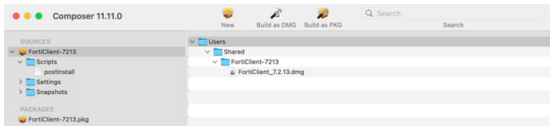
After compiling completes, a dialog appears confirming that the script appears to compile properly. This is expected.

11. Build your FortiClient package file.
    a. Under *SOURCES* in Jamf Composer, click on the *FortiClient-7213* folder.
    b. Click *Build as PKG*. You will be prompted to save the PKG file a location that you select on your end device.



The PKG file normally takes less than a minute to build.

    c. When the compilation is done, *FortiClient-7213.pkg* appears in Jamf Composer under the *PACKAGES* section.



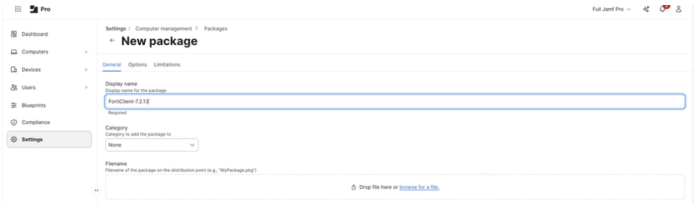
Deploying FortiClient using the package file

It is recommended to push the configuration profile before deploying FortiClient on the endpoint to ensure all required permissions are set correctly. See Configuring a configuration profile on page 761.

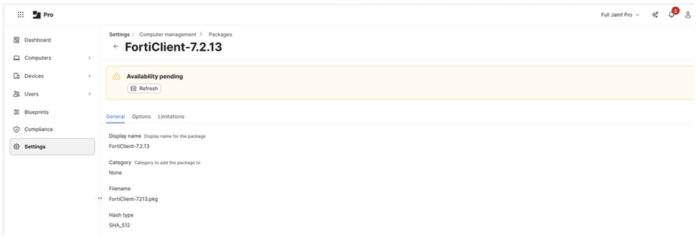
If you are re-installing FortiClient using Jamf, redeploy the Configuration Profile first and then the Policy. If you are not re-installing FortiClient, additional FortiTray VPN extension prompts may display.

To deploy FortiClient:

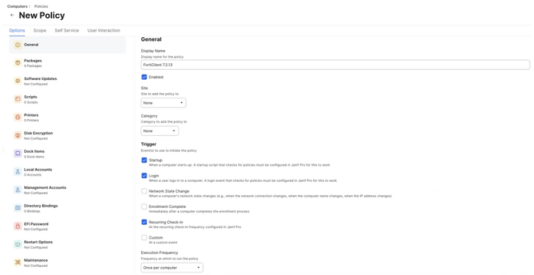
1. Locate the package file you created in a previous step. See Preparing FortiClient package using Jamf Composer on page 765.
2. Upload this package to Jamf Pro under *Settings > Computer Management > Packages*.
3. Click *+New*.
    a. Configure the Display Name as *FortiClient-7.2.13*.
    b. Browse and select your FortiClient-7213.pkg file. It may take a few minutes to upload.



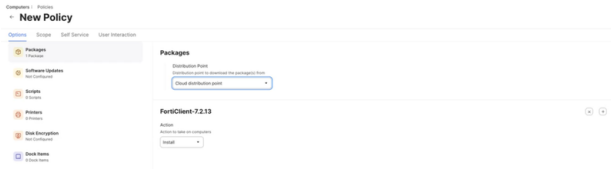
c. Click *Refresh* to ensure upload is complete.



4. Navigate to *Computers* > *Content Management* > *Policies* and configure the following settings:
   a. Click *New*.
   b. Under *Options*, add the *Display Name* `FortiClient 7.2.13`.
   c. Enabled the triggers:
      - *Startup*
      - *Login*
      - *Recurring Check-in*



   d. Select *Packages*.
   e. Click *Configure* and select your *FortiClient-7.2.13* package.
   f. Select the preferred *Distribution point* > *Cloud Distribution Point*.
   g. Set *Action* to *Install*.

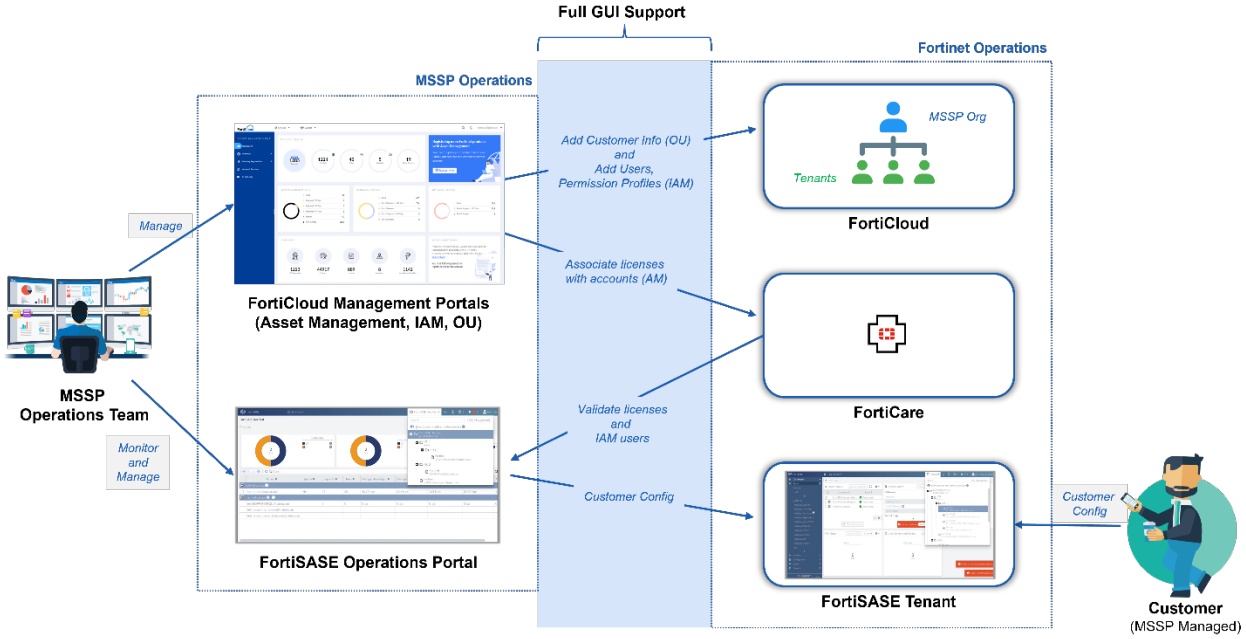


5. Click *Save* to deploy the package to all or selected endpoints.

MSSP portal

FortiSASE includes a portal that managed security service providers (MSSP) can use to offer their end customers a managed FortiSASE service by performing the following management functions for multitenant FortiSASE deployments:

- Monitor tenants' FortiSASE instances
- Access and manage tenants' FortiSASE instances



The FortiSASE MSSP portal is based on the use of FortiCloud Identity & Access Management (IAM) users and the FortiCloud organizational unit structure. For details, see Organization Portal and Identity & Access Management (IAM), respectively.

Considerations

See Considerations on page 770.

Considerations

- The managed security service provider portal does not require a subscription. However, there is a limit on the number of member accounts that you can join to an organization. See Standard versus unlimited access

to the Organization Portal.

- When configuring IAM users for an organization, you typically configure the user type as *Organization* with a *Permission Scope* configured to an organization unit (OU) or sub-OU. These users can access the MSSP portal. IAM users where the user type is configured as *Local* can directly access the FortiSASE portal into a specific tenant's instance. However, they cannot access the MSSP portal.
- When an IAM user with access to only a single account logs in to the FortiSASE portal, the FortiSASE portal for the instance loads instead of the MSSP portal.
- When new member accounts with new placeholder email addresses, also known as placeholder accounts, have been added to sub-OUs, administrators of these sub-OUs can provision new instances associated with these placeholder accounts from the MSSP portal

Configuration workflow



Ensure that you are aware of MSSP portal Considerations on page 770.

The workflow for configuring FortiCloud Identity Access & Management (IAM) users and organization units (OU) and using the managed security service provider (MSSP) portal is as follows:

1. Using the FortiCloud Organization portal:
   a. Enable organizations. See Enabling Organizations.
   b. Create an organization. See Creating an organization.
   c. Add one or more OUs. See Adding and deleting OUs.
   d. Add accounts to OUs by doing one of the following:
      - Invite FortiCloud accounts to join OUs. See Invitations and Creating invitation tokens. Then approve invitations to FortiCloud accounts. See Invitation Approval for details.
      - Create new member accounts linked to a real email address or a new placeholder email address generated at the same time as the member account. See Creating new Member Accounts.
2. Using the FortiCloud IAM portal:
   a. Set up a resource-based permission profile allowing IAM users to access FortiSASE as a portal. See Resource-based permissions on page 772.
   b. Configure IAM users. See Creating users, user groups, and roles within Organizations and Adding IAM users.
3. From the FortiSASE portal:
   a. When an IAM user logs in to FortiSASE for the first time, there are some preliminary steps to complete to validate the new IAM user. See Validating new IAM users.
   b. Access the MSSP portal using an IAM user corresponding to the root account. See Accessing the MSSP portal on page 781.
   c. Monitor tenants' FortiSASE instances. See Monitoring a tenant's instance on page 782.

d. Manage tenants' FortiSASE instances. See Managing a tenant's instance on page 783.

> For initially provisioning a tenant's FortiSASE instance, you can use one of the following approaches:
> - By directly logging in to the FortiSASE portal, the customer's tenant administrator can provision the instance themselves.
> - From the MSSP portal, the MSSP operations team with administrator access to the tenant can provision the instance and preconfigure it on behalf of the tenant.

For details on configuring FortiCloud OUs and adding FortiCloud accounts to OUs, see Organization Portal.

For details on creating new member accounts and managing them, see Creating new Member Accounts and Managing Member Accounts.

For details on configuring FortiCloud IAM users and permission profiles, see Identity & Access Management (IAM).

Resource-based permissions

Permission control is global to the FortiSASE portal and provides the following privileges for each resource:

- No access
- Read/write access
- Read-only access

> If an Identity & Access Management (IAM) user is assigned a permissions profile with no access configured for all FortiSASE portal resources, then the IAM user cannot log into the FortiSASE portal.

The FortiSASE portal has the following resource categories:

Resource	Provide control over...
User & Authentication on page 773	User and authentication related settings.
Policy on page 774	Agent, proxy, and SPA policies.
Logging on page 775	Logging and reports features.
Monitoring on page 776	Monitoring features including FortiView, Digital Experience Monitoring, Managed Endpoints, and other monitor widgets.
Dashboards on page 777	Dashboard features.
Network on page 778	Network features including edge devices, SPA, DNS, hosts, services, and feeds.
System on page 779	System settings.
Security on page 779	Security profile groups and security features.

Resource	Provide control over...
Endpoint Management on page 780	Managed Endpoints page, endpoint profiles, and zero trust network access (ZTNA) settings.
Infrastructure on page 780	FortiSASE provisioning.

See Permission profiles within Organizations.

Access to specific pages and actions require permissions to multiple resources.

> In the table below, for entries marked with *Read-only access* involving allow or show actions, this privilege indicates the minimum privilege level required, which means the higher privilege level of *Read/Write access* can also be used in these cases.
>
> On the other hand, for entries marked with *Read-only access* involving blocking or hiding actions, this privilege is the only privilege needed to achieve the desired actions.

User & Authentication

Action	User & Authentication	Monitoring	Endpoint Management	System
Allow viewing of *Connected Users* page, and *Remote Users* and *User Connection Monitor* widgets	Read-only access			
Onboard users button redirects to *Client Onboarding* documentation	Read-only access			
Block import and export of users and groups	Read-only access			
Allow viewing of users, PKI users, and groups	Read-only access			
Allow viewing of LDAP and RADIUS servers and users	Read-only access			
Hide *SSO > Agent* page	Read-only access			
Allow editing of *SSO > Agent* page	Read/write access		Read/write access	
Make *Show in FortiView* unavailable in *User Connection Monitor*	Read/write access	No access		
Make *View Endpoint Details* unavailable in *Managed Endpoints* widget/page	Read/write access		No access	

Action	User & Authentication	Monitoring	Endpoint Management	System
Hide *SSO* > *Proxy* page	Read/write access			No access

Policy

Action	Policy	User & Authentication	Network	Logging	Monitoring	Security	Endpoint Management
Allow users and groups to be viewed from policies	Read/write access	Read-only access					
Allow users and groups to be created inline from policies	Read/write access	Read/write access					
Allow creating hosts, feeds, and services inline within policies	Read/write access		Read/write access				
Hide private access policies	Read/write access		No access				
Allow creating ZTNA tags in-line within policies	Read/Write access						Read/Write access

Action	Policy	User & Authentication	Network	Logging	Monitoring	Security	Endpoint Management
Allow *Show Matching Traffic Logs* when a policy is right-clicked	Read/Write access			Read-only access			
Allow *Show in FortiView* when a policy is right-clicked	Read/Write access				Read-only access		
Allow creating security profile groups inline within policies	Read/Write access					Read-only access	

Logging

Action	Logging	Network
Allow downloading of generated reports	Read-only access	
Allow scheduled reports to be viewed	Read-only access	
Allow *Operations* > *Logs* > *Settings* page to be viewed	Read-only access	
Hide private access tab from *Traffic* logs	Read/Write access	No access

Monitoring

Action	Monitoring	User & Authentication	Dashboards	Network	Endpoint Management
Hide *FortiView* monitors, *Digital Experience Monitoring (DEM)*, *Managed Endpoints*, *User Connection Monitor*, *Application Bandwidth*, and *Bandwidth Monitor* widgets	No access				
Show *Asset Map*, *DEM*, *Managed Endpoints*, and *Connected Users* pages	Read-only access				
Hide *Subscribe* button from *Health* widget	Read-only access				
Allow downloading FortiClient logs from *Endpoint* details slide-in	Read/Write access				Read-only access
Allow requesting FortiClient logs from *Endpoint* details slide-in	Read/Write access				Read/Write access
Allow DEM endpoint features from *Endpoint* details slide-in	Read/Write access				Read/Write access
Block ability to modify *Management Connection* status of endpoints	Read/Write access				No access
Allow add, edit, delete of FortiView monitors in *Dashboards*	Read/Write access		Read/Write access		

Action	Monitoring	User & Authentication	Dashboards	Network	Endpoint Management
Hide SPA hubs and edge devices from *Asset Map*	Read/Write access			No access	
Hide *Connected Users* link from *Asset Map*	Read/Write access	No access			
Hide *Deauthenticate* button from *Connected Users* page and *User Connection Monitor* widget	Read/Write access	Read-only access			

Dashboards

Action	Dashboards	User & Authentication	Monitoring	Network	Security	Endpoint Management
Block ability to create, edit, delete, and resize widgets	Read-only access					
Block ability to add FortiView and monitor widgets	Read/Write access		No access			
Block ability to add widgets related to private access and edge devices	Read/Write access			No access		
Block ability to add *Managed Endpoints* and *Vulnerability*	Read/Write access					No access

Action	Dashboards	User & Authentication	Monitoring	Network	Security	Endpoint Management
Summary widgets						
Block ability to add *User Connection Monitor* and *Remote Users* widgets	Read/Write access	No access				
Block ability to add *Internet Access Security Status* widget	Read/write access				No access	

Network

Action	Network
Show *Edge Devices (FortiAPs, FortiExtenders, FortiGates)*, *Secure Private Access*, *DNS*, *Hosts*, *Services* and *Feeds* pages	Read-only access
Hide *Update authentication method*, *Service Connection Priorities*, *Edit* and *Delete* buttons from *Operations > Connectivity > Secure private access*	Read-only access
Hide *Create*, *Edit*, and *Delete* buttons for *Hosts*, *Services*, *Feeds*, and *DNS* pages	Read-only access
Disable *Authorize*, *Deauthorize*, and *Disconnect* actions for Edge Devices	Read-only access
Hide notifications for newly discovered edge devices	Read-only access

System

Action	Network
Block import, download, and delete actions for certificates	Read-only access
Block save and edit of HTML templates	Read-only access
Block create, edit, and delete of images in *HTML templates* > *Images* tab	Read-only access
Hide *System* section	No access

Security

Action	Security	Logging	Monitoring	Network
Block ability to create, edit, or delete security profile groups	Read-only access			
Block ability to enable or disable security features	Read-only access			
Block ability to create, edit, or delete profile resources	Read-only access			
Hide *View Logs* buttons from all security features	Read/Write access	No access		
Hide *View All* buttons from all security features	Read/Write access		No access	
Display threat data in the security features cards	Read/Write access	Read-only access	Read-only access	
Hide the *Private Access* tab in the *Security* > *Security profiles* page	Read/Write access			No access
Show the *Private Access* tab and allow renaming, deleting, and customizing of private access security profile groups	Read/Write access			Read-only access

Endpoint Management

Action	Endpoint Management	Monitoring
Allow downloading FortiClient logs from *Endpoint* details slide-in	Read-only access	Read/Write access
Allow requesting FortiClient logs from *Endpoint* details slide-in	Read/Write access	Read/Write access
Allow DEM endpoint features from *Endpoint* details slide-in	Read/Write access	Read/Write access
Block ability to modify *Management Connection* status of endpoints	Read-only access	
Hide *More Options* > *Show in FortiView* in *Managed Endpoints* page	Read/Write access	No access

Infrastructure

Action	Infrastructure
Block provisioning of FortiSASE instance	Read-only access or No access

Using the MSSP portal

After configuring the required settings in the FortiCloud Identity & Access Management (IAM) portal and FortiCloud Organization portal, you can access the managed security service provider (MSSP) portal.

The MSSP portal allows MSSP administrators to provide a managed FortiSASE service to end customers by performing these tasks:

1. When an IAM user logs in to FortiSASE for the first time, there are some preliminary steps to complete to validate the new IAM user. See Validating new IAM users.
2. Access the MSSP portal using an IAM user corresponding to the root account. See Accessing the MSSP portal on page 781.
3. Monitor the status of a tenant's FortiSASE instance. See Monitoring a tenant's instance on page 782.
4. Manage a tenant's FortiSASE instance, namely, to preconfigure it prior to delivery to the end customer, troubleshoot it, and resolve any configuration issues that the end customer reports. See Managing a tenant's instance on page 783.

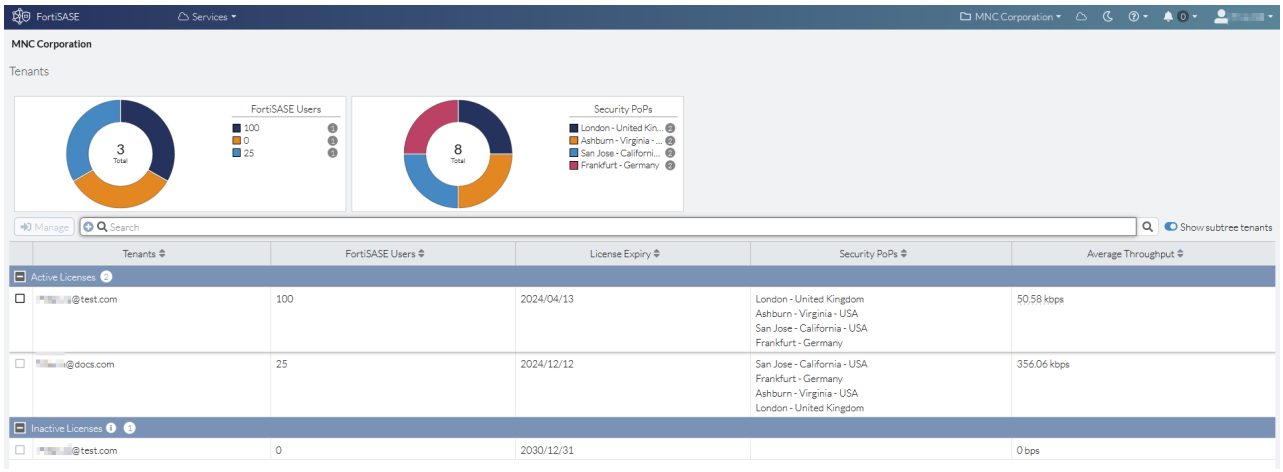
Accessing the MSSP portal

Ensure that you are aware of MSSP portal Considerations on page 770.

The managed security service provider (MSSP) portal requires configuring an Identity & Access Management (IAM) user corresponding to the root account, as Adding IAM users describes.

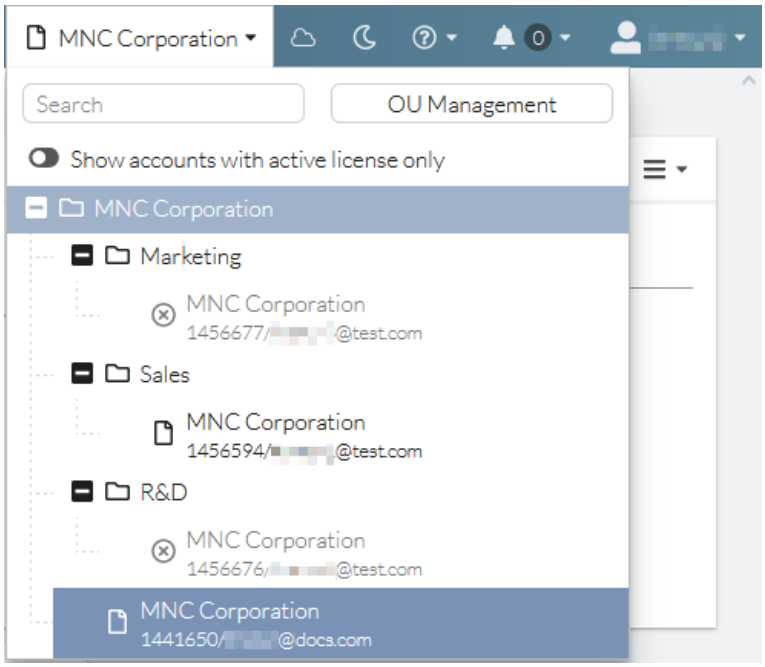
To access the MSSP portal from the FortiSASE portal:

1. Go to the FortiSASE portal.
2. Click *SSO Login*.
3. Click *Sign in as IAM user*.
4. Log in with the user credentials from the CSV that you downloaded when creating the IAM user in To create an IAM user with the wizard. The MSSP portal for the organization displays.



To access the MSSP portal from within a FortiSASE instance:

1. From within a FortiSASE instance, select the context switch dropdown menu. Accounts within the organization display.
2. Select the organization or sub-organization units (OU) to enter the MSSP portal for the selected context. In the example, selecting the top-level organization MNC Corporation displays FortiSASE instances for all OUs. Selecting the Sales OU displays FortiSASE instances for that OU only.



Monitoring a tenant's instance

Once logged into the managed security service provider portal, the administrator CAN monitor the following FortiSASE tenant data:

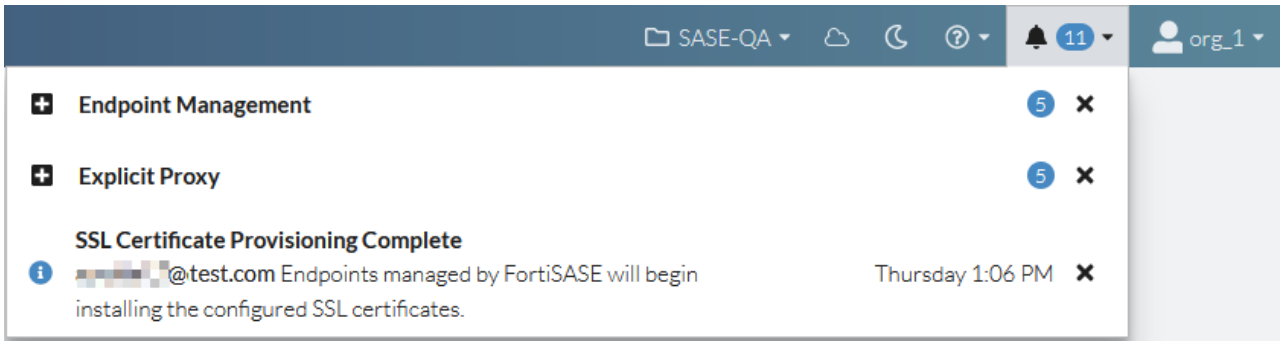
- Pie charts showing the distribution of FortiSASE users for active and inactive subscriptions and the distribution of security points of presence (PoP)
- Tenant entries separated into *Active Licenses* and *Inactive Licenses* categories. The *Inactive Licenses* category is for tenants for which data is not yet available for instances that are not yet provisioned.
- When *Show subtree tenants* is enabled, tenants for second- and third-level organization units (OU) display. When this toggle is disabled, only tenants for the first-level OU (top-level organization only) display.
- Columns with data display. The following lists all available columns. Bolded columns display by default:

Column	Description
Tenants	FortiSASE tenant listed with its Identity & Access Management user email address.
FortiSASE Users	Number of licensed users associated with the tenant.
License Expiry	FortiSASE user license expiry date.
Security PoPs	List of security PoPs associated with a tenant.
Average Throughput*	Average transmitted data rate through the tenant's instance.
Average Egress In*	Average received data rate for tenant's egress interface.
Average Egress Out*	Average transmitted data rate for tenant's egress interface.

Column	Description
Average Ingress In*	Average received data rate for tenant's ingress interface.
Average Ingress Out*	Average transmitted data rate for tenant's ingress interface.

* Bandwidth shown is an average for the last 24 hours.

- The bell icon in the banner displays notifications for all tenants within the selected OU. If you select a sub-OU, the MSSP portal filters notifications for that sub-OU.



Managing a tenant's instance

Ensure that you are aware of MSSP portal Considerations on page 770.

A managed security service provider (MSSP) administrator can use the MSSP portal to select a tenant and manage its FortiSASE instance. This allows the MSSP administrator to preconfigure the instance prior to handing off the instance to end customer and to troubleshoot and resolve any configuration issues if the end customer reports any issues with the instance.

For initially provisioning a tenant's FortiSASE instance, you can use one of the following approaches:

- By directly logging in to the FortiSASE portal, the customer's tenant administrator can provision the instance themselves.
- From the MSSP portal, the MSSP operations team with administrator access to the tenant can provision the instance and preconfigure it on behalf of the tenant.

To manage a tenant's FortiSASE instance from the MSSP portal using the Manage button:

1. From the MSSP portal, in the *Active License* category, click a tenant.
2. Click *Manage*.
3. The tenant's FortiSASE instance loads as if you logged into the FortiSASE portal using the Identity & Access Management (IAM) user account associated with the instance.
4. Perform any configuration within the FortiSASE instance with the same permissions as the IAM user account associated with the instance.

To manage a tenant's FortiSASE instance from the MSSP portal using the context switch dropdown menu:

1. From within a FortiSASE instance, select the context switch dropdown menu. Accounts within the organization display.
2. Enable *Show accounts with active license only* to filter the dropdown menu to only display organization units and accounts with active subscriptions.
3. Select the IAM user or member account (with a real or placeholder email address) whose FortiSASE instance you want to manage.
4. The tenant's FortiSASE instance as if you had logged into the FortiSASE portal using the account associated with the instance.
5. Perform any configuration within the FortiSASE instance with the same permissions as the account associated with the instance.

SPA for an MSSP hub

For the MSSP hub use case, see SPA for an MSSP hub.

Central management for MSSP tenant

See Central management for MSSP tenants on page 712.

Troubleshooting

FortiSASE supports the FortiGate Support Tool. The FortiGate Support Tool is a Google Chrome extension that can execute background debugs on the FortiSASE GUI to troubleshoot errors. Using the tool, you can create a file to provide to the Fortinet Support for troubleshooting. See Troubleshooting Tip: GUI slowness and errors via FortiGate support tool.

FAQs

Dedicated public IP addresses

All FortiSASE instances with a Standard, Advanced or Comprehensive remote user subscription includes dedicated public IP addresses per Security PoP by default.

What is the expected impact of applying source IP address anchoring to an existing FortiSASE instance once all proper licensing is in place?

> For source IP address anchoring, you must purchase another dedicated public IP address add-on subscription with four additional dedicated IP addresses beyond the initial number of dedicated IP addresses per security PoP. You can allocate the additional four dedicated IP addresses as desired for source IP address anchoring rules such as all in a single security PoP, one per security PoP, or any combination in between.

Source IP address anchoring is an additional feature beyond dedicated IP address provisioning and may require an extra two to four hours to implement on an existing FortiSASE instance, depending on the complexity of requirements.

Subscriptions

I am an existing customer with a registered legacy FortiSASE device-based subscription (EMS05-434) or a registered FortiSASE user-based subscription (EMS05-553). I want to purchase the FortiSASE standard user subscription (EMS05-547), Advanced user subscription (EMS05-676) or the Comprehensive user subscription (EMS05-759). What should I do?

You cannot combine or directly convert the device-based and user-based subscriptions.

No FortiSASE reconfiguration is required. The process involves proper FortiSASE subscription management with the assistance of Fortinet Customer Service.

Therefore, as an existing customer, you must follow this process:

- If your subscription has a remaining term and has not yet expired, do the following:
  a. Contact your Fortinet Sales or Partner contact to provide you with assistance with converting the existing subscription to a FortiSASE user Standard, Advanced or Comprehensive subscription. See the FortiSASE Ordering Guide.
  b. Contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal to review subscription conversion options available for your device-based (EMS05-434) or user-based subscription (EMS05-553).
- If your subscription expired, do the following:
  a. Contact your Fortinet Sales or Partner contact to purchase a new FortiSASE user Standard, Advanced or Comprehensive subscription. See the FortiSASE Ordering Guide.
  b. Once you have purchased a new FortiSASE user subscription, contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team assists you with removing the expired subscription from your account and applying the new one to your account. The FortiSASE serial number (SN) and configuration are preserved.

I am an existing customer with the FortiSASE standard user subscription (EMS05-547) and want to upgrade to an Advanced user subscription (EMS05-676) or the Comprehensive user subscription (EMS-759). What should I do?

No other FortiSASE reconfiguration is required. The subscription upgrade requires proper FortiSASE subscription management with the assistance of Fortinet Customer Service.

Therefore, as an existing customer, you must follow this process:

1. Obtain a FortiSASE Advanced or Comprehensive user subscription by doing one of the following:
   - If your subscription has a remaining term and has not yet expired, contact your Fortinet Sales or Partner contact to provide you with assistance with co-terming the existing subscription to a FortiSASE Advanced or Comprehensive user subscription. This requires obtaining a co-term quote from the Fortinet Renewals team. See the FortiSASE Ordering Guide.
   - If your subscription expired, contact your Fortinet Sales or Partner contact to purchase a new FortiSASE Advanced or Comprehensive user subscription. See the FortiSASE Ordering Guide.
2. Once you have a converted FortiSASE subscription or have purchased a new FortiSASE user subscription, contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team assists you with removing the older subscription from your account and applying the new one to the account. The FortiSASE SN and configuration are preserved.

I am an existing customer with the FortiSASE standard user subscription (EMS05-547), Advanced user subscription (EMS05-676), or Comprehensive user subscription (EMS-759). I want to shift to using FortiSASE user subscriptions in FortiFlex. What should I do?

Shifting from term-based licensing to FortiFlex licensing results in a new FortiSASE SN being created. In other words, a new FortiSASE instance with default configuration is created.

The FortiSASE configuration is lost after the licensing shift and there is no option to restore the old configuration on the new FortiSASE instance. Therefore, FortiSASE reconfiguration is required. Performing this licensing shift before fully deploying FortiSASE is strongly recommended. Before proceeding with these steps, ensure you are familiar with the configured features and their settings and the use cases serviced by your current FortiSASE deployment and understand the consequences of this subscription shift.

This subscription shift requires proper FortiSASE subscription management with the assistance of Fortinet Customer Service.

Therefore, as an existing customer, you must follow this process:

1. Contact your Fortinet Sales or Partner contact to purchase new FortiFlex Program and Point Pack SKUs for access to the FortiFlex portal from within your FortiCloud account and then register these registration codes to your account. See the FortiFlex Program Ordering Guide.
2. Contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team assists you with these steps:
   a. Removing the older subscription from your account
   b. Creating a new Technical Support ticket to engage Fortinet technical teams to request the deletion the old instance on the backend (may take up to two business days).
3. Once the older subscription has been removed from your account and the old instance has been deleted, in the FortiFlex portal, create a FortiSASE configuration and entitlement to generate a FortiSASE user subscription.
4. At this point, a new FortiSASE SN is created. In other words, a new FortiSASE instance with default configuration is created. The FortiSASE configuration is lost after the licensing shift, and there is no option to restore the old configuration on the new FortiSASE instance. Therefore, FortiSASE reconfiguration is required. Configure your FortiSASE instance with desired features from your previous deployment.
5. Perform the configuration in FortiSASE by logging in with the root principal email.
   a. Review FortiSASE documentation for details on configuring features.
   b. Review FortiSASE 4-D deployment guides for details on configuring common use cases and deployments.
   c. For Advanced or Comprehensive subscriptions, use assisted onboarding. See *FortiSASE Support Services* in the FortiSASE Ordering Guide.
6. If you want Fortinet to perform the endpoint management configuration in FortiSASE, purchase Fortinet Professional Services, and request the advanced deployment service or custom service engagement. See *FortiSASE Support Services* in the FortiSASE Ordering Guide.

I am an existing customer with the FortiSASE standard user subscription in FortiFlex and want to upgrade to the Advanced user subscription in FortiFlex or the Comprehensive user subscription in FortiFlex. What should I do?

No other FortiSASE reconfiguration is required. However, this requires the customer to change the configuration for a FortiSASE service offering in the FortiFlex portal. See FortiFlex Administration Guide.

> The customer must perform the action of changing the configuration for a FortiSASE service offering in the FortiFlex portal. Fortinet Customer Service is strictly prohibited from making any changes in the customer's FortiFlex portal.

As an existing customer, you must follow this process:

1. Access the FortiFlex portal from the Services menu in the Asset Management portal.
2. Go to *Configurations* and edit the corresponding configuration with the Standard package.
3. In the *Manage Configuration* page, change the *Service Package* from *Standard* to *Advanced* or *Comprehensive* as needed by your requirements and save these changes.
4. In the *Update Configuration* confirmation prompt, click *Confirm*.

Considerations:

- Upgrading from the Standard to Advanced or Comprehensive service package does not change the FortiFlex FortiSASE instance SN and does not require any contract deregistration since FortiFlex entitlements are embedded in the serial number.
- Changes in the configuration of the FortiFlex portal take effect immediately on the FortiFlex FortiSASE serial number.
- When upgrading your instance from a Standard subscription to an Advanced or Comprehensive subscription, you must open a FortiCare Support Portal ticket to request to enable dedicated public IP addresses on your FortiSASE instance. You must first remove any references to edge devices in policies before requesting to enable dedicated public IP addresses in your FortiSASE instance.

I am an existing partner with the FortiSASE Standard Not-for-Resale (NFR) subscription (EMS05-684) and want to change to the Advanced NFR subscription (EMSAN-676). What should I do?

> Although FortiSASE instance reconfiguration is not required, the FortiSASE SN will change and may not be reflected on FortiClient endpoints immediately. It may take up to 24 hours followed by the Endpoint Management keepalive interval of 60 seconds after endpoints obtain Internet access before the new FortiSASE SN is reflected on FortiClient endpoints. During this time, endpoint connectivity to FortiSASE may not work on endpoints.
>
> After the new FortiSASE SN is reflected on endpoints, you must reinstall FortiClient to restore DEM functionality.
>
> Therefore, a scheduled maintenance window of 24 hours plus the time required to reinstall FortiClient on endpoints is required for this change and must be taken into consideration.

The subscription change requires proper FortiSASE subscription management with the assistance of Fortinet Customer Service and a scheduled maintenance window of up to 24 hours plus the time required to reinstall FortiClient on endpoints.

Therefore, as an existing partner, you must follow this process:

1. Before your existing FortiSASE Standard NFR subscription expires, contact your Fortinet Sales representative to purchase a new FortiSASE Advanced NFR subscription.
2. Contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team assists you with exchanging the existing Standard NFR contract with the new Advanced NFR contract. The FortiSASE instance configuration is preserved.
3. Although FortiSASE instance reconfiguration is not required, the FortiSASE SN will change and may not be reflected on FortiClient endpoints immediately.
   - It may take up to 24 hours followed by the Endpoint Management keepalive interval of 60 seconds after endpoints obtain Internet access before the new FortiSASE SN is reflected on FortiClient endpoints.
   - To check the FortiSASE SN in FortiClient, go to the *Zero Trust Telemetry* tab and in *Managed by FortiClient Cloud* click on the hamburger icon. You should see a SN beginning with *FCTEMS*.
   - You should take note of your previous SN and periodically check FortiClient to see if the new SN has been reflected.
   - While waiting for the new FortiSASE SN to be reflected on FortiClient endpoints, endpoint connectivity to FortiSASE may not work on endpoints.
4. After the new FortiSASE SN is reflected on FortiClient endpoints, you must schedule a maintenance window to reinstall FortiClient on endpoints to restore DEM functionality. You must use the executable version of the FortiClient installer to install the DEM agent on Windows endpoints.

Security PoPs

For my new FortiSASE instance, during initial provisioning I receive the message “Error 21400.4: Failed to configure Security PoP”. How can I resolve this issue?

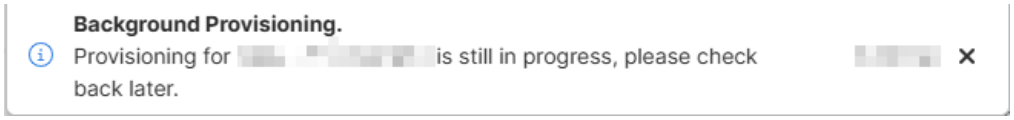
For your new FortiSASE instance, you may see the error message *Error 21400.4: Failed to configure Security PoP during initial provisioning*:



This error message indicates that provisioning could not be completed. You must contact FortiCare Support for further assistance.

For my new FortiSASE instance, I observed the notification “Background provisioning: Provisioning for <security PoP> is still in progress, please check back later.” Should I be concerned with this message?

For your new FortiSASE instance, after logging into FortiSASE, you may see the notification *Background provisioning: Provisioning for < Security PoP> is still in progress, please check back later*.



You should not be concerned with this message, which indicates that the FortiSASE has detected that a site provision has not completed successfully and triggers its recovery mechanism to handle this case. Site provisioning should be completed successfully in the background after seeing this message.

What is the expected impact of applying any security point of presence (PoP) changes to an existing FortiSASE instance once all proper licensing is in place?

The number of security PoPs that remote users can access depends on the FortiSASE subscription tier and number of users. See Number of security data centers accessible per subscription on page 801.

The following impact is expected for an existing FortiSASE instance for any security PoP changes, such as adding or deleting security PoPs:

- Approximately a two to four-hour scheduled maintenance window
- Occasionally, DNS may resolve to the incorrect security PoP due to health check application so users may be directed to the wrong security PoPs and must manually reconnect once completed for best performance.

When connecting to FortiSASE, my endpoint seems to be directed to a security PoP which is not the closest one provisioned to my geographical location. What causes this behavior and how can I troubleshoot it?

FortiSASE directs your endpoint to the closest security PoP based on the specific geolocation information of your endpoint's public IP address, that is, the IP address that your endpoint uses for egress traffic to the internet.

To ensure the most precise direction of traffic, you should use a resolving name server which implements the Extension Mechanisms for DNS (EDNS) Client Subnet extension, or ECS extension. This extension attempts to forward the specific source IP address or /24 subnet originating the DNS lookup back to the authoritative DNS server for a more specific lookup response, rather than using the default lookup response in the cache.

Most traffic direction issues observed are the result of using a DNS server that does not support the ECS extension, and users being directed to resolving name servers which are not physically near their users. This results in poor performance even outside of traffic sent to FortiSASE, as traffic is directed to servers that are not geographically near the user.

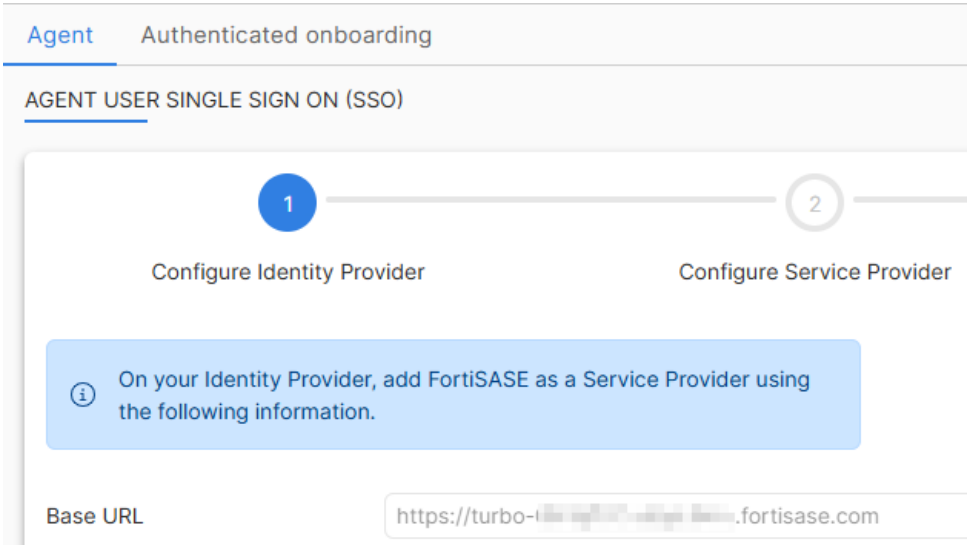
If you are intermittently ending up in different security PoPs from the same physical location, it is also possible that your system's defined resolving name servers are geolocating to different locations.

If you are seeing an issue even when using a DNS provider that supports the ECS extension, open a ticket with FortiCare Support that includes the results of the following troubleshooting steps.

To troubleshoot DNS lookups:

For all following steps, you first must disconnect from FortiSASE.

1. Determine the resolving nameserver IP address.
   a. Use one of these methods:
      - Simple (Windows, macOS, or Linux): run `nslookup`:
        `nslookup whoami.akamai.com`
        The IP address returned for this lookup of http://whoami.akamai.com is the resolving name server's public IP address.
      - Advanced (macOS or Linux): run `dig` using this command in a terminal:
        `for i in {1..10}; do dig +short resolver-identity.cloudfront.net; sleep 11; done;`
        If your system has multiple defined nameservers, or you are using an Anycast service, the lookup may come from multiple source IP addresses. This output provides you with an assortment of IP addresses used to troubleshoot.
   b. For the resolving nameserver IP address, look up its geolocation returned in public sources such as the FortiGuard IP Geolocation Service. If the results are not near your physical location, this may be why you are being directed to the wrong security PoP.
2. Determine if your resolving name server supports ECS for increased accuracy by using one of these methods:
   - Simple (Windows or macOS or Linux): run `nslookup`:
     `nslookup -type=txt o-o.myaddr.l.google.com`
   - Advanced (macOS or Linux): run `dig`:
     `dig +nocl TXT o-o.myaddr.l.google.com`
   - Review the TXT records returned in the answer section of the `nslookup` or `dig` output. The TXT record containing an IP address only is the DNS resolver IP address. If the output returns a second TXT record, the DNS resolver supports the ECS extension. If the output does not return a second TXT record, the DNS resolver does not support the ECS extension.
3. Determine what security PoP your endpoint will be routed to based on your configured resolving name server.
   a. Determine the FortiSASE domain name.
      i. Go to *Access & authentication* > *SSO*.
      ii. View the URL in the *Base URL* field and note the FortiSASE domain name after the https:// string. In the example, the FortiSASE domain name is turbo-a1p0hv3p.edge.prod.fortisase.com.



   b. Determine the IP address of the FortiSASE domain name using one of these methods, replacing `turbo-<xyz>.edge.prod.fortisase.com` with the domain name found in the previous step:

i. Windows, use `nslookup`:
`nslookup turbo-<xyz>.edge.prod.fortisase.com`
ii. Mac/Linux, use `dig`:
`dig turbo-<xyz>.edge.prod.fortisase.com`
iii. For the IP address of the FortiSASE domain name, look up its geolocation returned in public sources such as the FortiGuard IP Geolocation Service. This is the geolocation of the security PoP that your endpoint would be routed to.

Shifting from FortiClient EMS to FortiSASE

I am an existing customer with an EMS on-premise deployment. How can I move my endpoints to FortiSASE?

FortiSASE includes its own EMS instance as part of the service, which it requires for proper orchestration of the solution. Therefore, customers with an existing EMS solution must shift to using the FortiSASE EMS instance.

The shift from an existing EMS on-premise deployment to FortiSASE does not preserve EMS configuration because the configuration will be replaced with configuration defined for FortiSASE after the process completes. You must configure endpoint features supported in FortiSASE. See How can I configure FortiSASE for endpoint management? on page 797

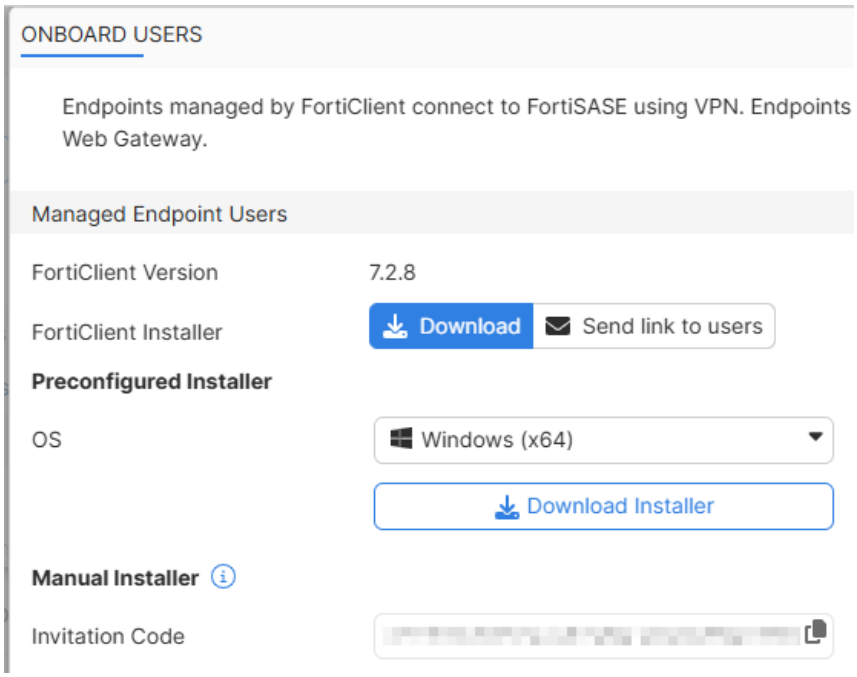
The following process allows shifting endpoints from EMS to FortiSASE without the need for a third-party endpoint management system.

Follow this process:

1. Contact your Fortinet Sales or Partner contact to perform one of these steps:
   - For an existing FortiClient subscription, such as the FortiClient FortiTrust subscription, to provide you with assistance with converting it to a FortiSASE user-based Standard, Advanced or Comprehensive subscription
   - For an expired FortiClient subscription, to provide you assistance with purchasing a new FortiSASE user-based subscription

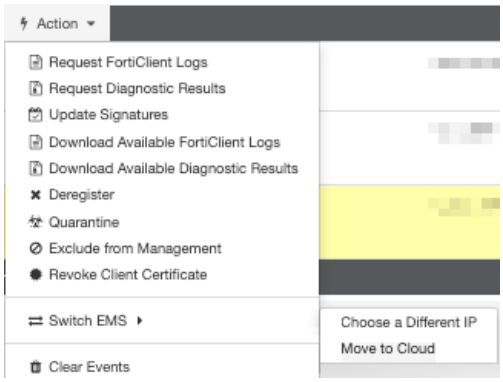
   See the FortiSASE Ordering Guide.
2. Once you have a FortiSASE user-based subscription, contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team assists you with these steps:
   a. Removing the FortiClient FortiTrust subscription from your FortiCloud root principal account, which may take up to three business days
   b. Applying the new FortiSASE user-based subscription to your account
3. Log in to the FortiSASE portal and provision your instance according to the steps in the Cloud Deployment guide, if you have not provisioned it.
4. In the FortiSASE portal, obtain the invitation code as follows:
   a. Go to *Monitoring* > *Dashboards* > *Status*.
   b. Under the *Remote users* widget, click *Onboard Users*. If this widget does not exist, click *Add Widget* and add a new *Remote users* widget.

c. In *Onboarding*, under *Managed Endpoint Users* and under *Manual Installer*, click the copy icon to the right of *Invitation Code* to copy the invitation code to the clipboard.

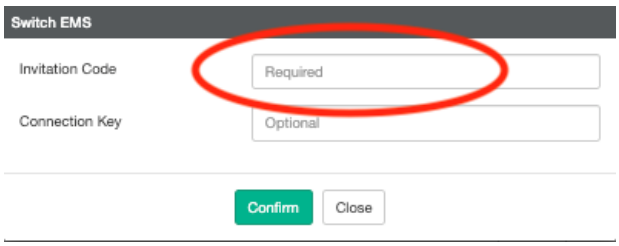


d. Paste the invitation code to a text file for later use.

5. In the EMS GUI, move the FortiClient endpoints as follows:
   a. Go to *Endpoints*.
   b. Select the desired endpoints to move.
   c. Select *Action > Switch EMS > Move to Cloud*.



   d. In the *Switch EMS* dialog, in the *Invitation Code* field, copy and paste the invitation code obtained from FortiSASE.



6. At this point, FortiSASE must be configured for endpoint management. See How can I configure FortiSASE for endpoint management? on page 797

I am an existing customer with a FortiClient Cloud deployment. What is the path to move to a FortiSASE deployment?

FortiSASE includes its own instance of EMS as part of the service, and it is required for proper orchestration of the solution. Therefore, customers with an existing FortiClient EMS solution will need to shift to using the FortiSASE instance of EMS.

Currently, the shift from an existing FortiClient Cloud to FortiSASE does not preserve FortiClient Cloud configuration because it will be replaced with configuration defined for FortiSASE after the process is completed. You must configure endpoint features supported in FortiSASE. See How can I configure FortiSASE for endpoint management? on page 797

The process below should allow endpoints to be shifted from FortiClient Cloud to FortiSASE without the need for a third-party endpoint management system.

This process should take one business week to complete. During this process, you cannot perform any provisioning of your new FortiSASE instance.

You must follow this process:

1. Contact your Fortinet Sales or Partner contact to perform one of these steps:
   - For an existing FortiClient subscription, a.k.a. the FortiClient FortiTrust subscription, to provide you with assistance with converting it to a FortiSASE user-based Standard, Advanced or Comprehensive subscription
   - For an expired FortiClient subscription, to provide you assistance with purchasing a new FortiSASE user-based subscription.

   See theFortiSASE Ordering Guide.
2. Once you have a FortiSASE user-based subscription, to request the shift from using your FortiClient Cloud instance to using your FortiSASE instance for endpoint management, contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team will assist you with these steps:
   a. Removing the FortiClient FortiTrust subscription from your FortiCloud root principal account (may take up to three business days).
   b. Creating a new Technical Support ticket to engage Fortinet technical teams to complete the request on the backend (may take up to two business days).
   c. Applying the new FortiSASE user-based subscription to your account.
3. Once the FortiClient Cloud subscription removal has completed, you will be informed via a Technical Support ticket update to either provision your FortiSASE instance on your own or to provide confirmation that Fortinet can provision your instance on your behalf.
4. After some time, the telemetry connection of each of the endpoints will be disconnected from FortiClient Cloud and will connect to the FortiSASE instance of EMS.

- Endpoints should connect to FortiSASE EMS.
- There is no need to restart FortiClient or the endpoint. Simply wait for the next Telemetry synchronization event, which is typically within 60 seconds.

5. At this point, FortiSASE must be configured for endpoint management. See How can I configure FortiSASE for endpoint management? on page 797

How can I configure FortiSASE for endpoint management?

Shifting from an on-premise EMS or a FortiClient Cloud instance to FortiSASE does not preserve EMS configuration.

You cannot configure some configuration settings from EMS or FortiClient Cloud in FortiSASE because FortiSASE does not support some FortiClient features. See Supported FortiClient features.

You must configure endpoint management features in the FortiSASE instance of EMS using the FortiSASE portal. This requires hands-on configuration time with the following options:

- To perform the configuration themselves, follow these steps:
  a. Review FortiSASE documentation, namely the 4-D FortiSASE Endpoint Management Deployment Guide, for details on configuring endpoint management features.
  b. Purchase an Advanced or Comprehensive subscription and use *Assisted Onboarding*. See *FortiSASE Support Services* in the FortiSASE Ordering Guide.
  c. Perform the configuration in FortiSASE by logging in with the root principal email.
- If you want Fortinet to perform the endpoint management configuration in FortiSASE, purchase Fortinet Professional Services. See *FortiSASE Support Services* in the FortiSASE Ordering Guide.

Shifting from standalone VPN-only FortiClient (free) to FortiSASE

I am an existing customer with a FortiClient VPN-only standalone endpoints connecting to FortiGate using SSL or IPsec connections. What is the path to move my endpoints to FortiSASE?

Shifting from a FortiClient VPN-only standalone deployment to FortiSASE requires purchasing additional FortiSASE subscriptions and redeployment of the FortiClient version with additional modules provided by FortiSASE on all endpoints. See the FortiSASE Ordering Guide and contact your Fortinet Sales/Partner/Reseller for licensing details and support options.

Standalone VPN-only FortiClient has a limited feature set. Endpoints with Standalone VPN-only FortiClient are not licensed for management connection to FortiClient EMS.

For FortiGate administrators, a free version of FortiClient VPN is available which supports basic IPsec and SSL and does not require registration with EMS. This version does not include central management, technical support, or some advanced features. The free VPN-only client does support SAML. See Standalone VPN client or FortiClient standalone and licensed version feature comparison.

Shifting to FortiSASE involves these shifts:

	FortiClient VPN-only standalone deployment	FortiSASE deployment
Security Services	FortiOS platform and FortiGuard Services	
Licensing	None	User-based licensing
Endpoint Deployment	Free FortiClient VPN-only version	FortiClient version provided by FortiSASE service
Remote user connectivity	SSL, IPsec	IPsec
Technical Support	None	Included with user-based licensing

FortiSASE supports remote user connectivity from FortiClient using IPsec.

For new instances, the recommended version is FortiClient 7.4.6 for instances with IPsec remote agent support enabled which includes remote user connectivity to FortiSASE using IPsec.

For existing instances, the recommended version is FortiClient 7.2.14 for instances with IPsec remote agent support enabled which includes remote user connectivity to FortiSASE using IPsec. This includes all new instances created between 24.4.b.1 and 25.4.c.

The recommended version is FortiClient 7.2.14 for instances with remote user connectivity to FortiSASE using SSL for instances created before 24.4.b.1.

See Product integration and support.

Starting in FortiSASE 24.4.b.1, IPsec remote agent support is enabled by default on new instances.

For instances created before 24.4.b.1, implementing IPsec remote agent support is a significant mode change that impacts the overall operation of the FortiSASE instance. It has several constraints and is subject to continual improvements.

- It cannot be disabled or reverted without significant data loss and service disruption.
- Fortinet recommends that a request to implement IPsec remote agent support be raised only after careful consideration and understanding of impact and service disruptions.

See IPsec remote agent support on page 54.

To move endpoints to FortiSASE, the following steps are required:

1. Purchase FortiSASE licensing from Fortinet Sales/Partner/Reseller. See FortiSASE Ordering Guide for FortiSASE licensing and support options.
2. Plan and schedule a full redeployment of FortiClient on the endpoints, which involves these steps:
   a. Uninstall FortiClient VPN-only standalone.
   b. Install the full FortiClient version currently supported with FortiSASE.
   c. Depending on the configured FortiClient installer type in FortiSASE, complete post-install steps. See Managed endpoint client onboarding on page 731.
      - *Pre-configured*: installer is preconfigured to connect with FortiSASE, that is, the invitation code is built-in.
      - *Manual*: after downloading and launching the installer, users must manually enter the invitation code sent in the email.
3. Configure FortiSASE for endpoint management. See How can I configure FortiSASE for endpoint management? on page 797

Appendix A - FortiSASE data centers

Remote users in mainland China connecting to a FortiSASE security point of presence (PoP) outside the country for secure internet access may encounter suboptimal performance, including slower or less direct routing to the nearest FortiSASE security PoP. This is largely due to the impact of the regulatory framework controlling internet traffic in and out of mainland China, which can result in delays, traffic filtering, or throttling that affects overall connectivity and performance.

The following provides information about FortiSASE data centers or security PoPs available through the *FortiSASE Status* page, global data centers list, and egress IP addresses feed. The following also provides information about the number of security data centers accessible per subscription.

Status page

To view real-time information on the current status of data centers, visit the FortiSASE Status page at https://status.fortisase.com and click the plus sign (+) next to *Fortinet Cloud Locations* or *Public Cloud Locations*.

Global data centers list

For a table of global data center information for FortiSASE, see Global data centers.

Access locations list

For a table of public cloud locations with network edge capabilities, see Appendix A1 - Access locations on page 803.

Egress IP addresses feed

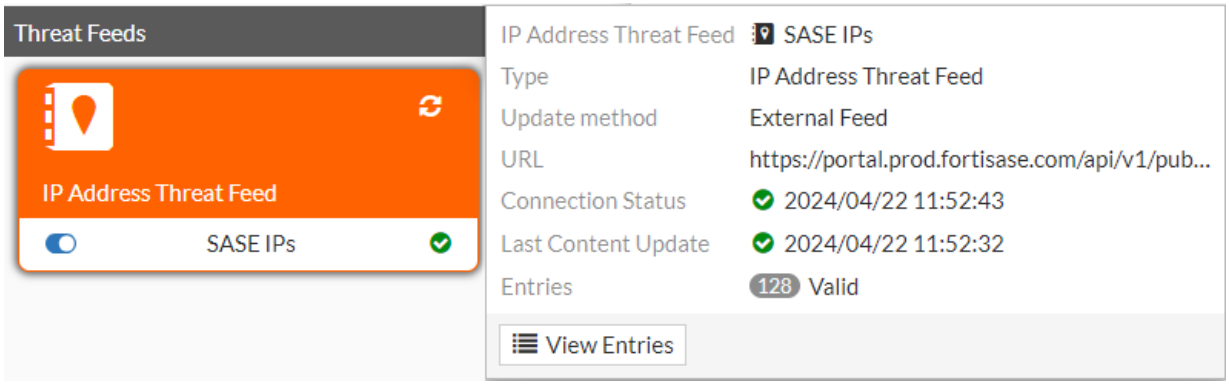
A consumable feed of the FortiSASE egress IP addresses is available at https://portal.prod.fortisase.com/api/v1/public/egress/ips.

You can use this list in access control lists to allow access to internal applications from FortiSASE only.

The following describes how to configure a threat feed using this feed in FortiOS. For information on threat feeds, see Threat feeds.

To create a threat feed using the FortiSASE egress IP address feed:

1. Go to *Security Fabric > External Connectors*.
2. Click *Create New*.
3. Under *Threat Feeds*, select *IP Address*.
4. In the *URL of external resource* field, enter https://portal.prod.fortisase.com/api/v1/public/egress/ips
5. Disable *HTTP basic authentication*.
6. Ensure that *Status* is enabled.
7. Configure other fields as desired, then click *OK*.
8. To confirm that you configured the feed correctly, wait until the GUI displays that the connection succeeded. Hover over the feed to see the connection status, last update time, and number of entries. You can use this feed to configure policies in FortiOS.



Considerations

- For instances equipped with dedicated public IP addresses (via SKU addition or through Standard, Advanced or Comprehensive subscriptions), the egress IP API does not include the IP addresses associated with each FortiSASE security PoP as they are customer-specific.
- The egress IP addresses feed includes IP addresses for log forwarding and the FortiSASE Endpoint Management Service. Having administrators of all instances, including those with dedicated IP addresses, use the egress IP addresses feed to allowlist traffic from both FortiSASE services based on their specific needs is recommended.

Number of security data centers accessible per subscription

The number of data centers with security capabilities that are accessible by remote users depends on the FortiSASE subscription tier and number of users, or user bands, applied to your FortiSASE instance. See the

following table:

FortiSASE subscription	Number of security data centers accessible per user band		
	50-99 users	100-199 users	200+ users
Standard	2 to 4	2 to 4	2 to 4
Advanced			
Comprehensive	1	1 to 2	1 to 4
Not-for-Resale (NFR)	2 (50 users)	N/A	N/A
Advanced NFR			

For the FortiGate SASE bundle subscription, the FortiGate model in use determines the number of available FortiSASE security PoPs or data centers available. See Product integration and support.

For the following subscription tiers, you can purchase access to additional security data centers with the corresponding FortiSASE Security PoP Add-on subscription:

FortiSASE subscription	Security PoP Add-on subscription
Standard	Fortinet Security PoP Add-on (1 to 16 locations)
Advanced	
Comprehensive	• Fortinet Security PoP Add-on (1 to 16 locations) • Public Cloud Location Add-on (1 to 16 locations) • Global Region Add-on (unlimited number of locations selected from existing and future Fortinet Cloud and Public Cloud locations)

See the FortiSASE Ordering Guide.

Considerations

- New instances with the FortiSASE Comprehensive subscription applied can select a combination of Fortinet and Public Cloud locations during initial provisioning. The maximum number of Fortinet and Public Cloud data centers accessible still depends on the number of users specified for the Comprehensive subscription and the specific security PoP add-on subscriptions applied.
- Fortinet Location and Public Cloud Location Branch On-ramp licenses can be applied to a FortiSASE instance with the Comprehensive or Advanced subscription. On-ramp locations can only be provisioned based on the licenses registered, be that a Fortinet Location or Public Cloud Location.
- With the Fortinet security PoP add-on subscription or Public Cloud Region Add-on subscription and different FortiSASE subscription tiers, access to a maximum of 16 additional security data centers, or a maximum total of 20 security data centers, is possible.
- With the Global Region Add-on subscription added to an instance with the FortiSASE Comprehensive subscription:

    - An unlimited number of security data centers selected from existing and future Fortinet Cloud and Public Cloud locations is possible.
    - Fortinet Cloud locations except for Hong Kong and Dubai - UAE onshore locations are selected by default. As needed, you can select an unlimited number of Public Cloud locations or deselect any number of Fortinet Cloud locations.
- During initial provisioning, you can select fewer security sites than the maximum you are entitled to. In this case, upon each login, the FortiSASE portal prompts you to select up to the maximum number of security sites. If you add additional security sites using this prompt, then FortiSASE allows for increasing the number of security sites without FortiCare Support. FortiSASE may experience up to 10 minutes of downtime when you apply the subscription. If any errors occur, FortiSASE cannot automatically rollback without FortiCare Support. For provisioning, you must select a minimum of two security sites for redundancy.
- As the number of users and bandwidth increases, dynamic scaling of FortiSASE customer environments is required by adding additional dedicated IP addresses to the instance's security PoPs to support a higher session count. When this occurs, the following administrator updates are required, if applicable to customer environments:
    - Depending on the size of the customer, the mode configuration private IP address space used by IPsec between the FortiGate SPA hub and security PoPs should be configured as a /24 subnet. In some cases, it may need to be even larger than a /24 subnet. See IPsec VPN configuration.
    - If the FortiGate SPA hub has policies that restrict access, ensure these policies are configured to accomodate the IPsec mode configuration private IP address space. See Restricting access using a FortiGate SPA hub/spoke policy on page 146.
    - When FortiSASE remote users are on a customer premise where outbound filtering is used, ensure that the security PoP public IP addresses specified in those filters are updated to include the new addresses.
    - It is common for SaaS applications to implement conditional access based on source IP addresses. Since user traffic steered to FortiSASE is sourced with the security POP public IP, ensure conditional access rules in SaaS applications are updated to include the new addresses.
    - The currently configured IPAM pool size needs to large enough to account for additional subnets associated with the added public IP addresses. Each public IP address requires at least 1 /20 subnet from the IPAM pool. See IPAM on page 278.

Appendix A1 - Access locations

The following table lists public cloud locations with network edge capabilities also known as access locations (noted by *Access Location* column with *Yes*). See Network edge locations.

Access locations whose naming convention includes *-E* are designed for user traffic to securely enter the public cloud network through the closest location. Therefore, when provisioning your instance in the FortiSASE portal, the administrator can only select corresponding public cloud locations whose naming convention includes *-G* because those locations include security capabilities. See Global data centers.

Cloud	Location	Analytics location	Endpoint management location	Access location	Availability
Public	Amsterdam - Netherlands (AMS-E1)	No	No	Yes	Comprehensive Subscription
Public	Ashburn - Virginia - USA (IAD-E1)	No	No	Yes	Comprehensive Subscription
Public	Athens - Greece (ATH-E1)	No	No	Yes	Comprehensive Subscription
Public	Atlanta - Georgia - USA (ATL-E1)	No	No	Yes	Comprehensive Subscription
Public	Auckland - New Zealand (AKL-E1)	No	No	Yes	Comprehensive Subscription
Public	Aurora - Illinois - USA (ORD-E1)	No	No	Yes	Comprehensive Subscription
Public	Austin - Texas - USA (AUS-E1)	No	No	Yes	Comprehensive Subscription
Public	Bangkok - Thailand (BKK-E1)	No	No	Yes	Comprehensive Subscription
Public	Barcelona - Spain (BCN-E1)	No	No	Yes	Comprehensive Subscription
Public	Berlin - Germany (BER-E1)	No	No	Yes	Comprehensive Subscription
Public	Bogotá - Colombia (BOG-E1)	No	No	Yes	Comprehensive Subscription
Public	Boston - Massachusetts - USA (BOS-E1)	No	No	Yes	Comprehensive Subscription
Public	Brisbane - Australia (BNE-E1)	No	No	Yes	Comprehensive Subscription
Public	Brussels - Belgium (BRU-E1)	No	No	Yes	Comprehensive Subscription
Public	Bucharest - Romania (OTP-E1)	No	No	Yes	Comprehensive Subscription

Cloud	Location	Analytics location	Endpoint management location	Access location	Availability
Public	Budapest - Hungary (BUD-E1)	No	No	Yes	Comprehensive Subscription
Public	Buenos Aires - Argentina (EZE-E1)	No	No	Yes	Comprehensive Subscription
Public	Busan - South Korea (PUS-E1)	No	No	Yes	Comprehensive Subscription
Public	Calgary - Canada (YYC-E1)	No	No	Yes	Comprehensive Subscription
Public	Canberra - Australia (CBR-E1)	No	No	Yes	Comprehensive Subscription
Public	Cape Town, South Africa (CPT-E1)	No	No	Yes	Comprehensive Subscription
Public	Chennai - India (MAA-E1)	No	No	Yes	Comprehensive Subscription
Public	Chicago - Illinois – USA (CHI-E1)	No	No	Yes	Comprehensive Subscription
Public	Columbus - Ohio - USA (CMH-E1)	No	No	Yes	Comprehensive Subscription
Public	Copenhagen - Denmark (CPH-E1)	No	No	Yes	Comprehensive Subscription
Public	Council Bluffs - Iowa - USA (OMA-E1)	No	No	Yes	Comprehensive Subscription
Public	Dallas - Texas - USA (DFW-E1)	No	No	Yes	Comprehensive Subscription
Public	Dammam - Saudi Arabia (DMM-E1)	No	No	Yes	Comprehensive Subscription
Public	Delhi - India (DEL-E1)	No	No	Yes	Comprehensive Subscription
Public	Denver - Colorado - USA (DEN-E1)	No	No	Yes	Comprehensive Subscription

Cloud	Location	Analytics location	Endpoint management location	Access location	Availability
Public	Doha - Qatar (DOH-E1)	No	No	Yes	Comprehensive Subscription
Public	Dubai - United Arab Emirates (DXB-E1)	No	No	Yes	Comprehensive Subscription
Public	Dublin - Ireland (DUB-E1)	No	No	Yes	Comprehensive Subscription
Public	Düsseldorf - Germany (DUS-E1)	No	No	Yes	Comprehensive Subscription
Public	Frankfurt - Germany (FRA-E1)	No	No	Yes	Comprehensive Subscription
Public	Fujairah - United Arab Emirates (FJR-E1)	No	No	Yes	Comprehensive Subscription
Public	Geneva - Switzerland (GVA-E1)	No	No	Yes	Comprehensive Subscription
Public	Hamburg - Germany (HAM-E1)	No	No	Yes	Comprehensive Subscription
Public	Helsinki - Finland (HEL-E1)	No	No	Yes	Comprehensive Subscription
Public	Hong Kong - China (HKG-E1)	No	No	Yes	Comprehensive Subscription
Public	Houston - Texas - USA (IAH-E1)	No	No	Yes	Comprehensive Subscription
Public	Hsinchu - Taiwan (TPE-E1)	No	No	Yes	Comprehensive Subscription
Public	Hyderabad - India (HYD-E1)	No	No	Yes	Comprehensive Subscription
Public	Jakarta - Indonesia (JKT-E1)	No	No	Yes	Comprehensive Subscription
Public	Johannesburg - South Africa	No	No	Yes	Comprehensive Subscription

Cloud	Location	Analytics location	Endpoint management location	Access location	Availability
	(JNB-E1)				
Public	Kansas City - Missouri - USA (MCI-E1)	No	No	Yes	Comprehensive Subscription
Public	Kolkata - India (CCU-E1)	No	No	Yes	Comprehensive Subscription
Public	Kuala Lumpur - Malaysia (KUL-E1)	No	No	Yes	Comprehensive Subscription
Public	Kyiv - Ukraine (KBP-E1)	No	No	Yes	Comprehensive Subscription
Public	Lagos - Nigeria (LOS-E1)	No	No	Yes	Comprehensive Subscription
Public	Las Vegas - Nevada - USA (LAS-E1)	No	No	Yes	Comprehensive Subscription
Public	Lisbon - Portugal (LIS-E1)	No	No	Yes	Comprehensive Subscription
Public	London - United Kingdom (LON-E1)	No	No	Yes	Comprehensive Subscription
Public	Los Angeles - California - USA (LAX-E1)	No	No	Yes	Comprehensive Subscription
Public	Madrid - Spain (MAD-E1)	No	No	Yes	Comprehensive Subscription
Public	Manchester - United Kingdom (MAN-E1)	No	No	Yes	Comprehensive Subscription
Public	Manila - Philippines (MNL-E1)	No	No	Yes	Comprehensive Subscription
Public	Marseille - France (MRS-E1)	No	No	Yes	Comprehensive Subscription
Public	Melbourne - Australia (MEL-E1)	No	No	Yes	Comprehensive Subscription

Cloud	Location	Analytics location	Endpoint management location	Access location	Availability
Public	Milan - Italy (MIL-E1)	No	No	Yes	Comprehensive Subscription
Public	Miami - Florida - USA (MIA-E1)	No	No	Yes	Comprehensive Subscription
Public	Minneapolis - Minnesota - USA (MSP-E1)	No	No	Yes	Comprehensive Subscription
Public	Mombasa - Kenya (MBA-E1)	No	No	Yes	Comprehensive Subscription
Public	Montreal - Canada (YMQ-E1)	No	No	Yes	Comprehensive Subscription
Public	Mumbai - India (BOM-E1)	No	No	Yes	Comprehensive Subscription
Public	Munich - Germany (MUC-E1)	No	No	Yes	Comprehensive Subscription
Public	Muscat - Oman (MCT-E1)	No	No	Yes	Comprehensive Subscription
Public	New York - New York - USA (JFK-E1)	No	No	Yes	Comprehensive Subscription
Public	Osaka - Japan (OSA-E1)	No	No	Yes	Comprehensive Subscription
Public	Oslo - Norway (OSL-E1)	No	No	Yes	Comprehensive Subscription
Public	Palo Alto - California - USA (SFO-E1)	No	No	Yes	Comprehensive Subscription
Public	Paris - France (PAR-E1)	No	No	Yes	Comprehensive Subscription
Public	Perth - Australia (PER-E1)	No	No	Yes	Comprehensive Subscription
Public	Philadelphia - Pennsylvania - USA (PHL-E1)	No	No	Yes	Comprehensive Subscription
Public	Phoenix - Arizona	No	No	Yes	Comprehensive

Cloud	Location	Analytics location	Endpoint management location	Access location	Availability
	- USA (PHX-E1)				Subscription
Public	Portland - Oregon - USA (PDX-E1)	No	No	Yes	Comprehensive Subscription
Public	Prague - Czechia (PRG-E1)	No	No	Yes	Comprehensive Subscription
Public	Querétaro - Mexico (QRO-E1)	No	No	Yes	Comprehensive Subscription
Public	Rio de Janeiro - Brazil (GIG-E1)	No	No	Yes	Comprehensive Subscription
Public	Rome - Italy (FCO-E1)	No	No	Yes	Comprehensive Subscription
Public	Salt Lake City - Utah - USA (SLC-E1)	No	No	Yes	Comprehensive Subscription
Public	San Antonio - Texas - USA (SAT-E1)	No	No	Yes	Comprehensive Subscription
Public	San Jose - California - USA (SJC-E1)	No	No	Yes	Comprehensive Subscription
Public	Santa Clara - California - USA (SJC-E2)	No	No	Yes	Comprehensive Subscription
Public	Santiago - Chile (SCL-E1)	No	No	Yes	Comprehensive Subscription
Public	Seattle - Washington - USA (SEA-E1)	No	No	Yes	Comprehensive Subscription
Public	Seoul - South Korea (SEL-E1)	No	No	Yes	Comprehensive Subscription
Public	Singapore - Republic of Singapore (SIN-E1)	No	No	Yes	Comprehensive Subscription
Public	São Paulo - Brazil (SAO-E1)	No	No	Yes	Comprehensive Subscription

Cloud	Location	Analytics location	Endpoint management location	Access location	Availability
Public	Sofia - Bulgaria (SOF-E1)	No	No	Yes	Comprehensive Subscription
Public	Stockholm - Sweden (ARN-E1)	No	No	Yes	Comprehensive Subscription
Public	Sydney - Australia (SYD-E1)	No	No	Yes	Comprehensive Subscription
Public	Taipei - Taiwan (TPE-E1)	No	No	Yes	Comprehensive Subscription
Public	Tel Aviv - Israel (TLV-E1)	No	No	Yes	Comprehensive Subscription
Public	Tokyo - Japan (TYO-E1)	No	No	Yes	Comprehensive Subscription
Public	Toronto - Canada (YTO-E1)	No	No	Yes	Comprehensive Subscription
Public	Turin - Italy (TRN-E1)	No	No	Yes	Comprehensive Subscription
Public	Vancouver - Canada (YVR-E1)	No	No	Yes	Comprehensive Subscription
Public	Vienna - Austria (VIE-E1)	No	No	Yes	Comprehensive Subscription
Public	Warsaw - Poland (WAW-E1)	No	No	Yes	Comprehensive Subscription
Public	Zagreb - Croatia (ZAG-E1)	No	No	Yes	Comprehensive Subscription
Public	Zürich - Switzerland (ZRH-E1)	No	No	Yes	Comprehensive Subscription

Appendix B - REST API

See the FortiSASE REST API reference on the Fortinet Developer Network.

Appendix C - Tunnel performance

Latency

High latency can have a significant impact on a user's observed internet performance.

When using FortiSASE, the goal is to ingress and egress traffic from the Fortinet network while introducing the smallest possible amount of network latency. FortiSASE achieves this by using high-quality internet service providers (ISP) and internet exchange points to minimize network hops.

In general, physical distance (e.g. the speed of light) and third party ISP routing to the last-mile introduce most network latency between the user and FortiSASE security point of presence (PoP).

Evaluating and selecting security PoPs for lowest latency

Prior to provisioning FortiSASE, evaluating which FortiSASE security PoP will provide the lowest latency to your end users' locations and selecting these during provisioning is recommended.

To determine this, you can test the egress IP addresses in Appendix A - FortiSASE data centers on page 800 via `ping`, `traceroute`, or `mtr`. Alternatively, you can perform basic speed tests or advanced speed tests using `iperf3` with https://speed.fortisase.com/. See Technical Tip: Proper Bandwidth test with FortiSASE SIA VPN.

Keep these latency thresholds in mind when evaluating these selections:

Latency level	Impact to performance	Latency (milliseconds (ms))
Ideal	Best performance	< 20 ms
Acceptable	Slightly impacted	20-60 ms
High	Moderately impacted	60-100 ms
Extreme	Significantly impacted	> 100 ms

Jitter and packet loss

Even if you observe ideal latency of under 20 ms in testing, packet loss and jitter can significantly impact performance.

- Jitter should be under 30 ms.
- Packet loss should be 0%.

You will observe significant degradation particularly for real-time communications (VoIP, video, and so on) beyond 30 ms of jitter and/or 1% packet loss.

Resolving increased latency with SSL support for DTLS

While downloading a large file (100 MB or above) when using FortiSASE, you may observe increased latency (280 ms or above). SSL support for DTLS is supported in FortiClient to resolve increase latency. See Supported FortiClient features.

Starting in 23.4.b, DTLS support is enabled by default for existing and new FortiSASE instances.

Appendix D - Maximum values

This topic provides minimum and maximum values for configuration settings in FortiSASE:

Setting	Minimum value	Maximum value
Dedicated IPs per Fortinet cloud security PoP	1	5
Dedicated IPs per public cloud security PoP		
Edge devices: FortiExtender as FortiSASE LAN extension	0	1024
External feeds External host feeds do not have a category ID, and as such, they are not counted towards the maximum value.		21
Host addresses		20000
Number of ports per *Security* > *Services* entry		16
Secure private access service connections (hubs)		12
Agent and proxy policies combined		10000
Zero trust network access connection rules		32000
Security profile groups		245

Appendix E - Monthly maintenance

This topic describes the monthly maintenance schedule and impact for FortiSASE.

Monthly maintenance impact

During a scheduled maintenance window, Fortinet performs a rolling software update, which means not all instances are upgraded at the same time, with some instances still running the previous software version.

There is potential for short connectivity impact (approximately one to two minutes) for each customer instance and the configuration portal while these components are updated.

Endpoint management functionalities, including endpoint profile configuration and some zero trust network access (ZTNA) functionality, may be intermittently inaccessible while the upgrade is occurring.

For a list of new features included in the FortiSASE software release, see What's new.

Monthly maintenance schedule



To change your FortiSASE instance's maintenance window, contact Fortinet Support to request a change through a new technical support ticket. See Security PoPs on page 791 for details on the impact of any security PoP changes.

Typically, Fortinet performs monthly software upgrades for customers' FortiSASE instances during the first or second week of the month.

To minimize customer impact, rolling software upgrades are performed per region within an eight-hour maintenance window outside of business hours for the customer's primary security PoP at the equivalent local time:

Group	Time range EST (UTC)	Time range EDT (UTC)
Maintenance window group 1	12 PM to 8 PM EST (17:00-01:00 UTC)	12 PM to 8 PM EDT (16:00-00:00 UTC)
Maintenance window group 2	6 AM to 2 PM EST (11:00-19:00 UTC)	6 AM to 2 PM EDT (10:00-18:00 UTC)
Maintenance window group 2 (Japan)	9 AM to 5 PM EST (14:00-22:00 UTC)	9 AM to 5 PM EDT (13:00-21:00 UTC)
Maintenance window group 3	4 PM to 12 AM EST (next day) (21:00-05:00 UTC)	4 PM to 12 AM EST (next day) (20:00-04:00 UTC)

To change your default upgrade window to a preferred maintenance time slot, see Software audit & version on page 252.

In addition to these maintenance window groupings, there is a *Later* group that a tenant can request to be included in, which schedules their upgrade during the last possible maintenance window (group 3) for upgrades. Contact Fortinet Support to request a schedule change through a new technical support ticket.

Maintenance window group 1: 12 PM to 8 PM EST/EDT

Fortinet cloud locations	Public cloud locations
Bangalore	Amsterdam
Dubai	Auckland
Frankfurt	Damman
Hong Kong	Doha
Istanbul	Dubai
Johannesburg	Frankfurt
Madrid	Hamina
Paris	Hong Kong
Pune	Jakarta
Valbonne	Johannesburg
	Madrid
	Manila
	Melbourne
	Milan
	Mumbai
	Paris
	Perth
	St.Ghislain
	Taipei
	Tel Aviv
	Warsaw
	Zurich

Maintenance window group 2: 6 AM to 2 PM EST/EDT

Fortinet cloud locations	Public cloud locations
Dallas/Plano	Chicago
San Jose	Dallas
Singapore	Las Vegas
Sydney	Portland
Vancouver	Querétaro
	Seoul
	Singapore

Maintenance window group 2 (Japan): 9 AM to 5 PM EST/EDT

Fortinet cloud locations	Public cloud locations
Komagome	Osaka
Tokyo	

This maintenance window is the default for new instances with Japanese security PoPs selected, and for existing instances with Japanese security PoPs with this window selected by their administrators.

Maintenance window group 3: 4 PM to 12 AM EST/EDT

Fortinet cloud locations	Public cloud locations
Ashburn	Ashburn
London	Buenos Aires
Miami	Dublin
Ottawa	Lima
Sao Paulo	London
Toronto	Miami
	Santiago
	Sao Paulo
	Toronto

The *Later* group of instances to be upgraded is included in this maintenance window. See the note in Monthly maintenance schedule on page 815.

Appendix F - Security and compliance

For up-to-date information on Fortinet's security practices and compliance posture, see the Fortinet Trust Resource Center.



www.fortinet.com

Copyright© 2026 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.