FORTINET
High Performance Network Security

FortiPortal User Guide

VERSION 5.3.2

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

January 8, 2020

FortiPortal User Guide

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
January 8, 2020	Initial release for FortiPortal 5.3.2

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.

NOTE: 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:

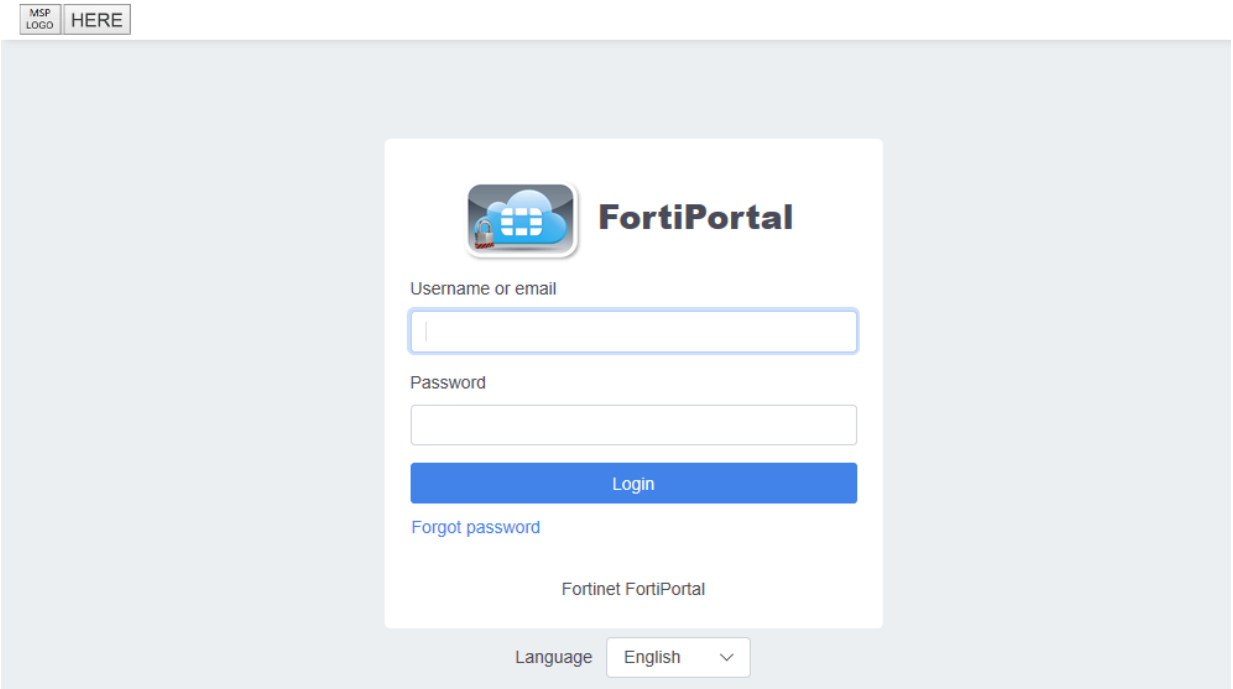
- *Help*—additional window that displays the Help pages
- *Alerts*—pop-up window that displays the unread alerts
- *Change Password*—raises a dialog box for password change
- *Logout*—log out of the tool

The left panel might contain the following selections:

- *Dashboard*—widgets that display information about the FortiPortal (FP)
- *Policy & Objects*—pages for viewing and modifying security policy, 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

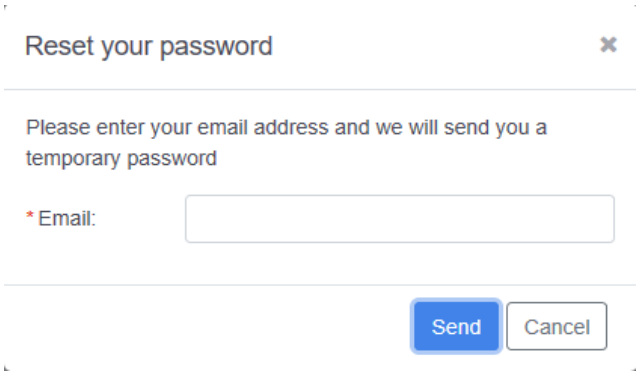
When you open FortiPortal to log in ito the system, you see a custom landing page. The following figure shows the default landing page:



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

Reset password

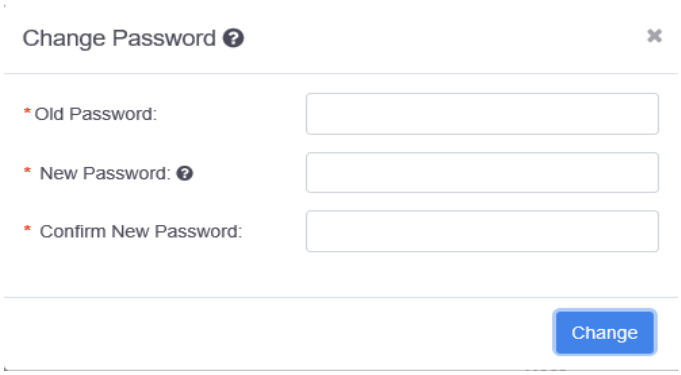
On the Login page, select the *Forgot password* link to display a dialog window:



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:

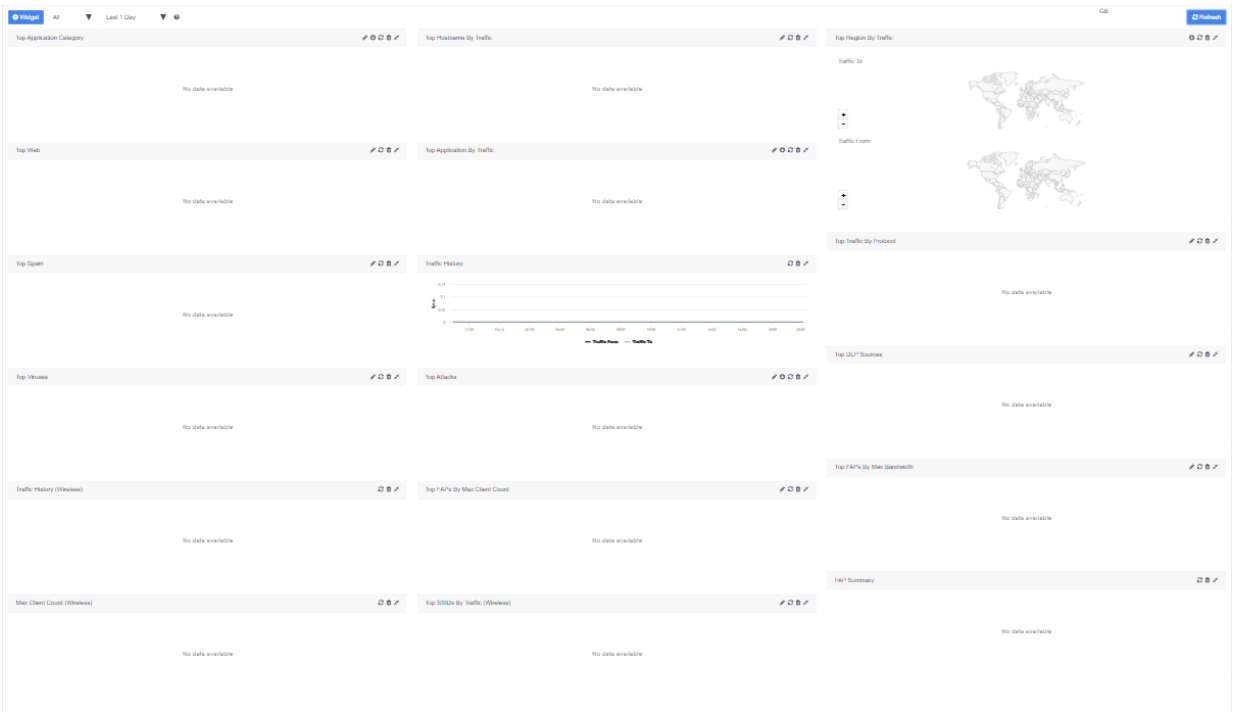


Enter your existing password and a new password that will take effect on your next login attempt.

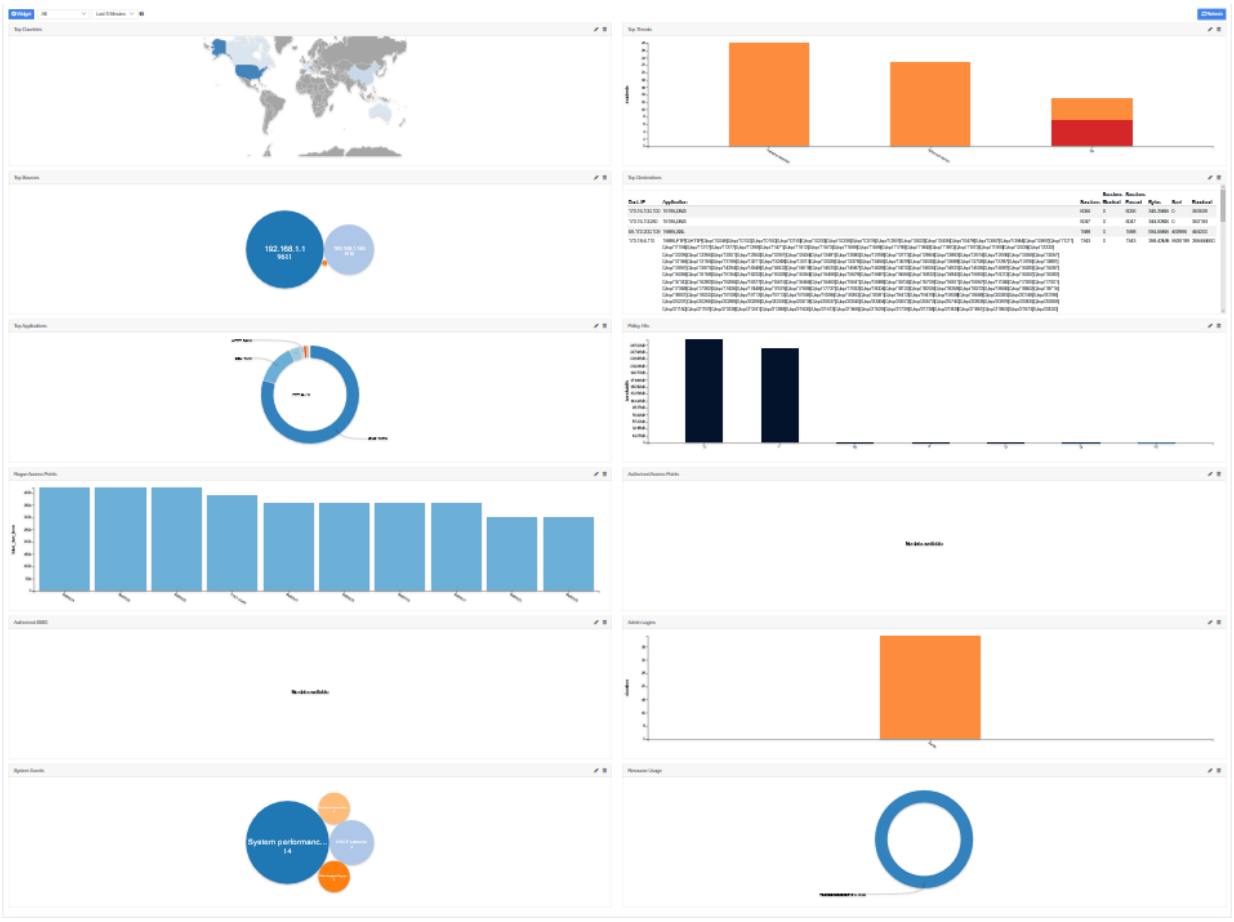
Dashboard

The dashboard displays different views of the security event logs and other information. The content depends on whether FortiPortal is using collectors to collect logs from FortiAnalyzer (Collector mode) or collects logs directly from FortiAnalyzer (FortiAnalyzer).

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



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 Collector mode, the general widgets are as follows:

- Top Application Category
- Top Hostname by Traffic
- Top Region by Traffic
- Top Web
- Top Application by Traffic
- Top Spam
- Traffic History
- Top Traffic By Protocol
- Top Viruses
- Top Attacks
- Top DLP Sources

In Collector mode, the following widgets are associated with the wireless controllers and endpoints:

- Traffic History (Wireless)
- Top 5 FAPs by Max Client Count
- Top 5 FAPs by Max Bandwidth

- Max Client Count (Wireless)
- Top SSIDs by Traffic (Wireless)
- FAP Summary

In Collector mode, the following widgets are associated with the sandbox:

- Sandbox Scanning Statistics
- Top Sandbox Hosts
- Top Sandbox Malware
- Sandbox Scanning Statistics Graphs

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:

- *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 Collector mode, the top banner on each widget provides some or all of the following controls:

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

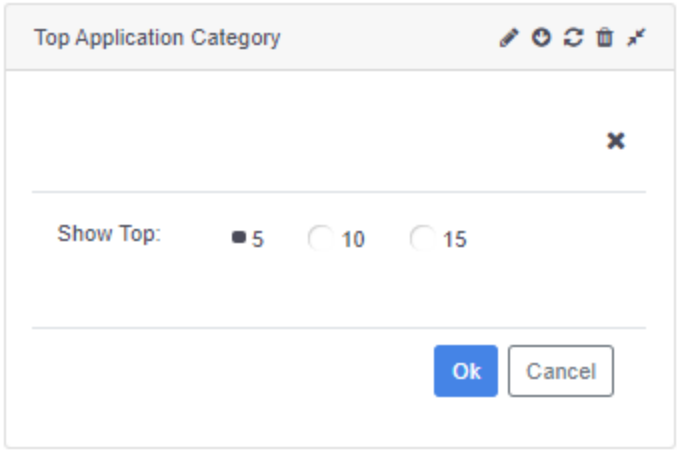
- *Collapse/Expand*—display or hide the widget's content
- *Drag and Drop*—using the menu bar

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

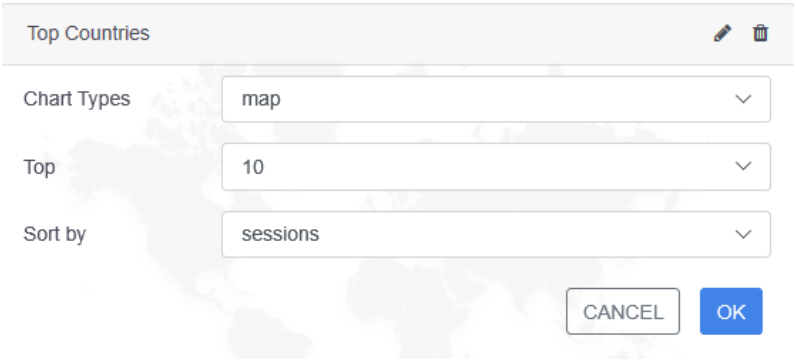
- *Drill-down*—visible in the widgets that support drill-down capability
- *Edit Settings*—edit the widget
- *Refresh*—refresh the data
- *Delete*—delete the widget

Edit settings

In Collector mode, selecting the Edit Settings icon opens a window within the widget that allows you to select the top N entries:



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 Collector mode, the following widgets support the drill-down capability:

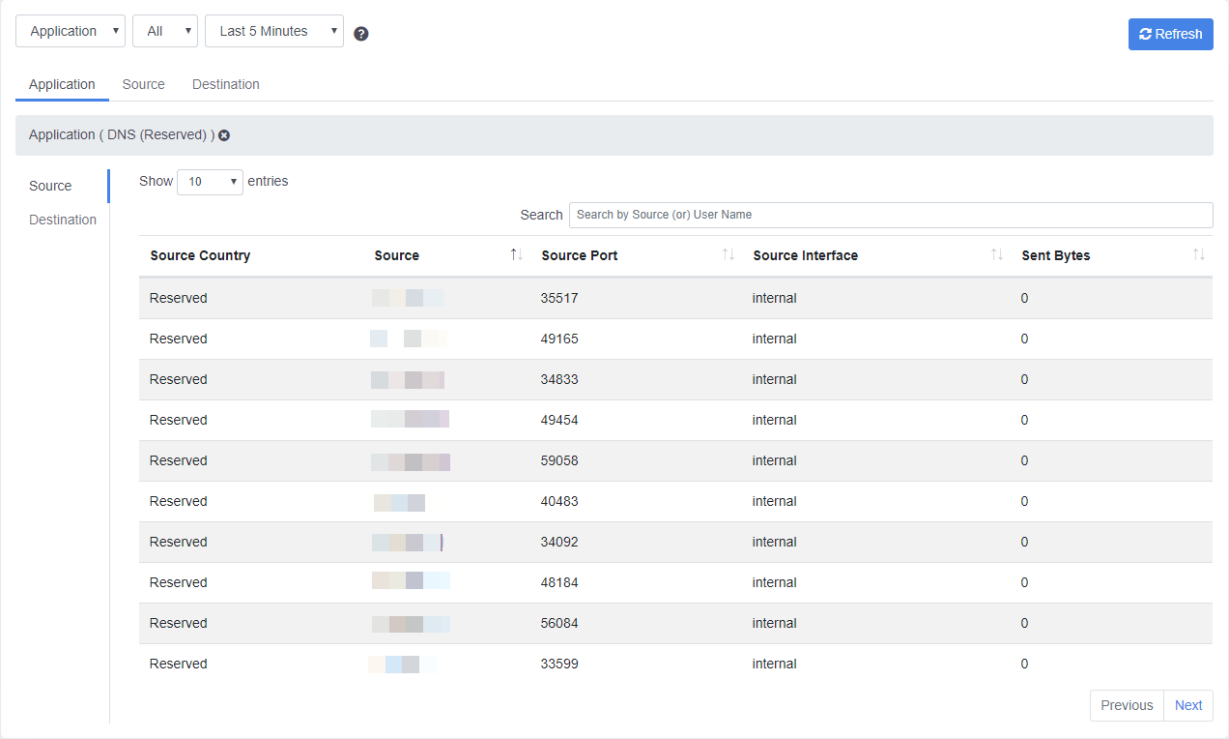
- Top Application Category
- Top Region by Traffic

- Top Application By Traffic
- Top Attacks

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

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

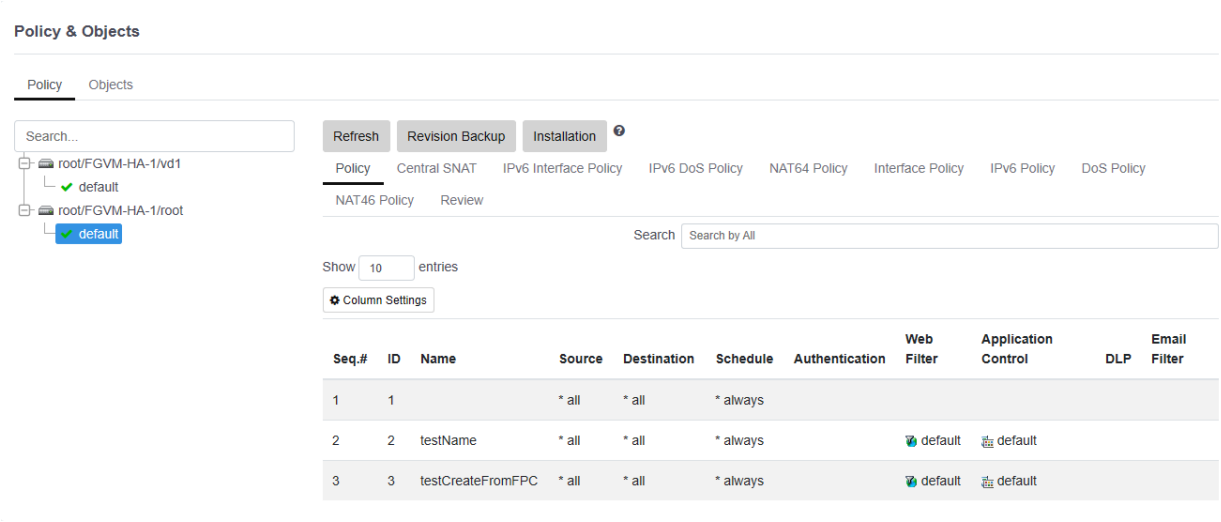
Each of these widgets displays a graph or bar chart with the top N results, where the result is an application, region, traffic, or attack (depending on the widget). When you select one of the results, the View page opens with a view filtered by that result. The view filter is listed above the table.



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

Policy

Go to *Policy & Objects* > *Policy* 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 main panel and a left side panel that provides a hierarchical view of the policies. When you select an entry in the left panel, 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

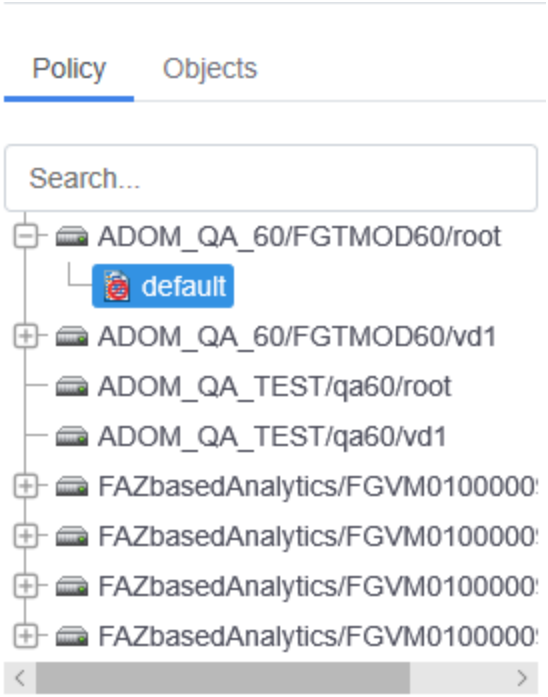
The system can save only one revision of the current policy and object data. The new revision overwrites the existing backup (if one exists).

Observe the following restrictions:

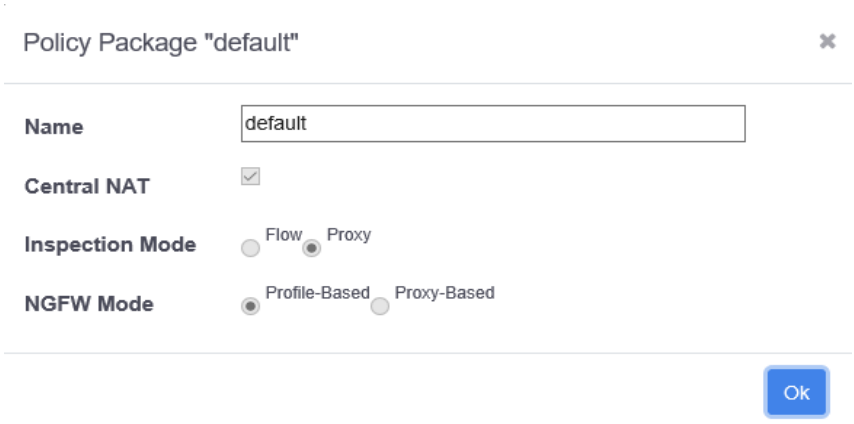
- Customer must be part of only one ADOM.
- No other customer can be part of that ADOM.

Viewing policy package settings

Policy packages are listed on the left side of the *Policy* tab.



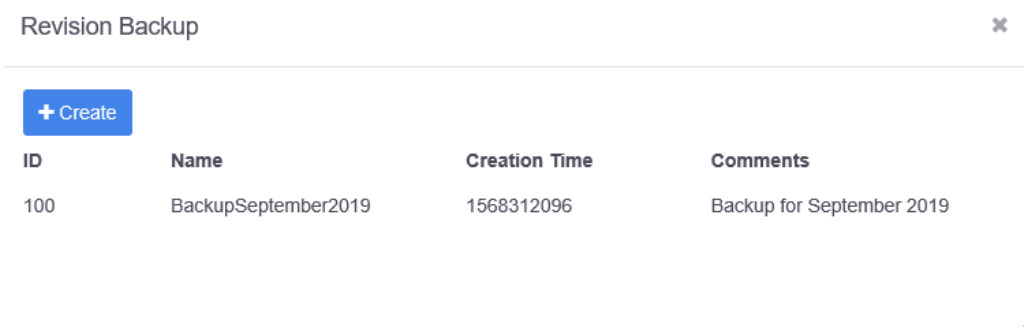
To check settings that affect all policies in a package, right-click on the name of the policy package and select *View Package Settings*.



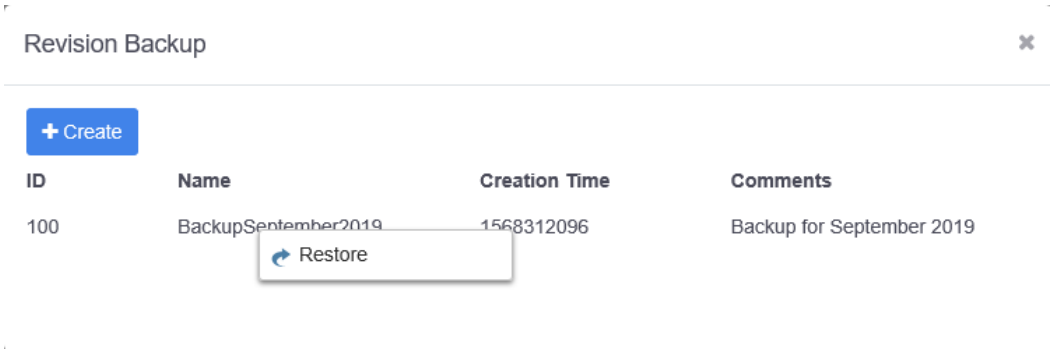
NOTE: The Policy Package dialog box includes the inspection mode for FortiManager 5.6 and later. All policies in a policy package must have the same inspection mode. For FortiManager 5.4 and later, the default setting for the inspection mode is *Proxy*.

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*.



Configuring policies

Go to *Policy & Objects* > *Policy* > *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, we display a warning message and restrict 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.

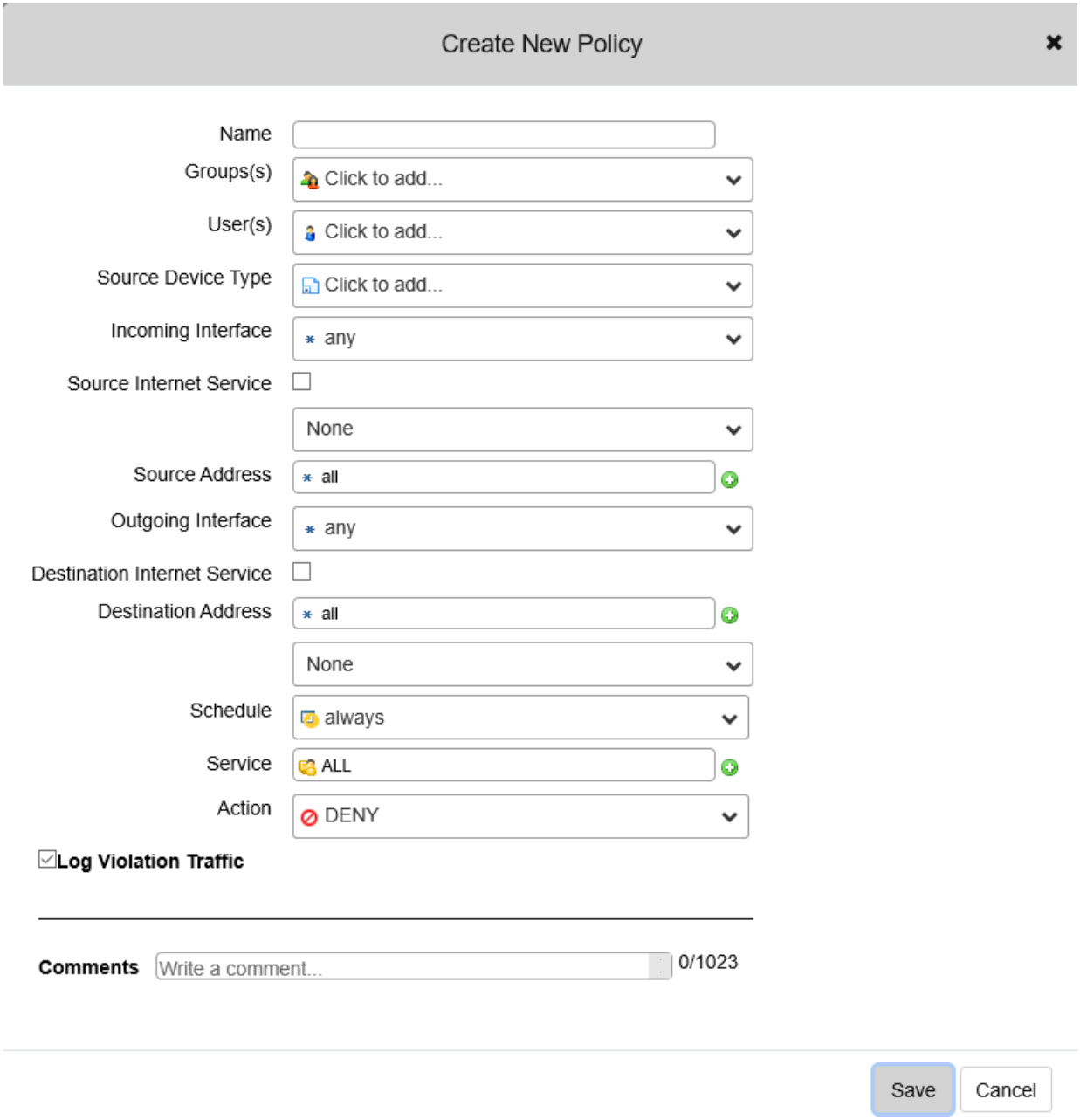
Policy fields

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 Device Type	Select which traffic-sending devices 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 *Fixed Port*.

Settings	Guidelines
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 *Generate Logs when Session Starts* and *Capture Packets*.
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.
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 form:



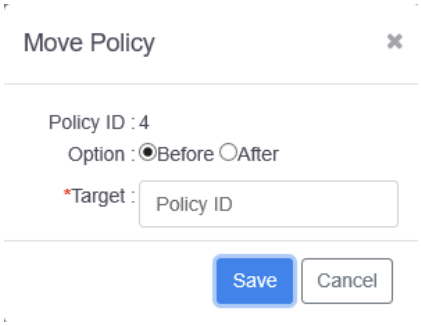
Moving a policy

NOTE: 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 (**NOTE: 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.

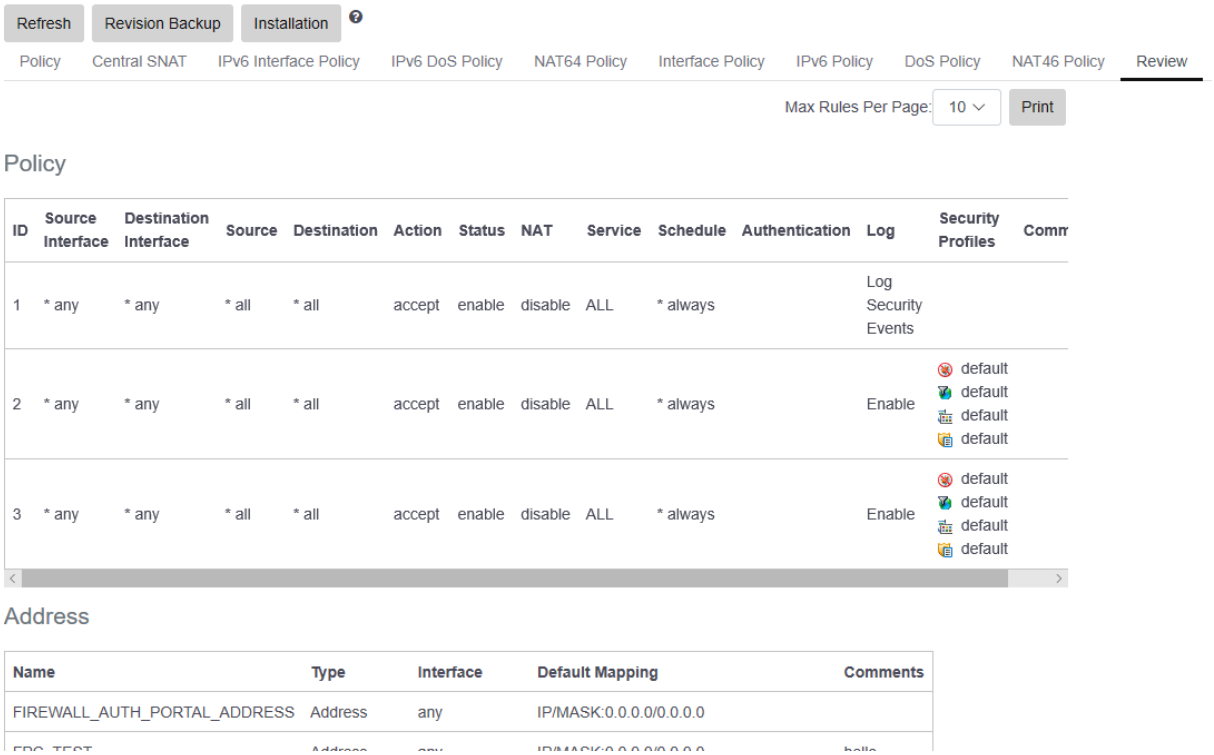
For additional information about policy types, refer to the chapter on Policy and Objects in the FortiManager Administrative Guide.

Installing policies

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

Reviewing policies

Go to *Policy & Objects* > *Policy* > *Review* to see all policies and firewall objects that have been configured.

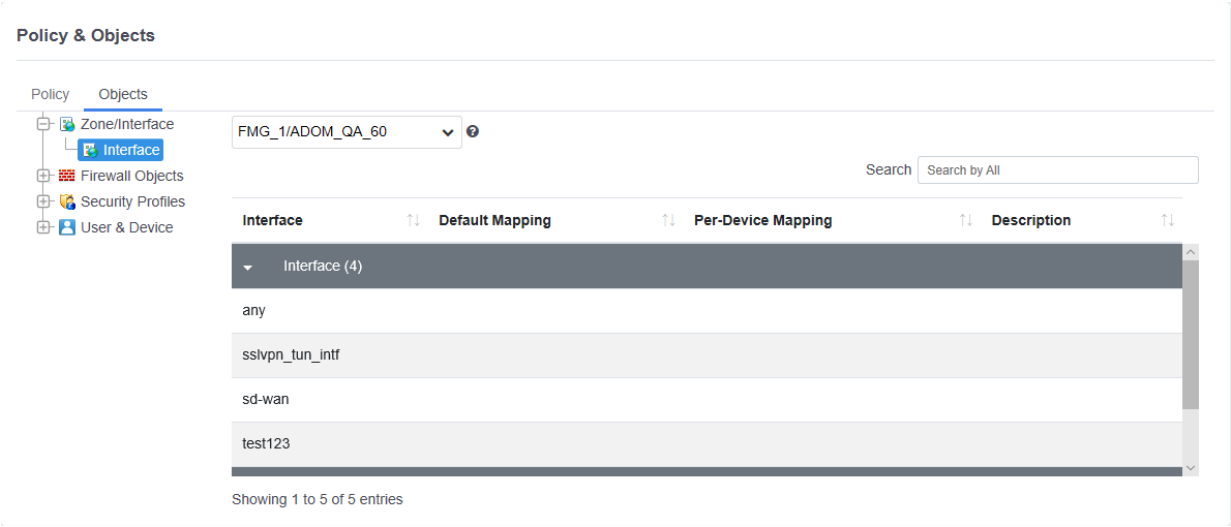


You can select the maximum number of rules to display.

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

Objects

The *Policy & Objects* > *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 main panel and a left side panel that provides a hierarchical view of the objects. When you select an object in the left 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 pull-down selector above the main panel.

Types of objects

The page displays the following object categories:

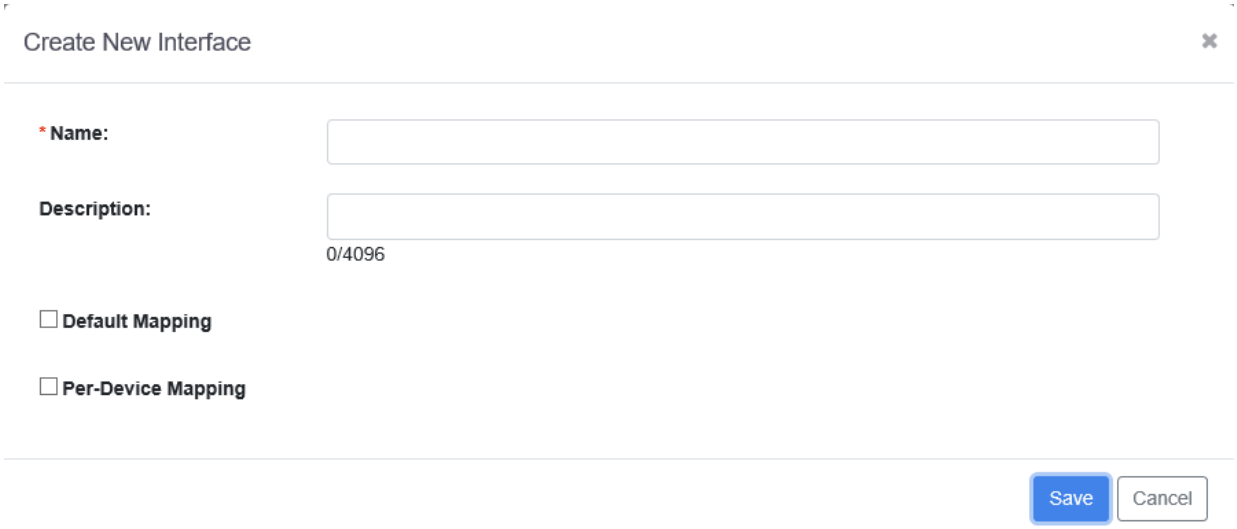
- Zone/Interface
- Firewall Objects
- Security Profiles
- User & Device

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 form.



The following figure shows the Create New Zone form.

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):

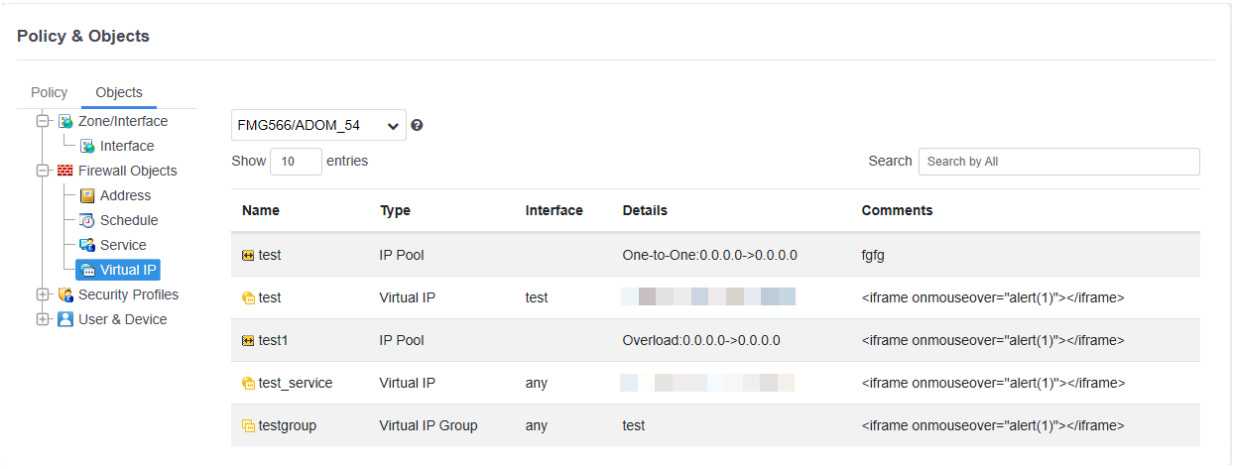
- *IP*—IP protocol number
- *TCP/UDP/SCP*—source and destination port range

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 FPC Virtual IP object display:



FPC 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

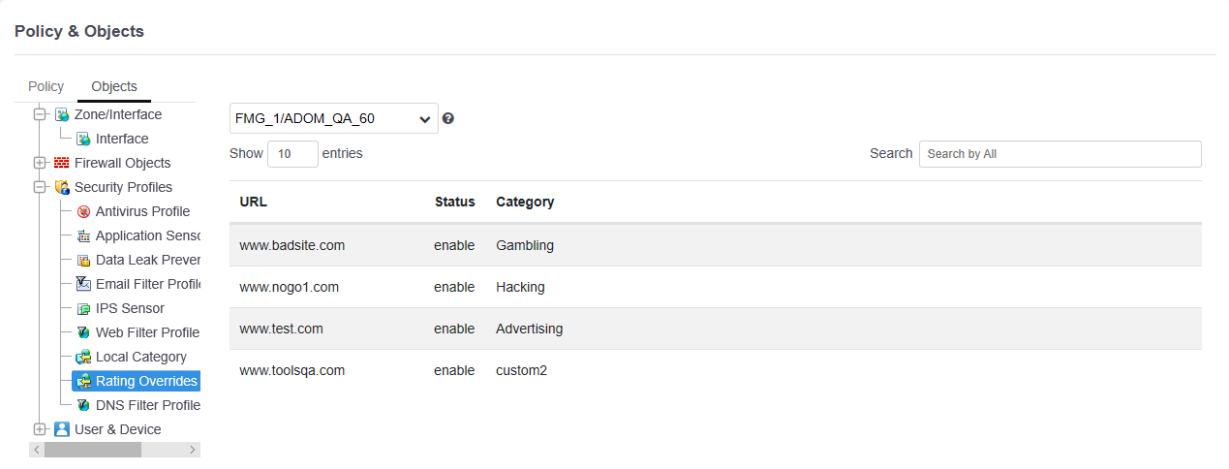
Local Category (security profile introduced with FortiPortal 1.2.0)

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)

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

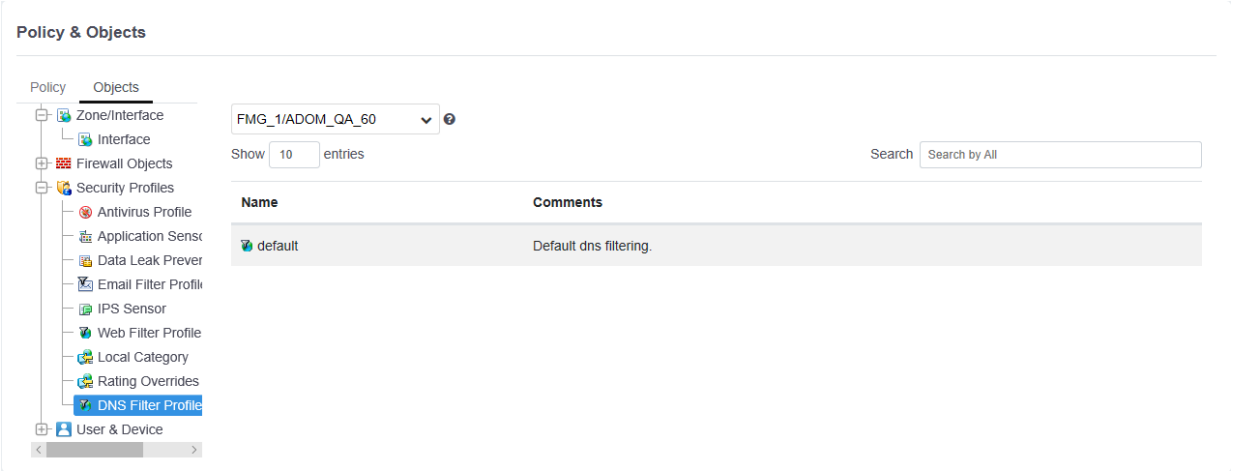
You can configure DNS web filtering to allow, block, or monitor access to web content according to FortiGuard categories. When DNS web filtering is enabled, your FortiPortal must use the FortiGuard DNS service for DNS lookups. DNS lookup requests sent to the FortiGuard DNS service return with an IP address 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 form.

You can also create a domain filter in the Create New DNS Filter Profile or Edit DNS Filter Profile form. 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:



User & Device

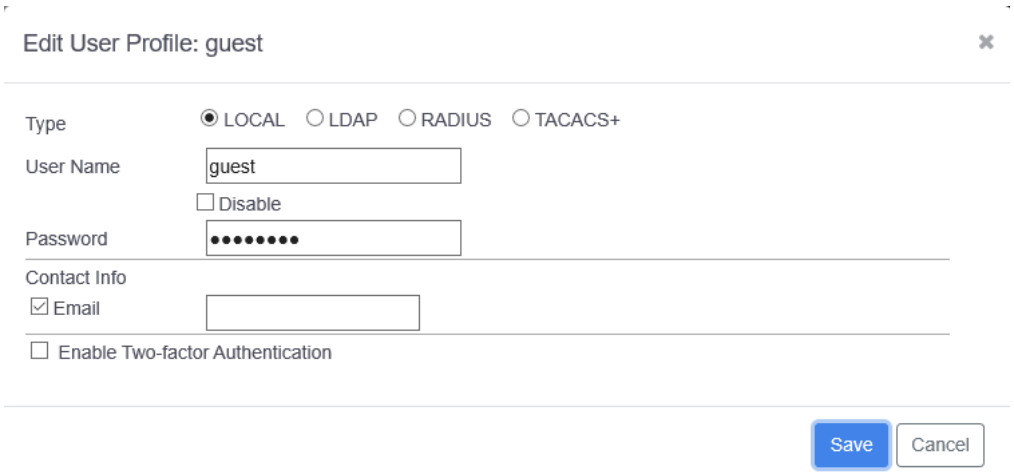
Security policies may allow access to specified users and user groups only (the object types in the User & Device category).

For additional information about users and user groups, refer to FortiOS Handbook: Authentication.

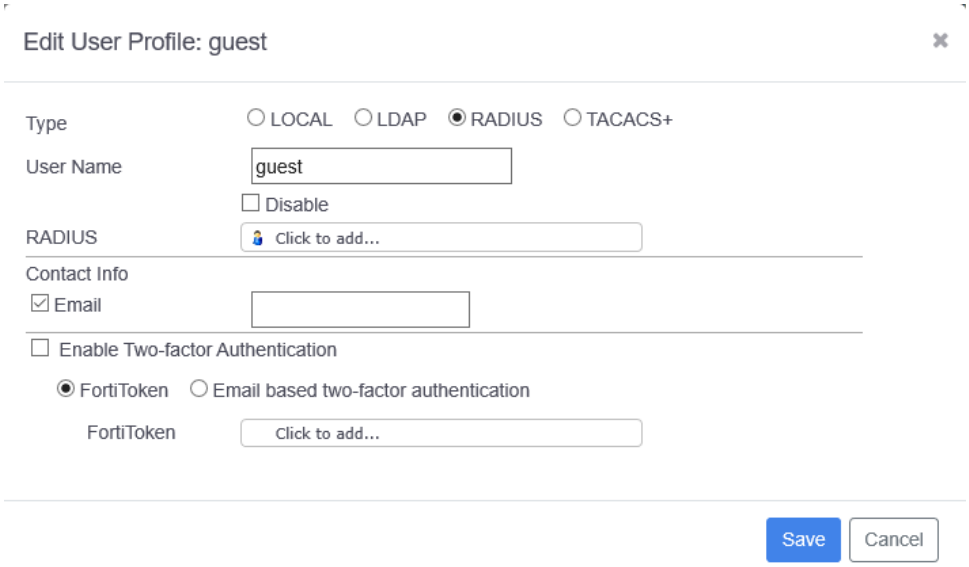
User Definition

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 form for a local user:



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



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 *Policy & Objects* > *Objects*.
2. In the User & Device tree, 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.

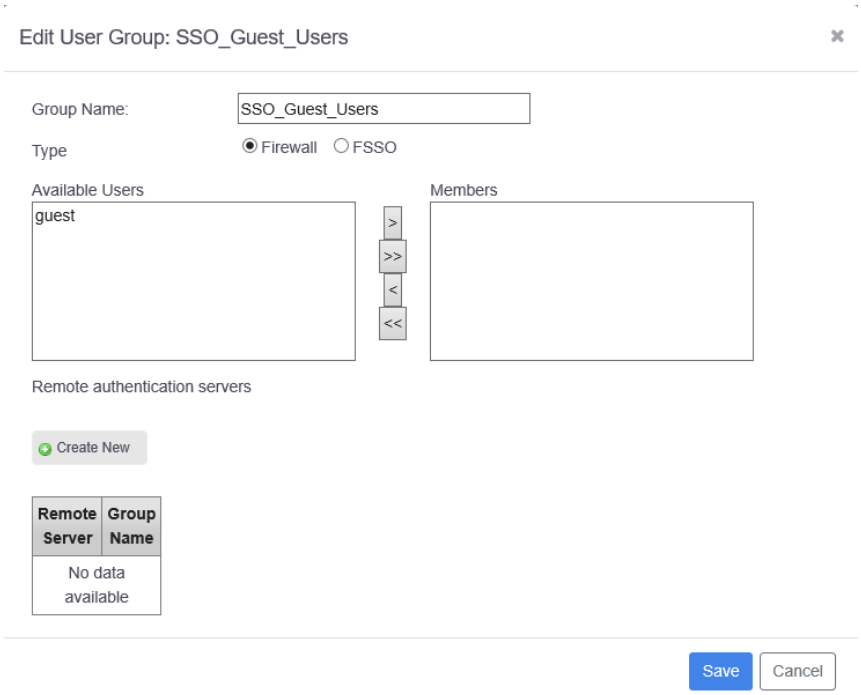
   The code will be generated and emailed at the time of logon, so you must have email access at that time to be able to receive the code.

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.



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.

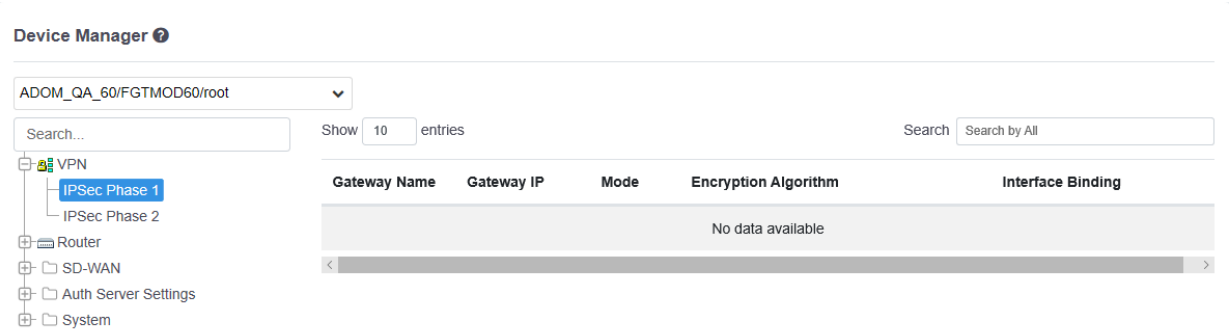
Device Manager

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 tree on the Device Manager tab displays a list of configurations for Internet Protocol Security (IPsec) Phase 1 and Phase 2.



Configuring VPNs

Use the VPN area 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 tree.
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 33 and "IPSec phase-2

fields" on page 35.

4. Select *Save*.

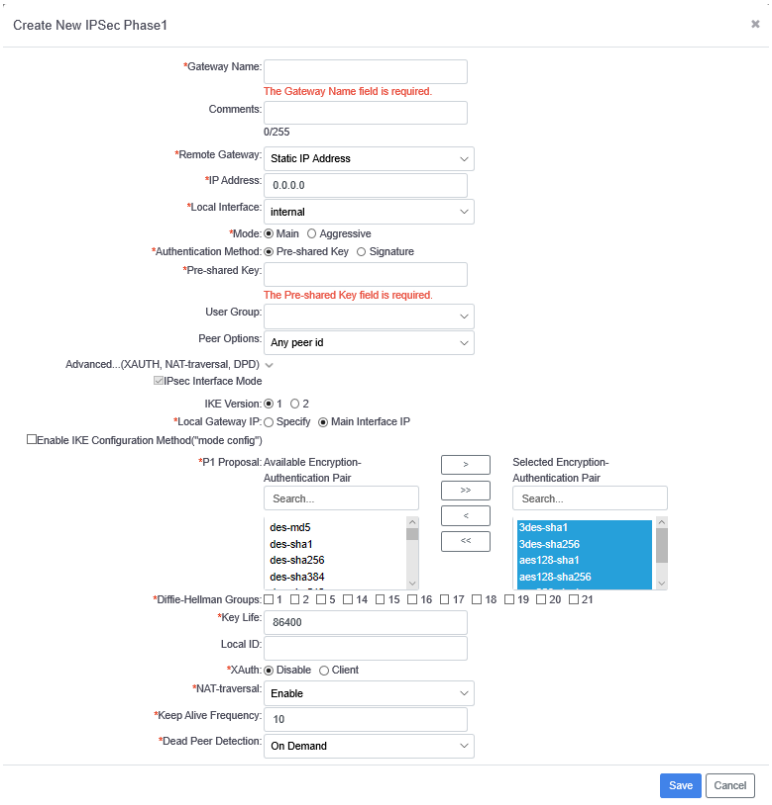
Updating an IPSec phase-1 or phase-2 configuration

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

IPSec phase-1 fields



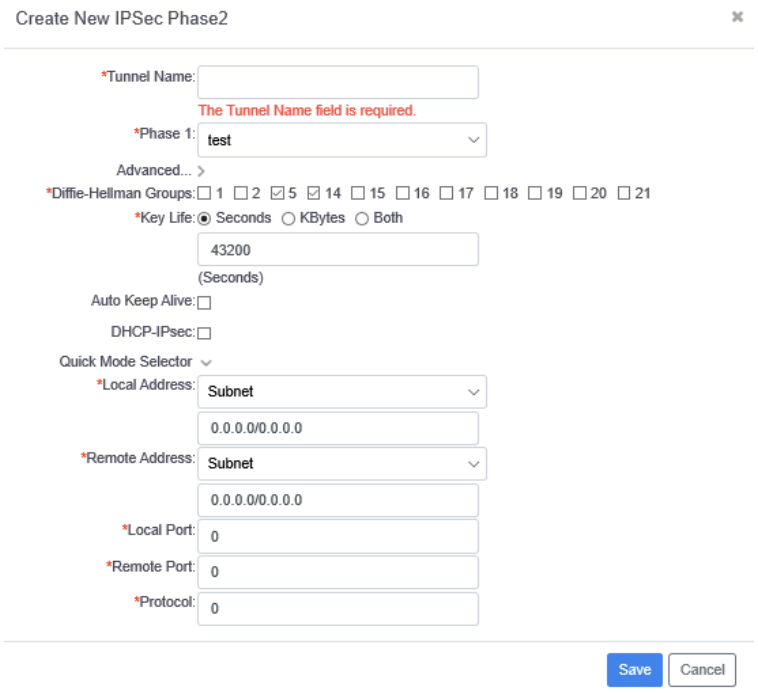
The Create New IPSec Phase1 and Edit IPSec Phase1 forms contain the following fields:

Settings	Guidelines
Gateway Name	Required. Type a name for this Phase-1 configuration. The value is a string with a maximum of 15 characters.

Settings	Guidelines
Comments	Type an optional description. The value is a string with a maximum of 255 characters.
Remote Gateway	Required. Select *Static IP Address*, *Dialup user*, or *Dynamic DNS*.
IP Address	Required if you select *Static IP Address*. Type the IPv4 address.
Dynamic DNS	Required if you select *Dynamic DNS*. Type the fully qualified domain name.
Local Interface	Required. Select an interface from the drop-down list or select *any*.
Mode	Required. Select *Main* or *Aggressive* for the phase-1 mode.
Authentication Method	Required. Select *Pre-shared Key* or *Signature* for the authentication method.
Pre-shared Key	If *Pre-shared Key* 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 *Pre-shared Key* 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 *Signature* is selected, this field is available but optional. Select a certificate from the drop-down list.
Peer Options	If *Signature* is selected, this field is available but optional. Select *Any peer id* or *One peer id*.
peer id	If *One peer id* 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 *Specify* or *Main Interface IP*. If you select *Specify*, 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.

Settings	Guidelines
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.
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 *Disable* or *Client* for the XAUTH type. The default is *Disable*.
NAT-traversal	Select *Disable*, *Enable*, or *Forced*. The default is *Enable*.
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 *Disable*, *On Idle*, or *On Demand*.

IPSec phase-2 fields



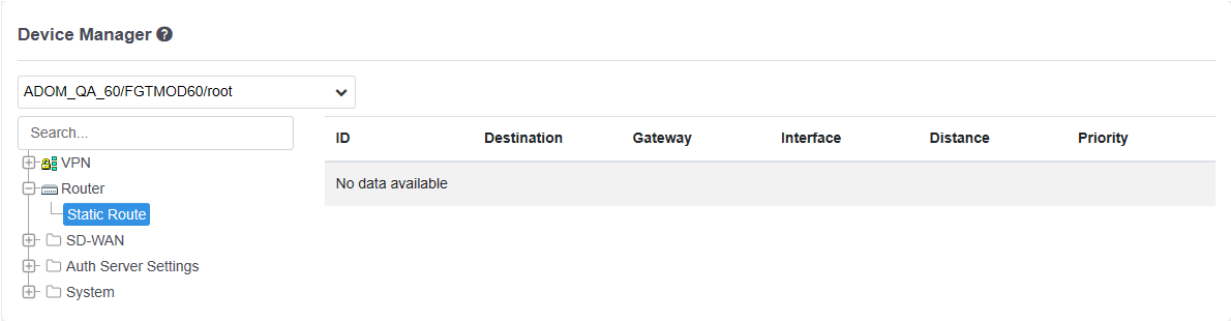
The Create New IPSec Phase2 and Edit IPSec Phase2 forms contain the following fields:

Settings	Guidelines
Tunnel Name	Required. Type a name for this Phase-2 configuration. The value is a string with a maximum of 35 characters.
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 *Seconds*, *KBytes*, or *Both*. • If *Seconds* is selected, type the number of seconds. The default is 43200. The value range is 120-172800. • If *KBytes* is selected, type the number of KB. The default is 5120. The value range is 5120-4294967295. • If *Both* 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	

Settings	Guidelines
Local Address	Select *Subnet*, *IP Range*, *IP Address*, or *Named Address*. • If *Subnet* is selected, enter an IP address and netmask. • If *IP Range* is selected, enter the first IP address and the last IP address in the range. • If *IP Address* is selected, enter an IPv4 address. • If *Named Address* is selected, select from the drop-down list.
Remote Address	Select *Subnet*, *IP Range*, *IP Address*, or *Named Address*. • If *Subnet* is selected, enter an IP address and netmask. • If *IP Range* is selected, enter the first IP address and the last IP address in the range. • If *IP Address* is selected, enter an IPv4 address. • If *Named Address* 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 tree on the Device Manager tab displays a list of static routes.



Configuring static routes

Use the Router area to define static routes.

In this area, the following actions are available:

- *Search*—enter text to search for in the table
- *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 tree.
2. Right-click a static route and select *Create New Route*. If the table is blank, right-click under the column headings and select *Create New Route*.
3. Enter values in the relevant fields. See "Router" on page 37.
4. Select *Save*.

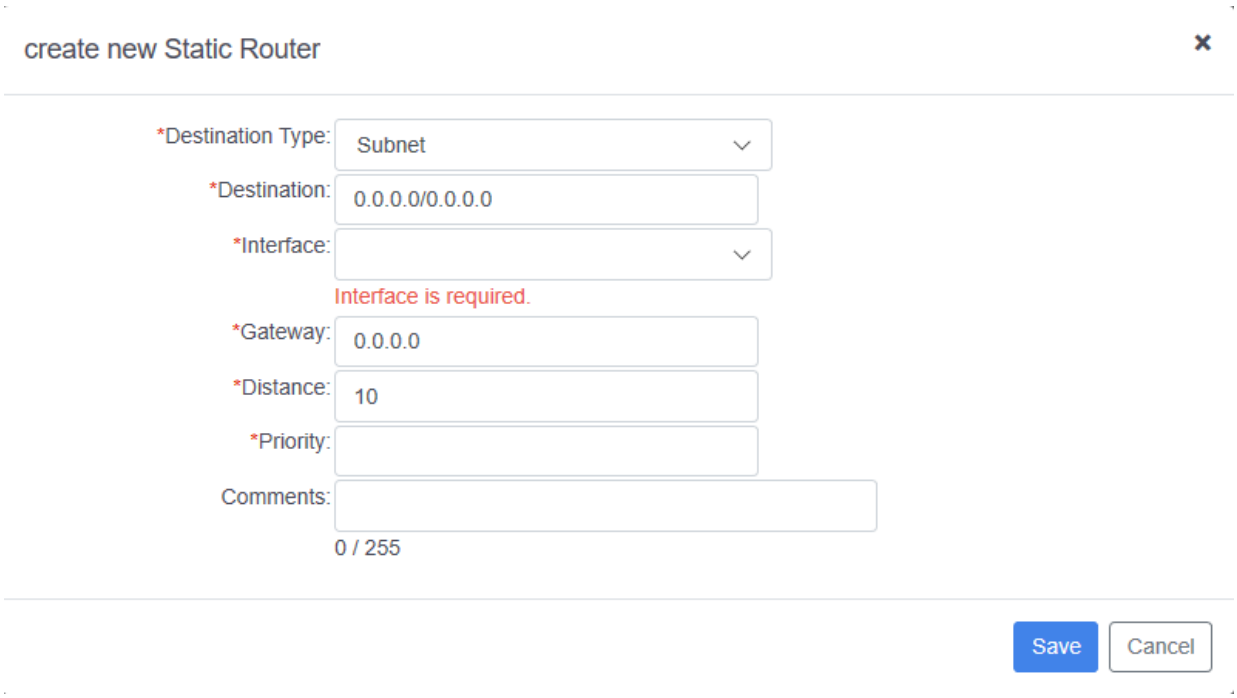
Updating a static route

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

Static route fields



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

Settings	Guidelines
Destination Type	Required. Select *Subnet*, *Named Address*, or *Internet Service* for the destination type. • If *Subnet* is selected, enter destination IP address and netmask. • If *Named Address* is selected, select from the drop-down list. • If *Internet Service* is selected, select the Internet service from the drop-down list.
Destination	Required. If you selected *Subnet* as the destination type, enter the destination IP address and netmask.
Internet Service	Required. If you selected *Internet Service* 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.
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

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

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.

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.

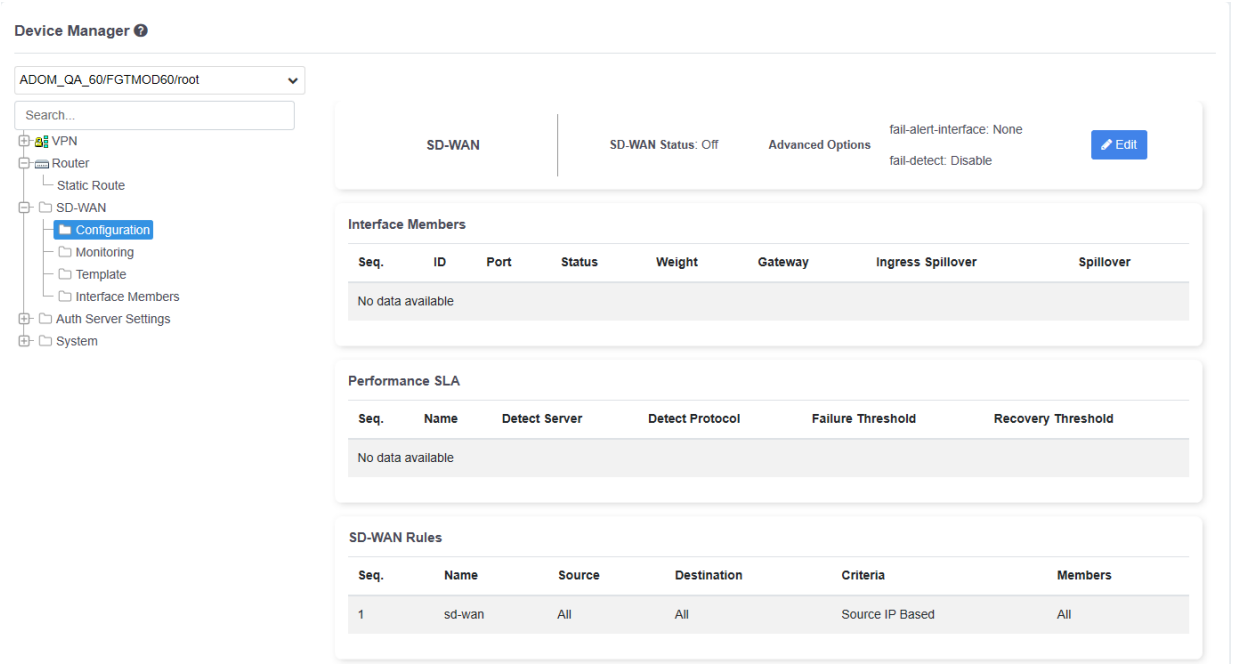
Use the SD-WAN tree on the Device Manager tab to perform the following tasks:

- 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

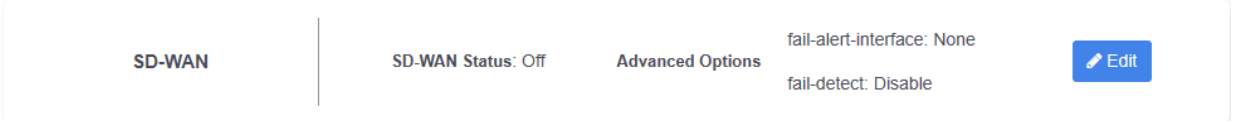
To configure an SD-WAN for a group of interfaces:

1. Select *Configuration* from the SD-WAN tree.
2. Enable the SD-WAN status. See Enable the SD-WAN status.
3. Define which physical FortiPortal interfaces belong to the SD-WAN. See Define which physical FortiPortal interfaces belong to the SD-WAN.
4. Define a new performance service level agreement (SLA). See Define a new performance SLA.
5. 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 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.

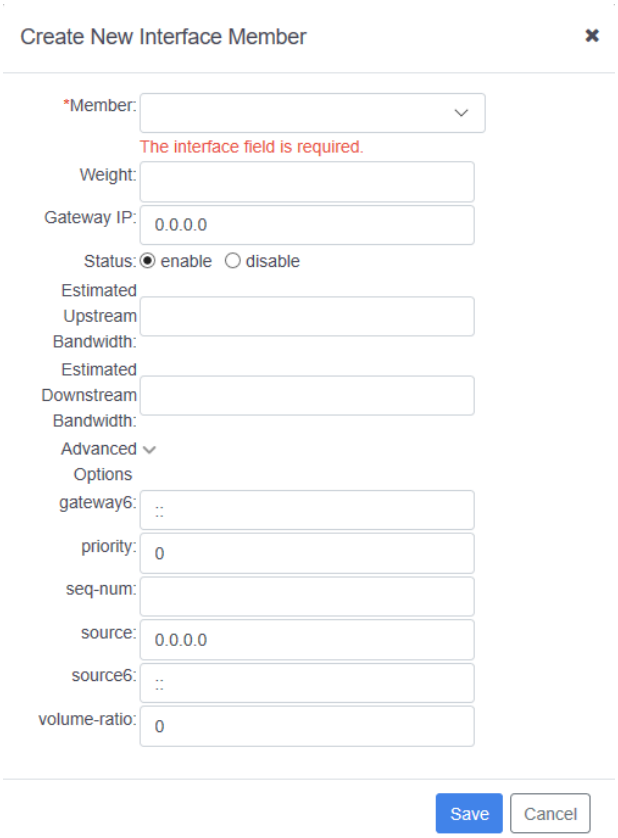
In the Interface Members area, the following actions are available:

- *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 tree.
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 41.
4. Select *Save*.

Interface member fields



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

Settings	Guidelines
Member	Required. Select one of the available physical interfaces.
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.
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.
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.

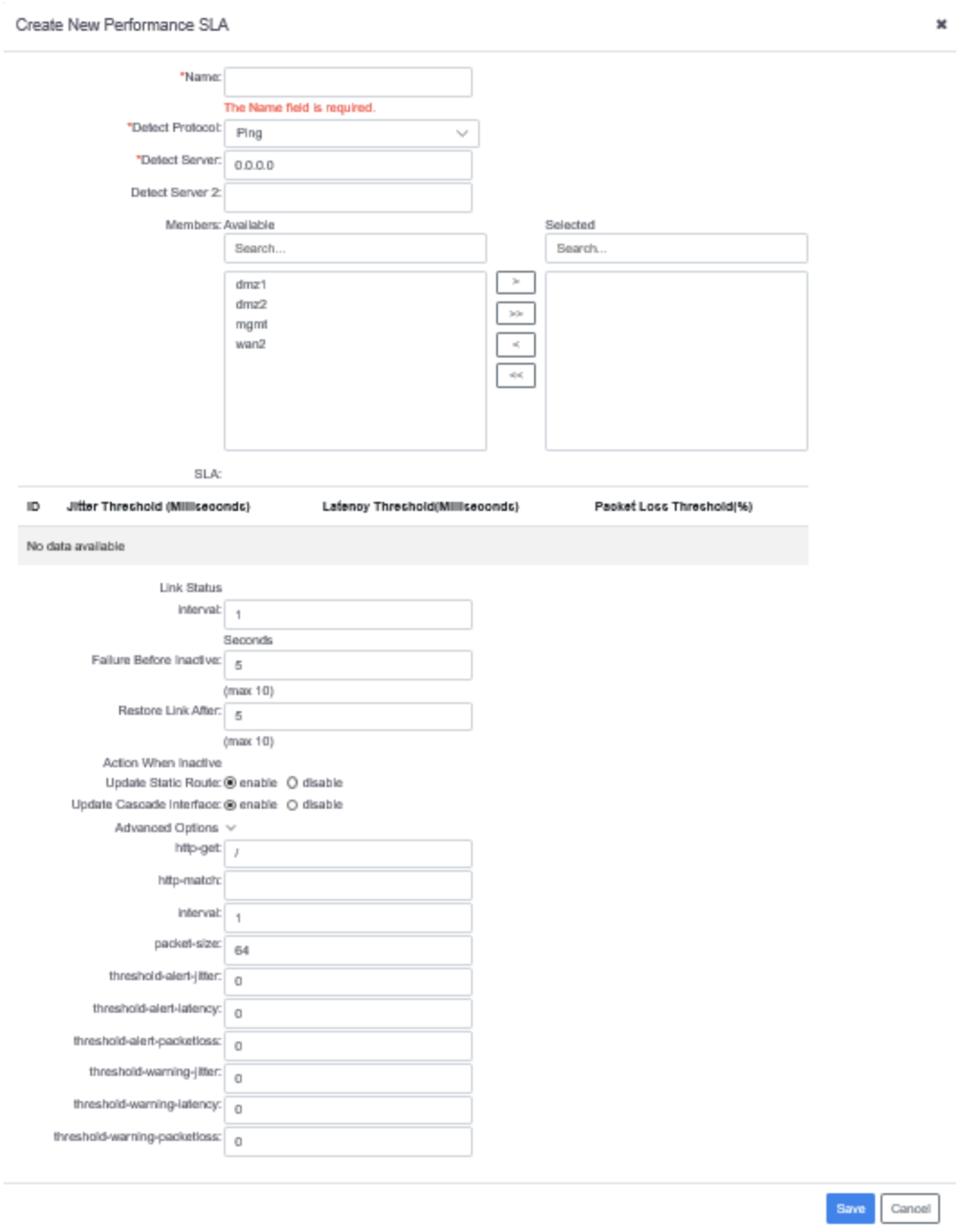
In Performance SLA area, the following actions are available:

- *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 tree.
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 43.
4. Select *Save*.

Performance SLA fields



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

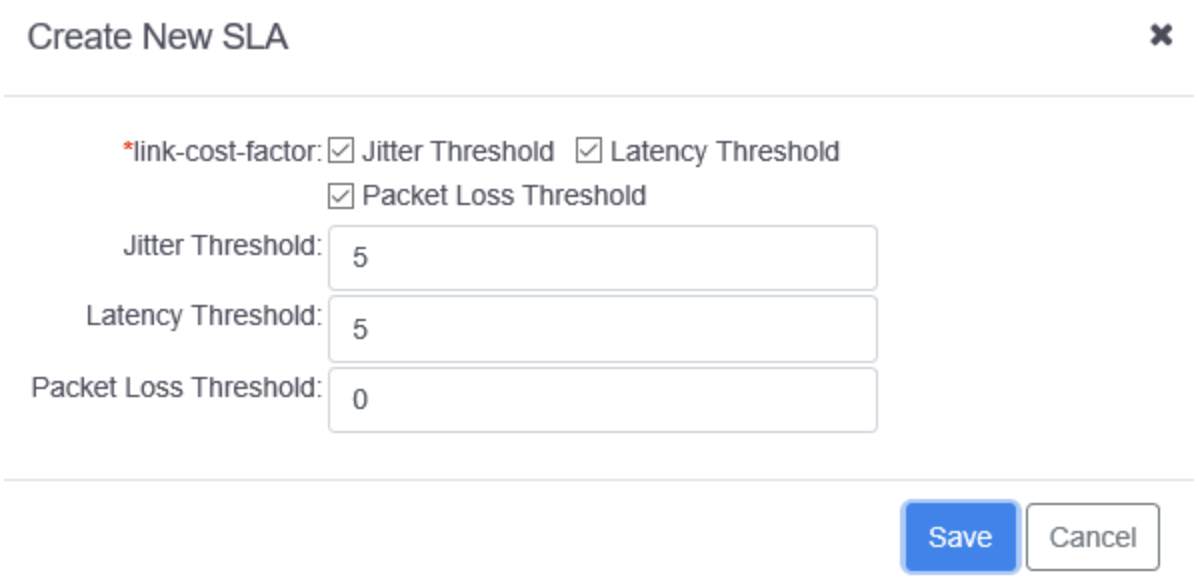
Settings	Guidelines
Name	Required. Name of the performance SLA.
Detect Protocol	Required. Protocol used to determine if the FortiPortal unit can communicate with the server. Select *Ping*, *TCP ECHO*, *UDP ECHO*, *HTTP,* or *TWAMP*.
Detect Server	Required. IPv4 address of the server.
Detect Server 2	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 45.
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.
Update Cascade Interface	Enable or disable update cascade interface.
Advanced Options	
http-get	URL used to communicate with the server if the protocol 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.

Settings	Guidelines
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 tree.
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 45.
5. Select *Save* to save your SLA configuration.
6. Select *Save* to save your performance SLA configuration.

SLA fields



The Create New SLA and Edit SLA forms 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: *Jitter Threshold*, *Latency Threshold*, and *Packet Loss Threshold*. 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.

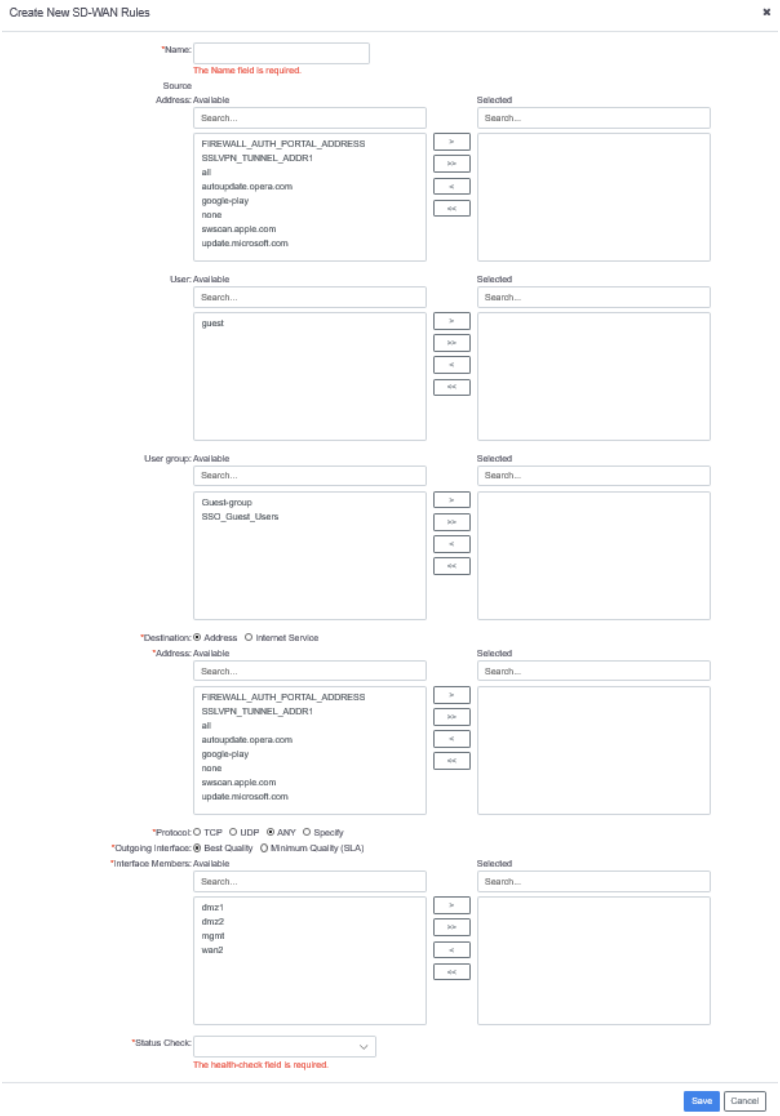
In the SD-WAN Rules area, the following actions are available:

- *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 tree.
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 43.
4. Select *Save*.

SD-WAN rule fields



The Create New SD-WAN Rules and Edit SD-WAN Rules forms 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.

Settings	Guidelines
User group	Select the user groups from the Available list and then select > to move them to the Selected list.
Destination	Required. Select *Address* to use destination addresses or select *Internet Service* to use destination Internet services.
Address	Required. Available if Destination is set to *Address*. 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 *Address*. Select *TCP*, *UDP*, *ANY*, or *Specify*. If you select *Specify*, enter the protocol number, type of service, and bit mask.
Internet Service	Available if Destination is set to *Internet Service*. 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 *Internet Service*. 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 *Internet Service*. 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 *Internet Service*. 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 *Internet Service*. 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 *Internet Service*. Select the application groups from the Available list and then select > to move them to the Selected list.
Outgoing Interface	Required. Select *Best Quality* or *Minimum Quality (SLA)*.
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 *Best Quality*. Select the appropriate performance SLA to use for the status check.
Required SLA Target	Required. Available if Outgoing Interface is set to *Minimum Quality (SLA)*. 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.

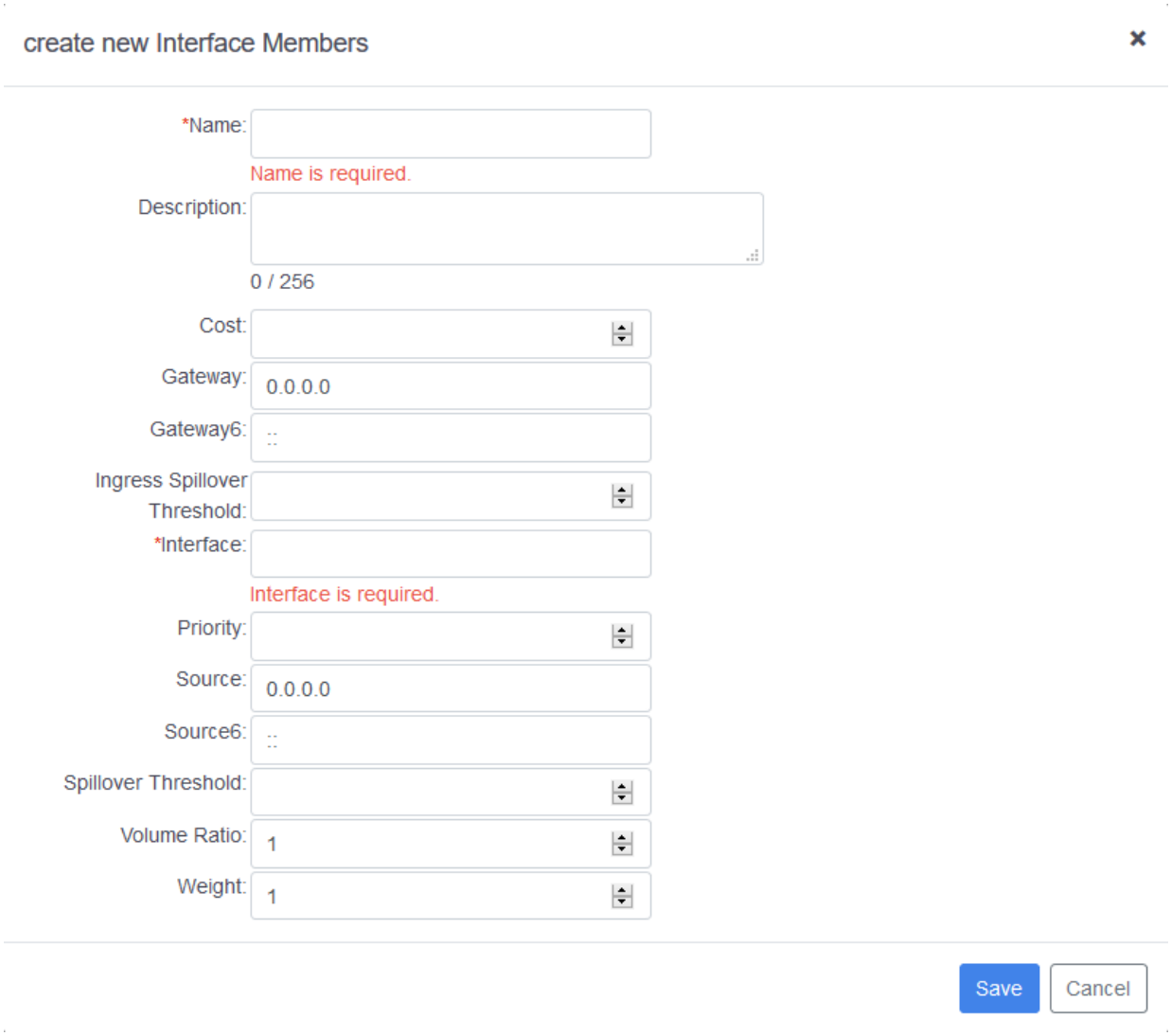
On the SD-WAN > Interface Members page, the following actions are available:

- *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 tree.
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 41.
4. Select *Save*.

Interface member fields



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

Settings	Guidelines
Name	Required. Name of the new interface member.
Description	Description of the new interface member.
Cost	Cost of the interface. **NOTE:** The Cost field is not displayed when the ADOM version is 6.2 or higher.
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.

Settings	Guidelines
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.

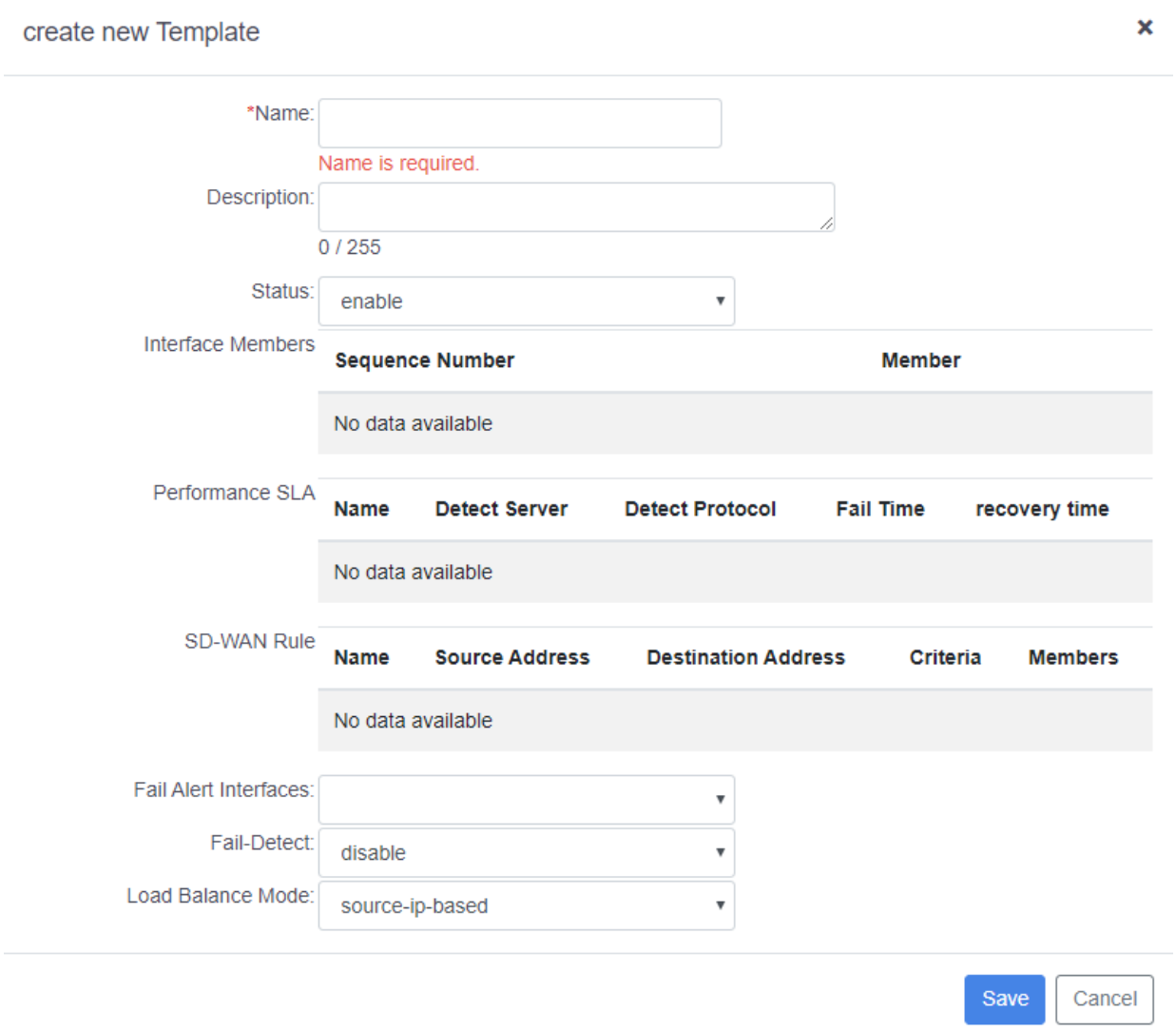
In this area, the following actions are available:

- *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 tree.
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



The Create New Template and Edit Template forms contain the following fields:

Settings	Guidelines
Name	Required. Name of the new template
Description	Description of the new template.
Status	Select *enable* 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 53.

Settings	Guidelines
Performance SLA	Define a new performance service level agreement (SLA). See "Define a performance SLA for the SD-WAN template" on page 54.
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 58.
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 *enable* or *disable* to change whether the SD-WAN Internet connection is checked.
Load Balance Mode	SD-WAN supports five load-balance modes: • Source IP (`source-ip-based`): SD-WAN will load balance the traffic equally among its members according to a hash algorithm based on the source IP addresses. • Session (`weight-based`): SD-WAN will load balance the traffic according to the session numbers ratio among its members. • Spillover (`usage-based`): SD-WAN will use the first member until the bandwidth reaches its limit, then use the second, and so on. • Source-Destination IP (`source-dest-ip-based`): 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 (`measured-volume-based`): SD-WAN will load balance the traffic according to the bandwidth ratio among its members.

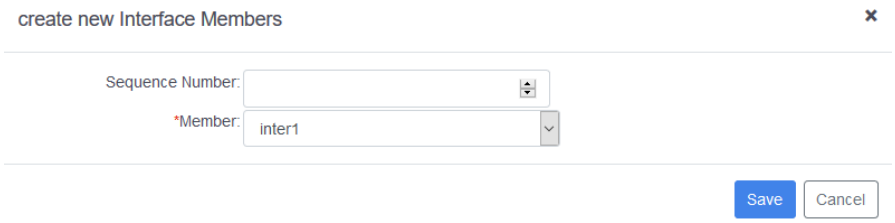
Define which physical interfaces belong to the SD-WAN template

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 tree.
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 54.
5. Select *Save*.

Interface members fields for an SD-WAN template



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

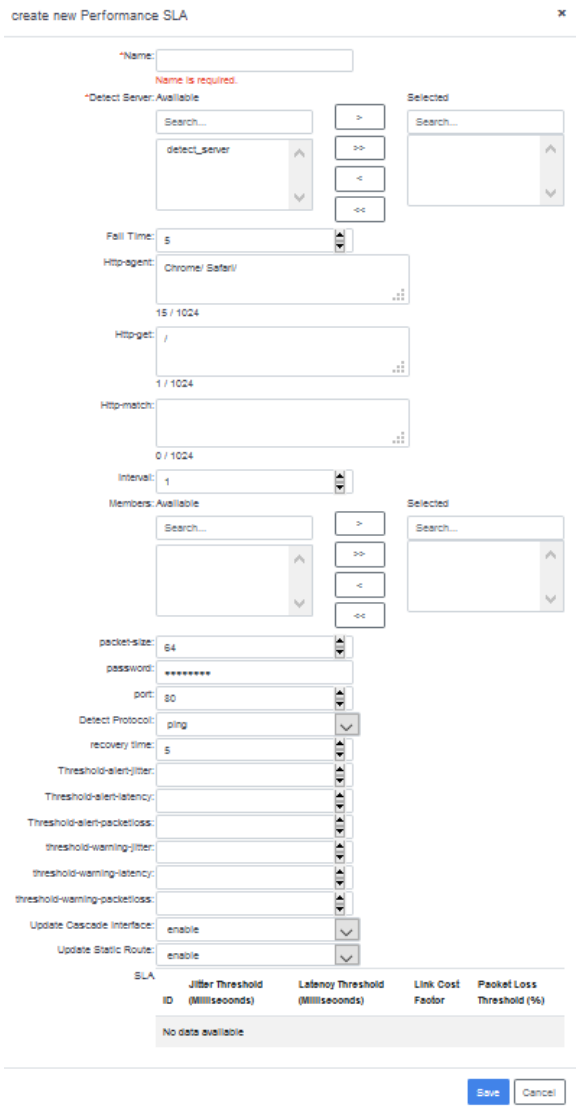
Define a performance SLA for the SD-WAN template

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 tree.
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 55.
5. Select *Save*.

Performance SLA fields for an SD-WAN template



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.

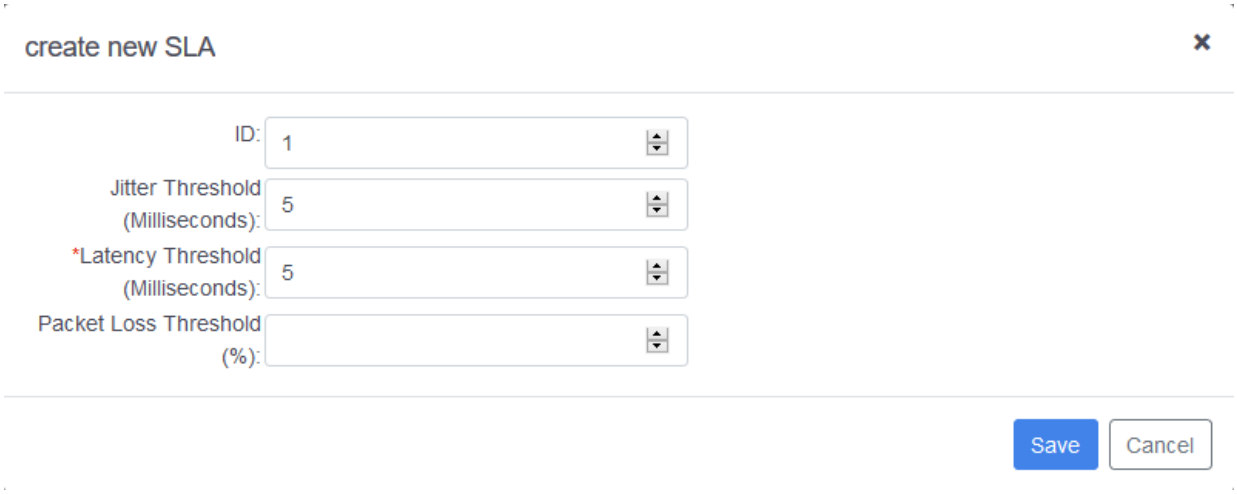
Settings	Description
Http-match	Response string expected from the server if the protocol is HTTP.
Interval	Status check interval, or the time between attempting to connect to the server. The default is 5 seconds; the range is 1 - 3600 seconds.
Outgoing interface	This field is available only if you are using ADOM 6.0 or 6.2 with FortiManager 6.0 or 6.2. • If you are using ADOM 6.2 and FortiManager 6.2, select *Auto*, *Manual*, *Minimum Quality (Maximum Bandwidth)*, *Best Quality (Priority)*, or *Lowest Quality (SLA)*. • If you are using ADOM 6.0 and FortiManager 6.2): select *Auto*, *Manual*, *Minimum Quality (Maximum Bandwidth)*, or *Best Quality(Priority)*. • If you are using ADOM 6.0 and FortiManager 6.0): select *Minimum Quality (Maximum Bandwidth)* or *Best Quality (Priority)*.
Members	Select the interfaces from the Available Members list and then select > to move them to the Selected Members list. If you selected *Manual* for the outgoing interface, select a single interface from the drop-down list.
quality-link	If you selected *Auto* for the outgoing interface, select the quality link from the drop-down list. This field is available only if you are using FortiManager 6.2.
Criteria	If you selected *Auto* for the outgoing interface, select the creiteria from the drop-down 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 *udp-echo*, *ping*, *tcp-echo*, *http*, *twamp*, or *ping6*.
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.

Settings	Description
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.
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 tree.
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 "Performance SLA fields for an SD-WAN template" on page 1.
6. Select *Save* to save your SLA configuration.
7. Select *Save* to save your performance SLA configuration.

SLA fields for an SD-WAN template



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.

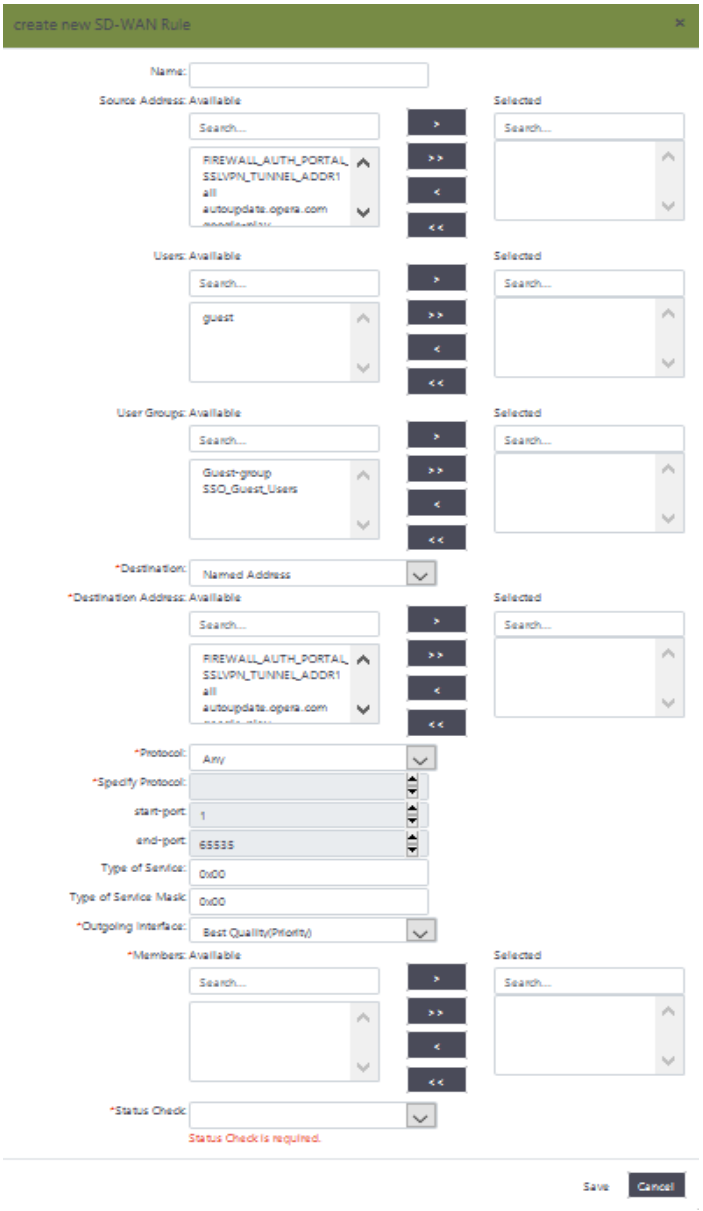
Define SD-WAN rules for the SD-WAN template

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 tree.
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" on page 39.
5. Select *Save*.

SD-WAN rule fields for an SD-WAN template



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.

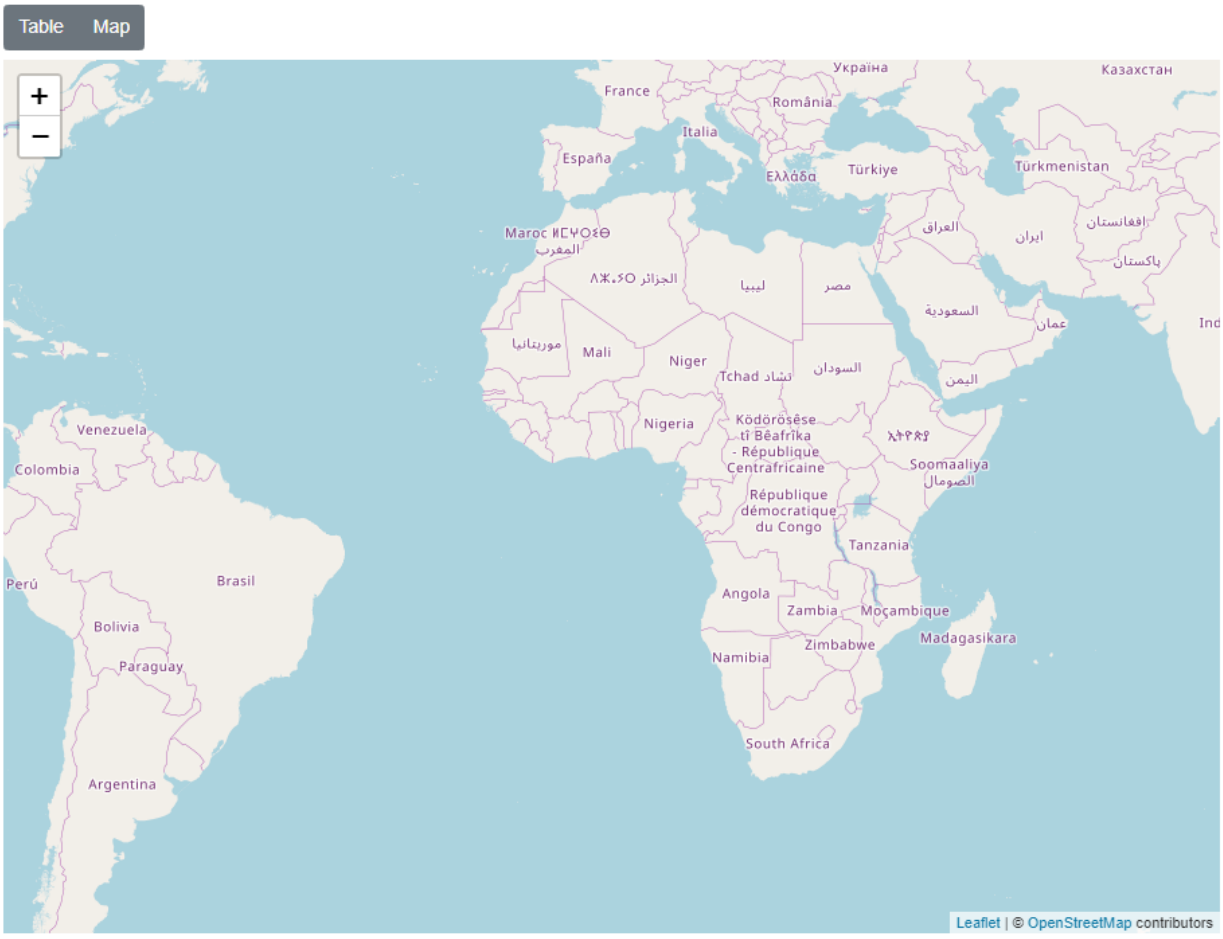
Settings	Description
User Groups	Select the user groups from the Available list and then select > to move them to the Selected list.
Destination	Required. Select *Named Address* to use destination addresses or select *Internet Service* to use destination Internet services.
Destination Address	Required. Available if Destination is set to *Named Address*. 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 *Address*. Select *TCP*, *UDP*, *ANY*, or *Specify*.
Specify Protocol	Required. If Protocol is set to *Specify*, 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 *Internet Service*. 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 *Internet Service*. 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 *Internet Service*. 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 *Internet Service*. 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 *Internet Service*. Enter the identifier of a control-based Internet service.
internet-service-ctrl-group	Available if Destination is set to *Internet Service*. Select the name of a control-based Internet service group.

Settings	Description
Outgoing Interface	Required. Select *Best Quality (Priority)* or *Minimum Quality (Maximize Bandwidth)*.
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 *Minimum Quality (Maximize Bandwidth)*. Select the appropriate performance SLA from the drop-down list.
Status Check	Required. Available if Outgoing Interface is set to *Best Quality (Priority)*. Select the appropriate performance SLA to use for the status check.

Monitoring the SD-WAN interfaces

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

By default, the Map view is displayed. 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.



Select *Table* to see a tabular presentation of the same data.

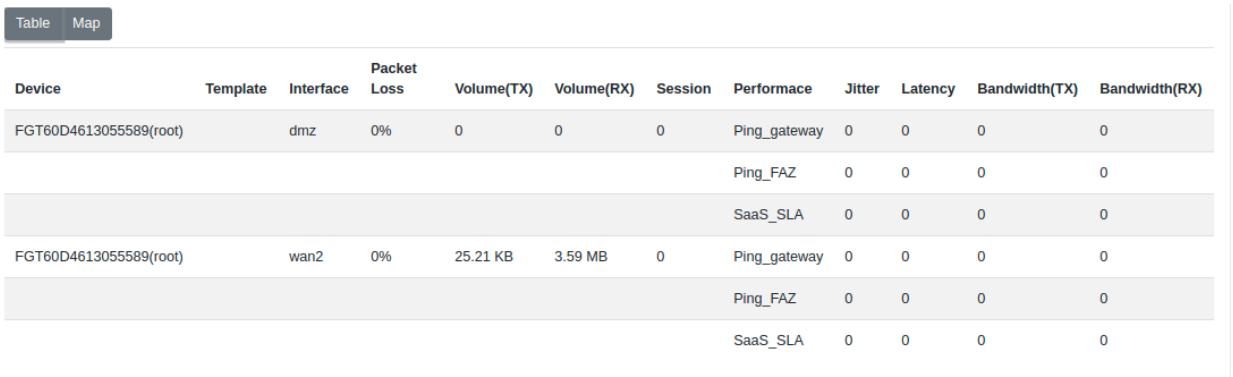


Table Map

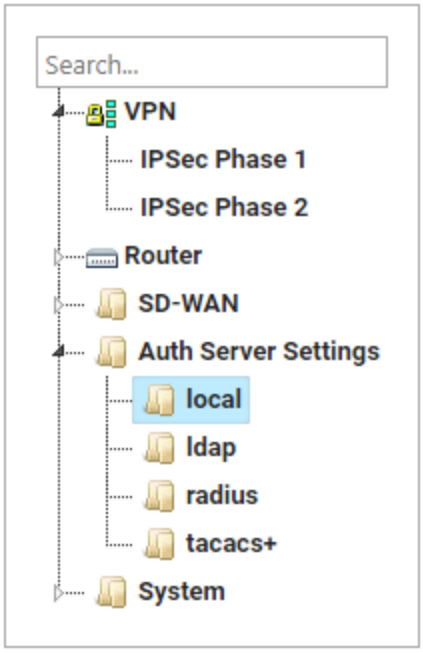
Device	Template	Interface	Packet Loss	Volume(TX)	Volume(RX)	Session	Performace	Jitter	Latency	Bandwidth(TX)	Bandwidth(RX)
FGT60D4613055589(root)		dmz	0%	0	0	0	Ping_gateway	0	0	0	0
							Ping_FAZ	0	0	0	0
							SaaS_SLA	0	0	0	0
FGT60D4613055589(root)		wan2	0%	25.21 KB	3.59 MB	0	Ping_gateway	0	0	0	0
							Ping_FAZ	0	0	0	0
							SaaS_SLA	0	0	0	0

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
- Add, update, and delete LDAP authentication settings
- Add, update, and delete RADIUS authentication settings
- Add, update, and delete TACACS+ authentication settings



Local authentication

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

Add local authentication settings

1. Select *local* from the Auth Server Settings tree.
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 64.
4. Select *Save*.

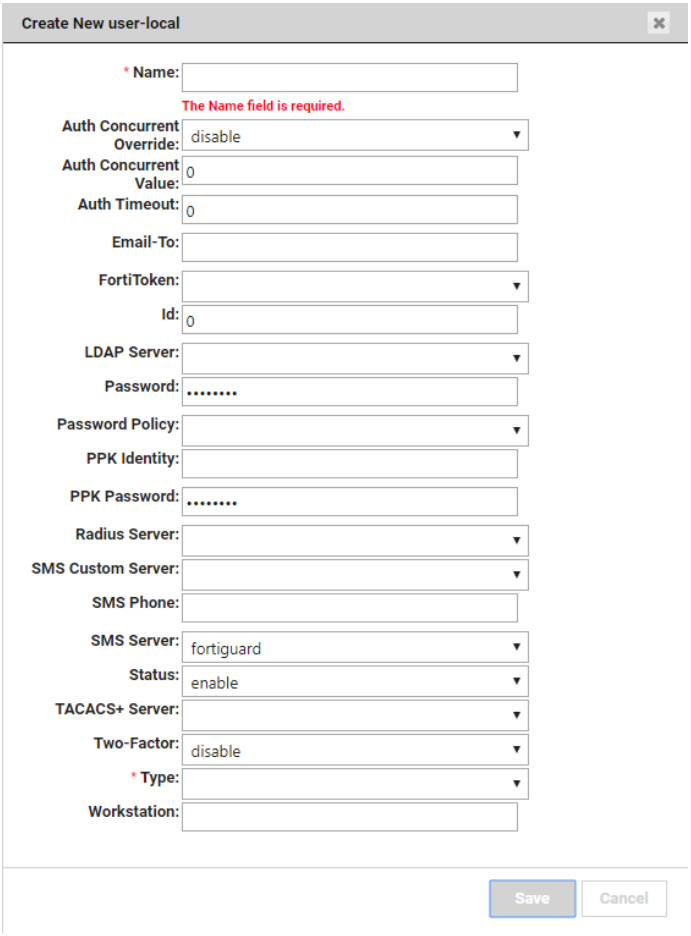
Update local authentication settings

1. Select *local* from the Auth Server Settings tree.
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 tree.
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



The Create New user-local and Edit user-local forms 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.
Email-To	Two-factor recipient's email address.
FortiToken	Two-factor recipient's FortiToken serial number.
Id	Local user ID.

Settings	Guidelines
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	Disable two-factor authentication or choose which two-factor authentication method is used: *fortitoken*—FortiToken *disable*—disable *sms*—SMS authentication code. *email*—Email authentication code.
Type	Required. Select the authentication method. *password*—Password authentication. *ldap*—LDAP server authentication. *tacacs+*—TACACS+ server authentication. *radius*—RADIUS server authentication.
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 tree.
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 67.
4. Select *Save*.

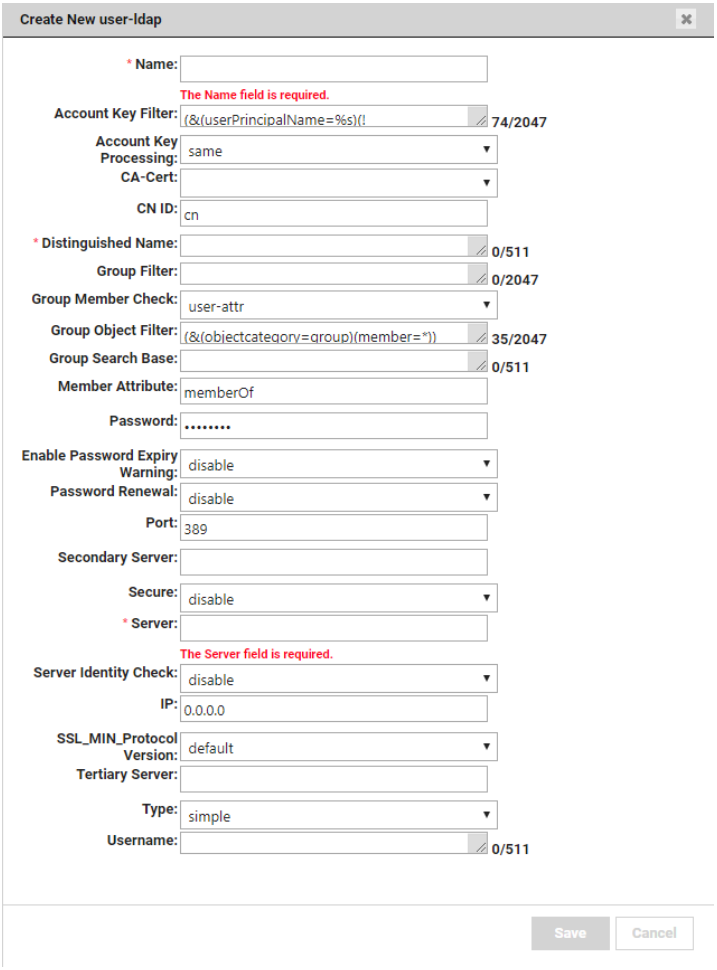
Update LDAP authentication settings

1. Select *ldap* from the Auth Server Settings tree.
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 tree.
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



The Create New user-ldap and Edit user-ldap forms 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: *same*—Same as the UPN. *strip*—Strip the domain string from UPN.
CA-Cert	CA certificate name.

Settings	Guidelines
CN ID	Common name identifier for the LDAP server. The common name identifier for most LDAP servers is `cn`.
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: *user-attr*—User attribute checking. *group-object*—Group object checking. *posix-group-object*—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: *starttls*—Use StartTLS. *disable*—No SSL. *ldaps*—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	The minimum supported protocol version for SSL/TLS connections. *SSLv3*—SSLv3. *default*—Follow system global setting. *TLSv1*—TLSv1. *TLSv1-2*—TLSv1.2. *TLSv1-1*—TLSv1.1.
Tertiary Server	The CN domain name or IP address of the tertiary LDAP server.
Type	Authentication type for LDAP searches: *anonymous*—Bind using anonymous user search. *simple*—Simple password authentication without search. *regular*—Bind using user name and password and then search.
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 tree.
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 70.
4. Select *Save*.

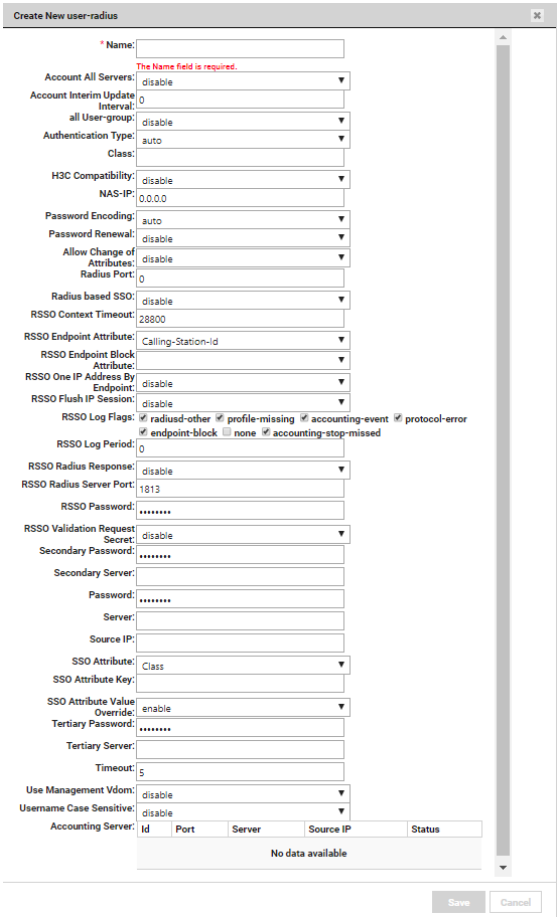
Update RADIUS authentication settings

1. Select *radius* from the Auth Server Settings tree.
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 tree.
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



The Create New user-radius and Edit user-radius forms 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 *disable*.
Account Interim Update Interval	The number of seconds between each accounting interim update message.
all User-group	Enable or disable whether this RADIUS server is automatically included in all user groups.

Settings	Guidelines
Authentication Type	Authentication methods/protocols permitted for this RADIUS server: *ms_chap*—Microsoft Challenge Handshake Authentication Protocol. *ms_chap_v2*—Microsoft Challenge Handshake Authentication Protocol version 2. *auto*—Use PAP, MSCHAP_v2, and CHAP (in that order). *chap*—Challenge Handshake Authentication Protocol. *pap*— 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: *auto*—Use original password encoding. *ISO-8859-1*—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	RADIUS attributes used to block a user: *Login-LAT-Service*—Use this attribute. *NAS-IP-Address*—Use this attribute. *Callback-Number*—Use this attribute. *NAS-Identifier*—Use this attribute. *Acct-Multi-Session-Id*—Use this attribute. *Login-LAT-Group*—Use this attribute. *Reply-Message*—Use this attribute. *User-Name*—Use this attribute. *Calling-Station-Id*—Use this attribute. *Filter-Id*—Use this attribute. *Framed-IP-Address*—Use this attribute. *Framed-IP-Netmask*—Use this attribute. *Login-IP-Host*—Use this attribute. *Callback-Id*—Use this attribute. *Class*—Use this attribute. *Framed-Route*—Use this attribute. *Acct-Session-Id*—Use this attribute. *Proxy-State*—Use this attribute. *Called-Station-Id*—Use this attribute. *Framed-AppleTalk-Zone*—Use this attribute. *Login-LAT-Node*—Use this attribute *Framed-IPX-Network*—Use this attribute.
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.
RSSO Log Flags	Events to log: *radiusd-other*—Enable this log type. *profile-missing*—Enable this log type. *accounting-event*—Enable this log type. *protocol-error*—Enable this log type. *endpoint-block*—Enable this log type. *none*—Disable all logging. *accounting-stop-missed*—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.

Settings	Guidelines
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.
SSO Attribute	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record: *Login-LAT-Service*—Use this attribute. *NAS-IP-Address*—Use this attribute. *Callback-Number*—Use this attribute. *NAS-Identifier*—Use this attribute. *Acct-Multi-Session-Id*—Use this attribute. *Login-LAT-Group*—Use this attribute. *Reply-Message*—Use this attribute. *User-Name*—Use this attribute. *Calling-Station-Id*—Use this attribute. *Filter-Id*—Use this attribute. *Framed-IP-Address*—Use this attribute. *Framed-IP-Netmask*—Use this attribute. *Login-IP-Host*—Use this attribute. *Callback-Id*—Use this attribute. *Class*—Use this attribute. *Framed-Route*—Use this attribute. *Acct-Session-Id*—Use this attribute. *Proxy-State*—Use this attribute. *Called-Station-Id*—Use this attribute. *Framed-AppleTalk-Zone*—Use this attribute. *Login-LAT-Node*—Use this attribute. *Framed-IPX-Network*—Use this attribute.
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.

Settings	Guidelines
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. Right-click in the Accounting Server table and select *Create New*.
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.

TACACS+ authentication

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

Add TACACS+ authentication settings

1. Select *tacacs+* from the Auth Server Settings tree.
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*.

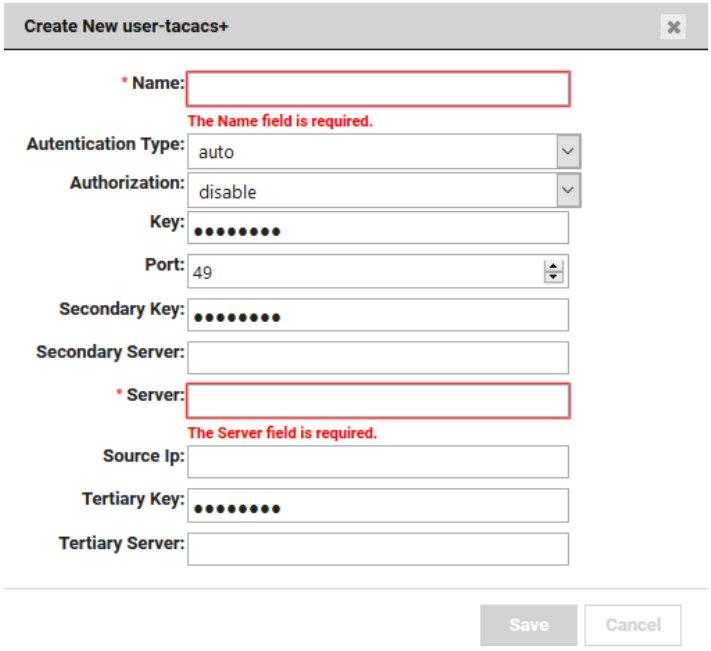
Update TACACS+ authentication settings

1. Select *tacacs+* from the Auth Server Settings tree.
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 tree.
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



The Create New user-tacacs+and Edit user-tacacs+ forms contain the following fields:

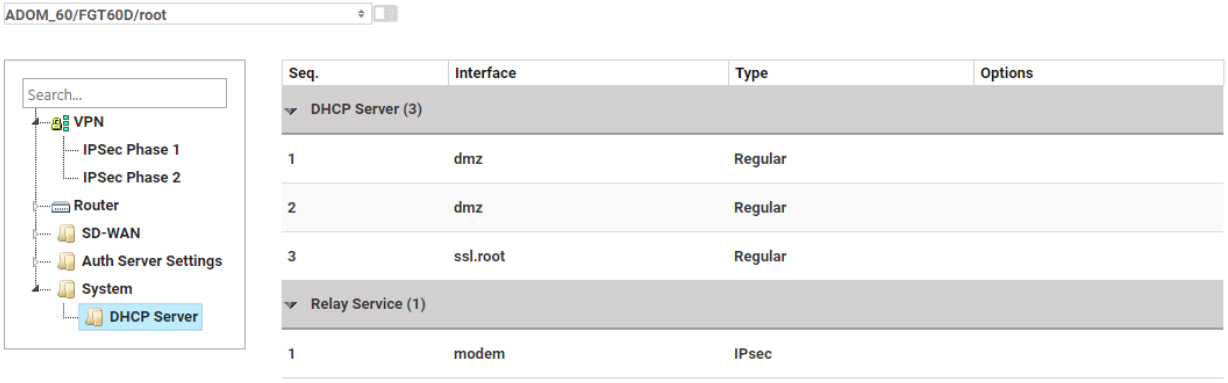
Settings	Guidelines
Name	Required. The TACACS+ server name.
Authentication Type	Authentication methods/protocols permitted for this TACACS+ server: *auto*—Use PAP, MSCHAP, and CHAP (in that order). *ms_chap*—Microsoft Challenge Handshake Authentication Protocol. *chap*—Challenge Handshake Authentication Protocol. *ascii*—ASCII. *pap*—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.
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.

Settings	Guidelines
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* tree 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 tree.
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 77.
4. Select *Save*.

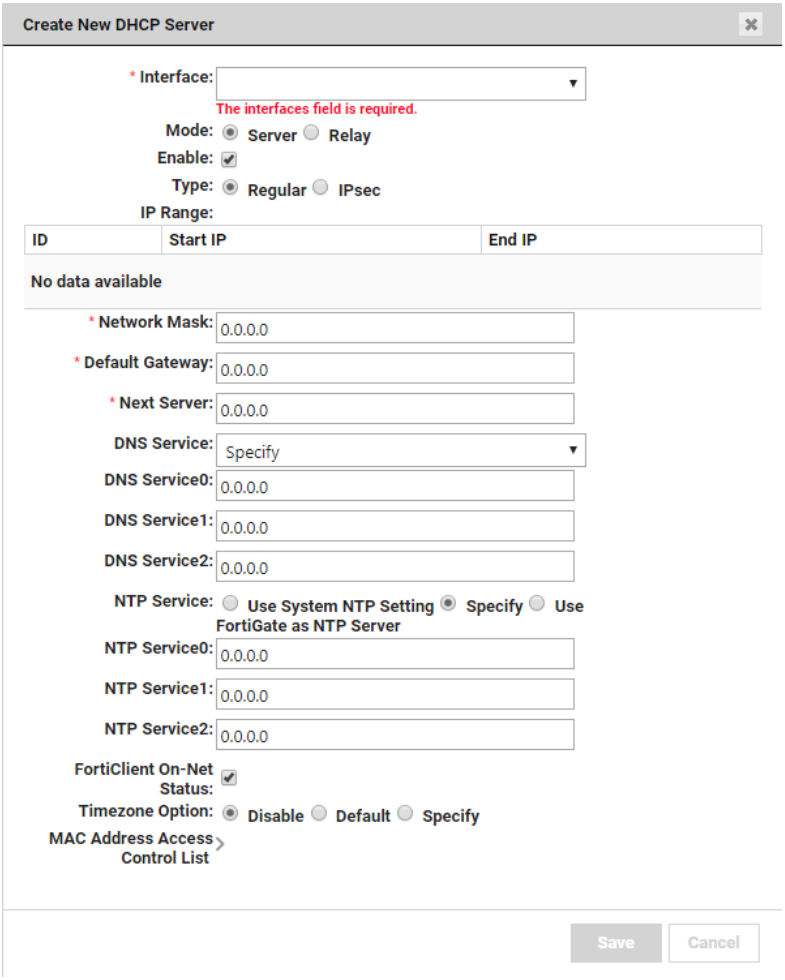
Updating a DHCP server

1. Select *DHCP Server* from the System tree.
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 tree.
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 forms contain the following fields:

Settings	Guidelines
Interface	The name of the interface.
Mode	Select *Server* to create a DHCP server.
Enable	Select this option to make the DHCP server active.
Type	Select *Regular* to use the DHCP in regular mode. Select *IPsec* 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 79.
Network Mask	Required. Netmask assigned by the DHCP server.

Settings	Guidelines
Default Gateway	Required. Default gateway IP address assigned by the DHCP server.
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: *Use System DNS Setting (Default)*—Clients are assigned the FortiGate device's configured DNS servers. *Specify*—Specify up to three DNS servers in the DHCP server configuration. *Same as interface IP (Local)*—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: *Use System NTP Setting*—The IP address of the interface the DHCP server is added to becomes the client's NTP server IP address. *Specify*—Specify up to three NTP servers in the DHCP server configuration. *Use FortiGate as NTP Server*—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.

Settings	Guidelines
Timezone Option	Options for the DHCP server to set the client's time zone. *Disable*—Do not set the client's time zone. *Default*—Clients are assigned the FortiGate device's configured time zone. *Specify*—Specify the time zone to be assigned to DHCP clients. If you select *Specify*, 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 79.

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, enter the option number in the ID field. **NOTE:** 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, enter the option number in the ID field. **NOTE:** 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 tree.
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 80.
4. Select *Save*.

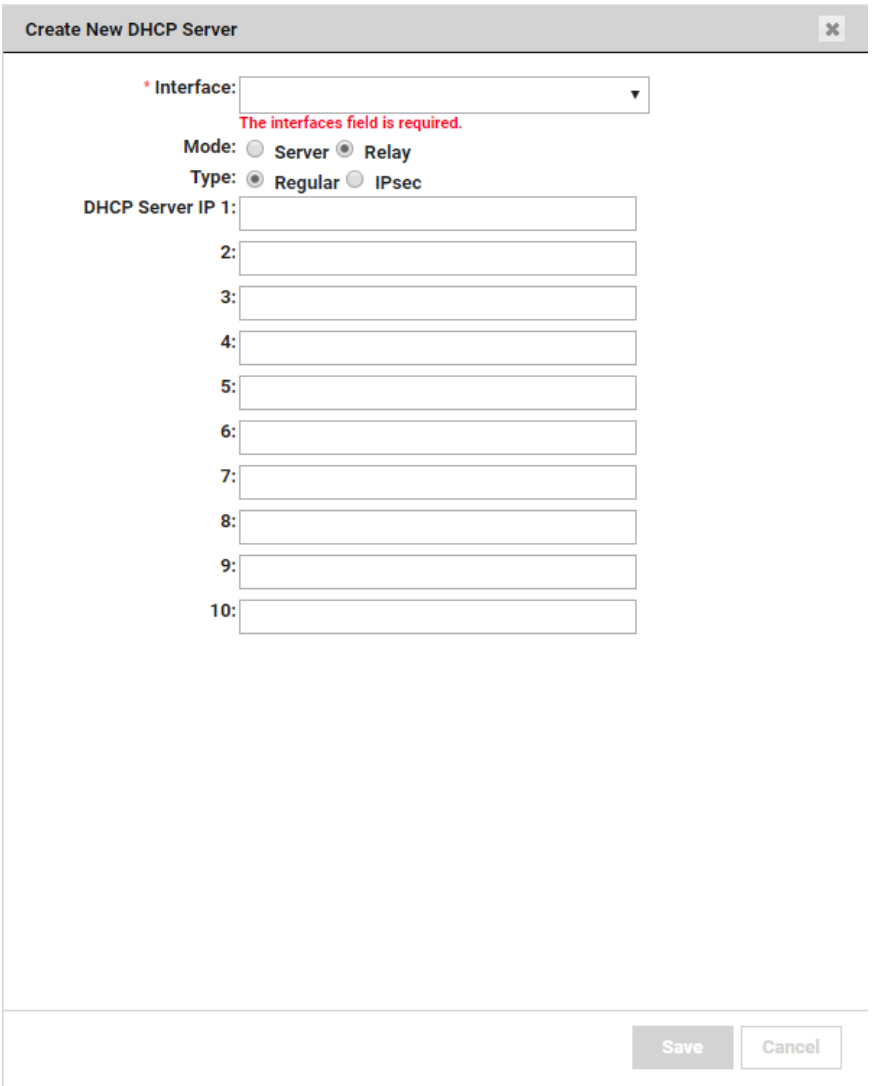
Updating a DHCP relay

1. Select *DHCP Server* from the System tree.
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 tree.
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 forms contain the following fields:

Settings	Guidelines
Interface	The name of the interface.
Mode	Select *Relay* to create a DHCP relay.
Enable	Select this option to make the DHCP server active.
Type	Select *Regular* to use the DHCP in regular mode. Select *IPsec* 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*—view the event logs grouped by application, attack or sandbox.
- *Scope*—view output for all sites or select a specific site
- *Set Filter*—filter the data (last hour, last day, last 7 days, or customize)
- *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 drop-down menu for selecting the number of entries to display. In Collector mode, the header also includes a search box, enabling you to search for the text in the following fields: User, Source, Source Information (Src.Inf), Destination, Destination Information (Dst.Inf) and Application.

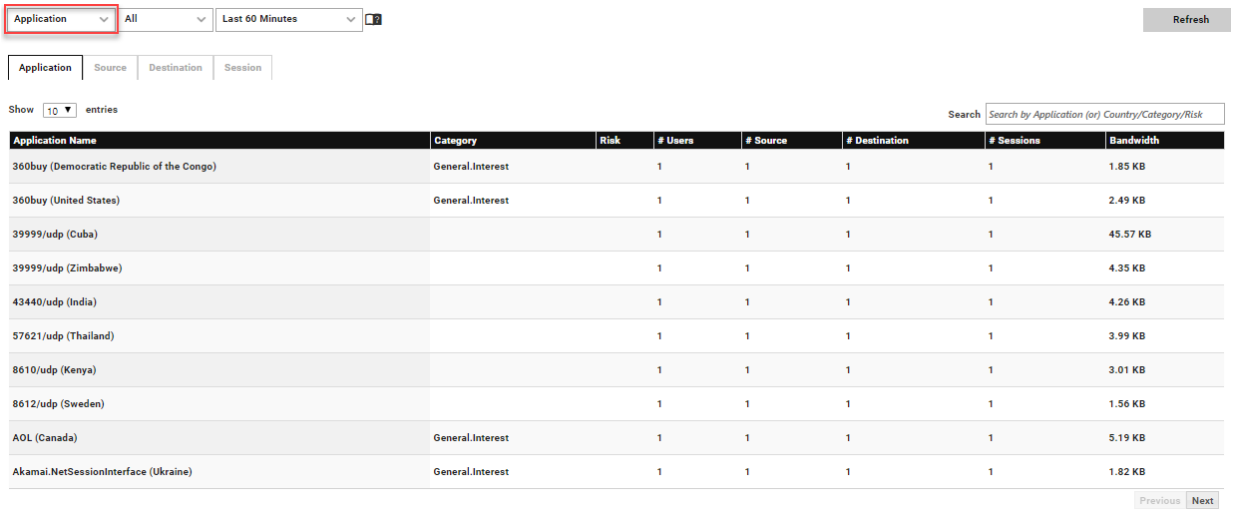
After you select *Application*, *Attack*, or *Sandbox*, you can select how to sort the event logs. Depending on the mode that FortiPortal is running in (Collector or FortiAnalyzer mode), the tabs available differ. The following tabs provide different views of the data:

- *Application*—arranged by application
- *Attack*—arranged by attack
- *Sandbox*—arranged by sandbox
- *Source*—arranged by the source FortiGate device
- *Destination*—arranged by the destination (IP address, protocol, port)
- *Session*—arranged by session (that is, a specific flow of packets between a source and destination). This tab is visible only when you have selected the Application view.
- *Log* —details of each event

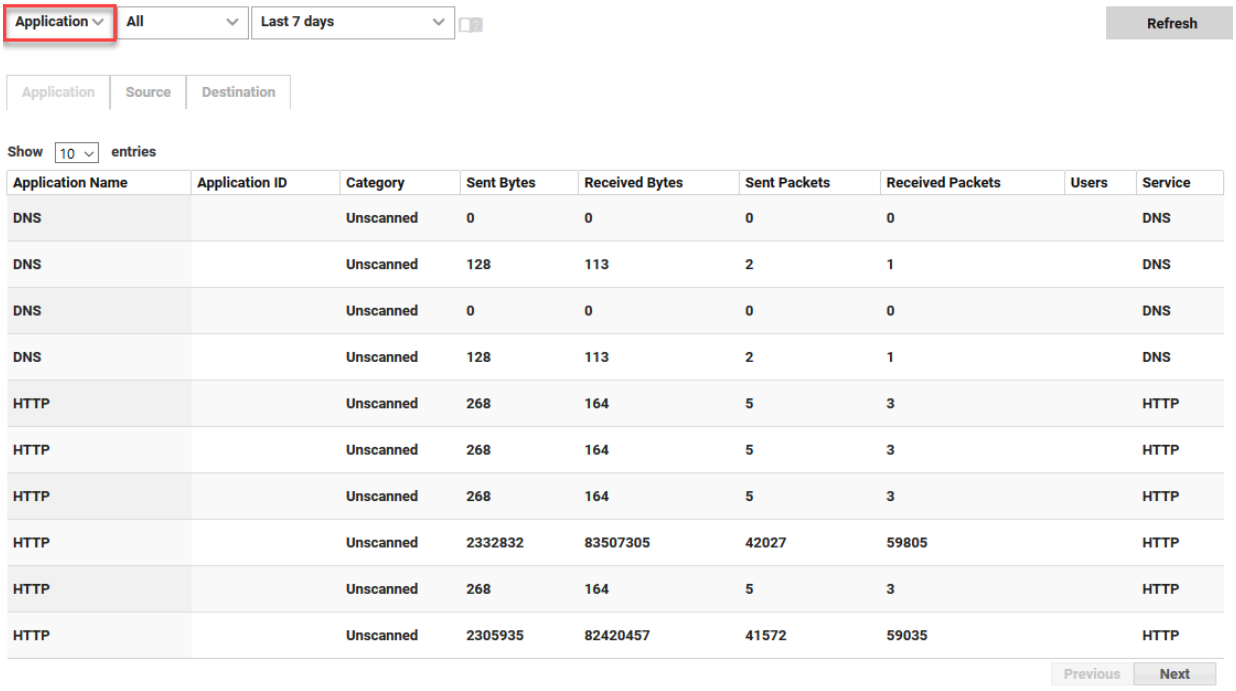
Application view

The *Application* tab under *View* displays event logs grouped by application. The display and information differ when FortiPortal is in Collector mode and FortiAnalyzer mode.

The follow figure shows an example of the *Application* tab when FortiPortal is in Collector mode:



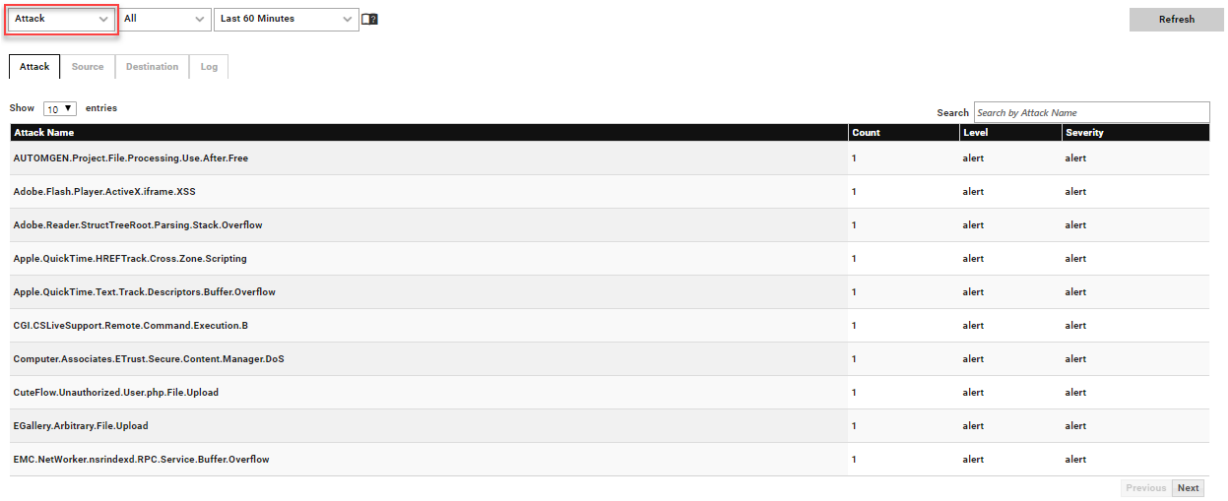
The follow figure shows an example of the *Application* tab when FortiPortal is in FortiAnalyzer mode:



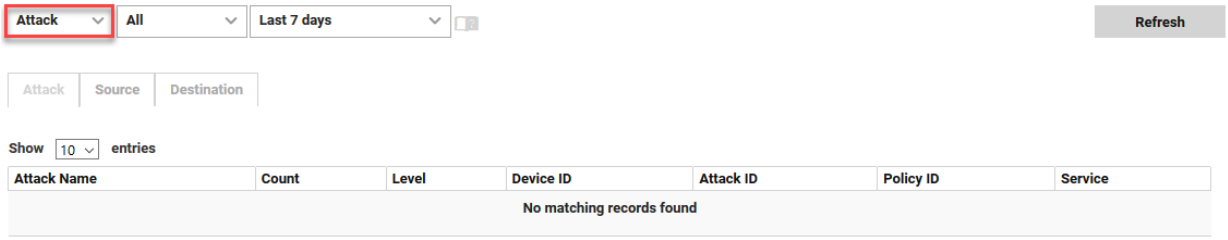
Attack view

The *Attack* tab under *View* displays event logs grouped by “attack.” The display and information differ when FortiPortal is in Collector mode and FortiAnalyzer mode.

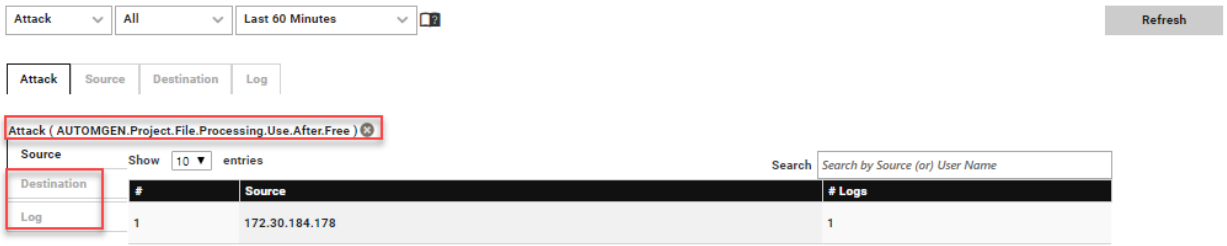
The follow figure shows an example of the *Attack* tab when FortiPortal is in Collector mode:



The follow figure shows an example of the *Attack* tab when FortiPortal is in FortiAnalyzer mode:

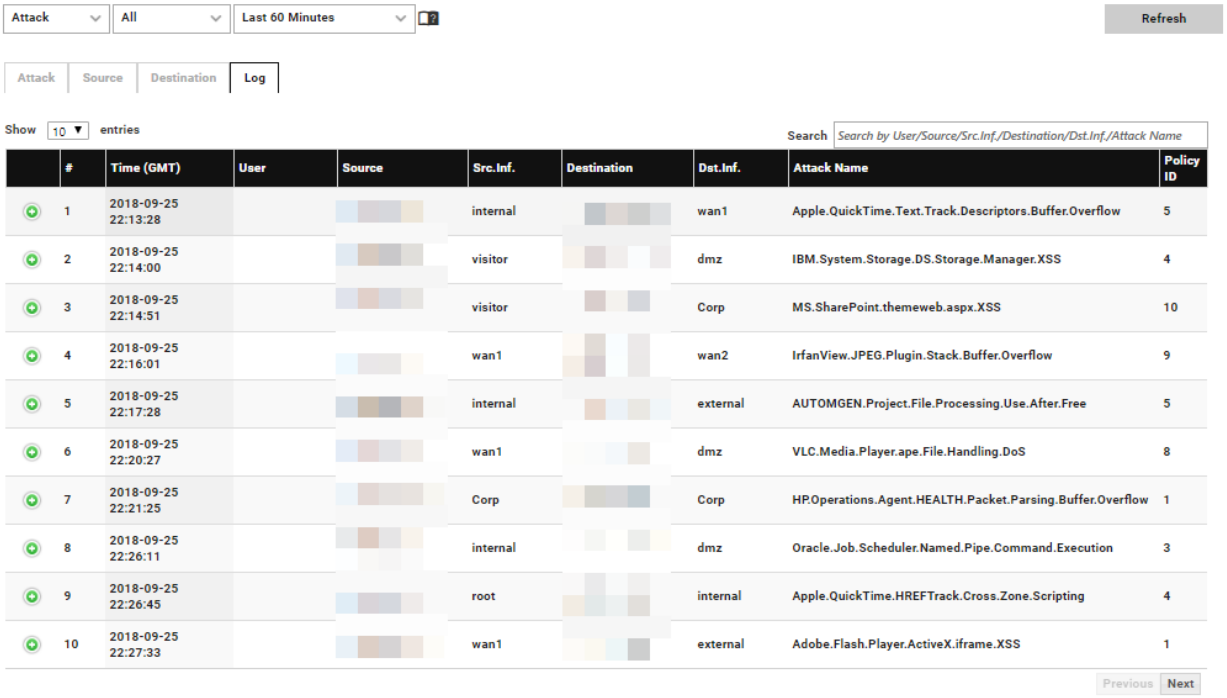


When you select one of the entries in the table, the system displays the first set of filtering. For each of the remaining filters, a vertical left menu includes buttons to perform the next level of filtering (see the following figure):



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

If you select *Attack* > *Log* (available in Collector mode), the system displays details of the attacks:

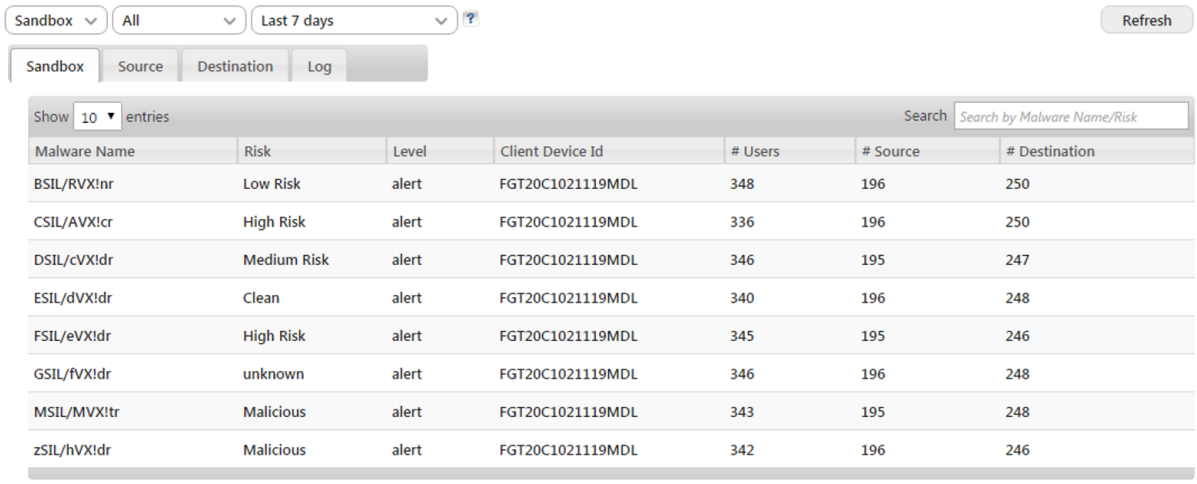


To the left of each entry, the system provides an expand button to display all of the fields associated with the log entry.

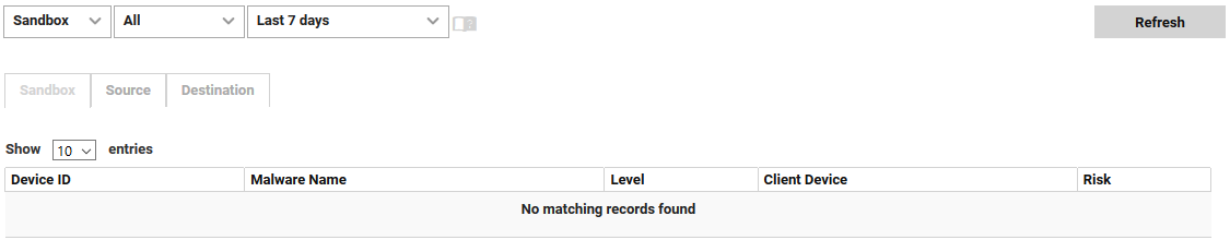
Sandbox view

The *Sandbox* tab under *View* displays event logs grouped by “sandbox.” The display and information differ when FortiPortal is in Collector mode and FortiAnalyzer mode.

The follow figure shows an example of the Sandbox tab when FortiPortal is in Collector mode:



The follow figure shows an example of the *Sandbox* tab when FortiPortal is in FortiAnalyzer mode:



Use the *Source* or *Destination* tab to filter the view. The *Log* tab in Collector mode shows the logs unfiltered.

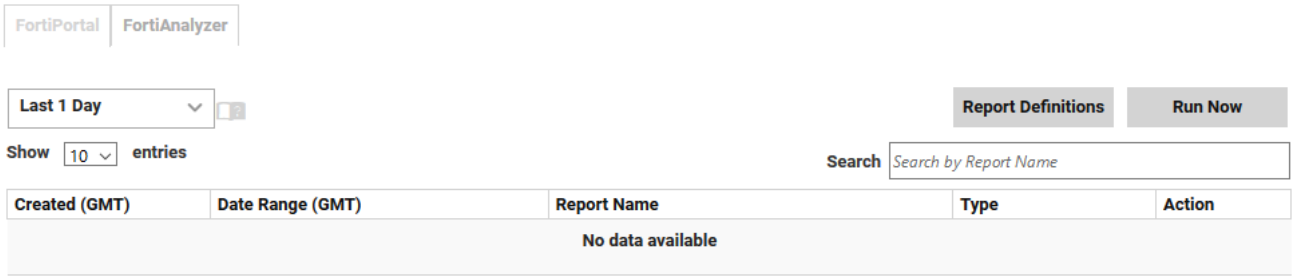
When you select one of the entries in the table, the sandbox view works like the attack view. The system displays the first set of filtering. For each of the remaining filters, a vertical left menu includes buttons to perform the next level of filtering.

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

If you select an individual log entry, the system displays the details of that entry.

Reports

The Reports page displays a list of available FortiPortal or FortiAnalyzer reports if the FortiPortal is running in Collector mode. If the FortiPortal is running in FortiAnalyzer mode, only FortiAnalyzer reports are available.



FortiPortal reports

The FortiPortal Reports page includes the following actions:

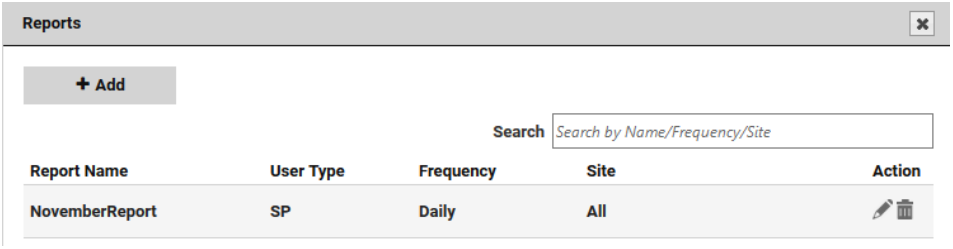
- *Set Filter*—filter the data (today, last 1 day, last 1 week, last 1 month, or customize a filter)
- *Report Definitions*—opens a pop-up window that lists the available reports
- *Run Now*—opens a pop-up window with a form to specify the report to be run
- *Search*—text search by report name

NOTE: The *Report Definitions* and *Run Now* buttons are visible only to users with the relevant permissions.

When you scroll over a entry in the reports table, the following icons appear in the Action column:

- *Download*—download the selected report
- *Delete*—delete the selected report

Report definition actions



The Report Definitions form contains the following actions:

- *Add*—open a new page with the form to add a report
- *Search*—enter text to search for report names containing that text

Run Now actions

The Run Now form contains the following selections:

Settings	Guidelines
Report Duration	Duration of data included in the report: last 1 day, last 1 week, last 1 month
Available/Selected Reports	Use the arrow keys to create a subset of available reports.
Available/Selected Sites	Use the arrow keys to create a subset of available sites. If none are selected, the report is run for all sites.
Language	Language for the report selected from the pull-down list
No of Rows	Number of rows of data to include in the report

Per-report actions

When you scroll over a entry in the reports list, the following icons appear in the Action column:

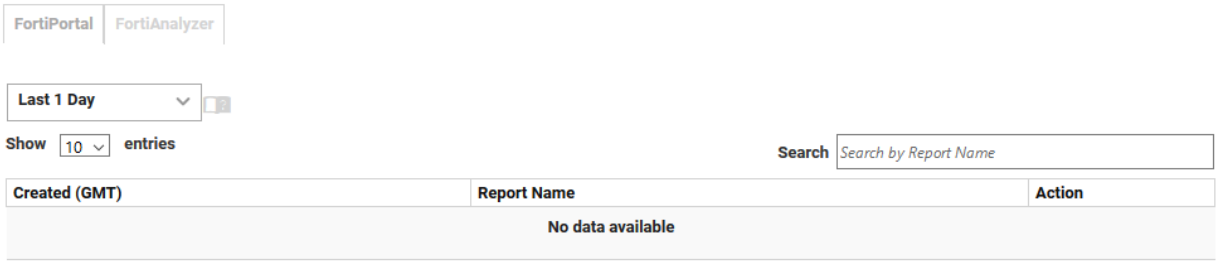
- *Edit*—opens a new page with the form to edit the selected report
- *Delete*—deletes this report

The Add Report and Edit Report forms contain the following selections:

Settings	Guidelines
Report Name	Name for the report
Frequency	Values include: daily, weekly, monthly
Available/Selected Reports	Use the arrow keys to create a sublist of available reports. Use the search boxes to filter the choices available.
Available/Selected Sites	Use the arrow keys to create a sublist of available sites. (If none are selected, the report is run for all sites.) Use the search boxes to filter the choices available.
Language	Language for the report from the pull-down list
No of Rows	Number of rows of data to include in the report
From Email	Email address from which the report will be sent
Email Text	Text for the body of the email

FortiAnalyzer reports

When you select the *FortiAnalyzer* tab, the FortiPortal displays a reports page:



This page includes the following actions:

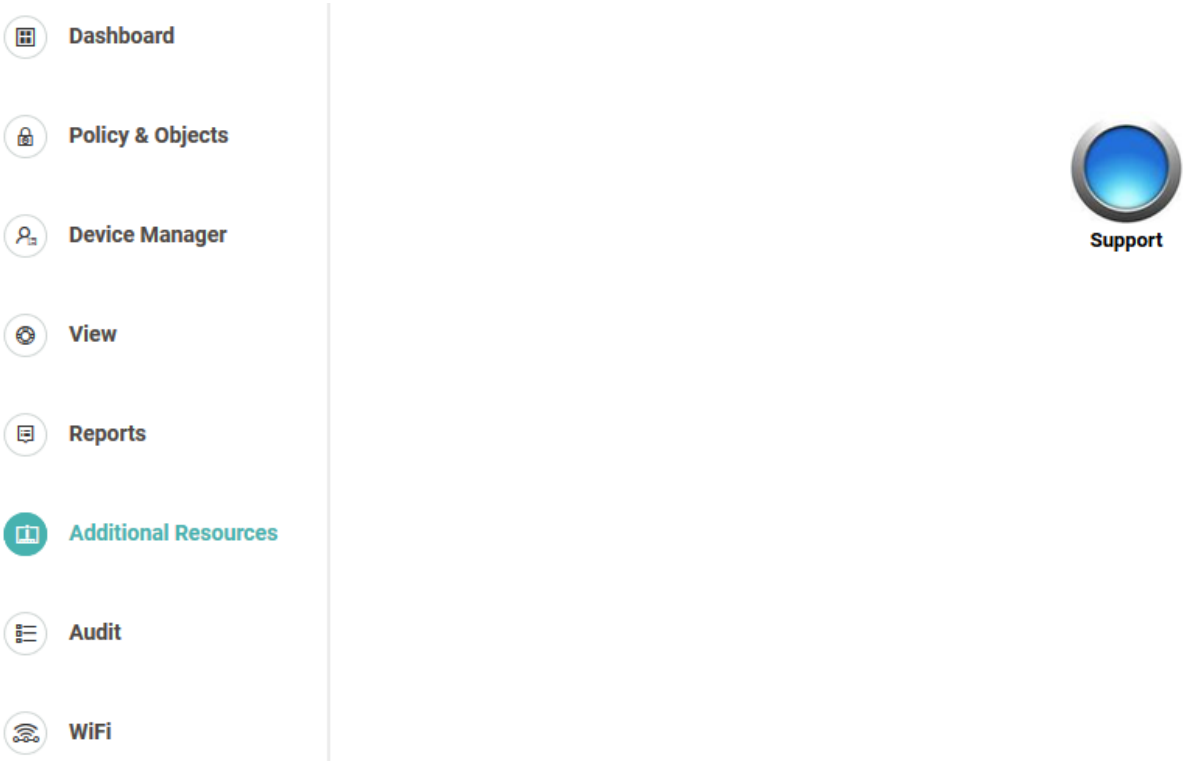
- *Set Filter*—filter the data (today, last 1 day, last 1 week, last 1 month, or customize a filter).
- *Search*—text search by report name

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

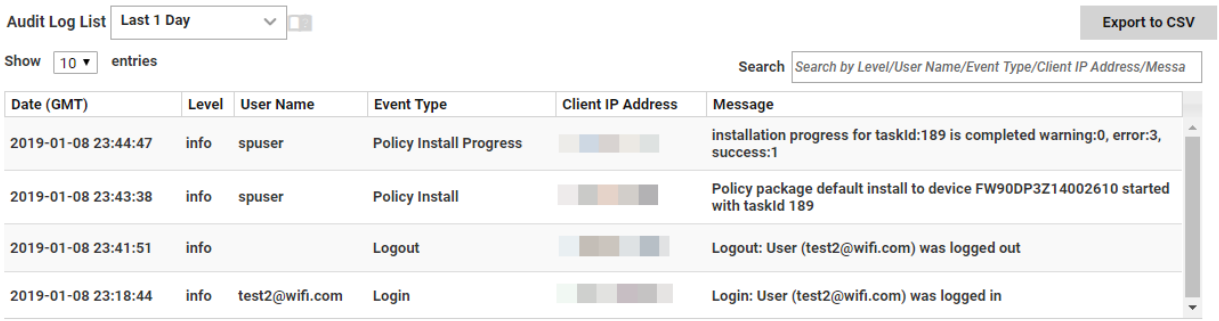
Additional Resources

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.



Audit

The Audit tab displays an log of user activity on the administrative web interface:

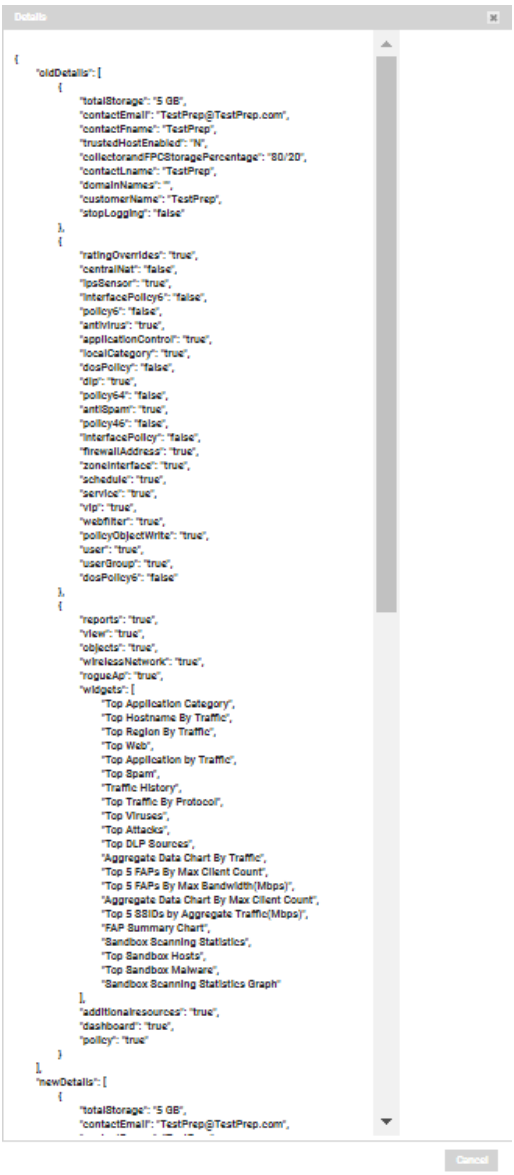


Page actions

- *Audit Log List*—set the duration of the logs to display (last 60 minutes, last 1 day, last 7 days, or customize)
- *Search*—use any column to search the audit log list by level, user name, event type, client IP address, or message
- *Export to CSV*—export the audit log list as a Comma-Separated Value (CSV) file

Per-audit actions

When you select the *Message* field for an *Edit Customer* audit entry, the system opens a pop-up window to display the details of the change. The details window shows the original ("oldDetails") and new ("newDetails") field values.


Details
{
"oldDetails": [
{
"totalStorage": "5 GB",
"contactEmail": "TestPrep@TestPrep.com",
"contactFname": "TestPrep",
"trustedHostEnabled": "N",
"collectorandFPCStoragePercentage": "80/20",
"contactLname": "TestPrep",
"domainNames": "",
"customerName": "TestPrep",
"stopLogging": "false"
},
{
"ratingOverrides": "true",
"centralNat": "false",
"ipsSensor": "true",
"interfacePolicy6": "false",
"policy6": "false",
"antivirus": "true",
"applicationControl": "true",
"localCategory": "true",
"dosPolicy": "false",
"dlp": "true",
"policy64": "false",
"antiSpam": "true",
"policy46": "false",
"interfacePolicy": "false",
"firewallAddress": "true",
"zoneInterface": "true",
"schedule": "true",
"service": "true",
"vip": "true",
"webfilter": "true",
"policyObjectWrite": "true",
"user": "true",
"userGroup": "true",
"dosPolicy6": "false"
},
{
"reports": "true",
"view": "true",
"objects": "true",
"wirelessNetwork": "true",
"rogueAp": "true",
"widgets": [
"Top Application Category",
"Top Hostname By Traffic",
"Top Region By Traffic",
"Top Web",
"Top Application by Traffic",
"Top Spam",
"Traffic History",
"Top Traffic By Protocol",
"Top Viruses",
"Top Attacks",
"Top DLP Sources",
"Aggregate Data Chart By Traffic",
"Top 5 FAPs By Max Client Count",
"Top 5 FAPs By Max Bandwidth(Mbps)",
"Aggregate Data Chart By Max Client Count",
"Top 5 SSIDs by Aggregate Traffic(Mbps)",
"FAP Summary Chart",
"Sandbox Scanning Statistics",
"Top Sandbox Hosts",
"Top Sandbox Malware",
"Sandbox Scanning Statistics Graph"
],
"additionalresources": "true",
"dashboard": "true",
"policy": "true"
}
],
"newDetails": [
{
"totalStorage": "5 GB",
"contactEmail": "TestPrep@TestPrep.com",
Cancel

WiFi

Use the WiFi tab for the following:

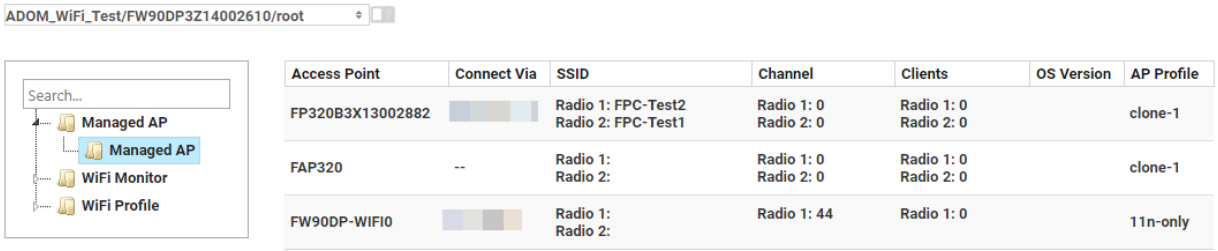
- Update or delete managed access points (APs). See Managed AP.
- Monitor rogue access points, Fortinet access points (FAPs), and SSIDs. See WiFi Monitor.
- Update or delete access point profiles and add, update, or delete SSIDs. See WiFi Profile.

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:



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

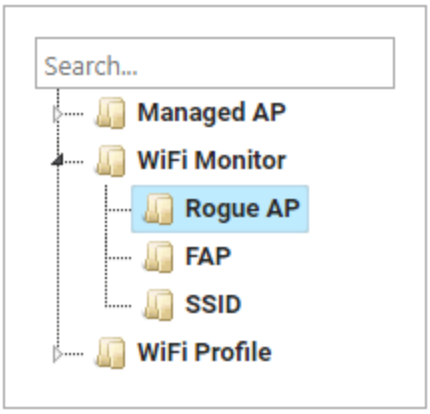
1. Right-click a managed AP in the list and select *Delete*.
2. Select *Yes* to confirm your choice.

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

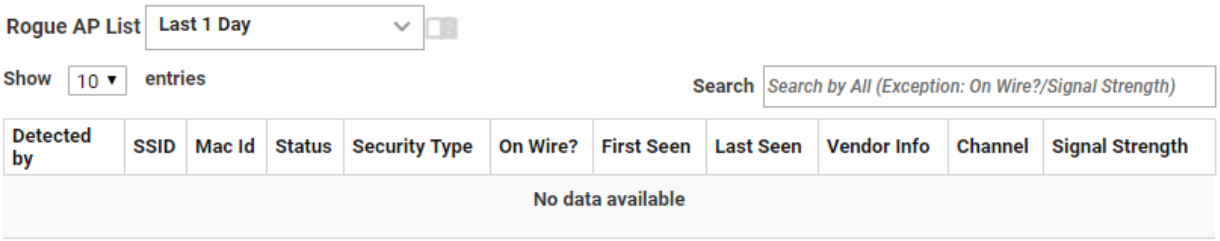


Rogue AP

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

- *Rogue AP List*—filter the data (last 60 Minutes, last 1 day, last 7 days, or customize 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:

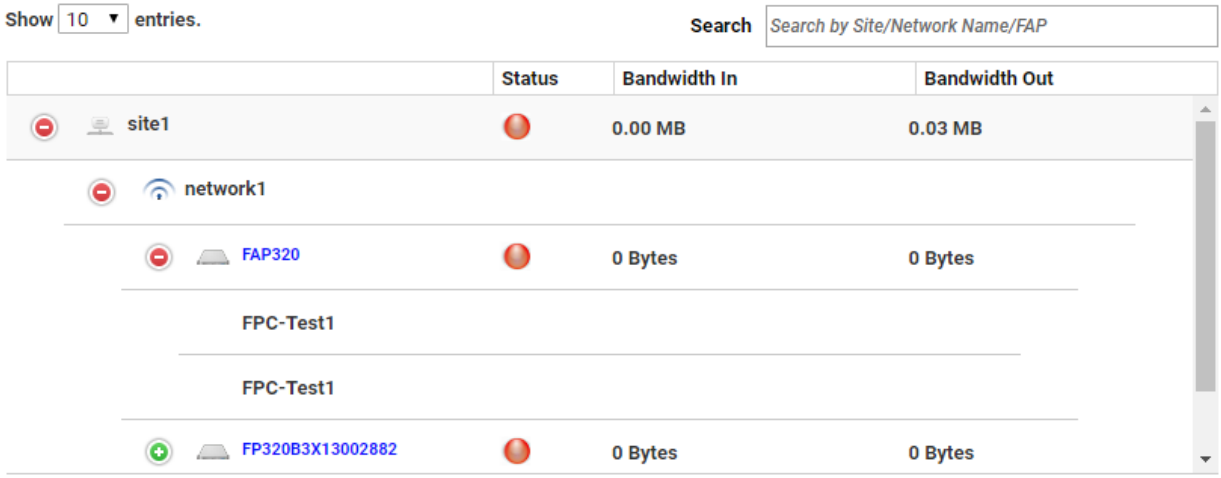


FAP

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

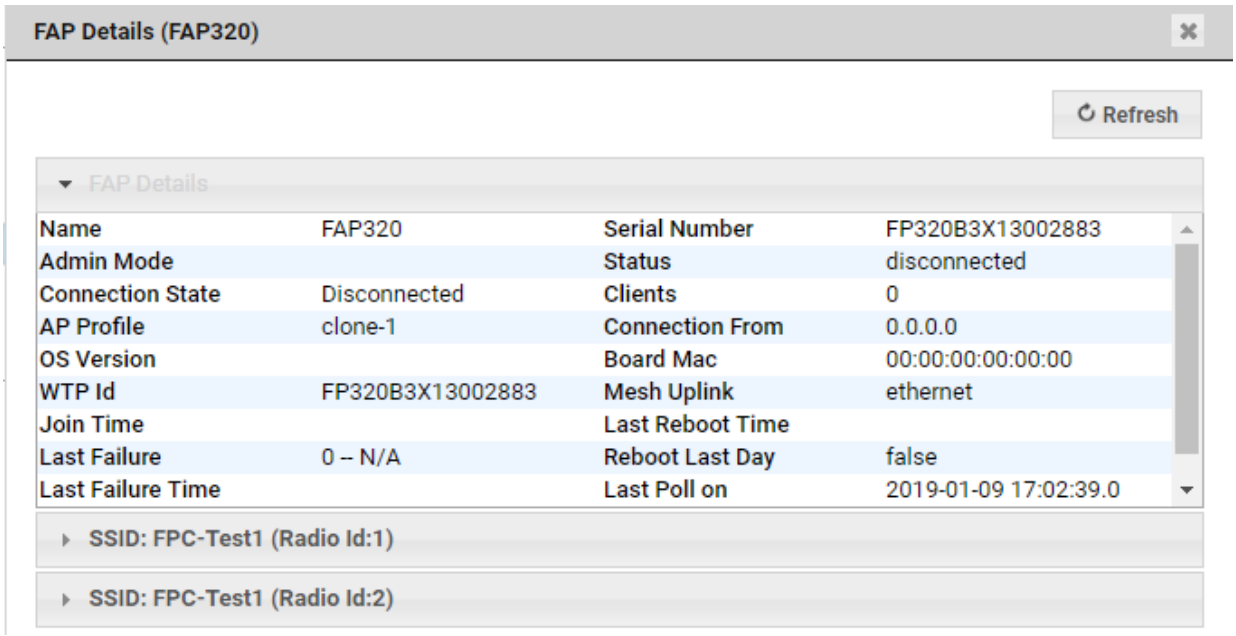
- *Show x entries*—drop-down menu to set the number of entries per page
- *Search*—search by site, network name, or device.

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.



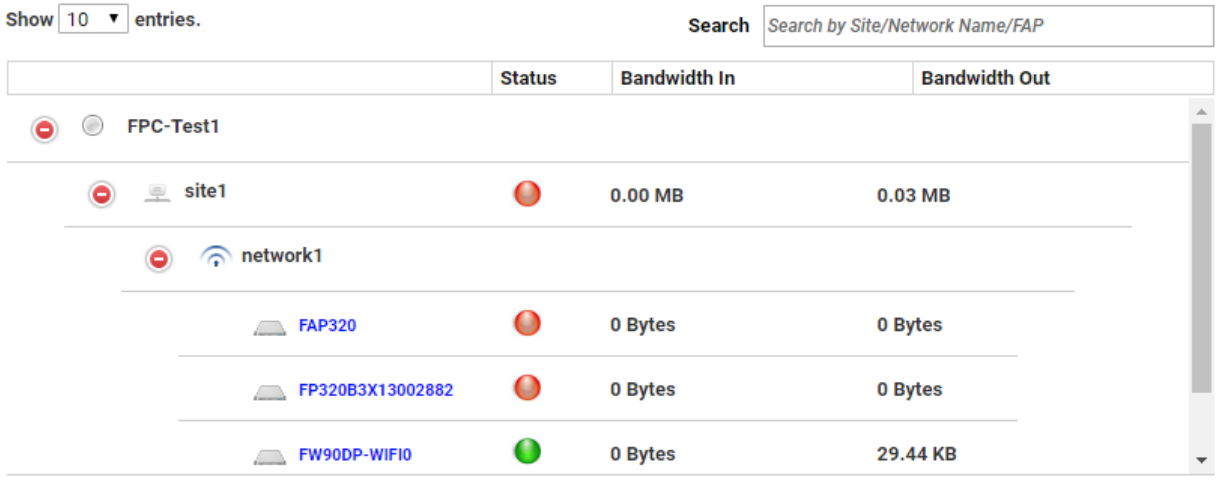
Additional information about Fortinet wireless networks is available in the wireless chapter of the FortiOS handbook.

SSID

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

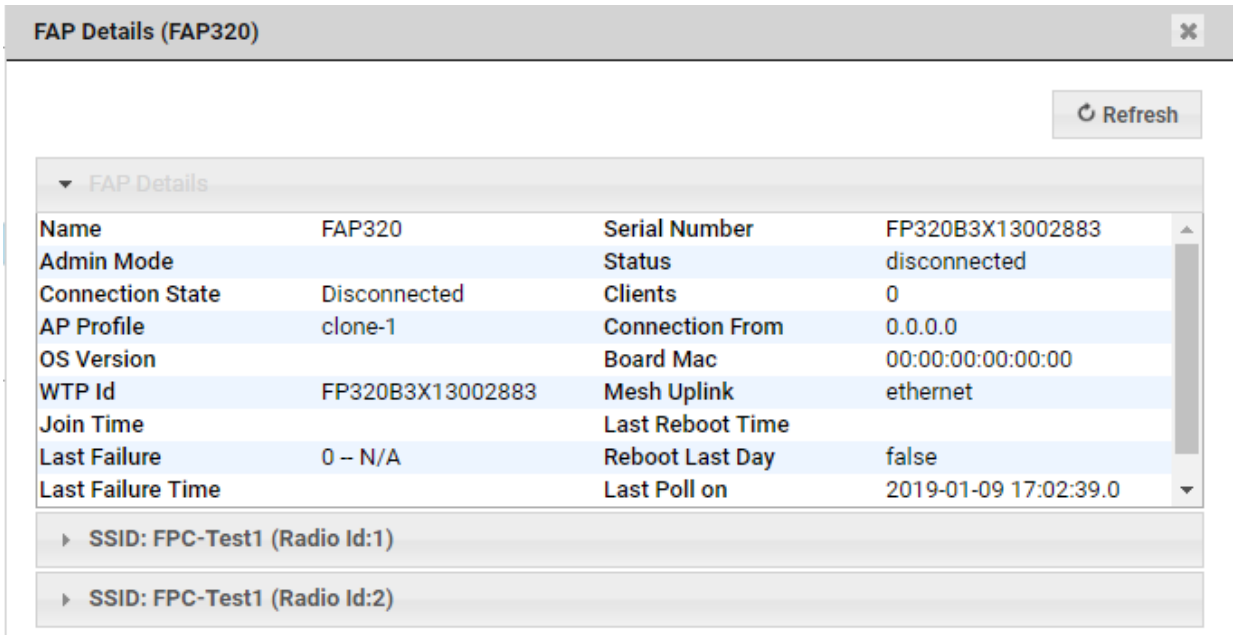
- *Show x entries*—drop-down menu to set the number of entries per page
- *Search*—search by site, network name, or device.

The following figure shows the SSID page:



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.

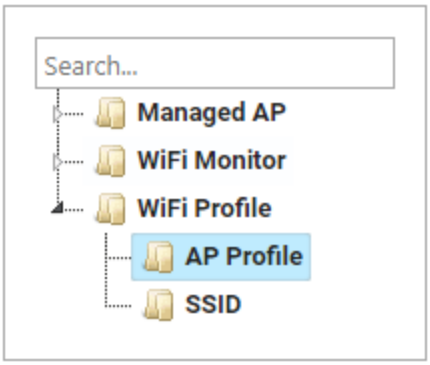


Additional information about Fortinet wireless networks is available in the wireless chapter of the FortiOS handbook.

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:

Seq.	Name	Platform	Radio 1	Radio 2	Comment
1	11n-only	FortiWiFi local radio	2.4GHz 802.11n/g/b		
2	AP-11N-default	Default 11n AP	2.4GHz 802.11n/g/b		
3	Clone of FAP320B_for_test	FAP320B	5GHz 802.11n/a	2.4GHz 802.11n/g/b	
4	FAP112B-clone	FAP112B	2.4GHz 802.11n/g/b		
5	FAP112B-default	FAP112B	2.4GHz 802.11n/g/b		
6	FAP112D-default	FAP112D	2.4GHz 802.11n/g/b		
7	FAP11C-default	FAP11C	2.4GHz 802.11n/g/b		
8	FAP14C-default	FAP14C	2.4GHz 802.11n/g/b		
9	FAP210B-default	FAP210B	2.4GHz 802.11n/g/b		
10	FAP21D-default	FAP21D	2.4GHz 802.11n/g/b		
11	FAP220B-default	FAP220B/221B	5GHz 802.11n/a	2.4GHz 802.11n/g/b	
12	FAP221C-default	FAP221C	2.4GHz 802.11n/g/b	5GHz 802.11ac/n/a	

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:

Seq.	Name	SSID	Traffic Mode	Security Mode	Schedule	Data Encryption	Maximum Clients
1	DFS_323C	DFS_323C	Local Bridge	Open	Always	AES	0
2	FPC-Captive-0	fortinet	Tunnel	WPA2 Only Personal	Always	AES	0
3	FPC-Test1	FPC-Test1	Tunnel	WPA2 Only Personal	Always	AES	0
4	FPC-Test2	FPC-Test2	Tunnel	WPA2 Only Personal	Always	AES	0
5	S311_DFS	S311S_DFS_VAP	Local Bridge	Open	Always	AES	0
6	wifi	fpc_test	Tunnel	WPA2 Only Personal	Always	AES	0

Add an SSID

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

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*.

Update an SSID

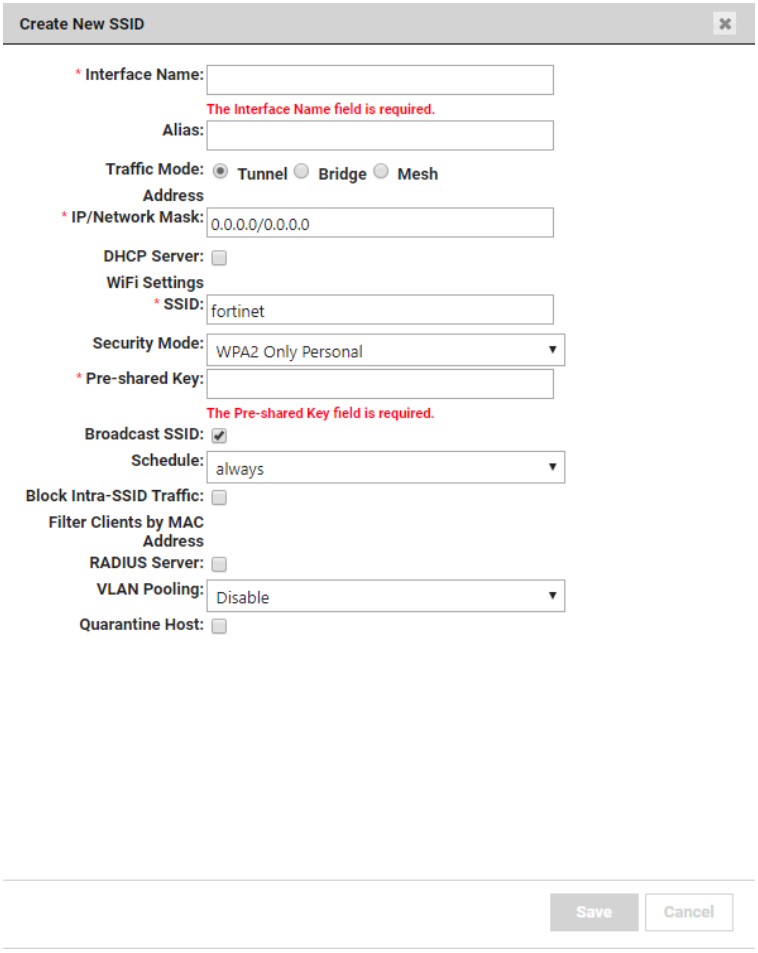
To edit an SSID, you must have read-only or read-write permission for DHCP.

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

Delete an SSID

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

SSID fields



The Create New SSID and Edit SSID forms 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: *Tunnel*—Data for WLAN passes through WiFi Controller. This is the default. *Bridge*—FortiAP unit Ethernet and WiFi interfaces are bridged. *Mesh*—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.

Settings	Guidelines
DHCP Server	If you selected the Tunnel traffic mode, you can select *DHCP Server* to assign IP addresses to clients. If you select *DHCP Server*, right-click in the Addrss Range table and select *Create New* to define the IP address range for a DHCP server on the FortiPortal unit. You also need to enter the netmask if you select *DHCP Server*.
SSID	Enter the SSID. By default, this field contains `fortinet`.
Security Mode	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. *Captive Portal*—authenticates users through a customizable web page. *WPA2 Only Personal*—WPA2 is WiFi Protected Access version 2. There is one pre-shared key (password) that all users use. *WPA2 Only Enterprise*—similar to WPA2 Only Personal but is best used for enterprise networks. Each user is separately authenticated by user name and password.
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 *always* or *none*.
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	In an SSID, you can define a VLAN pool. As clients associate to an AP, they are assigned to a VLAN. If you selected the Tunnel or Bridge traffic mode, select one of the following options: *Disable*—This option is selected by default and no VLAN pools are used. *Managed AP Group*—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. *Round Robin*—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. *Hash*—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.

Settings	Guidelines
Quarantine Host	Enable this option to quarantine devices that are connected in Tunnel traffic mode.

FORTINET

High Performance Network Security