



FortiPortal - User Guide

Version 6.0.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



July 2, 2020

FortiPortal 6.0.0 User Guide

37-600-645479-20200702

TABLE OF CONTENTS

Change Log	5
FortiPortal web interface	6
Landing page	7
Reset password	8
Change Password	9
Dashboard	10
Page actions	11
Widget actions	11
Policy	13
Policy tab column settings	13
Policy data refresh	13
Revision backup	13
Viewing policy package settings	14
Creating and restoring policy revisions	14
Configuring policies	15
Adding a new policy	15
Updating a policy	15
Deleting a policy	15
Enabling or disabling a policy	15
Policy fields	15
Moving a policy	17
Re-installing the policy	18
Installing policies	18
Reviewing policies	19
Objects	20
Types of objects	20
Zone/Interface	20
Firewall Objects	21
Security Profiles	22
User & Device	24
Configuring objects	26
Adding a new object	26
Updating an object	26
Deleting an object	26
Device Manager	27
VPN	27
Configuring VPNs	27
Router	32
Configuring static routes	32
SD-WAN	34
Configuring an SD-WAN for a group of interfaces	34
Configuring an SD-WAN for an ADOM	42

Create an SD-WAN template	44
Monitoring the SD-WAN interfaces	51
Auth Server Settings	53
Local authentication	54
LDAP authentication	56
RADIUS authentication	60
TACACS+ authentication	66
DHCP Server	68
DHCP Server	68
Relay Service	71
DHCP relay fields	72
View	73
Application view	73
Attack view	74
Sandbox view	74
VPN view	75
Reports	76
Page actions	76
Additional Resources	77
Audit	78
Page actions	78
Per-audit actions	78
WiFi	79
Managed AP	80
Update a managed AP	80
Delete a managed AP	80
WiFi Monitor	80
Rogue AP	81
FAP	81
SSID	82
WiFi Profile	82
AP Profile	83
SSID	83

Change Log

Date	Change Description
2020-07-02	Initial release.

FortiPortal web interface

To analyze your event log data in the FortiPortal, customize reports, view the status of your network devices, view and configure security policies, you can use the FortiPortal web interface.

After a successful log in, the interface displays the dashboard page.



To select a different language for this session, log out and select a language on the log-in page.

The top banner is common for all of the pages and includes the following action buttons:

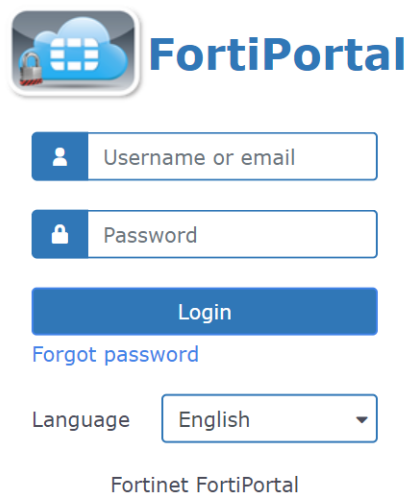
- *Help*—additional window that displays the Help pages
- *Alerts*— window that displays the unread alerts
- *Change Password*—raises a dialog box for password change
- *Logout*—log out of the tool

The left panel might contain the following selections:

- *Dashboard*—widgets that display information about the FortiPortal (FP)
- *Policy* —page for viewing and modifying security policies
- *Objects*— page for viewing and modifying firewall objects and security profiles
- *Device Manager*—manage virtual private networks (VPNs) and static routes
- *View*—different views of the security event logs
- *Reports*—lists of available reports
- *Additional Resources*—page to launch external pages such as a ticketing system
- *Audit*—a log of user activity on the Administrative Web Interface
- *WiFi*—wireless networks, listed by site or by SSID

Landing page

When you open FortiPortal to log in to the system, you see a custom landing page. The following figure shows the default landing page:

The image shows the FortiPortal login interface. At the top left is the FortiPortal logo, which consists of a blue cloud icon with a white grid pattern and a red padlock, followed by the text "FortiPortal" in a bold blue font. Below the logo are two input fields: the first is labeled "Username or email" with a person icon, and the second is labeled "Password" with a padlock icon. Below these fields is a blue "Login" button. Under the "Login" button is a link that says "Forgot password". Below the "Forgot password" link is a "Language" label followed by a dropdown menu currently set to "English". At the bottom of the interface is the text "Fortinet FortiPortal".

FortiPortal

Username or email

Password

Login

[Forgot password](#)

Language English

Fortinet FortiPortal

FortiPortal supports the following languages: English, French, German, Portuguese, Romanian, Spanish, and Italian.

Reset password

On the Login page, select the *Forgot password* link to display a dialog window:

Reset your password

✕

Please enter your email address and we will send you a temporary password

* Email:

Send

Cancel

Enter the email address associated with your user account. The system resets your password and sends you a temporary password by email.

Change Password

Selecting the *Change Password* icon on the page banner displays this dialog window:

Change Password ⓘ

Old Password

New Password

Confirm New Password

Save

Cancel

Enter your existing password and a new password that will take effect on your next login attempt.

Dashboard

The dashboard displays different views of the security event logs and other information.

When FortiPortal is running in FortiAnalyzer mode, the dashboard looks like the following:



As shown in the figures, the dashboard is organized as a set of widgets.

In FortiAnalyzer mode, the following widgets are available:

- Top Countries
- Top Threats
- Top Sources
- Top Destinations
- Top Applications
- Policy Hits
- Rogue Access Points
- Authorized Access Points
- Authorized SSIDs
- WiFi Clients
- Admin Logins
- System Events
- Resource Usage

Page actions

The following actions are available on the dashboard:

- *Add Widget*—add a widget to the dashboard
- *Scope*—view widget output (All, site, or wireless)
- *Filter*—filter the data (last 5 minutes to last 7 days or a custom filter)
- *Refresh*—refresh the data

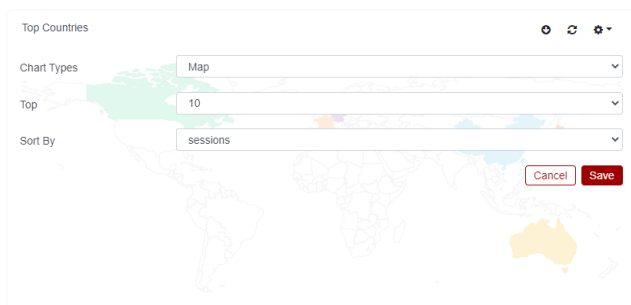
Widget actions

In FortiAnalyzer mode, the top banner on each widget provides some or all of the following controls:

- *Drill-down*—visible in the widgets that support drill-down capability
- *Edit Settings*—edit the widget
- *Refresh*—refresh the data
- *Delete*—delete the widget

Edit settings

In FortiAnalyzer mode, selecting the *Edit Settings* icon opens a window within the widget allows you to select the chart type, top N results, and how to sort the data.



Drill-down capability

The drill-down icon (🔍) indicates that you can get more information about the data displayed in the widget.

In FortiAnalyzer mode, the following widgets support the drill-down capability:

- Top Countries
- Top Threats
- Top Sources
- Top Destinations
- Top Applications

Each of these widgets displays a graph or bar chart with the top N results, where the result is an application, region, traffic, or attack (depending on the widget). When you select one of the results, the View page opens with a view filtered by that result. The view filter is listed above the table.

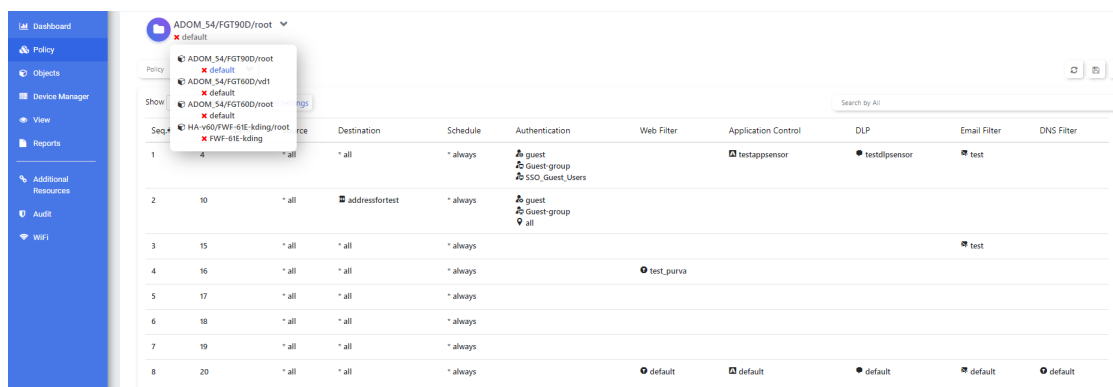
Application Name	Application ID	Category	Sent Bytes	Received Bytes	Sent Packets	Received Packets	Users	Service
Anydesk-Anydesk (France)		Unknown	232	172	6	4	hexu	ANYDESK-ANYDESK
Anydesk-Anydesk (France)		Unknown	1152	944	22	18		ANYDESK-ANYDESK
udp/5355		Unscanned	0	0	0	0		UDP/5355
udp/5355		Unscanned	0	0	0	0		UDP/5355
udp/5355		Unscanned	0	0	0	0		UDP/5355

The application name in each table entry also displays the region name (in brackets).

Policy

Go to *Policy* and select *Policy* from the dropdown list. Click on the current policy package to see a hierarchical view of the policy packages.

Each package might be associated with either one or more FortiGate devices or VDOMs or all devices within an ADOM.



The page includes a dropdown list and a hierarchical view of policies at the top. When you select an entry in the hierarchical view, the main panel displays the policy data associated with that entry.

Policy tab column settings

You can select the columns to display in the *Policy* tab:

1. Select the *Column Settings* button to display the Column Settings form.
2. Select the columns you want to display, clear the columns that you want to hide, and select *Apply*.

Policy data refresh

The policy information is refreshed every hour from the FortiManager. You can also refresh the data on demand by selecting the *Refresh* button.

Revision backup

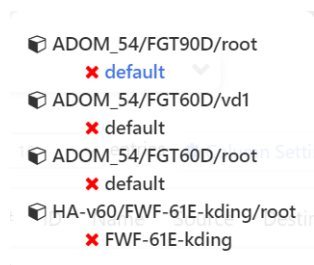
The system can save only one revision of the current policy and object data. The new revision overwrites the existing backup (if one exists).

Observe the following restrictions:

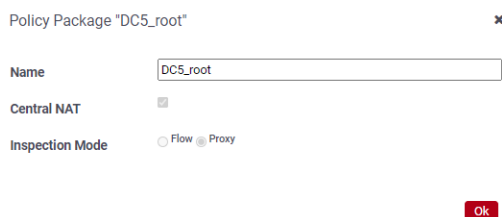
- Customer must be part of only one ADOM.
- No other customer can be part of that ADOM.

Viewing policy package settings

Policy packages are listed at the top of the *Policy* pane.



To check settings that affect all policies in a package, click on the eye icon next to the policy package to view it.

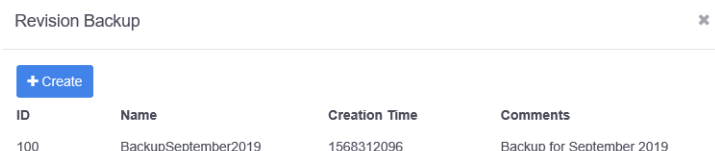


The Policy Package dialog box includes the inspection mode for FortiManager 5.6 and later. All policies in a policy package must have the same inspection mode. For FortiManager 5.4 and later, the default setting for the inspection mode is *Proxy*.

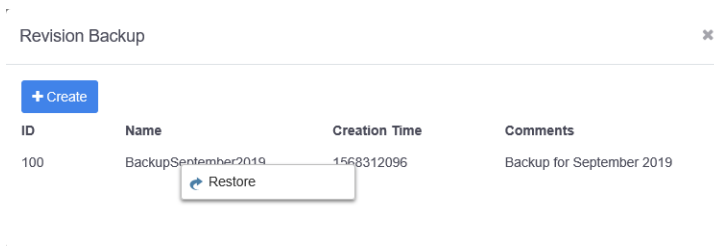
Creating and restoring policy revisions

Select the *Revision Backup* button to open the *Revision Backup* window.

Select the *Create* button to define a backup of the current policy and object data. If one exists, the *Revision Backup* window provides details:



To restore the backup, right-click the entry and select *Restore*.



ID	Name	Creation Time	Comments
100	BackupSeptember2019	1568312096	Backup for September 2019

Configuring policies

Go to *Policy* to create and edit policies.

Your service provider can grant write access to your policies. If so, you are enabled to add/edit/delete, enable/disable, and change the order of the policies. If not, FortiPortal displays a warning message and restricts the data in the Policy page to read-only.

Adding a new policy

1. Right-click a policy in the list and select *Create New*.
2. Enter values in the relevant fields and select *Save*.

Updating a policy

1. Right-click the policy in the list and select *Edit*.
2. Modify the relevant fields and select *Save*.

Deleting a policy

Right-click the policy in the list and select *Delete*.

Enabling or disabling a policy

Right-click the policy in the list and select *Enable* or *Disable*. A policy in disabled state is marked with a red circle in the Seq.# column.

Policy fields

The Create New Policy/Edit Policy form contains the following fields (see the figure after the table for an example form):

Settings	Guidelines
Name	Type a name for this policy.
Groups(s)	Select one or more user groups from the drop-down list that will be controlled by this policy.
User(s)	Select one or more users from the drop-down list that will be controlled by this policy.
Source Address	Select to add one or more address objects.
Outgoing Interface	Select one or more interfaces from the drop-down list.
Destination Address	Select to add one or more address objects.
Schedule	Select one entry from the drop-down list.
Service	Select one or more services from the drop-down list.
Action	Accept or deny.
If the action is set to Deny	
Log Violation Traffic	Select this check box to create a log for each denied packet.
If the action is set to Accept	
NAT	If you select this option, network address translation is used.
Use Destination Interface Address	Select to use the destination interface address. This setting is enabled by default. Optionally, select <i>Fixed Port</i> .
Dynamic IP Pool	If you select this option, specify the IP pool to use.
Logging Options	Logging Options
No Log	No log is generated.
Log Security Events	Creates a log for each security event.
Log All Sessions	Logs all sessions. Requires extensive system resources and storage space. If you select this option, you can optionally select <i>Generate Logs when Session Starts</i> and <i>Capture Packets</i> .
Other Options	
Enable Web Cache	Enable web caching for this traffic.
Enable WAN Optimization	Enable WAN Optimization for this traffic.
Enable Disclaimer	Enable Disclaimer for this type of traffic.
Redirect URL	Configure the redirect URL of the disclaimer.
Resolve User Names Using FSSO Agent	Authenticate user credentials with FortiAuthenticator.
Security Profiles	Enable one or more security profiles for this traffic and then select the appropriate profiles to use.

Settings	Guidelines
Traffic Shaping	Apply traffic shaping to this traffic. The amount of shaping applied depends on the traffic priority that you configure (Guaranteed, High, Medium, Low).
Reverse Direction Traffic Shaping	Apply traffic shaping to the traffic coming in the reverse direction.
Per-IP Traffic Shaping	Apply the traffic shaping per-IP.
Add tags	You can add tags for tag management. Type a tag in the text field and select the add icon to apply the tag to the policy.
Comments	Type optional comments for the policy.

The following figure shows the *Create New Policy* dialog:

Create New Policy

Name:

Groups(s):

User(s):

Incoming Interface:

Source Internet Service: ☐

Source Address:

Outgoing Interface:

Destination Internet Service: ☐

Destination Address:

Schedule:

Service:

Action:

☒ Log Violation Traffic

Comments: 0/1023

Moving a policy

Policy move is not supported for FortiManager 5.4.0 or later release.

To change the order of the policies:

1. Right-click the policy in the list and select *Move*.
The system opens a dialog box, showing the policy ID of the selected policy.
2. Select the option of *Before* or *After*.

3. Enter the target Policy ID.



Enter the ID, NOT the sequence number.

The system moves the selected policy to before/after the target.

Re-installing the policy

After you add or change a policy, select *Installation* to view the installation targets. Right-click a target and select *Re-install* to re-install the policy packages to the assigned devices.

For additional information about policy types, refer to the chapter on Policy and Objects in the [FortiManager Administrative Guide](#).

Installing policies

Go to *Policy > Installation* to install or reinstall policy packages.

To install a policy package:

1. Go to *Policy* and click the policy package to open a hierarchical view of the policy packages.
2. Select the policy package of your choice and click *Installation*.

The *Policy Package* dialog box opens.

Installation Target	Policy Package Status
<input checked="" type="checkbox"/> FortiGate-VM64-154[root]	installed
<input type="checkbox"/> FortiGate-VM64-155[root]	installed

By default, the device that your policy package is listed under is selected in the *Policy Package* dialog box.

3. Select one or more devices from the list.
4. Click *Install*.
The progress bar on the *Policy Package* dialog shows the status of the installation.
5. Once the policy package is installed, click *Finish*.

Reviewing policies

Click *Policy* , from the dropdown list, select *Review* to see all policies and firewall objects that have been configured.

Policy

ID	Source Interface	Destination Interface	Source	Destination	Action	Status	NAT	Service	Schedule	Authentication	Log	Security Profiles	Comments
1	OL_INET_0 OL_MPLS_0	port10	* all	* all	accept	enable	enable	ALL	* always		Log Security Events	no-inspection	
6	OL_INET_0 OL_MPLS_0	port1	* all	* all	accept	enable	enable	ALL	* always		Log Security Events	no-inspection	
3	port2 port3	port10	* all	* all	accept	enable	enable	ALL	* always		Log Security Events	no-inspection default	
4	OL_INET_0 OL_MPLS_0	OL_INET_0 OL_MPLS_0	* all	* all	accept	enable	disable	ALL	* always		Log Security Events	no-inspection	

Address

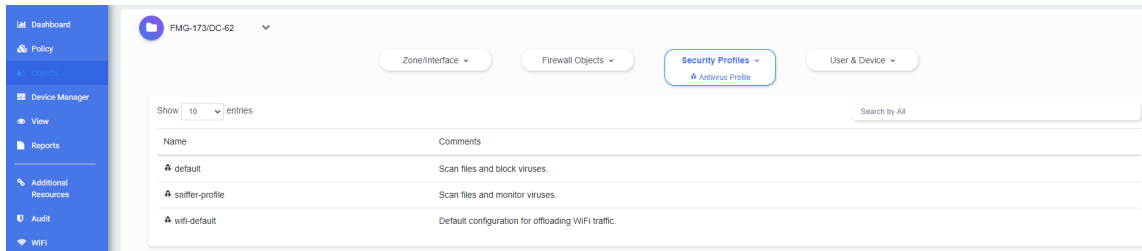
Name	Type	Interface	Default Mapping	Comments
FABRIC_DEVICE	Address	any	IP/MASK:0.0.0.0/0.0.0.0	IPv4 addresses of Fabric Devices.
FGT4_internal	Address	any	IP/MASK:10.100.4.0/255.255.255.0	
FGT5_internal	Address	any	IP/MASK:10.100.5.0/255.255.255.0	
FIREWALL_AUTH_PORTAL_ADDRESS	Address	any	IP/MASK:0.0.0.0/0.0.0.0	
G Suite	Address Group		gmail.com, wildcard.google.com	
HUB1_internal	Address	any	IP/MASK:10.201.1.0/255.255.255.0	

You can select the maximum number of rules to display.

Select *Print* to send the information to a printer or to create a PDF file.

Objects

The *Objects* page provides a view of the objects that are defined in the FortiManager devices. Objects can include items such as addresses, services, intrusion protection definitions, anti-virus signatures and web-filtering profiles. You can use an object in more than one policy to avoid repeating data in multiple places.



The page includes a left panel and dropdown menus at the top that lets you access the objects. When you select an object in the dropdown menu, the main panel displays the data associated with that object. This data is displayed for the selected ADOM. You can select a different ADOM using the dropdown list above the main panel.

Types of objects

The page displays the following object categories:

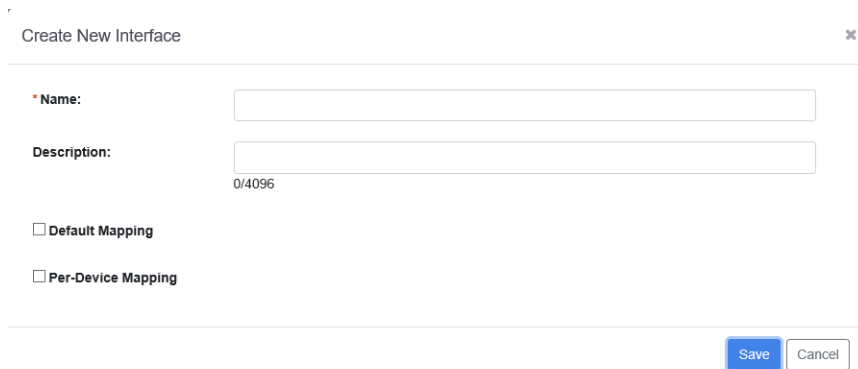
- [Zone/Interface](#)
- [Firewall Objects](#)
- [Security Profiles](#)
- [User & Device](#)

These objects are described in the following sections.

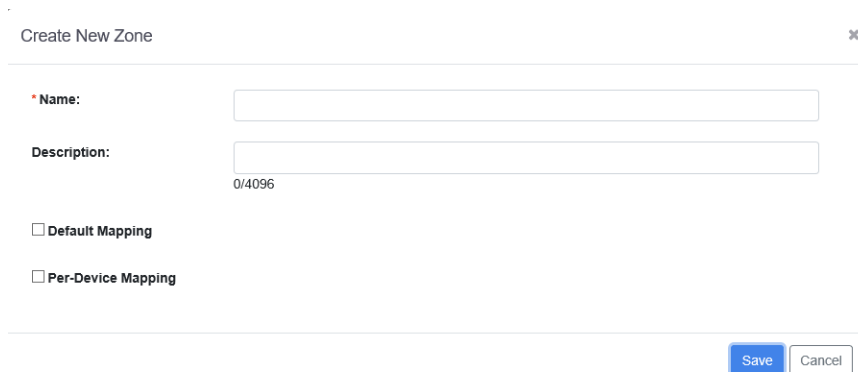
Zone/Interface

You can define a dynamic interface or a dynamic zone. A dynamic zone allows you to specify multiple interfaces.

The following figure shows the *Create New Interface* dialog.



The following figure shows the *Create New Zone* dialog.



Specify the name of the dynamic interface or zone, add an optional description, and select one of the default mappings. You can also specify dynamic mapping for a device by selecting *Per-Device Mapping*.

Firewall Objects

Firewall objects include address, schedule, service and virtual IP. For additional information about the object types, see [FortiOS Object Configuration](#).

Address

You can specify an address as a country, an FQDN or as an IP subnet and mask. The address can apply to all interfaces, or you can configure a specific interface.

You can also create an Address Group, which defines a group of related addresses.

Schedule

You can specify a set of days and time ranges with recurring or one-time schedules.

Service

Although numerous services are already configured, the system allows for administrators to configure their own.

The service object specifies the protocol and any additional information required to identify the service (which depends on the protocol):

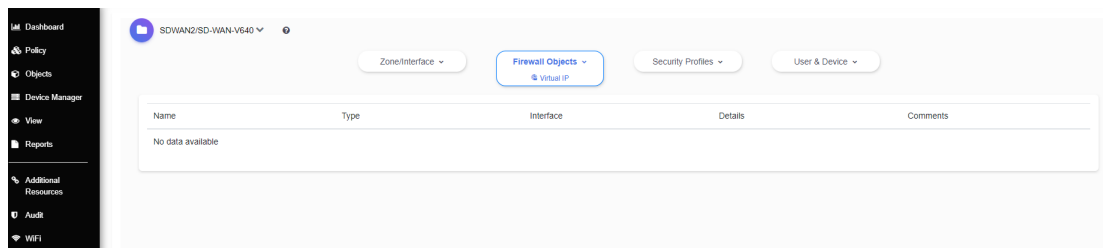
- *IP*—IP protocol number
- *TCP/UDP/SCP*—source and destination port range

You can also create a service group, which defines a group of related services.

Virtual IP

The Virtual IP objects map external IP addresses to internal addresses.

The following figure shows the *Virtual IP* object display:



FortiPortal supports the following Virtual IP object types:

- *IPv4 Virtual IP*—uses static NAT to map a range of external addresses to an internal address range
- *IPv4 Virtual IP Group*—defines a group of one or more Virtual IPs, for ease of administration
- *IP Pool*—defines an IP address or range of IP addresses to use as the source address (rather than the IP address of the interface)

Security Profiles

Security profiles are described in detail in the [FortiGate Security Profiles](#) document and in the online help files at [FortiOS Security Profiles](#).

The following security profiles are supported on FortiPortal:

- Antivirus Profile
- Application Sensor
- Data Leak Prevention Sensor
- Email Filter Profile
- IPS Sensor
- Web Filter Profile
- Local Category
- Rating Overrides
- DNS Filter Profile

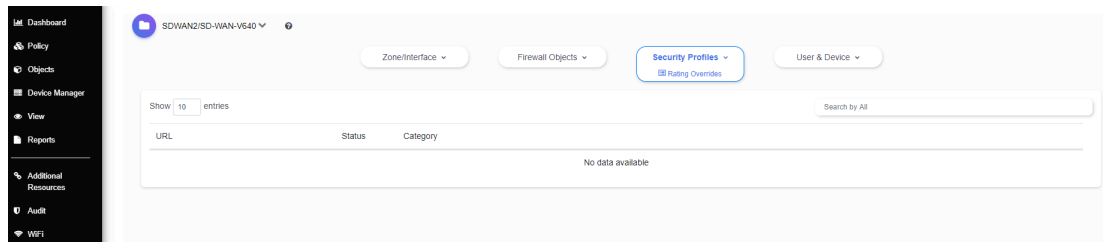
Local Category (security profile introduced with FortiPortal 1.2.0)

You can create a local category and then use Rating Override to assign URLs to the new category.

Rating Overrides (security profile introduced with FortiPortal 1.2.0)

Use a *Rating Override* object to override the Fortinet rating for a URL. The [Security Profiles](#) document contains additional information about local categories and rating overrides.

The following figure displays rating overrides:



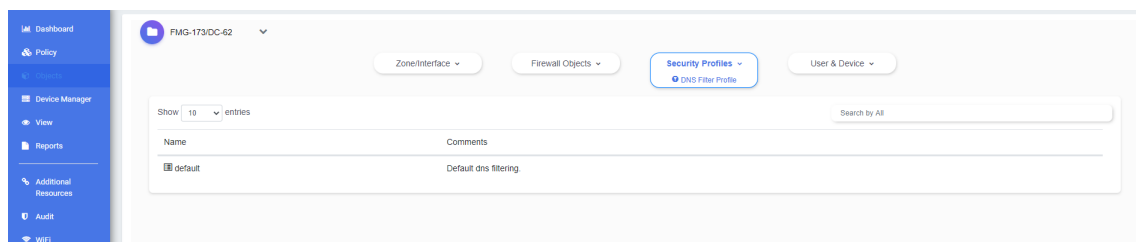
DNS Filter Profile (security profile introduced with FortiPortal 5.3.0)

You can configure DNS web filtering to allow, block, or monitor access to web content according to FortiGuard categories. When DNS web filtering is enabled, your FortiPortal must use the FortiGuard DNS service for DNS lookups. DNS lookup requests sent to the FortiGuard DNS service return with an IP address and a domain rating that includes the FortiGuard category of the web page.

FortiGuard maintains a database containing a list of known botnet command and control (C&C) addresses. This database is updated dynamically and stored on the FortiGate and requires a valid FortiGuard AntiVirus subscription. When you block DNS requests to known botnet C&C addresses, using IPS, DNS lookups are checked against the botnet C&C database. All matching DNS lookups are blocked. Matching uses a reverse prefix match, so all sub-domains are also blocked. To enable this feature, enable *Block DNS requests to known botnet C&C* in the *Create New DNS Filter Profile* or *Edit DNS Filter Profile* dialog.

You can also create a domain filter in the *Create New DNS Filter Profile* or *Edit DNS Filter Profile* dialog. The DNS domain filter allows you to block, allow, or monitor DNS requests by using IPS to look inside DNS packets and match the domain being looked up with the domains on the static URL filter list. If there is a match, the DNS request can be blocked, monitored, or allowed. If blocked, the DNS request is blocked and so the user cannot look up the address and connect to the site. If allowed, access to the site is allowed even if another method is used to block it.

The following figure displays a DNS filter profile:



The DNS filter profile only supports ADOM version 5.4 or higher.

User & Device

Security policies may allow access to specified users and user groups only (the object types in the User & Device category).

For additional information about users and user groups, refer to [FortiOS Handbook: Authentication](#).

User Definition

You can create local (accounts stored on the FortiGate unit), or remote users (accounts stored on a remote authentication server). FortiGate supports LDAP, RADIUS, and TACACS+ servers.

The following figure shows the *Edit User* dialog for a local user:

The screenshot shows the 'Edit User Profile: guest' dialog box. The 'Type' section has radio buttons for LOCAL (selected), LDAP, RADIUS, and TACACS+. The 'User Name' field contains 'guest'. There is a 'Disable' checkbox which is unchecked. The 'Password' field is masked with dots. The 'Contact Info' section has a checked 'Email' checkbox and an empty text field. At the bottom, there is an unchecked 'Enable Two-factor Authentication' checkbox. 'Save' and 'Cancel' buttons are at the bottom right.

For a remote user, you need to specify the remote server, as shown in the following figure:

The screenshot shows the 'Edit User Profile: guest' dialog box for a remote user. The 'Type' section has radio buttons for LOCAL, LDAP, RADIUS (selected), and TACACS+. The 'User Name' field contains 'guest'. There is a 'Disable' checkbox which is unchecked. The 'RADIUS' section has a 'Click to add...' button. The 'Contact Info' section has a checked 'Email' checkbox and an empty text field. Below this, there is an unchecked 'Enable Two-factor Authentication' checkbox. Under it, there are two radio buttons: 'FortiToken' (selected) and 'Email based two-factor authentication'. Below 'FortiToken' is a 'Click to add...' button. 'Save' and 'Cancel' buttons are at the bottom right.

Two-Factor Authentication

Two-factor authentication methods, including FortiToken, provide additional security. You can also enable two-factor authentication using FortiAuthenticator.

To use two-factor authentication:

1. Go to *Objects*.
2. In the *User & Device* dropdown menu, select *User Definition*.
3. Right-click under the header row and select *Create New* or right-click an existing user definition and select *Edit*.

4. Select *Enable Two-factor Authentication*.

5. If you want to use a FortiToken for two-factor authentication, select *FortiToken*.

FortiToken is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit authentication code. This code is entered with a user's user name and password as two-factor authentication. The code displayed changes every 60 seconds, and when not in use the LCD screen is blanked to extend the battery life.

There is also a mobile phone application, FortiToken Mobile, that performs much the same function.

FortiTokens have a small hole in one end. This is intended for a lanyard to be inserted so the device can be worn around the neck, or easily stored with other electronic devices. Do not put the FortiToken on a key ring as the metal ring and other metal objects can damage it. The FortiToken is an electronic device like a cell phone and must be treated with similar care.

Any time information about the FortiToken is transmitted, it is encrypted. When the FortiPortal unit receives the code that matches the serial number for a particular FortiToken, it is delivered and stored encrypted. This is in keeping with the Fortinet's commitment to keeping your network highly secured.

FortiTokens can be added to user accounts that are local, IPsec VPN, SSL VPN, and even Administrators. A FortiToken can be associated with only one account on one FortiPortal unit.

If you lose your FortiToken, your account can be locked so that it will not be used to falsely access the network. Later if found, that FortiToken can be unlocked on the FortiPortal unit to allow access once again.

6. If you want to receive an email for two-factor authentication, select *Email based two-factor authentication* and Email (under Contact Info) and enter an email address.

Two-factor email authentication sends a randomly generated six digit numeric code to the specified email address. Enter that code when prompted at logon. This token code is valid for 60 seconds. If you enter this code after that time, it will not be accepted.

A benefit is that you do not require mobile service to authenticate. However, a potential issue is if your email server does not deliver the email before the 60 second life of the token expires.

The code will be generated and emailed at the time of logon, so you must have email access at that time to be able to receive the code.

7. Select *Save*.

User Group

A user group is a list of user identities. To add or edit a user group, right-click *Edit* under the header row to display the Edit User Group form. Then, select group members from the *Available Users* list.

After you set the group type and add members, you cannot change the group type without removing its members. If you change the type, any members will be removed automatically.

Edit User Group: SSO_Guest_Users
✕

Group Name:

Type
☒ Firewall
☐ FSSO

Available Users

guest

Members

>
>>
<
<<

Remote authentication servers

Create New

Remote Server	Group Name
No data available	

Save

Cancel

Configuring objects

Your service provider may grant write access to some or all of your policy objects. If so, you are enabled to add/edit/delete the objects displayed on the page. If not, we display a warning and set the data to read-only.

Adding a new object

1. Right-click any object in the list and select *Create New*.
2. Modify the relevant fields and select *Save*.

Updating an object

1. Right-click the object in the list and select *Edit*.
2. Modify the relevant fields and select *Save*.

Deleting an object

1. Right-click the object in the list and select *Delete*.
2. Modify the relevant fields and select *Save*.

If the new or updated object is used in any policy, select *Installation* in the *Policy* tab to re-install the policy packages to the assigned devices.

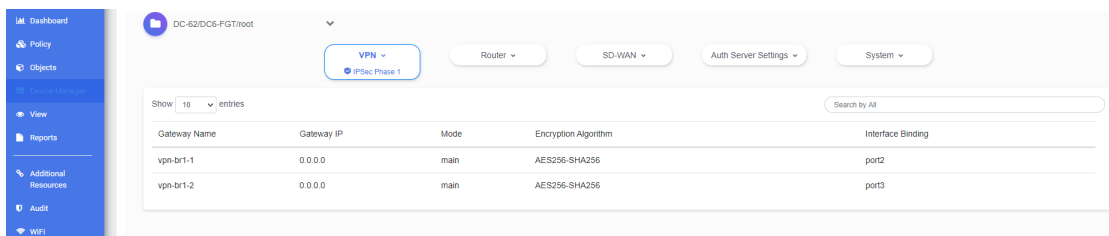
Device Manager

Use the *Device Manager* tab for the following:

- Configure IPsec phase 1 and phase 2. See [VPN](#).
- Define static routes. See [Router](#).
- Configure a software-defined wide area network (SD-WAN). See [SD-WAN](#).
- Set up authentication servers. See [Auth Server Settings](#).
- Set up DHCP servers. See [DHCP Server](#).

VPN

The *VPN* dropdown menu on the *Device Manager* tab displays a list of configurations for Internet Protocol Security (IPsec) Phase 1 and Phase 2.



Gateway Name	Gateway IP	Mode	Encryption Algorithm	Interface Binding
vpn-br1-1	0.0.0.0	main	AES256-SHA256	port2
vpn-br1-2	0.0.0.0	main	AES256-SHA256	port3

Use the *VPN* dropdown menu to [configure VPNs](#).

Configuring VPNs

Use the *VPN* pane to configure IPsec phase 1 and phase 2. You must have at least one IPsec phase-1 configuration and at least one IPsec phase-2 configuration.

In this area, the following actions are available:

- *Show x Entries*—use the drop-down menu to set the number of entries to display
- *Search*—enter text to search for in the table
- *Create New*—configure the IPsec phase 1 or the IPsec phase 2
- *Edit*—change an existing IPsec phase-1 or IPsec phase-2 configuration
- *Delete*—delete an IPsec phase-1 or IPsec phase-2 configuration

Creating an IPsec phase-1 or phase-2 configuration

1. Select *IPsec Phase 1* or *IPsec Phase 2* from the *VPN* dropdown menu.
2. Right-click a configuration and select *Create New*. If the table is blank, right-click under the column headings and select *Create New*.

3. Enter values in the relevant fields and select **Save**. See [IPSec phase-1 fields on page 28](#) and [IPSec phase-2 fields on page 30](#).
4. Select **Save**.

Updating an IPSec phase-1 or phase-2 configuration

1. Select *IPSec Phase 1* or *IPSec Phase 2* from the *VPN* dropdown menu.
2. Right-click a configuration and select *Edit*.
3. Update the values that have changed.
4. Select **Save**.

Deleting an IPSec phase-1 or phase-2 configuration

1. Select *IPSec Phase 1* or *IPSec Phase 2* from the *VPN* dropdown menu.
2. Right-click a configuration and select *Delete*.

IPSec phase-1 fields

Create New IPSec Phase1

*Gateway Name: The Gateway Name field is required.

Comments:

*Remote Gateway: Static IP Address

*IP Address: 0.0.0.0

*Local Interface: internal

*Mode: ☒ Main ☐ Aggressive

*Authentication Method: ☒ Pre-shared Key ☐ Signature

*Pre-shared Key: The Pre-shared Key field is required.

User Group:

Peer Options: Any peer id

Advanced... (XAUTH, NAT-traversal, DPD) ☐ IPSec Interface Mode

IKE Version: ☒ 1 ☐ 2

*Local Gateway IP: ☐ Specify ☒ Main Interface IP

☐ Enable IKE Configuration Method ("mode config")

*P1 Proposal: Available Encryption-Authentication Pair

Search...

des-md5
des-sha1
des-sha256
des-sha384

> >> < <<

Selected Encryption-Authentication Pair

Search...

3des-sha1
3des-sha256
aes128-sha1
aes128-sha256

*Diffie-Hellman Groups: ☐ 1 ☐ 2 ☐ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21

*Key Life: 86400

Local ID:

*XAuth: ☒ Disable ☐ Client

*NAT-traversal: Enable

*Keep Alive Frequency: 10

*Dead Peer Detection: On Demand

Save Cancel

The *Create New IPsec Phase1* and *Edit IPsec Phase1* dialogs contain the following fields:

Settings	Guidelines
Gateway Name	Required. Type a name for this Phase-1 configuration. The value is a string with a maximum of 15 characters.
Comments	Type an optional description. The value is a string with a maximum of 255 characters.
Remote Gateway	Required. Select <i>Static IP Address</i> , <i>Dialup user</i> , or <i>Dynamic DNS</i> .
IP Address	Required if you select <i>Static IP Address</i> . Type the IPv4 address.
Dynamic DNS	Required if you select <i>Dynamic DNS</i> . Type the fully qualified domain name.
Local Interface	Required. Select an interface from the drop-down list or select <i>any</i> .
Mode	Required. Select <i>Main</i> or <i>Aggressive</i> for the phase-1 mode.
Authentication Method	Required. Select <i>Pre-shared Key</i> or <i>Signature</i> for the authentication method.
Pre-shared Key	If <i>Pre-shared Key</i> is selected, this field is required. Type a string for the pre-shared key. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.
User Group	If <i>Pre-shared Key</i> is selected, this field is available but optional. Enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers.
Certificate Name	If <i>Signature</i> is selected, this field is available but optional. Select a certificate from the drop-down list.
Peer Options	If <i>Signature</i> is selected, this field is available but optional. Select <i>Any peer id</i> or <i>One peer id</i> .
peer id	If <i>One peer id</i> is selected, this field is required. Enter the peer ID to uniquely identify one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. The value is a string with a maximum of 255 characters.
Advanced...(XAUTH, NAT-traversal, DPD)	
Local Gateway IP	Select <i>Specify</i> or <i>Main Interface IP</i> . If you select <i>Specify</i> , type the IPv4 address in the field.
P1 Proposal	Select the encryption and authentication algorithms. You can select more than one. Use the arrows to move the algorithms from Available Encryption-Authentication Pair box to the Selected Encryption-Authentication Pair box.
Diffie-Hellman Groups	Select one or more of the following Diffie-Hellman (DH) groups: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode. By default, 5 and 14 are selected.

Settings	Guidelines
Key Life	Type the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172800 seconds. The default is 86400.
Local ID	A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The Local ID uniquely identifies one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. Type a string with a maximum of 63 characters.
XAuth	Select <i>Disable</i> or <i>Client</i> for the XAUTH type. The default is <i>Disable</i> .
NAT-traversal	Select <i>Disable</i> , <i>Enable</i> , or <i>Forced</i> . The default is <i>Enable</i> .
Keep Alive Frequency	If NAT traversal is enabled or forced, type a keep-alive frequency setting (10-900 seconds). The default is 10. The value range is 10-900.
Dead Peer Detection	Select <i>Disable</i> , <i>On Idle</i> , or <i>On Demand</i> .

IPSec phase-2 fields

Create New IPSec Phase2 ✕

*Tunnel Name:

The Tunnel Name field is required.

*Phase 1:

Advanced... >

*Diffie-Hellman Groups: ☐ 1 ☐ 2 ☒ 5 ☒ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21

*Key Life: ☒ Seconds ☐ KBytes ☐ Both

(Seconds)

Auto Keep Alive: ☐

DHCP-IPsec: ☐

Quick Mode Selector

*Local Address:

*Remote Address:

*Local Port:

*Remote Port:

*Protocol:

The *Create New IPSec Phase2* and *Edit IPSec Phase2* dialogs contain the following fields:

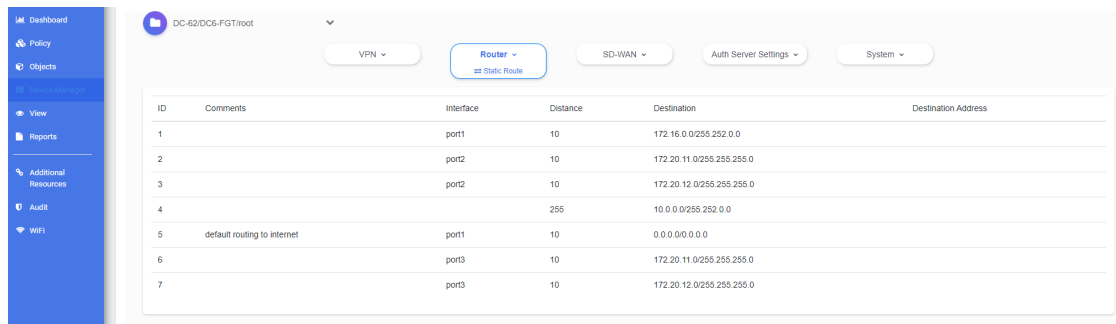
Settings	Guidelines
Tunnel Name	Required. Type a name for this Phase-2 configuration. The value is a string with a maximum of 35 characters.

Settings	Guidelines
Phase 1	Required. Select an IPSec Phase-1 configuration.
Advanced	
P2 Proposal	Select the encryption and authentication algorithms. You can select more than one. Use the arrows to move the algorithms from Available Encryption-Authentication Pair box to the Selected Encryption-Authentication Pair box.
Replay Detection	Select to enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel. The default is selected.
Perfect forward secrecy (PFS)	Select to enable or disable perfect forward secrecy (PFS). Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever the key life expires. The default is selected.
Diffie-Hellman Groups	Required. Select one or more of the following Diffie-Hellman (DH) groups: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode. By default, 5 and 14 are selected.
Key Life	Required. Select the PFS key life. Select <i>Seconds</i> , <i>KBytes</i> , or <i>Both</i> . <ul style="list-style-type: none"> If <i>Seconds</i> is selected, type the number of seconds. The default is 43200. The value range is 120-172800. If <i>KBytes</i> is selected, type the number of KB. The default is 5120. The value range is 5120-4294967295. If <i>Both</i> is selected, type the number of seconds and the number of KB.
Auto Keep Alive	Optional. Select to enable or disable autokey keep alive. The phase 2 SA has a fixed duration. If there is traffic on the VPN as the SA nears expiry, a new SA is negotiated and the VPN switches to the new SA without interruption. If there is no traffic, the SA expires and the VPN tunnel goes down. A new SA will not be generated until there is traffic. The Autokey Keep Alive option ensures that a new SA is negotiated even if there is no traffic so that the VPN tunnel stays up. The default is deselected.
DHCP-IPsec	Optional. The default is deselected.
Quick Mode Selector	
Local Address	Select <i>Subnet</i> , <i>IP Range</i> , <i>IP Address</i> , or <i>Named Address</i> . <ul style="list-style-type: none"> If <i>Subnet</i> is selected, enter an IP address and netmask. If <i>IP Range</i> is selected, enter the first IP address and the last IP address in the range. If <i>IP Address</i> is selected, enter an IPv4 address. If <i>Named Address</i> is selected, select from the drop-down list.
Remote Address	Select <i>Subnet</i> , <i>IP Range</i> , <i>IP Address</i> , or <i>Named Address</i> . <ul style="list-style-type: none"> If <i>Subnet</i> is selected, enter an IP address and netmask.

Settings	Guidelines
	<ul style="list-style-type: none"> If <i>IP Range</i> is selected, enter the first IP address and the last IP address in the range. If <i>IP Address</i> is selected, enter an IPv4 address. If <i>Named Address</i> is selected, select from the drop-down list.
Local Port	Enter the number of the local port. The default is 0 The maximum value is 65535.
Remote Port	Enter the number of the remote port. The default is 0 The maximum value is 65535.
Protocol	Enter the protocol number. The default is 0 The maximum value is 255.

Router

The *Router* dropdown menu on the *Device Manager* tab displays a list of static routes.



The screenshot shows the FortiGate Device Manager interface. On the left is a blue sidebar with navigation options: Dashboard, Policy, Objects, View, Reports, Additional Resources, Audit, and WiFi. The main content area has a top bar with a dropdown menu labeled 'DC-62/DC6-FGT/root'. Below this are several tabs: VPN, Router (selected), SD-WAN, Auth Server Settings, and System. The 'Router' tab is active, showing a table of static routes. The table has columns for ID, Comments, Interface, Distance, Destination, and Destination Address.

ID	Comments	Interface	Distance	Destination	Destination Address
1		port1	10	172.16.0.0/255.252.0.0	
2		port2	10	172.20.11.0/255.255.255.0	
3		port2	10	172.20.12.0/255.255.255.0	
4			255	10.0.0.0/255.252.0.0	
5	default routing to internet	port1	10	0.0.0.0/0.0.0.0	
6		port3	10	172.20.11.0/255.255.255.0	
7		port3	10	172.20.12.0/255.255.255.0	

Use the *Router* dropdown menu to [configure static routers](#).

Configuring static routes

Use the *Router* pane to define static routes.

Here, the following actions are available:

- *Create New*—define a static route
- *Edit*—change an existing static route
- *Delete*—delete a static route

Adding a new static route

1. Select *Static Route* from the *Router* dropdown menu.
2. Right-click a static route and select *Create New*.
If the table is blank, right-click under the column headings and select *Create New*.
3. Enter values in the relevant fields. See [Static route fields on page 33](#).
4. Select *Save*.

Updating a static route

1. Select *Static Route* from the *Router* dropdown menu.
2. Right-click a static route and select *Edit*.
3. Update the values that have changed.
4. Select *Save*.

Deleting a static route

1. Select *Static Route* from the *Router* dropdown menu.
2. Right-click a static route and select *Delete*.

Static route fields

The *Create New Static Router* and *Edit Static Router* dialog contain the following fields:

Settings	Guidelines
Destination Type	Required. Select <i>Subnet</i> , <i>Named Address</i> , or <i>Internet Service</i> for the destination type. <ul style="list-style-type: none"> • If <i>Subnet</i> is selected, enter destination IP address and netmask. • If <i>Named Address</i> is selected, select from the drop-down list. • If <i>Internet Service</i> is selected, select the Internet service from the drop-down list.
Destination	Required. If you selected <i>Subnet</i> as the destination type, enter the destination IP address and netmask.
Internet Service	Required. If you selected <i>Internet Service</i> as the destination type, select the Internet service from the drop-down list.
Interface	Required. Select the network interface that connects to the gateway from the drop-down list.
Gateway	Required. Enter an IPv4 address for the next hop.
Distance	Required. Enter the distance. The default is 10. The maximum is 255.

Settings	Guidelines
Priority	Required. Enter the priority. The default is 0. The maximum is 4294967295
Comments	Optional. Enter a description of the static route. The value is a string with a maximum of 255 characters.

SD-WAN

An SD-WAN is a virtual interface that consists of a group of member interfaces that can be connected to different link types. The FortiPortal unit groups all physical member interfaces into a single virtual interface, which is the SD-WAN interface. SD-WAN simplifies your network configuration because you configure a single set of routes and firewall policies and apply them to all member interfaces. You also configure various types of criteria that the FortiPortal unit then uses to select the best links for your network traffic.



The SD-WAN works only with ADOM 6.0 or higher in a per-device management mode.

You can configure an SD-WAN for a group of interfaces or for an ADOM. After you configure the SD-WAN, you can monitor the performance of SD-WAN interfaces and identify unhealthy devices.



To edit an SD-WAN configuration, you must have both read-write permission for SD-WAN and read permission for the interface.

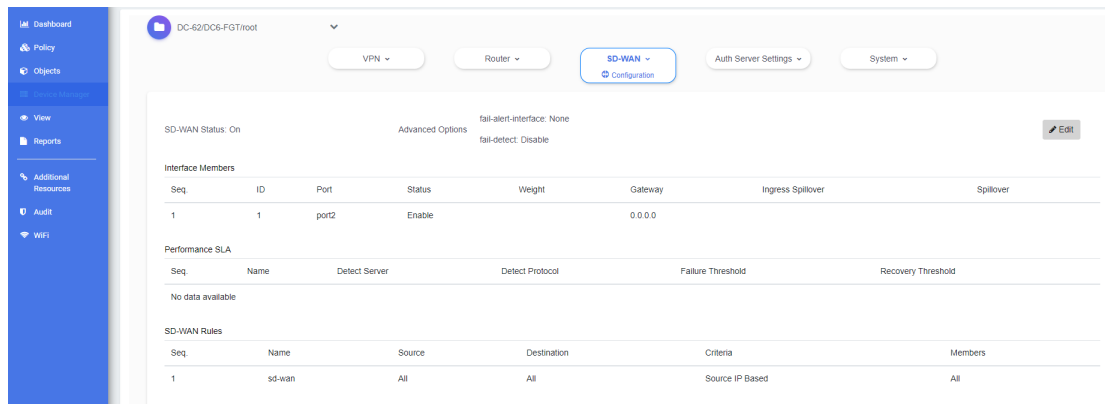
Use the *SD-WAN* dropdown menu on the *Device Manager* tab to perform the following tasks:

- [Configuring an SD-WAN for a group of interfaces](#)
- [Configuring an SD-WAN for an ADOM](#)
- [Monitoring the SD-WAN interfaces](#)

Configuring an SD-WAN for a group of interfaces

To configure an SD-WAN for a group of interfaces:

1. Go to *Device Manager* > *SD-WAN*.
2. Select *Configuration* from the *SD-WAN* dropdown menu.
3. Enable the *SD-WAN status*. See [Enable the SD-WAN status](#).
4. Define which physical FortiPortal interfaces belong to the SD-WAN. See [Define which physical FortiPortal interfaces belong to the SD-WAN](#).
5. Define a new performance service level agreement (SLA). See [Define a new performance SLA](#).
6. Define SD-WAN rules to control how sessions are distributed to physical interfaces in the SD-WAN. See [Define SD-WAN rules](#).



Enable the SD-WAN status

The SD-WAN pane on the *SD-WAN > Configuration* page displays the SD-WAN status, whether any physical interfaces will be alerted if the SD-WAN fails, and whether the SD-WAN Internet connection will be checked.



To change these settings in the GUI:

1. Select *Edit*.
2. Select *Enable* to enable the *SD-WAN status*.
3. Select a physical interface to alert if the SD-WAN fails, *None*, or *any*.
4. Select *Enable* or *Disable* to change whether the SD-WAN Internet connection is checked.
5. Select *Save* to make your changes.

Define which physical FortiPortal interfaces belong to the SD-WAN

Use the Interface Members area on the *SD-WAN > Configuration* pane to define which physical FortiPortal interfaces belong to the SD-WAN.

SD-WAN interfaces are the ports and interfaces that are used to run traffic. At least one interface must be configured for SD-WAN to function; up to 255 member interfaces can be configured.

In the *Interface Members* area, the following actions are available:

- *Create New*—define a new interface member
- *Edit*—change the settings for an existing interface member
- *Delete*—delete an interface member

To add a new interface member:

1. Select *Configuration* from the *SD-WAN* dropdown menu.
2. Right-click an interface member and select *Create New*. If the table is blank, right-click under the column headings and select *Create New*.

3. Enter values in the relevant fields. See [Interface member fields on page 43](#).
4. Select **Save**.

Interface member fields

Create New Interface Member

*Member: ▼
The interface field is required.

Gateway IP: 0.0.0.0

*Cost: 0

Status: ☒ enable ☐ disable

Estimated Upstream Bandwidth:

Estimated Downstream Bandwidth:

Advanced Options ▼

gateway6: ::

priority: 0

seq-num:

source: 0.0.0.0

source6: ::

volume-ratio: 0
The volume-ratio field must be 1 or more.

Save Cancel

The *Create New Interface Member* and *Edit Interface Member* dialogs contain the following fields:

Settings	Guidelines
Member	Required. Select one of the available physical interfaces.
Cost	. More traffic is directed to interfaces with higher costs. The cost field must be 0 or more.
Gateway IP	Enter the IPv4 address of the default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.
Status	Enable or disable this interface in the SD-WAN.
Estimated Upstream Bandwidth	Select the link based on the available bandwidth of outgoing traffic.
Estimated Downstream Bandwidth	Select the link based on the available bandwidth of incoming traffic.
Advanced Options	
gateway6	Enter the IPv6 address of the default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.
priority	Assign interfaces a priority based on the priority assigned to the interface.
seq-num	Member sequence number. The range is 0-4294967295.
source	Source IPv4 address name.

Settings	Guidelines
source6	Source IPv6 address name.
volume-ratio	Measured volume ratio (this value / sum of all values = percentage of link volume). The range is 0-255.

Define a new performance SLA

Use the Performance SLA area on the *SD-WAN > Configuration* page to configure SLA management.

If all links meet the SLA criteria, the FortiPortal unit uses the first link, even if that link is not the best quality link. If at any time, the link in use does not meet the SLA criteria, and the next link in the configuration meets the SLA criteria, the FortiPortal unit changes to that link. If the next link does not meet the SLA criteria, the FortiPortal unit uses the next link in the configuration if it meets the SLA criteria, and so on.

In *Performance SLA* area, the following actions are available:

- *Create New*—define a new performance SLA
- *Edit*—change an existing performance SLA
- *Delete*—delete a performance SLA

To add a new performance SLA:

1. Select *Configuration* from the *SD-WAN* dropdown menu.
2. Right-click a performance SLA and select *Create New*. If the table is blank, right-click under the column headings and select *Create New*.
3. Enter values in the relevant fields. See [Performance SLA fields on page 38](#).
4. Select *Save*.

Performance SLA fields

Create New Performance SLA

Name: The Name field is required.

*Detect Protocol:

*Detect Server:

Detect Server 2:

Members: Available

Search:

Selected

Search:

Members Available:

Selected:

SLA:

ID	Jitter Threshold (Milliseconds)	Latency Threshold (Milliseconds)	Packet Loss Threshold (%)
No data available			

Link Status

Interval: seconds

Failure Before Inactive: (max 10)

Restore Link After: (max 10)

Action When Inactive

Update Static Route: ☐ enable ☐ disable

Update Cascade Interface: ☐ enable ☐ disable

Advanced Options

http-get:

http-match:

Interval:

packet-size:

threshold-alert:

threshold-alert-latency:

threshold-alert-packetsize:

threshold-warning:

threshold-warning-latency:

threshold-warning-packetsize:

The *Create New Performance SLA* and *Edit Performance SLA* dialogs contain the following fields:

Settings	Guidelines
Name	Required. Name of the performance SLA.
Detect Protocol	Required. Protocol used to determine if the FortiPortal unit can communicate with the server. Select <i>Ping</i> , <i>TCP ECHO</i> , <i>UDP ECHO</i> , <i>HTTP</i> , or <i>TWAMP</i> .
Detect Server	Required. IPv4 address of the server.
Detect Server 2	IPv4 address of an optional second server.
Members	Required. Select the interfaces from the Available Members list and then select > to move them to the Selected Members list.
SLA	Configure the SLA. See SLA fields on page 39 .
Link Status	
interval	Status check interval, which is the time between attempting to connect to the server. The default is 5 seconds; the range is 1 - 3600 seconds.
Failure Before Inactive	Number of failures before server is considered lost. The default is 5; the range is 1 - 10.
Restore Link After	Number of successful responses received before server is considered recovered. The default is 5; the range is 1 - 10.
Action When Inactive	
Update Static Route	Enable or disable updating the static route.

Settings	Guidelines
Update Cascade Interface	Enable or disable update cascade interface.
Advanced Options	
http-get	URL used to communicate with the server if the protocol is HTTP.
http-match	Response string expected from the server if the protocol is HTTP.
interval	Status check interval, or the time between attempting to connect to the server. The default is 5 seconds; the range is 1 - 3600 seconds.
packet-size	Packet size of a Two-Way Active Measurement Protocol (TWAMP) test session. The range is 64-1024.
threshold-alert-jitter	Alert threshold for jitter. The default is 0 ms; the range is 0-4294967295 ms.
threshold-alert-latency	Alert threshold for latency. The default is 0 ms; the range is 0-4294967295 ms.
threshold-alert-packetloss	Alert threshold for packet loss. The default is 0 percent; the range is 0-100 percent.
threshold-warning-jitter	Warning threshold for jitter. The default is 0 ms ; the range is 0-4294967295 ms.
threshold-warning-latency	Warning threshold for latency. The default is 0 ms; the range is 0-4294967295 ms.
threshold-warning-packetloss	Warning threshold for packet loss. The default is 0 percent; the range is 0-100 percent.

To add a new SLA:

1. Select *Configuration* from the *SD-WAN* dropdown menu.
2. Right-click a performance SLA and select *Create New*. If the table is blank, right-click under the column headings and select *Create New*.
3. Right-click under the column headings in the SLA area and select *Create New*.
4. Enter values in the relevant fields. See [SLA fields on page 39](#).
5. Select *Save* to save your SLA configuration.
6. Select *Save* to save your performance SLA configuration.

SLA fields

Create New SLA
✕

*link-cost-factor: ☒ Jitter Threshold ☒ Latency Threshold ☒ Packet Loss Threshold

Jitter Threshold:

Latency Threshold:

Packet Loss Threshold:

The *Create New SLA* and *Edit SLA* dialogs contain the following fields:

Settings	Guidelines
link-cost-factor	Required. Criteria on which to base link selection. You can select one or more of the threshold values to use: <i>Jitter Threshold</i> , <i>Latency Threshold</i> , and <i>Packet Loss Threshold</i> . You need to enter a threshold value for each criterion that you select.
Jitter Threshold	Jitter for SLA to make decision in milliseconds. The default is 5; the range is 0-10000000.
Latency Threshold	Latency for SLA to make decision in milliseconds. The default is 5; the range is 0- 10000000.
Packet Loss Threshold	Packet loss for SLA to make decision in percentage. The default is 0; the range is 0-100.

Define SD-WAN rules

Use the SD-WAN Rules area on the *SD-WAN > Configuration* page to configure SD-WAN rules or priority rules (also called services) to control how sessions are distributed to physical interfaces in the SD-WAN.

In the *SD-WAN Rules* area, the following actions are available:

- *Create New*—define a new SD-WAN rule
- *Edit*—change an existing SD-WAN rule
- *Delete*—delete an SD-WAN rule

To add a new SD-WAN rule:

1. Select *Configuration* from the *SD-WAN* dropdown menu.
2. Right-click an SD-WAN rule and select *Create New*. If the table is blank, right-click under the column headings and select *Create New*.
3. Enter values in the relevant fields. See [Performance SLA fields on page 38](#).
4. Select *Save*.

SD-WAN rule fields

Create New SD-WAN Rules

*Name: The Name field is required.

Source

Address Available

Search...

FIREWALL_AUTH_PORTAL_ADDRESS
SSLVPN_TUNNEL_ADDR1
all
autoupdate.opera.com
google-play
none
samsung.apple.com
update.microsoft.com

Selected

Search...

User Available

Search...

guest

Selected

Search...

User group Available

Search...

Guest group
SDO_Guest_users

Selected

Search...

*Destination: ☒ Address ☐ Internet Service

*Address Available

Search...

FIREWALL_AUTH_PORTAL_ADDRESS
SSLVPN_TUNNEL_ADDR1
all
autoupdate.opera.com
google-play
none
samsung.apple.com
update.microsoft.com

Selected

Search...

*Protocol: ☐ TCP ☐ UDP ☒ ANY ☐ Specify

*Outgoing Interface: ☒ Best Quality ☐ Minimum Quality (SLA)

*Interface Members Available

Search...

dmz1
dmz2
mgmt
wan2

Selected

Search...

*Status Check: The health-check field is required.

Save Cancel

The *Create New SD-WAN Rules* and *Edit SD-WAN Rules* dialog contain the following fields:

Settings	Guidelines
Name	Required. Priority rule name.
Source Address	Select the source addresses from the Available list and then select > to move them to the Selected list.
User	Select the users from the Available list and then select > to move them to the Selected list.
User group	Select the user groups from the Available list and then select > to move them to the Selected list.
Destination	Required. Select <i>Address</i> to use destination addresses or select <i>Internet Service</i> to use destination Internet services.
Address	Required. Available if Destination is set to <i>Address</i> . Select the destination addresses from the Available list and then select > to move them to the Selected list.
Protocol	Required. Available if Destination is set to <i>Address</i> . Select <i>TCP</i> , <i>UDP</i> , <i>ANY</i> , or <i>Specify</i> . If you select <i>Specify</i> , enter the protocol number, type of service, and bit mask.
Internet Service	Available if Destination is set to <i>Internet Service</i> . Select the Internet services from the Available list and then select > to move them to the Selected list.

Settings	Guidelines
Internet Service Group	Available if Destination is set to <i>Internet Service</i> . Select the Internet service groups from the Available list and then select > to move them to the Selected list.
Custom Internet Service	Available if Destination is set to <i>Internet Service</i> . Select the custom Internet services from the Available list and then select > to move them to the Selected list.
Custom Internet Service Group	Required. Available if Destination is set to <i>Internet Service</i> . Select the custom Internet service groups from the Available list and then select > to move them to the Selected list.
Application	Available if Destination is set to <i>Internet Service</i> . Select the applications from the Available list and then select > to move them to the Selected list.
Application Group	Available if Destination is set to <i>Internet Service</i> . Select the application groups from the Available list and then select > to move them to the Selected list.
Outgoing Interface	Required. Select <i>Best Quality</i> or <i>Minimum Quality (SLA)</i> .
Interface Members	Required. Select the interfaces from the Available list and then select > to move them to the Selected list.
Status Check	Required. Available if Outgoing Interface is set to <i>Best Quality</i> . Select the appropriate performance SLA to use for the status check.
Required SLA Target	Required. Available if Outgoing Interface is set to <i>Minimum Quality (SLA)</i> . Select the appropriate performance SLA from the drop-down list.

Configuring an SD-WAN for an ADOM

To use this feature, you must have the following:

- ADOM version 6.0 or higher
- The templates are assigned to devices in the same ADOM.
- Central SD-WAN management is enabled in FortiManager for the ADOM being used.

To configure an SD-WAN for an ADOM:

1. Add a FortiManager with an ADOM. See the *FortiPortal Administration Guide*.
2. Add a customer with permission for the *Device Manager* tab. See the *FortiPortal Administration Guide*.
3. Add a customer site for the customer created in step 2 and assign the ADOM to the customer site. See the *FortiPortal Administration Guide*.
4. Add a customer user with access to the customer site created in step 3. See the *FortiPortal Administration Guide*.
5. The customer user created in step 4 specifies which ports are interface members of the SD-WAN. See [Specify the ports](#).
6. The customer user created in step 4 creates an SD-WAN template; defines the interface members from step 5, a performance SLA, and SD-WAN rules; and assigns the template to an ADOM. See [Create an SD-WAN template](#).

Specify the ports

Use the *SD-WAN > Interface Members* page to define which physical FortiPortal interfaces belong to the SD-WAN.

SD-WAN interfaces are the ports and interfaces that are used to run traffic. At least one interface must be configured for SD-WAN to function; up to 255 member interfaces can be configured.

On the *SD-WAN > Interface Members* page, the following actions are available:

- *Create New*—define a new interface member
- *Edit*—change the settings for an existing interface member
- *Delete*—delete an interface member

To add a new interface member:

1. Select *Interface Members* from the *SD-WAN* dropdown menu.
2. Right-click an interface member and select *Create New*. If the table is blank, right-click under the column headings and select *Create New*.
3. Enter values in the relevant fields. See [Interface member fields on page 36](#).
4. Select *Save*.

Interface member fields

create new Interface Members

*Name: Name is required.

Description: 0 / 256

Cost:

Gateway: 0.0.0.0

Gateway6: ::

Ingress Spillover Threshold:

*Interface: Interface is required.

Priority:

Source: 0.0.0.0

Source6: ::


Spillover Threshold:

Volume Ratio: 1

Weight: 1

The *Create New Interface Members* and *Edit Interface Members* dialog contain the following fields:

Settings	Guidelines
Name	Required. Name of the new interface member.
Description	Description of the new interface member.

Settings	Guidelines
Cost	Cost of the interface.
	 <p>The Cost field is not displayed when the ADOM version is 6.2 or higher.</p>
Gateway	Enter the IPv4 address of the default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.
Gateway6	Enter the IPv6 address of the default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.
Ingress Spillover Threshold	Ingress spillover threshold for this interface (0 - 16776000 kbit/s). When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.
Interface	Required. Type the name of one or more ports. Use a comma to separate multiple ports.
Priority	Assign the interface a priority.
Source	Source IPv4 address name.
Source6	Source IPv6 address name.
Spillover Threshold	Egress spillover threshold for this interface (0 - 16776000 kbit/s). When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.
Volume Ratio	Measured volume ratio (this value / sum of all values = percentage of link volume). The range is 0-255.
Weight	Weight of this interface for weighted load balancing. More traffic is directed to interfaces with higher weights. The weight must be in the range of 0-255.

Create an SD-WAN template

Use the *SD-WAN > Template* page to define an SD-WAN for an ADOM.

In this area, the following actions are available:

- *Create New*—define a new template
- *Edit*—change the settings for an existing template
- *Delete*—delete a template
- *Assign*—associate a template to an ADOM

To create a template and assign it:

1. Select *Template* from the *SD-WAN* dropdown menu.
2. Right-click a template and select *Create New*. If the table is blank, right-click under the column headings and select *Create New*.
3. Enter values in the relevant fields. See [Template fields](#).
4. Select *Save*.

5. Right-click a template and select *Assign*.
6. Select the site to assign the template to and then select *Save*.

Template fields

create new Template ✕

*Name:
Name is required.

Description:
 0 / 255

Status:

Interface Members

Sequence Number	Member
No data available	

Performance SLA

Name	Detect Server	Detect Protocol	Fail Time	recovery time
No data available				

SD-WAN Rule

Name	Source Address	Destination Address	Criteria	Members
No data available				

Fail Alert Interfaces:

Fail-Detect:

Load Balance Mode:

The *Create New Template* and *Edit Template* dialog contain the following fields:

Settings	Guidelines
Name	Required. Name of the new template
Description	Description of the new template.
Status	Select <i>enable</i> to enable the SD-WAN status.
Interface members	Define which physical FortiPortal interfaces belong to the SD-WAN. See Define which physical interfaces belong to the SD-WAN template on page 46 .
Performance SLA	Define a new performance service level agreement (SLA). See Define a performance SLA for the SD-WAN template on page 46 .
SD-WAN Rule	Define SD-WAN rules to control how sessions are distributed to physical interfaces in the SD-WAN. See Define SD-WAN rules for the SD-WAN template on page 49 .
Fail Alert Interfaces	Select a physical interface to alert if the SD-WAN fails. This field is not available if FortiManager 6.2 is being used.
Fail-Detect	Select <i>enable</i> or <i>disable</i> to change whether the SD-WAN Internet connection is checked.
Load Balance Mode	SD-WAN supports five load-balance modes: <ul style="list-style-type: none"> Source IP (<i>source-ip-based</i>): SD-WAN will load balance the traffic equally among its members according to a hash algorithm based on the source IP addresses.

Settings	Guidelines
	<ul style="list-style-type: none"> Session (<code>weight-based</code>): SD-WAN will load balance the traffic according to the session numbers ratio among its members. Spillover (<code>usage-based</code>): SD-WAN will use the first member until the bandwidth reaches its limit, then use the second, and so on. Source-Destination IP (<code>source-dest-ip-based</code>): SD-WAN will load balance the traffic equally among its members according to a hash algorithm based on both the source and destination IP addresses. Volume (<code>measured-volume-based</code>): SD-WAN will load balance the traffic according to the bandwidth ratio among its members.

Define which physical interfaces belong to the SD-WAN template

SD-WAN interfaces are the ports and interfaces that are used to run traffic. At least one interface must be configured for the SD-WAN to function; up to 255 member interfaces can be configured.

To define which physical interfaces belong to the SD-WAN template:

1. Select *Template* from the *SD-WAN* dropdown menu.
2. Right-click a template and select *Create New*. If the *Template* table is blank, right-click under the column headings and select *Create New*.
3. Right-click an interface member and select *Create New*. If the *Interface Members* table is blank, right-click under the column headings and select *Create New*.
4. Enter values in the relevant fields. See [Interface members fields for an SD-WAN template on page 46](#).
5. Select *Save*.

Interface members fields for an SD-WAN template

create new Interface Members ✕

Sequence Number:

Member:

Settings	Description
Sequence Number	Member sequence number. The range is 0-4294967295.
Member	Required. Select one of the available physical interfaces.

Define a performance SLA for the SD-WAN template

If all links meet the SLA criteria, the FortiPortal unit uses the first link, even if that link is not the best quality link. If at any time, the link in use does not meet the SLA criteria, and the next link in the configuration meets the SLA criteria, the FortiPortal unit changes to that link. If the next link does not meet the SLA criteria, the FortiPortal unit uses the next link in the configuration if it meets the SLA criteria, and so on.

To define a performance SLA for the SD-WAN template:

1. Select *Template* from the *SD-WAN* dropdown menu.
2. Right-click a template and select *Create New*. If the Template table is blank, right-click under the column headings and select *Create New*.
3. Right-click a performance SLA and select *Create New*. If the Performance SLA table is blank, right-click under the column headings and select *Create New*.
4. Enter values in the relevant fields. See [Performance SLA fields for an SD-WAN template on page 47](#).
5. Select *Save*.

Performance SLA fields for an SD-WAN template

The screenshot shows the 'create new Performance SLA' configuration window. It contains the following fields and options:

- Name:** A text field with a red asterisk indicating it is required.
- *Detect Server:** A section with a search bar and a list of available servers. A 'Selected' list is also present.
- Fail Time:** A numeric field set to 5.
- Http-agent:** A text field set to 'Chrome (Safe)'.
- Http-get:** A text field set to '/'.
- Http-match:** A text field set to '1 / 1024'.
- Interval:** A numeric field set to 1.
- Members:** A section with a search bar and a list of available members. A 'Selected' list is also present.
- packet-size:** A numeric field set to 64.
- password:** A text field with masked characters.
- port:** A numeric field set to 80.
- Detect Protocol:** A dropdown menu set to 'ping'.
- recovery time:** A numeric field set to 5.
- Thresholds:** A series of input fields for jitter, latency, link cost, and packet loss thresholds.
- Update Cascade Interface:** A checkbox set to 'enable'.
- Update Static Route:** A checkbox set to 'enable'.
- SLA:** A table with columns for Jitter Threshold (ID), Latency Threshold (Milliseconds), Link Cost Factor, and Packet Loss Threshold (%).

Settings	Description
Name	Required. Name of the performance SLA.
Detect Server	Required. Name of the server.
Fail Time	Number of retry attempts before the server is considered down.
Http-agent	String in the http-agent field in the HTTP header.
Http-get	If you are monitoring an HTML server you can send an HTTP-GET request with a custom string. Use this option to define the string.
Http-match	Response string expected from the server if the protocol is HTTP.

Settings	Description
Interval	Status check interval, or the time between attempting to connect to the server. The default is 5 seconds; the range is 1 - 3600 seconds.
Outgoing interface	<p>This field is available only if you are using ADOM 6.0 or 6.2 with FortiManager 6.0 or 6.2.</p> <ul style="list-style-type: none"> If you are using ADOM 6.2 and FortiManager 6.2, select <i>Auto</i>, <i>Manual</i>, <i>Minimum Quality (Maximum Bandwidth)</i>, <i>Best Quality (Priority)</i>, or <i>Lowest Quality (SLA)</i>. If you are using ADOM 6.0 and FortiManager 6.2): select <i>Auto</i>, <i>Manual</i>, <i>Minimum Quality (Maximum Bandwidth)</i>, or <i>Best Quality(Priority)</i>. If you are using ADOM 6.0 and FortiManager 6.0): select <i>Minimum Quality (Maximum Bandwidth)</i> or <i>Best Quality (Priority)</i>.
Members	<p>Select the interfaces from the Available Members list and then select > to move them to the Selected Members list.</p> <p>If you selected <i>Manual</i> for the outgoing interface, select a single interface from the dropdown list.</p>
quality-link	If you selected <i>Auto</i> for the outgoing interface, select the quality link from the dropdown list. This field is available only if you are using FortiManager 6.2.
Criteria	If you selected <i>Auto</i> for the outgoing interface, select the criteria from the dropdown list. This field is available only if you are using FortiManager 6.2.
packet-size	Packet size of a Two-Way Active Measurement Protocol (TWAMP) test session. The range is 64-1024.
password	TWAMP controller password in authentication mode size.
port	Port number of the traffic to be used to monitor the server.
Detect Protocol	Protocol used to determine if the FortiPortal unit can communicate with the server. Select <i>udp-echo</i> , <i>ping</i> , <i>tcp-echo</i> , <i>http</i> , <i>twamp</i> , or <i>ping6</i> .
recovery time	Number of successful responses received before server is considered recovered
Threshold-alert-jitter	Alert threshold for jitter. The default is 0 ms; the range is 0-4294967295 ms.
Threshold-alert-latency	Alert threshold for latency. The default is 0 ms; the range is 0-4294967295 ms.
Threshold-alert-packetloss	Alert threshold for packet loss. The default is 0 percent; the range is 0-100 percent.
threshold-warning-jitter	Warning threshold for jitter. The default is 0 ms; the range is 0-4294967295 ms.
threshold-warning-latency	Warning threshold for latency. The default is 0 ms; the range is 0-4294967295 ms.
threshold-warning-packetloss	Warning threshold for packet loss. The default is 0 percent; the range is 0-100 percent.
Update Cascade Interface	Enable or disable whether the cascade interface is updated.

Settings	Description
Update Static Route	Enable or disable whether the static route is updated.
SLA	Configure the SLA.

To define a performance SLA for the SD-WAN template:

1. Select *Template* from the *SD-WAN* dropdown menu.
2. Right-click a template and select *Create New*. If the Template table is blank, right-click under the column headings and select *Create New*.
3. Right-click a performance SLA and select *Create New*. If the Performance SLA table is blank, right-click under the column headings and select *Create New*.
4. Right-click under the column headings in the SLA table and select *Create New*.
5. Enter values in the relevant fields. See [SLA fields for an SD-WAN template on page 49](#).
6. Select *Save* to save your SLA configuration.
7. Select *Save* to save your performance SLA configuration.

SLA fields for an SD-WAN template

create new SLA ✕

ID:

Jitter Threshold (Milliseconds):

*Latency Threshold (Milliseconds):

Packet Loss Threshold (%):

Save

Cancel

Settings	Description
ID	SLA identifier.
Jitter Threshold	Jitter for SLA to make decision in milliseconds. The default is 5; the range is 0- 10000000.
Latency Threshold	Required. Latency for SLA to make decision in milliseconds. The default is 5; the range is 0- 10000000.
Packet Loss Threshold	Packet loss for SLA to make decision in percentage. The default is 0; the range is 0-100.

Define SD-WAN rules for the SD-WAN template

You can configure SD-WAN rules or priority rules (also called services) to control how sessions are distributed to physical interfaces in the SD-WAN.

To add a new SD-WAN rule for an SD-WAN template:

1. Select *Template* from the *SD-WAN* dropdown menu.
2. Right-click a template and select *Create New*. If the Template table is blank, right-click under the column headings and select *Create New*.
3. Right-click an SD-WAN rule and select *Create New*. If the table is blank, right-click under the column headings and select *Create New*.
4. Enter values in the relevant fields. See [SD-WAN rule fields for an SD-WAN template on page 50](#).
5. Select *Save*.

SD-WAN rule fields for an SD-WAN template

The screenshot shows the 'Create New SD-WAN Rule' configuration window. It contains the following sections:

- Name:** A text input field.
- Source Address:** An 'Available' list with search and scroll functions, and a 'Selected' list. Items in the available list include 'PREVAUTH_PORTAL...', 'SSUPTUNNEL_ADDR1', 'all', and 'autogate.opera.com'.
- Users:** An 'Available' list with search and scroll functions, and a 'Selected' list. The available list contains 'guest'.
- User Groups:** An 'Available' list with search and scroll functions, and a 'Selected' list. The available list contains 'Guest-group' and 'SSO_guestUsers'.
- Destination:** A dropdown menu set to 'Named Address'.
- Destination Address:** An 'Available' list with search and scroll functions, and a 'Selected' list. Items include 'PREVAUTH_PORTAL...', 'SSUPTUNNEL_ADDR1', 'all', and 'autogate.opera.com'.
- Protocol:** A dropdown menu set to 'Any'.
- Specify Protocol:** Fields for 'Startport' (1) and 'Endport' (65535).
- Type of Service:** A dropdown menu set to 'DSCP'.
- Type of Service Mask:** A dropdown menu set to 'DSCP'.
- Outgoing Interface:** A dropdown menu set to 'Best Quality(Priority)'.
- Members:** An 'Available' list with search and scroll functions, and a 'Selected' list.
- Status Check:** A dropdown menu.

A red error message 'Status Check is required.' is displayed at the bottom left. 'Save' and 'Cancel' buttons are at the bottom right.

Settings	Description
Name	Priority rule name.
Source Address	Select the source addresses from the Available list and then select > to move them to the Selected list.
Users	Select the users from the Available list and then select > to move them to the Selected list.
User Groups	Select the user groups from the Available list and then select > to move them to the Selected list.
Destination	Required. Select <i>Named Address</i> to use destination addresses or select <i>Internet Service</i> to use destination Internet services.

Settings	Description
Destination Address	Required. Available if Destination is set to <i>Named Address</i> . Select the destination addresses from the Available list and then select > to move them to the Selected list.
Protocol	Required. Available if Destination is set to <i>Address</i> . Select <i>TCP</i> , <i>UDP</i> , <i>ANY</i> , or <i>Specify</i> .
Specify Protocol	Required. If Protocol is set to <i>Specify</i> , enter the protocol number, type of service, and bit mask.
start-port	Integer value for starting TCP/UDP/SCTP destination port.
end-port	Integer value for ending TCP/UDP/SCTP destination port.
Type of Service	Type of service bit pattern.
Type of Service Mask	Type of service evaluated bits. This value determines which bits in the IP header's TOS field are significant.
Internet Service	Available if Destination is set to <i>Internet Service</i> . Select the Internet services from the Available list and then select > to move them to the Selected list.
Internet Service Group	Available if Destination is set to <i>Internet Service</i> . Select the Internet service groups from the Available list and then select > to move them to the Selected list.
Custom Internet Service	Available if Destination is set to <i>Internet Service</i> . Select the custom Internet services from the Available list and then select > to move them to the Selected list.
Custom Internet Service Group	Available if Destination is set to <i>Internet Service</i> . Select the custom Internet service groups from the Available list and then select > to move them to the Selected list.
internet-service-ctrl	Available if Destination is set to <i>Internet Service</i> . Enter the identifier of a control-based Internet service.
internet-service-ctrl-group	Available if Destination is set to <i>Internet Service</i> . Select the name of a control-based Internet service group.
Outgoing Interface	Required. Select <i>Best Quality (Priority)</i> or <i>Minimum Quality (Maximize Bandwidth)</i> .
Members	Required. Select the interfaces from the Available list and then select > to move them to the Selected list.
Required SLA Target	Required. Available if Outgoing Interface is set to <i>Minimum Quality (Maximize Bandwidth)</i> . Select the appropriate performance SLA from the dropdown list.
Status Check	Required. Available if Outgoing Interface is set to <i>Best Quality (Priority)</i> . Select the appropriate performance SLA to use for the status check.

Monitoring the SD-WAN interfaces

Use the *Device Manager > SD-WAN > Monitoring* page to check the performance of the SD-WAN interfaces.

By default, the table view is displayed.

SD-WAN-622/DC5/root

VPN Router SD-WAN Monitoring Auth Server Settings System

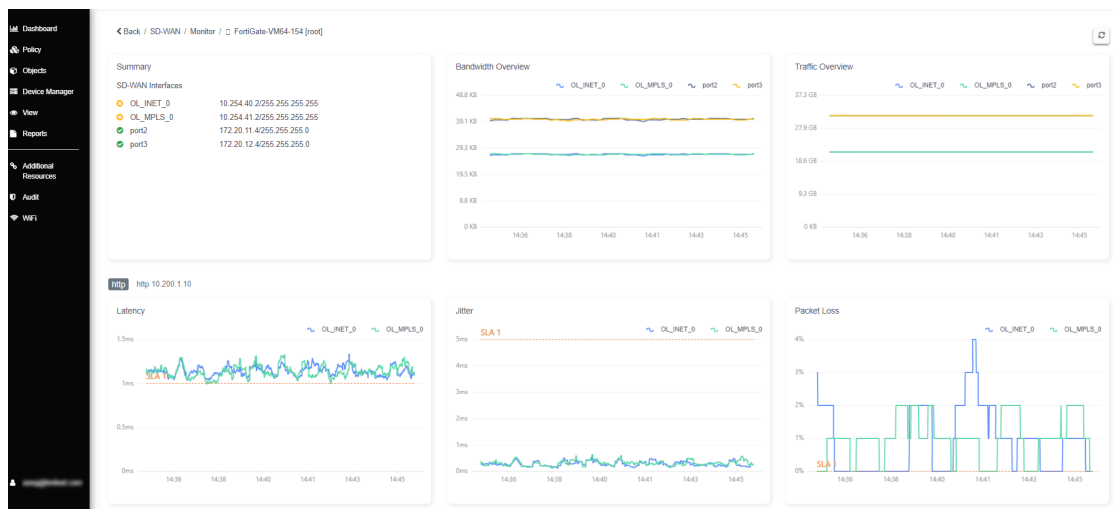
Table Map

Device(DEV)	Interface	Performance SLA	Jitter	Latency	Packet Loss	Session	Bandwidth(TX)	Bandwidth(RX)	Volume(TX)	Volume(RX)
FortiGate-VM64-154[root]	OL_INET_0	http	0.32	1.11	0%	4	8.73 Kbps	19.14 Kbps	6.41 GB	14.01 GB
		test_dc	0.14	0.42	0%					
	OL_MPLS_0	http	0.21	1.19	2%	5	8.61 Kbps	18.84 Kbps	6.41 GB	14.01 GB
		test_dc	0.12	0.47	0%					
	port2	test_Internet	0.08	0.13	0%	0	19.34 kbps	21.91 Kbps	14.22 GB	16.07 GB
FortiGate-VM64-155[root]	OL_INET_0	http	0.29	1.12	0%	4	8.73 kbps	19.14 Kbps	6.48 GB	14.2 GB
		test_dc	0.09	0.37	0%					
	OL_MPLS_0	http	0.28	1.09	0%	4	8.73 kbps	19.14 Kbps	6.48 GB	14.2 GB
		test_dc	0.15	0.43	0%					
	port2	test_Internet	0.05	0.13	0%	0	19.34 Kbps	21.91 Kbps	14.36 GB	16.26 GB
	port3	test_Internet	0.05	0.12	0%	0	19.35 kbps	21.92 Kbps	14.36 GB	16.27 GB

In the table view, select the device to open the *Monitoring* dashboard.

The *Monitoring* dashboard includes the following graphs:

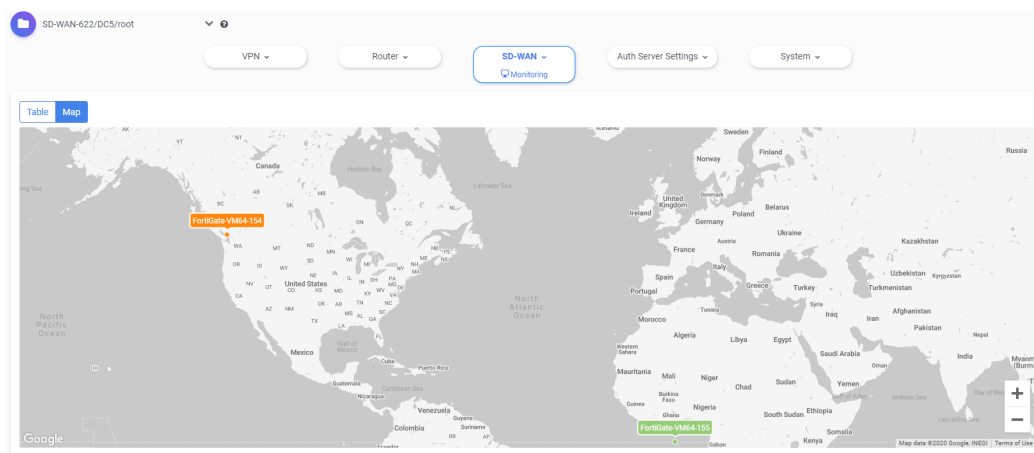
- Bandwidth Overview
- Traffic Overview
- Link health: jitter, latency, and packet loss.





Select **Map** to see a visual presentation of the same data.

The Map view allows you to visually monitor SD-WAN interfaces. Use your cursor to move the map around. Select **+** to zoom in on a location.

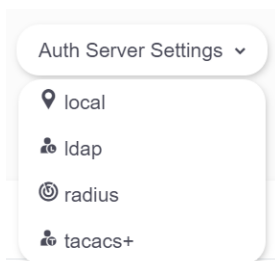


Auth Server Settings

You can set up local, LDAP, RADIUS, and TACACS+ authentication for FortiPortal users.

The *Auth Server Settings* tree on the *Device Manager* tab allows you to perform the following tasks:

- Add, update, and delete local authentication settings. See [Local authentication on page 54](#)
- Add, update, and delete LDAP authentication settings. See [LDAP authentication on page 56](#)
- Add, update, and delete RADIUS authentication settings. See [RADIUS authentication on page 60](#)
- Add, update, and delete TACACS+ authentication settings. See [TACACS+ authentication on page 66](#)



Local authentication

You can add, update, and delete local authentication settings.

Add local authentication settings

1. Select *local* from the *Auth Server Settings* dropdown menu.
2. Right-click in the local authentication table and select *Create New*.
3. Enter values in the relevant fields. See [Local authentication fields on page 55](#).
4. Select *Save*.

Update local authentication settings

1. Select *local* from the *Auth Server Settings* dropdown menu.
2. Right-click a local user and select *Edit*.
3. Update the values that you want to change.
4. Select *Save*.

Delete local authentication settings

1. Select *local* from the *Auth Server Settings* dropdown menu.
2. Right-click a local user and select *Delete*.
3. Select *Yes* in the confirmation dialog box to delete the local user.

Local authentication fields

Create New Local User [X]

Name*

Auth Concurrent Override

Auth Concurrent Value

Auth Timeout

Email-To

FortiToken

Id

LDAP Server

Password

Password Policy

PPK Identity

PPK Password

Radius Server

SMS Custom Server

SMS Phone

SMS Server

Status

TACACS+ Server

Two-Factor

user.local.two-factor-authentication

user.local.two-factor-notification

Type*

user.local.username-case-sensitivity

Workstation

Save

The *Create New Local User* and *Edit Local User* dialogs contain the following fields:

Settings	Guidelines
Name	Required. Enter the name of the local user.
Auth Concurrent Override	Enable or disable overriding the number of concurrent firewall use logins from the same user.
Auth Concurrent Value	The maximum number of concurrent logins permitted from the same user.
Auth Timeout	The number of minutes before the authentication timeout for a user is reached.

Settings	Guidelines
Email-To	Two-factor recipient's email address.
FortiToken	Two-factor recipient's FortiToken serial number.
Id	Local user ID.
LDAP Server	The name of the LDAP server with which the user must authenticate.
Password	Local user's password.
Password Policy	Password policy to apply to this user.
PPK Identity	Specify the Post-quantum Preshared Key (PKK) Identity for successful validation of PPK credentials in dynamic VPNs with peertype dialup.
PPK Password	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).
Radius Server	The name of the RADIUS server with which the user must authenticate.
SMS Custom Server	Two-factor recipient's SMS server.
SMS Phone	Two-factor recipient's mobile phone number.
SMS Server	Send SMS through FortiGuard or other external server.
Status	Enable or disable allowing the local user to authenticate with the FortiGate unit.
TACACS+ Server	The name of the TACACS+ server with which the user must authenticate.
Two-Factor	<p>Disable two-factor authentication or choose which two-factor authentication method is used:</p> <p><i>fortitoken</i>—FortiToken</p> <p><i>disable</i>—disable</p> <p><i>sms</i>—SMS authentication code.</p> <p><i>email</i>—Email authentication code.</p>
Type	<p>Required. Select the authentication method.</p> <p><i>password</i>—Password authentication.</p> <p><i>ldap</i>—LDAP server authentication.</p> <p><i>tacacs+</i>—TACACS+ server authentication.</p> <p><i>radius</i>—RADIUS server authentication.</p>
Workstation	If you want to limit the user to authenticate only from a particular workstation, enter the name of the remote user workstation

LDAP authentication

You can add, update, and delete LDAP authentication settings.

Add LDAP authentication settings

1. Select *ldap* from the *Auth Server Settings* dropdown menu.
2. Right-click in the LDAP authentication table and select *Create New*.
3. Enter values in the relevant fields. See [LDAP authentication fields on page 58](#).
4. Select *Save*.

Update LDAP authentication settings

1. Select *ldap* from the *Auth Server Settings* dropdown menu.
2. Right-click an LDAP server and select *Edit*.
3. Update the values that you want to change.
4. Select *Save*.

Delete LDAP authentication settings

1. Select *ldap* from the *Auth Server Settings* dropdown menu.
2. Right-click an LDAP server and select *Delete*.
3. Select *Yes* in the confirmation dialog box to delete the selected server.

LDAP authentication fields

Create New LDAP Server

Name*

Account Key Filter

((&(userPrincipalName=%s)(!(UserAccountControl:1.2.840.113556.1.4

Account Key Processing

same

CA-Cert

CN ID

cn

Distinguished Name*

Group Filter

Group Member Check

user-attr

Group Object Filter

(&(objectcategory=group)(member=*))

Group Search Base

user.ldap.interface

user.ldap.interface-select-method

auto

Member Attribute

memberOf

user.ldap.obtain-user-info

enable

Password

Enable Password Expiry Warning

disable

Password Renewal

disable

Port

389

user.ldap.search-type

Secondary Server

Secure

disable

Server*

Server Identity Check

enable

IP

0.0.0.0

SSL_MIN_Protocol Version

default

Tertiary Server

user.ldap.two-factor

disable

user.ldap.two-factor-authentication

user.ldap.two-factor-notification

Type

simple

user.ldap.user-info-exchange-server

No data available

Username

Save

Cancel

The *Create New LDAP Server* and *Edit LDAP Server* dialogs contain the following fields:

Settings	Guidelines
Name	Required. The LDAP server name.
Account Key Filter	Account key filter, using the user principal name (UPN) as the search filter.
Account Key Processing	Account key processing operation, either to keep or to strip the domain string of the UPN in the token: <i>same</i> —Same as the UPN. <i>strip</i> —Strip the domain string from UPN.
CA-Cert	CA certificate name.
CN ID	Common name identifier for the LDAP server. The common name identifier for most LDAP servers is <code>cn</code> .
Distinguished Name	Required. Distinguished name used to look up entries on the LDAP server.
Group Filter	The filter used for group matching.
Group Member Check	Group member checking methods: <i>user-attr</i> —User attribute checking. <i>group-object</i> —Group object checking. <i>posix-group-object</i> —POSIX group object checking.
Group Object Filter	The filter used for group searching.
Group Search Base	The search base used for group searching.
Member Attribute	The name of the attribute from which to get group membership.
Password	The password for initial binding.
Enable Password Expiry Warning	Enable or disable warnings before the password expires.
Password Renewal	Enable or disable online password renewal.
Port	The port to be used for communication with the LDAP server. The default is 389.
Secondary Server	The CN domain name or IP address of the secondary LDAP server.
Secure	The security protocol to be used for authentication: <i>starttls</i> —Use StartTLS. <i>disable</i> —No SSL. <i>ldaps</i> —Use LDAPS.
Server	Required. The CN domain name or IP address of the LDAP server.
Server Identity Check	Enable or disable whether the server identity is checked.
IP	The source IPv4 address for communications to LDAP server.

Settings	Guidelines
SSL_MIN_Protocol Version	<p>The minimum supported protocol version for SSL/TLS connections.</p> <p><i>SSLv3</i>—SSLv3.</p> <p><i>default</i>—Follow system global setting.</p> <p><i>TLSv1</i>—TLSv1.</p> <p><i>TLSv1-2</i>—TLSv1.2.</p> <p><i>TLSv1-1</i>—TLSv1.1.</p>
Tertiary Server	The CN domain name or IP address of the tertiary LDAP server.
Type	<p>Authentication type for LDAP searches:</p> <p><i>anonymous</i>—Bind using anonymous user search.</p> <p><i>simple</i>—Simple password authentication without search.</p> <p><i>regular</i>—Bind using user name and password and then search.</p>
Username	User name (full DN) for initial binding.

RADIUS authentication

You can add, update, and delete RADIUS authentication settings.

Add RADIUS authentication settings

1. Select *radius* from the *Auth Server Settings* dropdown menu.
2. Right-click in the RADIUS authentication table and select *Create New*.
3. Enter values in the relevant fields. See [RADIUS authentication fields on page 61](#).
4. Select *Save*.

Update RADIUS authentication settings

1. Select *radius* from the *Auth Server Settings* dropdown menu.
2. Right-click a RADIUS server and select *Edit*.
3. Update the values that you want to change.
4. Select *Save*.

Delete RADIUS authentication settings

1. Select *radius* from the *Auth Server Settings* dropdown menu.
2. Right-click a RADIUS server and select *Delete*.
3. Select *Yes* in the confirmation dialog box to delete the selected server.

RADIUS authentication fields

Create New Radius Server

Name*

Account All Servers

disable

Account Interim Update Interval

0

All User Group

disable

Authentication Type

auto

Class

H3C Compatibility

disable

Interface

Interface Select Method

auto

NAS-IP

0.0.0.0

Password Encoding

auto

Password Renewal

disable

Allow Change of Attributes

disable

Radius Port

0

Radius based SSO

disable

RSSO Context Timeout

28800

RSSO Endpoint Attribute

Calling-Station-Id

RSSO Endpoint Block Attribute

RSSO One IP Address By Endpoint

disable

RSSO Flush IP Session

disable

RSSO Log Flags

☒accounting-event
☒accounting-stop-missed
☒endpoint-block
☒Chrom
☒profile-missing
☒protocol-error
☒radiusd-other

RSSO Log Period

0

RSSO Radius Response

disable

RSSO Radius Server Port

1813

RSSO Password

RSSO Validation Request Secret

disable

Secondary Password

Secondary Server

Password

Server

Source IP

SSO Attribute

Class

SSO Attribute Key

SSO Attribute Value Override

enable

Tertiary Password

Tertiary Server

Timeout

5

Use Management Vidom

disable

Username Case Sensitive

disable

Accounting Server

Id

Server

Interface

Interface Select Method

Port

Action

No data available

Create New

Save Cancel

The *Create New Radius Server* and *Edit Radius Server* dialogs contain the following fields:

Settings	Guidelines
Name	Required. The RADIUS server name.
Account All Servers	Enable or disable the sending of accounting messages to all configured servers. The default is <i>disable</i> .
Account Interim Update Interval	The number of seconds between each accounting interim update message.

Settings	Guidelines
all User-group	Enable or disable whether this RADIUS server is automatically included in all user groups.
Authentication Type	Authentication methods/protocols permitted for this RADIUS server: <i>ms_chap</i> —Microsoft Challenge Handshake Authentication Protocol. <i>ms_chap_v2</i> —Microsoft Challenge Handshake Authentication Protocol version 2. <i>auto</i> —Use PAP, MSCHAP_v2, and CHAP (in that order). <i>chap</i> —Challenge Handshake Authentication Protocol. <i>pap</i> — Password Authentication Protocol.
Class	Class attribute name(s).
H3C Compatibility	Enable or disable compatibility with the H3C, a mechanism that performs security checking for authentication.
NAS-IP	IPv4 address used to communicate with the RADIUS server and used as NAS-IP-Address and Called-Station-ID attributes.
Password Encoding	Password encoding: <i>auto</i> —Use original password encoding. <i>ISO-8859-1</i> —Use ISO-8859-1 password encoding.
Password Renewal	Enable or disable password renewal.
Allow Change of Attributes	Enable or disable the overriding of an old attribute value with a new value for the same endpoint.
Radius Port	RADIUS service port number.
Radius based SSO	Enable or disable the RADIUS-based single sign-on feature.
RSSO Context Timeout	Time in seconds before the logged-out user is removed from the “user context list” of logged-on users.

Settings	Guidelines
RSSO Endpoint Block Attribute	<p>RADIUS attributes used to block a user:</p> <p><i>Login-LAT-Service</i>—Use this attribute.</p> <p><i>NAS-IP-Address</i>—Use this attribute.</p> <p><i>Callback-Number</i>—Use this attribute.</p> <p><i>NAS-Identifier</i>—Use this attribute.</p> <p><i>Acct-Multi-Session-Id</i>—Use this attribute.</p> <p><i>Login-LAT-Group</i>—Use this attribute.</p> <p><i>Reply-Message</i>—Use this attribute.</p> <p><i>User-Name</i>—Use this attribute.</p> <p><i>Calling-Station-Id</i>—Use this attribute.</p> <p><i>Filter-Id</i>—Use this attribute.</p> <p><i>Framed-IP-Address</i>—Use this attribute.</p> <p><i>Framed-IP-Netmask</i>—Use this attribute.</p> <p><i>Login-IP-Host</i>—Use this attribute.</p> <p><i>Callback-Id</i>—Use this attribute.</p> <p><i>Class</i>—Use this attribute.</p> <p><i>Framed-Route</i>—Use this attribute.</p> <p><i>Acct-Session-Id</i>—Use this attribute.</p> <p><i>Proxy-State</i>—Use this attribute.</p> <p><i>Called-Station-Id</i>—Use this attribute.</p> <p><i>Framed-AppleTalk-Zone</i>—Use this attribute.</p> <p><i>Login-LAT-Node</i>—Use this attribute.</p> <p><i>Framed-IPX-Network</i>—Use this attribute.</p>
RSSO One IP Address By Endpoint	Enable or disable the replacement of old IP addresses with new ones for the same endpoint on RADIUS accounting Start messages.
RSSO Flush IP Session	Enable or disable the flushing of user IP sessions on RADIUS accounting Stop messages.

Settings	Guidelines
RSSO Log Flags	Events to log: <i>radiusd-other</i> —Enable this log type. <i>profile-missing</i> —Enable this log type. <i>accounting-event</i> —Enable this log type. <i>protocol-error</i> —Enable this log type. <i>endpoint-block</i> —Enable this log type. <i>none</i> —Disable all logging. <i>accounting-stop-missed</i> —Enable this log type.
RSSO Log Period	How often (in seconds) that group event log messages are generated for dynamic profile events.
RSSO Radius Response	Enable or disable the sending of RADIUS response packets after receiving Start and Stop records.
RSSO Radius Server Port	The UDP port to listen on for RADIUS Start and Stop records.
RSSO Password	The RADIUS secret used by the RADIUS accounting server.
RSSO Validation Request Secret	Enable or disable the validation of the RADIUS request shared secret in the Start or End record.
Secondary Password	The secret key to access the secondary server.
Secondary Server	The CN domain name or IP address for the secondary RADIUS server.
Password	The pre-shared secret key used to access the primary RADIUS server.
Server	The primary RADIUS server CN domain name or IP address.
Source IP	The source IP address for communications to the RADIUS server.

Settings	Guidelines
SSO Attribute	<p>RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record:</p> <p><i>Login-LAT-Service</i>—Use this attribute.</p> <p><i>NAS-IP-Address</i>—Use this attribute.</p> <p><i>Callback-Number</i>—Use this attribute.</p> <p><i>NAS-Identifier</i>—Use this attribute.</p> <p><i>Acct-Multi-Session-Id</i>—Use this attribute.</p> <p><i>Login-LAT-Group</i>—Use this attribute.</p> <p><i>Reply-Message</i>—Use this attribute.</p> <p><i>User-Name</i>—Use this attribute.</p> <p><i>Calling-Station-Id</i>—Use this attribute.</p> <p><i>Filter-Id</i>—Use this attribute.</p> <p><i>Framed-IP-Address</i>—Use this attribute.</p> <p><i>Framed-IP-Netmask</i>—Use this attribute.</p> <p><i>Login-IP-Host</i>—Use this attribute.</p> <p><i>Callback-Id</i>—Use this attribute.</p> <p><i>Class</i>—Use this attribute.</p> <p><i>Framed-Route</i>—Use this attribute.</p> <p><i>Acct-Session-Id</i>—Use this attribute.</p> <p><i>Proxy-State</i>—Use this attribute.</p> <p><i>Called-Station-Id</i>—Use this attribute.</p> <p><i>Framed-AppleTalk-Zone</i>—Use this attribute.</p> <p><i>Login-LAT-Node</i>—Use this attribute.</p> <p><i>Framed-IPX-Network</i>—Use this attribute.</p>
SSO Attribute Key	The key prefix for SSO group value in the SSO attribute.
SSO Attribute Value Override	Enable or disable whether to override the old attribute value with a new value for the same endpoint.
Tertiary Password	The secret key to access the tertiary server.
Tertiary Server	The CN domain name or IP address for the tertiary RADIUS server.
Timeout	How often (in seconds) authentication requests are re-sent .
Use Management Vdom	Enable or disable whether to use the management VDOM to send requests.
Username Case Sensitive	Enable or disable whether user names are case sensitive.
Accounting Server	Additional accounting servers. See Add an accounting server .

Add an accounting server

1. Click *Create New* in the *Accounting Server* table.
2. In the *Id* field, enter an identifier for the accounting server.
3. In the *Port* field, enter the RADIUS accounting port number.
4. In the *Password* field, enter the secret key for the accounting server.
5. In the *Server* field, enter the server CN domain name or IP address.
6. In the *Source IP* field, enter the source IP address for communications to the RADIUS server.
7. In the *Status* field, select *enable* to make the accounting server active.
8. Select *Save* to save the settings.

create new Accounting Server

Id* 0

user.radius.accounting-server.interface

user.radius.accounting-server.interface-select-method auto

Port 0

Password

Server*

Source IP

Status disable

Save Cancel

TACACS+ authentication

You can add, update, and delete TACACS+ authentication settings.

Add TACACS+ authentication settings

1. Select *tacacs+* from the *Auth Server Settings* dropdown menu.
2. Right-click in the TACACS+ authentication table and select *Create New*.
3. Enter values in the relevant fields. See [TACACS+ authentication fields](#).
4. Select *Save*.

Update TACACS+ authentication settings

1. Select *tacacs+* from the *Auth Server Settings* dropdown menu.
2. Right-click a TACACS+ server and select *Edit*.
3. Update the values that you want to change.
4. Select *Save*.

Delete TACACS+ authentication settings

1. Select *tacacs+* from the *Auth Server Settings* dropdown menu.
2. Right-click a TACACS+ server and select *Delete*.
3. Select *Yes* in the confirmation dialog box to delete the selected server.

TACACS+ authentication fields

Create New TACACS+ ×

Name*

Authentication Type

auto

Authorization

disable

Interface

user,tacacs+ interface-select-method

auto

Key

Port

49

Secondary Key

Secondary Server

Server*

Source Ip

Tertiary Key

Tertiary Server

Save

Cancel

The *Create New TACACS+* and *Edit TACACS+* dialogs contain the following fields:

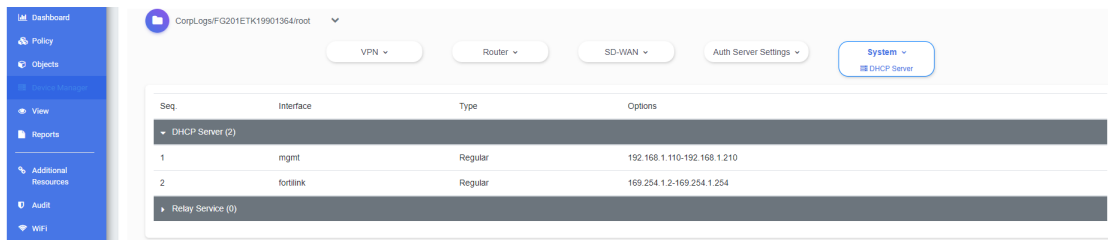
Settings	Guidelines
Name	Required. The TACACS+ server name.
Authentication Type	Authentication methods/protocols permitted for this TACACS+ server: <i>auto</i> —Use PAP, MSCHAP, and CHAP (in that order). <i>ms_chap</i> —Microsoft Challenge Handshake Authentication Protocol. <i>chap</i> —Challenge Handshake Authentication Protocol. <i>ascii</i> —ASCII. <i>pap</i> —Password Authentication Protocol.
Authorization	Enable or disable TACACS+ authorization.
Key	The key to access the primary server.
Port	The port number of the TACACS+ server.
Secondary Key	The key to access the secondary server.

Settings	Guidelines
Secondary Server	The CN domain name or IP address for the secondary TACACS+ server.
Server	Required. The CN domain name or IP address for the primary TACACS+ server.
Source Ip	The source IP address for communications to TACACS+ server.
Tertiary Key	The key to access the tertiary server.
Tertiary Server	The CN domain name or IP address for the tertiary TACACS+ server.

DHCP Server

The *System > DHCP Server* dropdown menu on the Device Manager tab allows you to perform the following tasks:

- Add, update, or delete a DHCP server.
- Add, update, or delete a DHCP relay.



DHCP Server

You can add, update, and delete DHCP servers.

Adding a DHCP server

1. Select *DHCP Server* from the *System* dropdown menu.
2. Right-click in the DHCP Server section of the table and select *Create New*.
3. Enter values in the relevant fields. See [DHCP server fields on page 69](#).
4. Select *Save*.

Updating a DHCP server

1. Select *DHCP Server* from the *System* dropdown menu.
2. Right-click a DHCP server and select *Edit*.
3. Update the values that you want to change.
4. Select *Save*.

Deleting a DHCP server

1. Select *DHCP Server* from the *System* dropdown menu.
2. Right-click a DHCP server and select *Delete*.
3. Select *Yes* in the confirmation dialog box to delete the selected DHCP server.

DHCP server fields

The *Create New DHCP Server* and *Edit DHCP Server* dialogs contain the following fields:

Settings	Guidelines
Interface	The name of the interface.
Mode	Select <i>Server</i> to create a DHCP server.
Enable	Select this option to make the DHCP server active.
Type	Select <i>Regular</i> to use the DHCP in regular mode. Select <i>IPsec</i> to use the DHCP in IPsec mode.
IP Range	DHCP IP address range. The IP range of each DHCP server must match the network address range. See Configure an IP range on page 70 .
Network Mask	Required. Netmask assigned by the DHCP server.
Default Gateway	Required. Default gateway IP address assigned by the DHCP server.

Settings	Guidelines
Next Server	Required. IP address of a server (for example, a TFTP sever) that DHCP clients can download a boot file from.
DNS Service	Options for assigning DNS servers to DHCP clients: <i>Use System DNS Setting (Default)</i> —Clients are assigned the FortiGate device's configured DNS servers. <i>Specify</i> —Specify up to three DNS servers in the DHCP server configuration. <i>Same as interface IP (Local)</i> —The IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.
DNS Service0	DNS server 1.
DNS Service1	DNS server 2.
DNS Service2	DNS server 3.
NTP Service	Options for assigning Network Time Protocol (NTP) servers to DHCP clients: <i>Use System NTP Setting</i> —The IP address of the interface the DHCP server is added to becomes the client's NTP server IP address. <i>Specify</i> —Specify up to three NTP servers in the DHCP server configuration. <i>Use FortiGate as NTP Server</i> —Clients are assigned the FortiGate device's configured NTP servers.
NTP Service0	NTP server 1.
NTP Service1	NTP server 2.
NTP Service2	NTP server 3.
FortiClient On-Net Status	Select this option to require all clients to have FortiClient installed in order to get access through the FortiGate.
Timezone Option	Options for the DHCP server to set the client's time zone. <i>Disable</i> —Do not set the client's time zone. <i>Default</i> —Clients are assigned the FortiGate device's configured time zone. <i>Specify</i> —Specify the time zone to be assigned to DHCP clients. If you select <i>Specify</i> , enter the two-digit code that corresponds to the appropriate time zone in the Timezone field.
MAC Address Access Control List	A MAC Address Access Control List (ACL) allows or blocks access on a network interface that includes a DHCP server. See Configure an MAC address access control list on page 71 .

Configure an IP range

1. Right-click in the *IP Range* table and select *Create New*.
2. In the Start IP field, enter the IPv4 address at the start of the IP address range.
3. In the End IP field, enter the IPv4 address at the end of the IP address range.

4. To add a DHCP option, under *Advanced Options*, enter the option number in the ID field .



The option number and value must be configured on the DHCP server.

5. Select *Yes* to save the IP range.

Configure an MAC address access control list

1. Right-click in the *MAC Address Access Control List* table and select *Create New*.
2. In the IP field, enter an IP address to allow or block.
3. In the MAC field, enter a MAC address to allow or block.
4. Select *Assign* to allow the IP address and MAC address, select *Block* to block the IP address and MAC address, or select *Reserved* to prevent the IP address and MAC address from being used in any rules.
5. In the Description field, enter an optional description of the MAC address access control list.
6. To add a DHCP option, under *Advanced Options*, enter the option number in the ID field.



The option number and value must be configured on the DHCP server.

7. Select *Yes* to save the MAC address access control list.

Relay Service

You can add, update, and delete DHCP relays.

Adding a DHCP relay

1. Select *DHCP Server* from the *System* dropdown menu.
2. Right-click in the Relay Service section of the table and select *Create New*.
3. Enter values in the relevant fields. See [DHCP relay fields on page 72](#).
4. Select *Save*.

Updating a DHCP relay

1. Select *DHCP Server* from the *System* dropdown menu.
2. Right-click a relay service and select *Edit*.
3. Update the values that you want to change.
4. Select *Save*.

Deleting a DHCP relay

1. Select *DHCP Server* from the *System* dropdown menu.
2. Right-click a relay service and select *Delete*.
3. Select *Yes* in the confirmation dialog box to delete the selected relay service.

DHCP relay fields

The *Create New DHCP Sever* and *Edit DHCP Server* dialogs contain the following fields:

Settings	Guidelines
Interface	The name of the interface.
Mode	Select <i>Relay</i> to create a DHCP relay.
Enable	Select this option to make the DHCP server active.
Type	Select <i>Regular</i> to use the DHCP in regular mode. Select <i>IPsec</i> to use the DHCP in IPsec mode.
DHCP Server IP 1-10	The IP addresses of the DHCP servers to use for the DHCP relay.

View

The *View* tab displays information about the security event logs. It contains filters and controls that allow you to group the event logs in different ways, and to drill down and view the details of a related set of event logs.

The following action buttons are available along the top of the page:

- *Application/Attack/Sandbox/VPN*—view the event logs grouped by application, attack, sandbox, or VPN.
- *Scope*—view output for all sites or select a specific site
- *Set Filter*—filter the data (last 5 minutes, last 30 minutes, last 60 minutes, last 4 hours, last 12 hours, last 1 day, last 7 days, or specify)
- *Refresh*—refresh the data
- *Sort*—Each column has a sorting feature, allowing you to sort data in ascending or descending order.

The table header provides a dropdown menu for selecting the number of entries to display.

After you select *Application*, *Attack*, *Sandbox*, or *VPN* you can select how to sort the event logs.

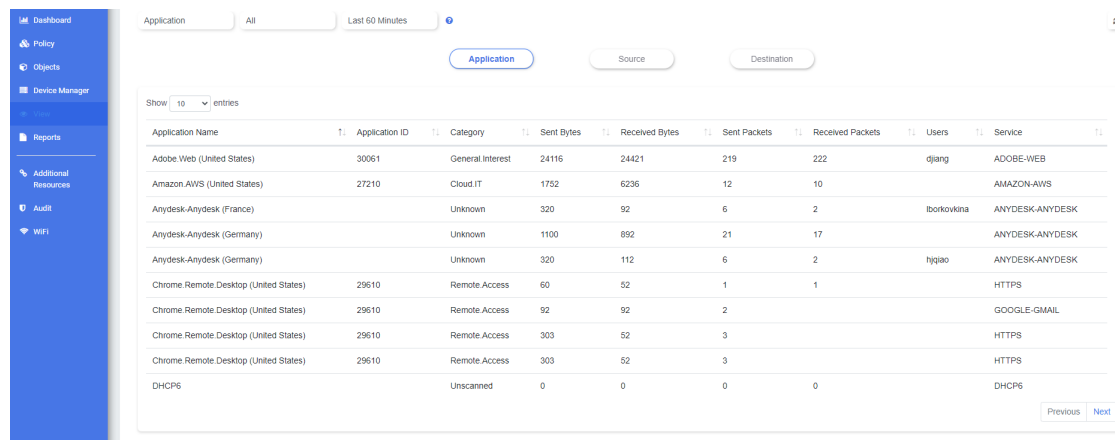
The following tabs provide different views of the data:

- *Application*—arranged by application. See [Application view on page 73](#).
- *Attack*—arranged by attack. See [Attack view on page 74](#).
- *Sandbox*—arranged by sandbox. See [Sandbox view on page 74](#).
- *VPN*—arranged by VPN. See [VPN view on page 75](#).
- *Source*—arranged by the source FortiGate device.
- *Destination*—arranged by the destination (IP address, protocol, port).

Application view

The *Application* tab under *View* displays event logs grouped by application.

The following figure shows an example of the *Application* tab:



Application Name	Application ID	Category	Sent Bytes	Received Bytes	Sent Packets	Received Packets	Users	Service
Adobe Web (United States)	30061	General Interest	24116	24421	219	222	djang	ADOBE-WEB
Amazon AWS (United States)	27210	Cloud.IT	1752	6236	12	10		AMAZON-AWS
Anydesk-Anydesk (France)		Unknown	320	92	6	2	Iborikovkina	ANYDESK-ANYDESK
Anydesk-Anydesk (Germany)		Unknown	1100	892	21	17		ANYDESK-ANYDESK
Anydesk-Anydesk (Germany)		Unknown	320	112	6	2	hygao	ANYDESK-ANYDESK
Chrome Remote Desktop (United States)	29610	Remote Access	60	52	1	1		HTTPS
Chrome Remote Desktop (United States)	29610	Remote Access	92	92	2			GOOGLE-GMAIL
Chrome Remote Desktop (United States)	29610	Remote Access	303	52	3			HTTPS
Chrome Remote Desktop (United States)	29610	Remote Access	303	52	3			HTTPS
DHCP		Unscanned	0	0	0	0		DHCP

Attack view

The *Attack* tab under *View* displays event logs grouped by “attack.”

The following figure shows an example of the *Attack* tab:

The screenshot shows the FortiGate web interface with the 'Attack' tab selected. The table displays the following data:

Attack Name	Count	Level	Device ID	Attack ID	Policy ID	Service
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS
DNS Amplification.Detection		alert	FGT37D4615801346	32784	19	DNS

When you select one of the entries in the table, the system displays the first set of filtering.

For each of the remaining filters, a horizontal left menu includes buttons to perform the next level of filtering (see the following figure):

The screenshot shows the FortiGate web interface with the 'Attack' tab selected. The 'Source' filter is applied, and the table displays the following data:

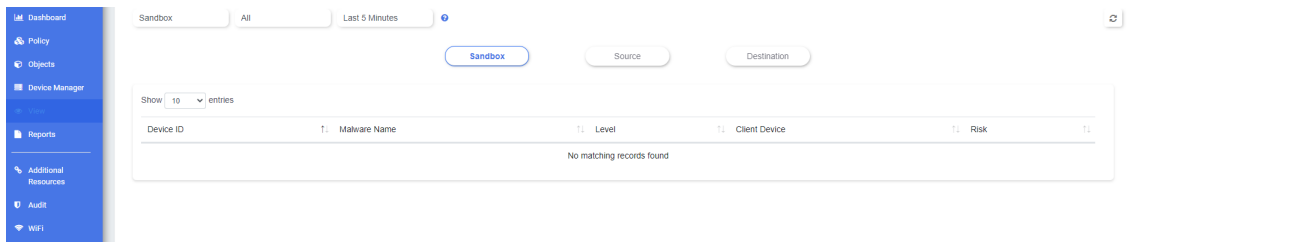
Source	Source Port	Source Interface
172.17.65.199	1025	64FortiGuardDev
172.17.65.199	1053	64FortiGuardDev
172.17.65.199	1174	64FortiGuardDev
172.17.65.199	1212	64FortiGuardDev
172.17.65.199	1374	64FortiGuardDev
172.17.65.199	1375	64FortiGuardDev
172.17.65.199	1376	64FortiGuardDev
172.17.65.199	1378	64FortiGuardDev
172.17.65.199	1378	64FortiGuardDev
172.17.65.199	1379	64FortiGuardDev

The applied filters are listed horizontally across the display (see the preceding figure). Select the x button beside the filter to remove that filter.

Sandbox view

The *Sandbox* tab under *View* displays event logs grouped by “sandbox.”

The following figure shows an example of the *Sandbox* tab:



Use the *Source* or *Destination* tab to filter the view.

When you select one of the entries in the table, the sandbox view works like the attack view. The system displays the first set of filtering. For each of the remaining filters, a horizontal left menu includes buttons to perform the next level of filtering.

The applied filters are listed across the display. Select the gray x button beside each to remove that filter.

VPN view

The *VPN* tab under *View* displays the VPN related information, allowing users to monitor SSL & Dialup IPsec and Site-to-Site IPsec VPN.

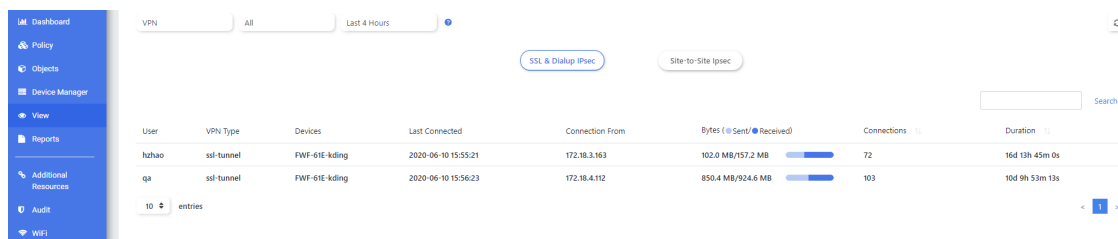
It gives the following details:

- VPN users
- Connection time
- Connecting location
- Duration

To open VPN view:

1. Go to *View* and from the dropdown menu at the top, select *VPN*.

The figure below shows an example of the *VPN* tab:



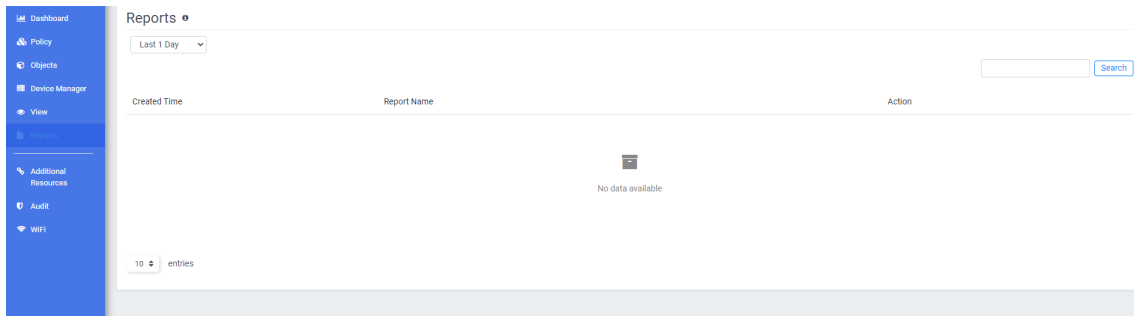
When *VPN* is selected from the dropdown list, the *View* page displays two tabs:

- *SSL & Dialup IPsec*
- *Site-to-Site IPsec*

By default, the *SSL & Dialup IPsec* tab is selected.

Reports

The *Reports* page displays a list of the available FortiAnalyzer reports.



Page actions

This page includes the following actions:

- *Set Filter*—filter the data (today, last 1 day, last 1 week, last 1 month, or specify).
- *Search*—text search by report name

When you scroll over a entry in the reports table, the following icon appears in the Action column:

- *Download*—downloads the selected report as a PDF file

Additional Resources

The *Additional Resources* tab displays *Help*, *Chat*, and *FAQ* buttons. If active, the button's text and image are selectable and open a new tab with the given URL. If disabled, the button's text and image cannot be selected.

Additional Resources



Audit

The *Audit* window displays a log of user activity on the Administrative Web Interface:

Audit Log List

Last 60 Minutes Export to CSV Search

Date(GMT)	Level	User Name	Event Type	Client IP Address	Message	Action
2020-06-24 15:35:13	Info	techdoc@fortinet.com	Login	192.168.1.1	Login User (techdoc@fortinet.com) was logged in	

10 entries 1

Page actions

- *Audit Log List*—set the duration of the logs to display (from last 5 minutes to last 7 days or customize)
- *Export to CSV*—export the audit log list as a Comma-Separated Value (CSV) file
- *Search*—use any column to search the audit log list by level, user name, event type, client IP address, or message
- *Show x entries*—use the drop-down menu to set the number of entries to display
- *Sort*—allows you to sort columns in ascending or descending order.

Per-audit actions

When you select the *Details* button for an audit entry for changed settings, the system opens a window to display the details of the change. The details window shows the original ("oldDetails") and new ("newDetails") field values.

Details

```
{
  "oldDetails": [
    {
      "serialNumber": "FGT6801100636412",
      "wifiFrequencyValue": "Every 15 Minutes",
      "port": 443,
      "ipAddress": "0.0.0.0",
      "wifiController": "No",
      "deviceName": "ADOM_QA_68/FGTH0060/root"
    }
  ],
  "newDetails": [
    {
      "serialNumber": "FGT6801100636412",
      "wifiFrequencyValue": "Every 15 Minutes",
      "port": 443,
      "ipAddress": "0.0.0.0",
      "wifiController": "Yes",
      "deviceName": "ADOM_QA_68/FGTH0060/root"
    }
  ]
}
```

Cancel

WiFi

Use the *WiFi* tab for the following:

- Update or delete managed access points (APs). See [Managed AP](#).
- Monitor rogue access points, Fortinet access points (FAPs), and SSIDs. See [WiFi Monitor](#).
- Update or delete access point profiles and add, update, or delete SSIDs. See [WiFi Profile](#).

Managed AP

The *Managed AP > Managed AP* tree on the *WiFi* tab allows you to view a list of managed access points (APs). The *Managed AP* page contains the following actions:

- *Edit*—Modify the managed AP.
- *Delete*—Remove the managed AP.

The following figure shows the *Managed AP* page:

WiFi ⓘ

HA-v60/FWF-61E-kding/root

- Managed AP
- WiFi Monitor
- WiFi Profile

Access Point	Connect Via	SSID	Channel	Clients	OS Version	AP Profile
test	---	Radio 1: Radio 2:	Radio 1: 0	Radio 1: 0		FAP24D-default
FWF61E-WIFI0	127.0.0.1	Radio 1: Radio 2:	Radio 1: 149	Radio 1: 1	FWF61E-v6.0-build303	11ac-only

Update a managed AP

1. Right-click a managed AP in the list and select *Edit*.
2. Make any changes.
3. Select *Save*.

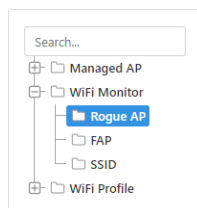
Delete a managed AP

1. Right-click a managed AP in the list and select *Delete*.
2. Select *Yes* to confirm your choice.

WiFi Monitor

The *WiFi Monitor* tree on the *WiFi* tab allows you to choose which wireless devices to monitor:

- Rogue access points (APs)
- Fortinet APs
- SSIDs

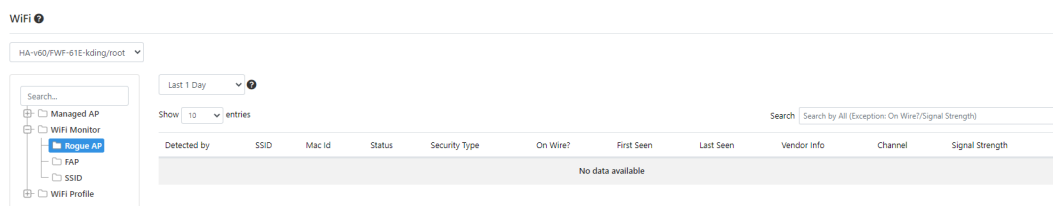


Rogue AP

The *Rogue AP* page displays a list of rogue access points detected on the network and contains the following actions:

- **Filter**—filter the data (last 60 Minutes, last 1 day, last 7 days, or specify a filter)
- **Show *x* entries**—drop-down menu to set the number of entries per page
- **Search**—search by any of the fields, except the On Wire? and Signal Strength fields.

The following figure shows the Rogue AP page:

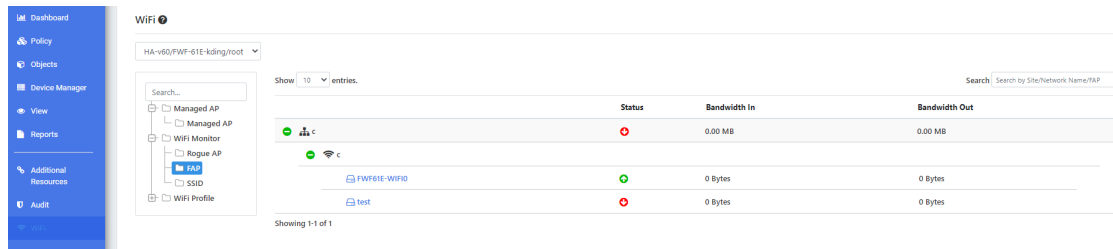


FAP

The *FAP* page displays the SSIDs for each FAP at each site and contains the following actions:

- **Show *x* entries**—drop-down menu to set the number of entries per page
- **Search**—search by site, network name, or device.

The following figure shows the FAP page:



Selecting the green + button adjacent to an entry expands the entry and shows the next level of data. Select a red — button to hide the data for an entry.

If you select the FAP name, the system opens a window to show the FAP details as well as details for each SSID.

FAP Details (FWF61E-WIFI0)



FAP Details			
Name	FWF61E-WIFI0	Serial Number	FWF61ETK18007356
Admin Mode		Status	connected
Connection State	Connected	Clients	1
AP Profile	11ac-only	Connection From	127.0.0.1
OS Version	FWF61E-v6.0-build303	Board Mac	e8:1c:ba:7b:80:60
WTP ID	FWF61E-WIFI0	Mesh Uplink	local
Join Time	2020-04-23 17:39:00.0	Last Reboot Time	2020-03-27 12:11:00.0
Last Failure	04/23/20 17:39	Reboot Last Day	false
Last Failure Time		Last Poll on	2020-06-12 21:58:08.0 GMT

Additional information about Fortinet wireless networks is available in the [wireless chapter](#) of the FortiOS handbook.

SSID

The *SSID* page displays assigned access points for the SSID and contains the following actions:

- *Show x entries*—drop-down menu to set the number of entries per page
- *Search*—search by site, network name, or device.

The following figure shows the SSID page:

	Status	Bandwidth In	Bandwidth Out
FPC-Test1			
site1		0.00 MB	0.03 MB
network1			
FAP320		0 Bytes	0 Bytes
FP320B3X13002882		0 Bytes	0 Bytes
FW90DP-WIFI0		0 Bytes	29.44 KB

Selecting the green + button adjacent to an entry expands the entry and shows the next level of data. Select a red — button to hide the data for an entry.

If you select the FAP name, the system opens a window to show the FAP details as well as details for each SSID.

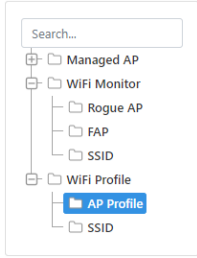
Name	FAP320	Serial Number	FP320B3X13002883
Admin Mode	Disconnected	Status	disconnected
Connection State	clone-1	Clients	0
AP Profile	clone-1	Connection From	0.0.0.0
OS Version	FP320B3X13002883	Board Mac	00:00:00:00:00:00
WTP Id	0 - N/A	Mesh Uplink	ethernet
Join Time		Last Reboot Time	
Last Failure		Reboot Last Day	false
Last Failure Time		Last Poll on	2019-01-09 17:02:39.0

Additional information about Fortinet wireless networks is available in the [wireless chapter](#) of the FortiOS handbook.

WiFi Profile

The *WiFi Profile* tree on the *WiFi* tab allows you to do the following:

- Update access point (AP) profiles
- Delete AP profiles
- Add SSIDs
- Update SSIDs
- Delete SSIDs



AP Profile

The following figure shows the *AP Profile* page:

WiFi ⓘ

HA-60/PWF-61E-kding/root

Search...

Managed AP

WiFi Monitor

Rogue AP

FAP

SSID

WiFi Profile

AP Profile

SSID

Seq.	Name	Platform	Radio 1	Radio 2	Comment
1	11ac-only	FortiWiFi local radio	5GHz 802.11ac/n		
2	11n-only	FortiWiFi local radio	2.4GHz 802.11n/g		
3	AP-11N-default	Default 11n AP	2.4GHz 802.11n/g		
4	FAP112B-default	FAP112B	2.4GHz 802.11n/g		
5	FAP112D-default	FAP112D	2.4GHz 802.11n/g		
6	FAP11C-default	FAP11C	2.4GHz 802.11n/g		
7	FAP14C-default	FAP14C	2.4GHz 802.11n/g		
8	FAP210B-default	FAP210B	2.4GHz 802.11n/g		
9	FAP21D-default	FAP21D	2.4GHz 802.11n/g		
10	FAP220B-default	FAP220B/221B	5GHz 802.11n/a	2.4GHz 802.11n/g	
11	FAP221C-default	FAP221C	2.4GHz 802.11n/g	5GHz 802.11ac/n/a	
12	FAP221E-default	FAP221E	2.4GHz 802.11n/g	5GHz 802.11ac/n/a	
13	FAP222B-default	FAP222B	2.4GHz 802.11n/g	5GHz 802.11n/a	
14	FAP222C-default	FAP222C	2.4GHz 802.11n/g	5GHz 802.11ac/n/a	
15	FAP222E-default	FAP222E	2.4GHz 802.11n/g	5GHz 802.11ac/n/a	
16	FAP223B-default	FAP223B	5GHz 802.11n/a	2.4GHz 802.11n/g	

Update an AP profile

1. Right-click an AP profile in the list and select *Edit*.
2. Make any changes.
3. Select *Save*.

Delete a managed AP

1. Right-click an AP profile in the list and select *Delete*.
2. Select *Yes* to confirm your choice.

SSID

The following figure shows the *SSID* page:

WiFi

HA-V60/FW-61E-kding/root

Search...

Managed AP

WiFi Monitor

Rogue AP

FAP

SSID

WiFi Profile

AP Profile

SSID

Seq	Name	SSID	Traffic Mode	Security Mode	Schedule	Data Encryption	Maximum Clients
1	test3	fortinet-kk	Tunnel	WPA2 Only Personal	None	AES	0
2	wifi	FW61E-Desktop	Tunnel	WPA2 Only Personal	Always	AES	0

Add an SSID

1. Right-click an SSID in the list and select *Create New*.
2. Enter values in the relevant fields. See [SSID fields](#).
3. Select *Save*.



To create an SSID, you must have read-only or read-write permission for DHCP.

Update an SSID

1. Right-click an SSID in the list and select *Edit*.
2. Make any changes.
3. Select *Save*.



To edit an SSID, you must have read-only or read-write permission for DHCP.

Delete an SSID

1. Right-click an SSID in the list and select *Delete*.
2. Select *Yes* to confirm your choice.

SSID fields

Create New SSID

* Interface Name:

The Interface Name field is required.

Alias:

Traffic Mode:

Tunnel

Bridge

Mesh

Address

* IP/Network Mask:

0.0.0.0/0.0.0.0

DHCP Server:

WiFi Settings

* SSID:

fortinet

Security Mode:

WPA2 Only Personal

* Pre-shared Key:

The Pre-shared Key field is required.

Broadcast SSID:

☒

Schedule:

always

Block Intra-SSID Traffic:

☐

Filter Clients by MAC

Address

RADIUS Server:

☐

VLAN Pooling:

Disable

Quarantine Host:

☐

Save

Cancel

The *Create New SSID* and *Edit SSID* dialogs contain the following fields:

Settings	Guidelines
Interface Name	Required. Enter a name for the SSID interface.
Alias	Enter an alternate interface name to remind you what this interface is being used for.
Traffic Mode	Select one of the following: <i>Tunnel</i> —Data for WLAN passes through WiFi Controller. This is the default. <i>Bridge</i> —FortiAP unit Ethernet and WiFi interfaces are bridged. <i>Mesh</i> —Radio receives data for WLAN from mesh backhaul SSID.
IP/Network Mask	If you selected the Tunnel traffic mode, this field is required. Enter the IP address and netmask for the SSID.
DHCP Server	If you selected the Tunnel traffic mode, you can select <i>DHCP Server</i> to assign IP addresses to clients. If you select <i>DHCP Server</i> , right-click in the Addrss Range table and select <i>Create New</i> to define the IP address range for a DHCP server on the FortiPortal unit. You also need to enter the netmask if you select <i>DHCP Server</i> .
SSID	Enter the SSID. By default, this field contains <code>fortinet</code> .

Settings	Guidelines
Security Mode	<p>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.</p> <p><i>Captive Portal</i>—authenticates users through a customizable web page.</p> <p><i>WPA2 Only Personal</i>—WPA2 is WiFi Protected Access version 2. There is one pre-shared key (password) that all users use.</p> <p><i>WPA2 Only Enterprise</i>—similar to WPA2 Only Personal but is best used for enterprise networks. Each user is separately authenticated by user name and password.</p>
Pre-shared Key	Required. Enter the encryption key that the clients must use.
Broadcast SSID	Optionally, disable broadcast of SSID. By default, the SSID is broadcast.
Schedule	Select when the SSID is enabled. You can select <i>always</i> or <i>none</i> .
Block Intra-SSID Traffic	Select to enable the unit to block intra-SSID traffic.
RADIUS Server	Select to use a RADIUS server. If you select this option, select the server name from the drop-down list.
VLAN Pooling	<p>In an SSID, you can define a VLAN pool. As clients associate to an AP, they are assigned to a VLAN.</p> <p>If you selected the Tunnel or Bridge traffic mode, select one of the following options:</p> <p><i>Disable</i>—This option is selected by default and no VLAN pools are used.</p> <p><i>Managed AP Group</i>—A VLAN pool can assign one of several available VLANs for network load balancing purposes. If you select Managed AP Group, select VLANs from the Available list and then select > or >> to move them to the Selected list.</p> <p><i>Round Robin</i>—The VLAN pool chooses the VLAN with the smallest number of clients. If the VLAN pool contains no valid VLAN ID, the SSID's static VLAN ID setting is used.</p> <p><i>Hash</i>—The VLAN pool chooses a VLAN based on a hash of the current number of SSID clients and the number of entries in the VLAN pool. If the VLAN pool contains no valid VLAN ID, the SSID's static VLAN ID setting is used.</p>
Quarantine Host	Enable this option to quarantine devices that are connected in Tunnel traffic mode.



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.