FORTINET®

High Performance Network Security

FortiPortal User Guide

Version 4.1.0

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

FORTINET®

September 20, 2017

FortiPortal User Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-09-20	FortiPortal 4.1.0 initial release

FortiPortal Web Interface

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

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

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 top banner includes the main menu, which contains the following selections:

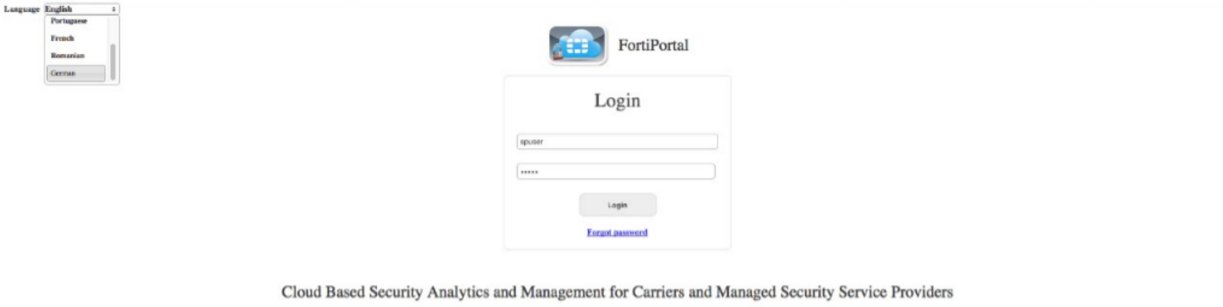
- **Dashboard** - widgets that display information about the FortiPortal (FP)
- **Policy & Objects** - pages for viewing and modifying security policy, firewall objects and security profiles
- **View** - different views of the security event logs
- **Wireless Networks** - wireless networks, listed by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

The top banner also displays your storage usage, including the storage limit allocated and the actual amount of storage currently in use.

Landing Page

When you open FortiPortal to login into the system, you see the following default landing page.

NOTE: With FortiPortal Version 3.2.1, you can now select German from this page.



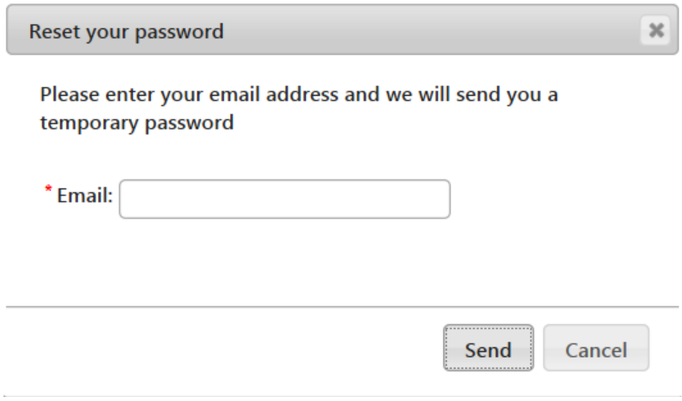
spuser

*****

Cloud Based Security Analytics and Management for Carriers and Managed Security Service Providers

Reset Password

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



Reset your password

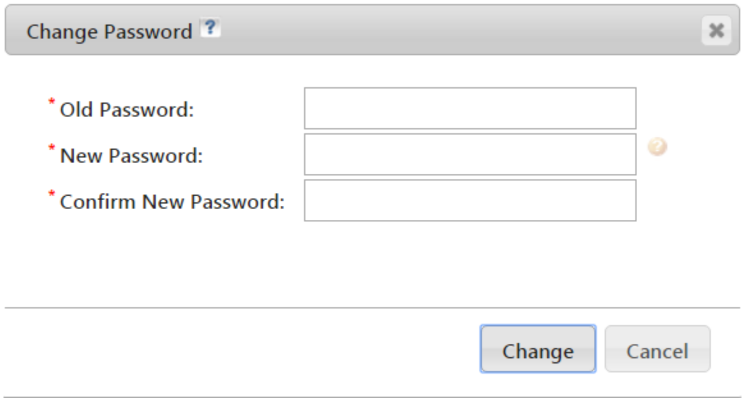
Please enter your email address and we will send you a temporary password

* Email:

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

Change Password

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



Change Password ?

* Old Password:

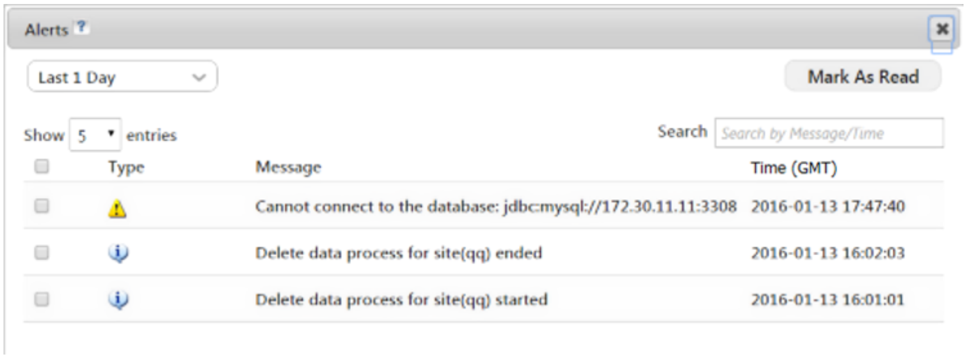
* New Password:

* Confirm New Password:

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

Alerts

Clicking the Alert icon displays a list of unread alerts:



□	Type	Message	Time (GMT)
□	⚠	Cannot connect to the database: jdbc:mysql://172.30.11.11:3308	2016-01-13 17:47:40
□	ℹ	Delete data process for site(qq) ended	2016-01-13 16:02:03
□	ℹ	Delete data process for site(qq) started	2016-01-13 16:01:01

For each alert, the page displays the following

- **Type** - severity of the alert (Informational or Warning)
- **Message** - text summary of the alert
- **Time** - time the alert was raised (displayed for GMT time zone).

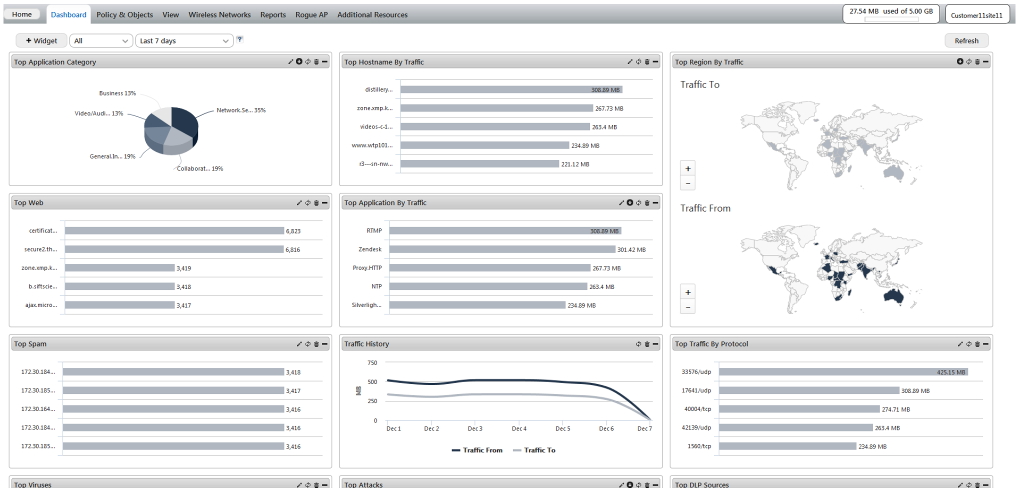
Page Actions

The Alerts page contains the following actions:

- **Filter** - filter the data (Last 60 Minutes, Last 1 day, Last 1 week)
- **Search** - enter text to search for alerts containing that text
- **Show *x* Entries** - use the drop-down selector to set the number of entries to display
- **Select** - select individual alerts, or select all alerts (select box in the column header)
- **Mark as Read** - mark selected alerts as read

Dashboard

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



As you can see, the dashboard is organized as a set of widgets The default widgets include the following:

- 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

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 (Mbps)
- Max Client Count (Wireless)
- Top 5 SSIDs by Traffic (Wireless)
- FAP Summary

The following widgets are associated with the sandbox:

- Sandbox Scanning Statistics
- Top Sandbox Hosts

- Top Sandbox Malware
- Sandbox Scanning Statistics Graphs

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 hour, last day, last 7 days, or a custom filter)
- **Refresh** - refresh the data

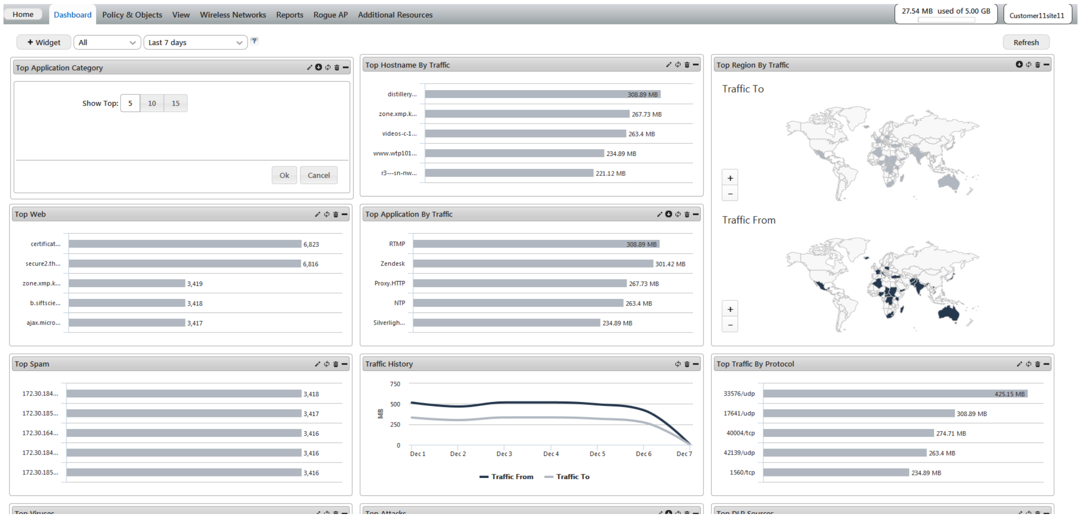
Widget Actions

The top banner on each widget provides some or all of the following controls:

- **Edit Settings** - edit the widge
- **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

Edit Widget

Clicking the Edit Settings icon opens a window within the widget that enables you to select the top N entries:

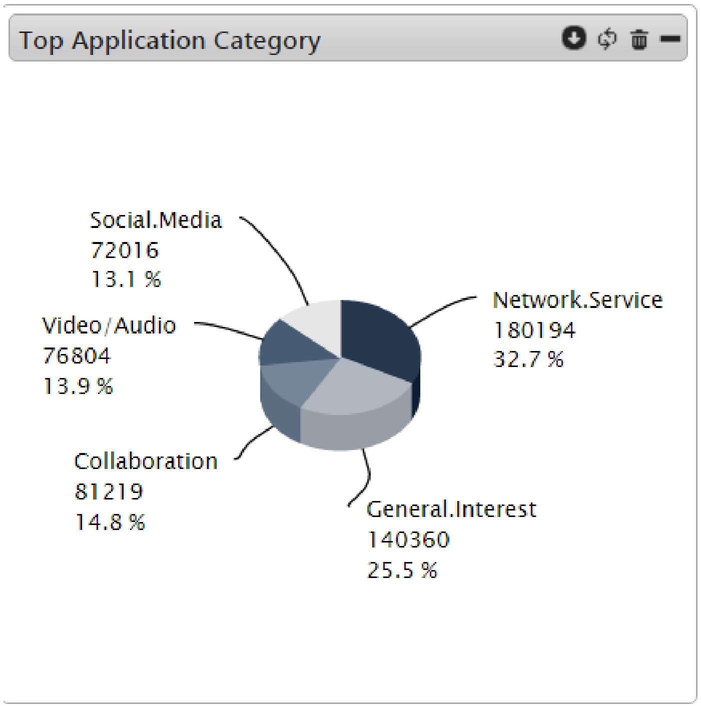


Drill-down Widget

The following widgets support the drill-down capability:

- Top Application Category
- Top Region by Traffic
- Top Application By Traffic
- Top Attacks

Each of these widgets displays a graph or bar chart with the top 5 results, where the result is an application, region, traffic, or attack (depending on the widget). When you click on one of the results, the Application view 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).

The View

This 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.

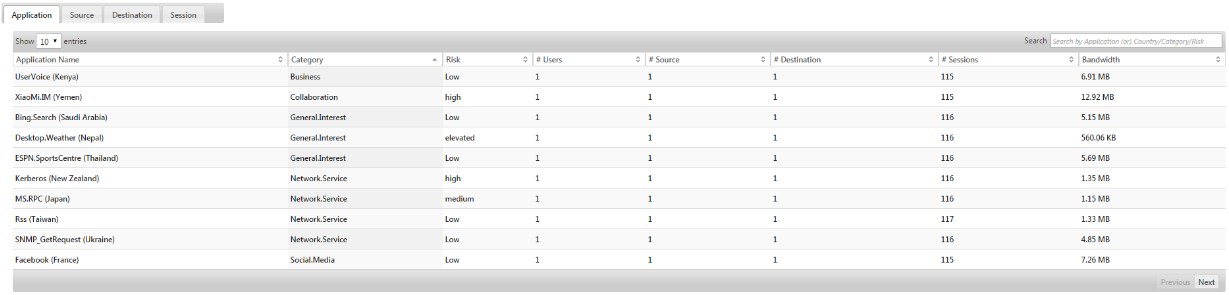
The table header provides a drop-down menu for selecting the number of entries to display. The header also includes a search box, enabling you to search for the text in the following fields: User, Source, Source Information (Src.Inf), Destination, Destination Information (Dst.Inf) and Application.

The following tabs provide different views of the data:

- **Source** - arranged by the source FortiGate device
- **Destination -** arranged by the destination (IP address, protocol, port)
- **Session** - arranged by session (i.e., a specific flow of packets between a source and destination). This tab is visible only when you have selected the Application view.

Application View

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

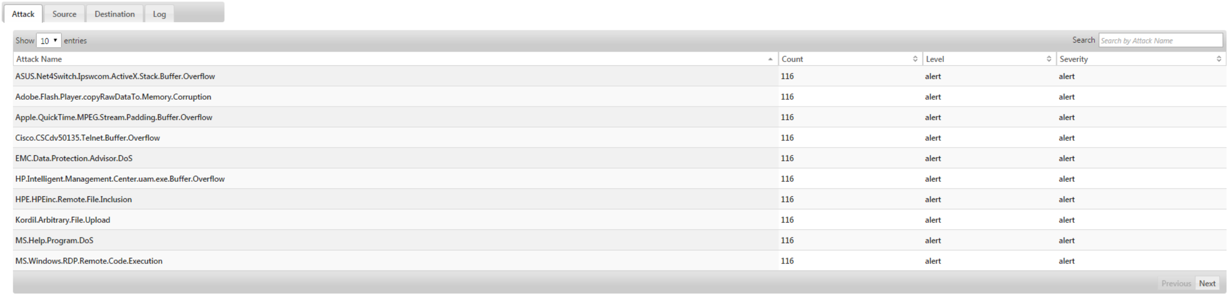


Application Name	Category	Risk	# Users	# Source	# Destination	# Sessions	Bandwidth
UserVoice (Kenya)	Business	Low	1	1	1	115	6.91 MB
XiaoMi.IM (Yemen)	Collaboration	high	1	1	1	115	12.92 MB
Bing.Search (Saudi Arabia)	General.Interest	Low	1	1	1	116	5.15 MB
Desktop.Weather (Nepal)	General.Interest	elevated	1	1	1	116	560.06 KB
ESPN.SportsCentre (Thailand)	General.Interest	Low	1	1	1	116	5.69 MB
Kerberos (New Zealand)	Network.Service	high	1	1	1	116	1.35 MB
MS.RPC (Japan)	Network.Service	medium	1	1	1	116	1.15 MB
Rss (Taiwan)	Network.Service	Low	1	1	1	117	1.33 MB
SNMP_GetRequest (Ukraine)	Network.Service	Low	1	1	1	116	4.85 MB
Facebook (France)	Social.Media	Low	1	1	1	115	7.26 MB

Note the name (in brackets).

Attack View

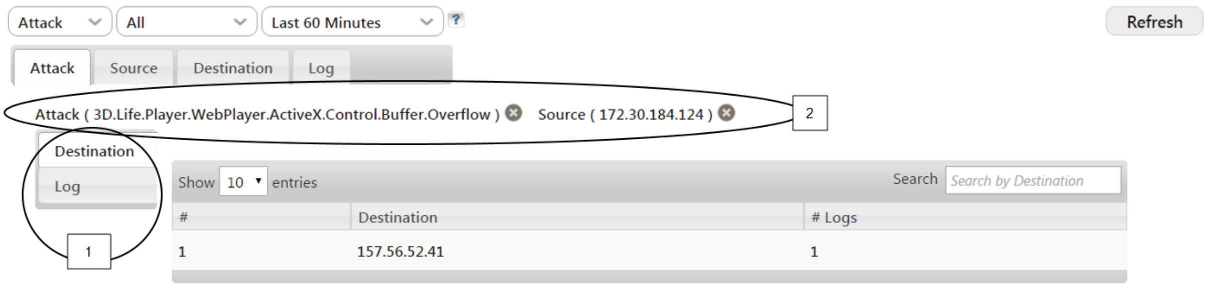
The **Attack** tab under **View** displays event logs grouped by "attack:"



Show 10 entries

Attack Name	Count	Level	Severity
ASUS.Net4Switch.Ipswcom.ActiveX.Stack.Buffer.Overflow	116	alert	alert
Adobe.Flash.Player.copyRawDataTo.Memory.Corruption	116	alert	alert
Apple.QuickTime.MPEG.Stream.Padding.Buffer.Overflow	116	alert	alert
Cisco.CSCdv50135.Telnet.Buffer.Overflow	116	alert	alert
EMC.Data.Protection.Advisor.DoS	116	alert	alert
HP.Intelligent.Management.Center.uam.exe.Buffer.Overflow	116	alert	alert
HPE.HPEinc.Remote.File.Inclusion	116	alert	alert
Kordil.Arbitrary.File.Upload	116	alert	alert
MS.Help.Program.DoS	116	alert	alert
MS.Windows.RDP.Remote.Code.Execution	116	alert	alert

When you click 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 **circle 1** below):



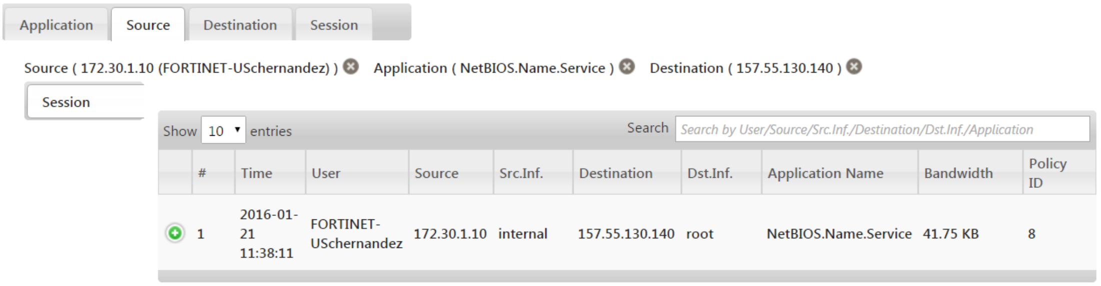
Attack (3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Overflow) ⊗ Source (172.30.184.124) ⊗

Show 10 entries

#	Destination	# Logs
1	157.56.52.41	1

The applied filters are listed across the display (**ellipse 2** in the preceding figure). Click the grey **x** button beside each filter to remove that filter.

If you click an individual log entry, the system displays its details:


Application
Source
Destination
Session
Session
Search
Search by User/Source/Src.Inf./Destination/Dst.Inf./Application

Source (172.30.1.10 (FORTINET-USchernandez)) ⊗ Application (NetBIOS.Name.Service) ⊗ Destination (157.55.130.140) ⊗

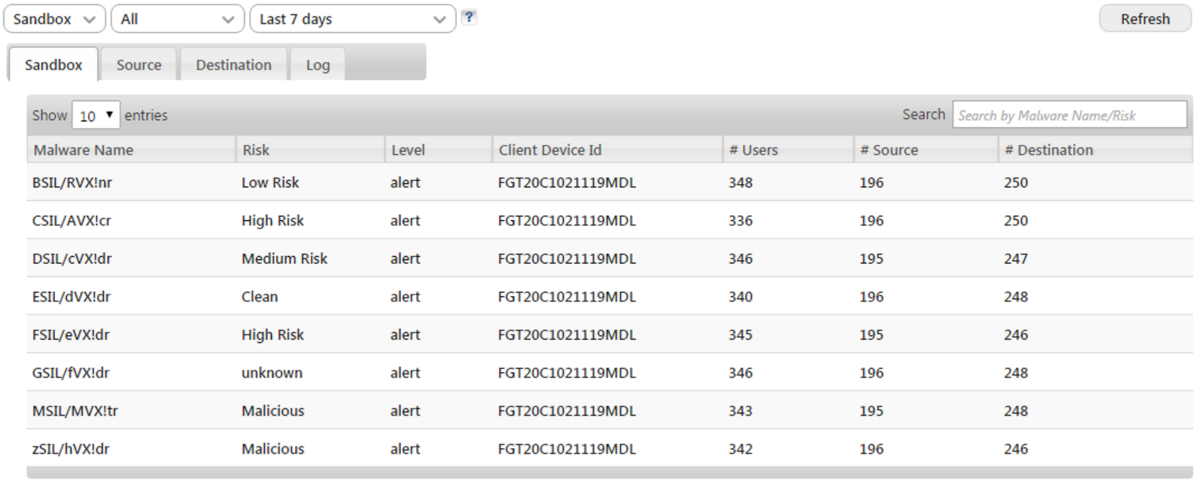
Show 10 entries

	#	Time	User	Source	Src.Inf.	Destination	Dst.Inf.	Application Name	Bandwidth	Policy ID
⊕	1	2016-01-21 11:38:11	FORTINET-USchernandez	172.30.1.10	internal	157.55.130.140	root	NetBIOS.Name.Service	41.75 KB	8

To the left of the 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:"



Malware Name	Risk	Level	Client Device Id	# Users	# Source	# Destination
BSIL/RVX!nr	Low Risk	alert	FGT20C1021119MDL	348	196	250
CSIL/AVX!cr	High Risk	alert	FGT20C1021119MDL	336	196	250
DSIL/cVX!dr	Medium Risk	alert	FGT20C1021119MDL	346	195	247
ESIL/dVX!dr	Clean	alert	FGT20C1021119MDL	340	196	248
FSIL/eVX!dr	High Risk	alert	FGT20C1021119MDL	345	195	246
GSIL/fVX!dr	unknown	alert	FGT20C1021119MDL	346	196	248
MSIL/MVX!tr	Malicious	alert	FGT20C1021119MDL	343	195	248
zSIL/hVX!dr	Malicious	alert	FGT20C1021119MDL	342	196	246

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

When you click 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. Click the grey **x** button beside each to remove that filter.

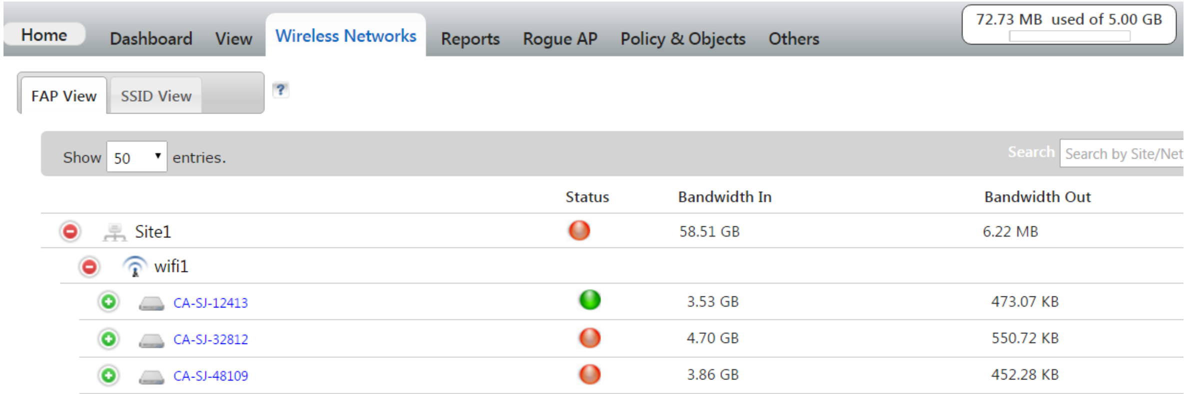
If you click an individual log entry, the system displays the details of that entry.

Wireless Networks

This tab displays information about the wireless networks.

You can select from two views, Fortinet Access Points (FAP) and SSID, which present the same information grouped in different ways:

- **FAP View** - displays the SSIDs for each FAP at each site (see the following figure)
- **SSID View** - displays the FAPs for each site for each SSID



Show 50 entries.

	Status	Bandwidth In	Bandwidth Out
Site1	🔴	58.51 GB	6.22 MB
wifi1			
CA-SJ-12413	🟢	3.53 GB	473.07 KB
CA-SJ-32812	🔴	4.70 GB	550.72 KB
CA-SJ-48109	🔴	3.86 GB	452.28 KB

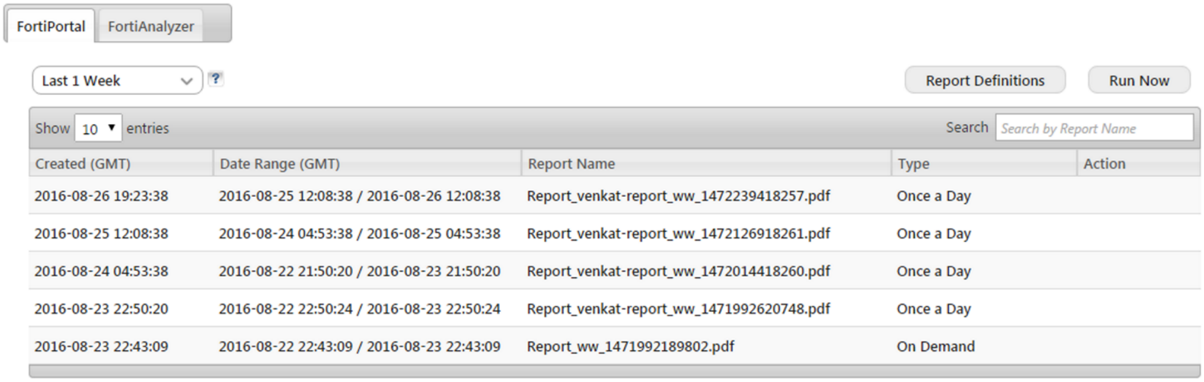
Clicking the green **+** button adjacent to an entry expands the entry and shows the next level of data. Click a red button to hide the data for an entry.

If you click on 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.

Reports

This tab displays a list of available FortiPortal or FortiAnalyzer reports:



Created (GMT)	Date Range (GMT)	Report Name	Type	Action
2016-08-26 19:23:38	2016-08-25 12:08:38 / 2016-08-26 12:08:38	Report_venkat-report_ww_1472239418257.pdf	Once a Day	
2016-08-25 12:08:38	2016-08-24 04:53:38 / 2016-08-25 04:53:38	Report_venkat-report_ww_1472126918261.pdf	Once a Day	
2016-08-24 04:53:38	2016-08-22 21:50:20 / 2016-08-23 21:50:20	Report_venkat-report_ww_1472014418260.pdf	Once a Day	
2016-08-23 22:50:20	2016-08-22 22:50:24 / 2016-08-23 22:50:24	Report_venkat-report_ww_1471992620748.pdf	Once a Day	
2016-08-23 22:43:09	2016-08-22 22:43:09 / 2016-08-23 22:43:09	Report_ww_1471992189802.pdf	On Demand	

FortiPortal Reports

The FortiPortal reports page includes the following actions:

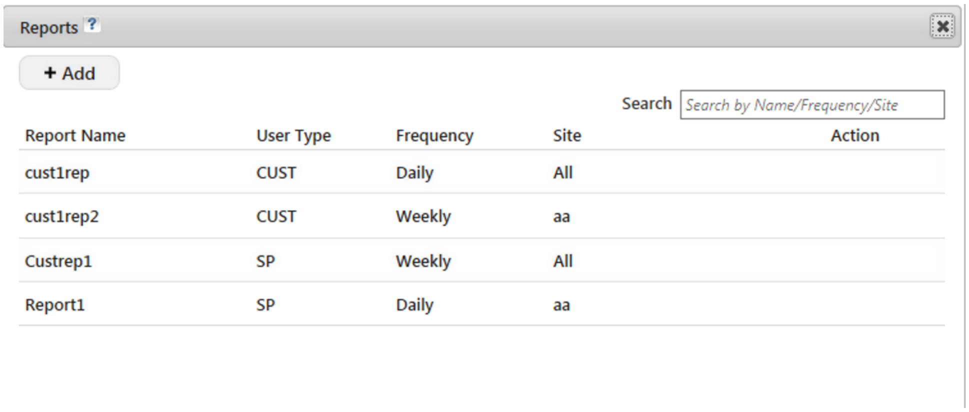
- **Set Filter** - filter the data (today, last 1 day, last 1 week, last 1 month, or customize a filter)
- **Report Definitions** - opens a pop-up window that lists the available reports
- **Run Now** - opens a pop-up window with a form to specify the report to be run
- **Search** - text search by report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



Report Name	User Type	Frequency	Site	Action
cust1rep	CUST	Daily	All	
cust1rep2	CUST	Weekly	aa	
Custrep1	SP	Weekly	All	
Report1	SP	Daily	aa	

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

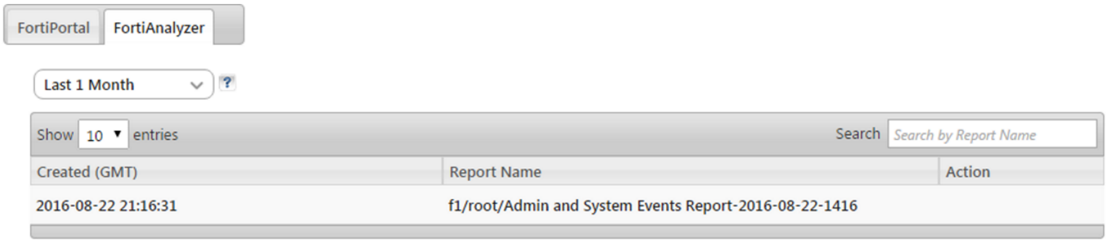
The Add Report and Edit Report forms contain the following selections:

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

Settings	Guidelines
From Email	Email address from which the report will be sent
Email Text	Text for the body of the email

FortiAnalyzer Reports

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



Created (GMT)	Report Name	Action
2016-08-22 21:16:31	f1/root/Admin and System Events Report-2016-08-22-1416	

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:

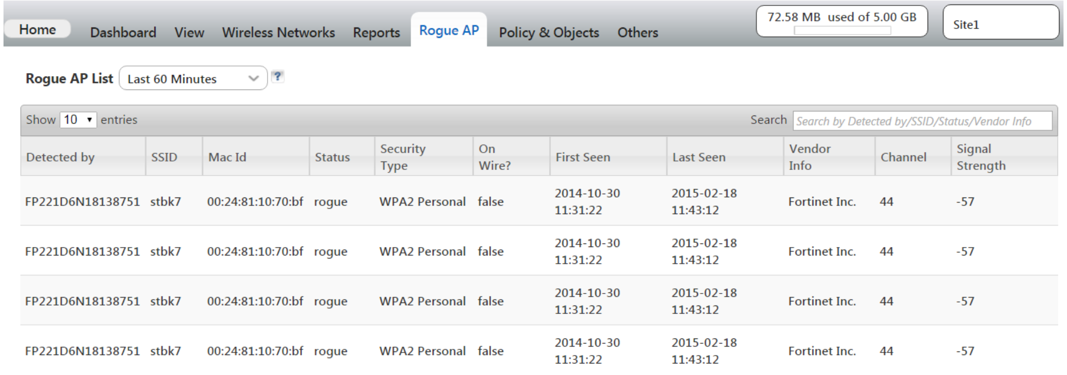
- **Download** - downloads the selected report as a PDF file

Rogue AP

This tab displays a list of rogue access points detected on the network and contains the following actions

- **Set Filter** - 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 the fields: Detected by, SSID, Status, Vendor information

The following figure shows the Rogue AP page:



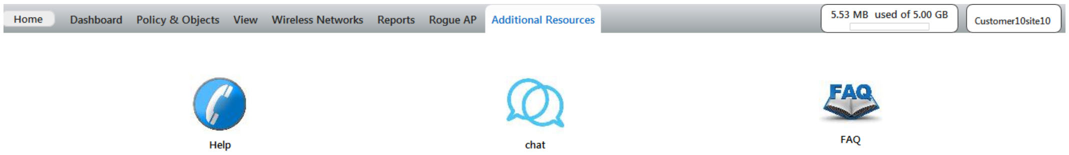
Rogue AP List Last 60 Minutes

Show 10 entries

Detected by	SSID	Mac Id	Status	Security Type	On Wire?	First Seen	Last Seen	Vendor Info	Channel	Signal Strength
FP221D6N18138751	stbk7	00:24:81:10:70:bf	rogue	WPA2 Personal	false	2014-10-30 11:31:22	2015-02-18 11:43:12	Fortinet Inc.	44	-57
FP221D6N18138751	stbk7	00:24:81:10:70:bf	rogue	WPA2 Personal	false	2014-10-30 11:31:22	2015-02-18 11:43:12	Fortinet Inc.	44	-57
FP221D6N18138751	stbk7	00:24:81:10:70:bf	rogue	WPA2 Personal	false	2014-10-30 11:31:22	2015-02-18 11:43:12	Fortinet Inc.	44	-57
FP221D6N18138751	stbk7	00:24:81:10:70:bf	rogue	WPA2 Personal	false	2014-10-30 11:31:22	2015-02-18 11:43:12	Fortinet Inc.	44	-57

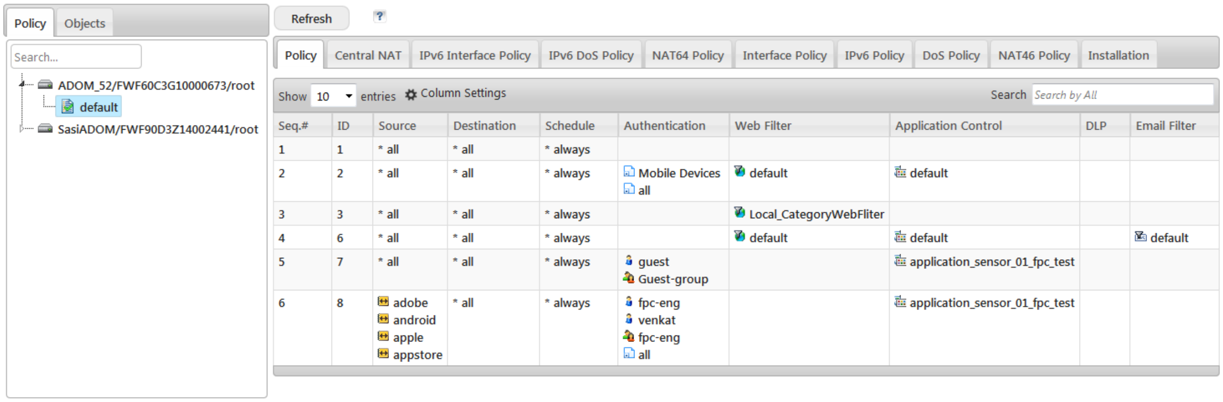
Additional Resources

This tab displays Help, Chat and FAQ buttons. If active, the button's text and image are clickable and open a new tab with the given URL. If disabled, the button's text and image are unclickable.



Policy

This tab under **Policy & Objects** provides 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.



Seq.#	ID	Source	Destination	Schedule	Authentication	Web Filter	Application Control	DLP	Email Filter
1	1	* all	* all	* always					
2	2	* all	* all	* always	Mobile Devices all	default	default		
3	3	* all	* all	* always		Local_CategoryWebFliter			
4	6	* all	* all	* always		default	default		default
5	7	* all	* all	* always	guest Guest-group		application_sensor_01_fpc_test		
6	8	adobe android apple appstore	* all	* always	fpc-eng venkat fpc-eng all		application_sensor_01_fpc_test		

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. Click the **Column Settings** button to display the Column Settings form.
2. Check the columns you want to display, un-check the columns that you want to hide, and click **Apply**.

Policy Data Refresh

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

Revision Backup

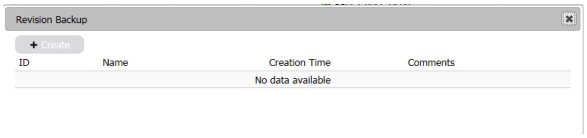
The system can save only one revision of the current policy and object data. The new revision overwrites the existing backup (if one exists).

Observe the following restrictions:

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

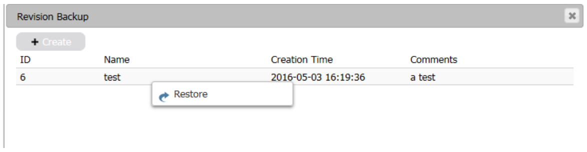
Creating and Restoring Policy Revisions

Click the **Revision Backup** button to open the Revision Backup window:



ID	Name	Creation Time	Comments
No data available			

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



ID	Name	Creation Time	Comments
6	test	2016-05-03 16:19:36	a test

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

Configuring 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 click **Save**.

Updating a Policy

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

Deleting a Policy

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

Enabling or Disabling a Policy

1. 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.

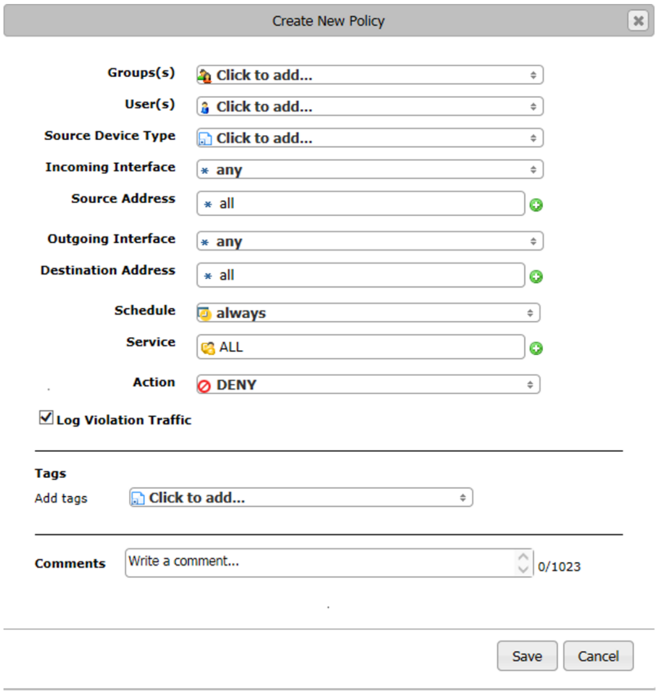
Policy Fields

The add/edit policy form contains the following fields (see the figure after the table for an example form):

Settings	Guidelines
Policy Subtype	Address or User Identity
Incoming Interface	Select one or more interfaces from the drop-down list.
Source Address	Click to add one or more address objects.
Outgoing Interface	Select one or more interfaces from the drop-down list.
Destination Address	Click 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.
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.
Additional field becomes visible if the action is set to Deny	
Log Violation Traffic	Click this checkbox to create a log for each denied packet.
Additional fields become visible if the action is set to Accept	
NAT	
Use Destination Interface Address	Select to use the destination interface address. This setting is enabled by default. Optionally, enable Fixed Port.
Dynamic IP Pool	If you check this option, specify the IP pool to use.
Use Central NAT Table	Uses the central NAT table for source IP mapping.
Logging Options	**Logging Options**
No Log	No log is generated.
Log Security Events	Creates a log for each security event.

Settings	Guidelines
Log All Sessions	Logs all sessions. Requires extensive system resources and storage space.
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.
Traffic Shaping	Apply traffic shaping to this traffic. The amount of shaping applied depends on the traffic priority that you configure (Guarenteed, 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.

The following figure shows the Create New Policy form:



Create New Policy

Groups(s)	Click to add...
User(s)	Click to add...
Source Device Type	Click to add...
Incoming Interface	any
Source Address	all
Outgoing Interface	any
Destination Address	all
Schedule	always
Service	ALL
Action	DENY

☑ Log Violation Traffic

Tags

Add tags: Click to add...

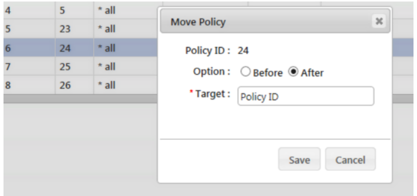
Comments: Write a comment... 0/1023

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.



4	5	* all
5	23	* all
6	24	* all
7	25	* all
8	26	* all

Policy ID : 24

Option : ○ Before ● After

* Target : Policy ID

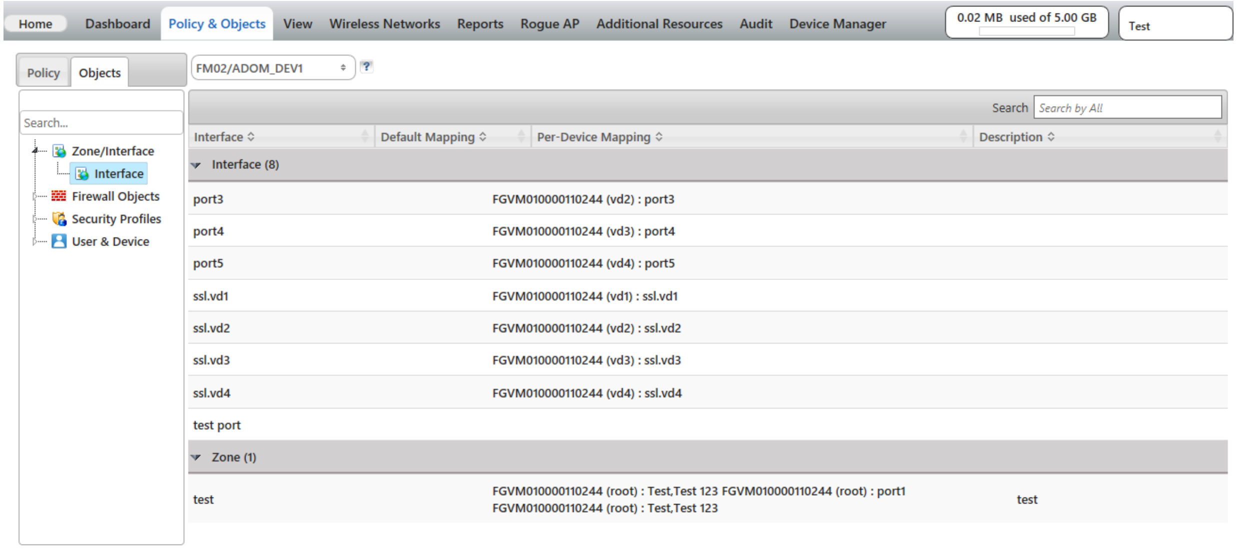
Re-installing the Policy

After you add or change a policy, click **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.

Objects

This tab under **Policy & Objects** 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.



Interface	Default Mapping	Per-Device Mapping	Description
Interface (8)			
port3		FGVM010000110244 (vd2) : port3	
port4		FGVM010000110244 (vd3) : port4	
port5		FGVM010000110244 (vd4) : port5	
ssl.vd1		FGVM010000110244 (vd1) : ssl.vd1	
ssl.vd2		FGVM010000110244 (vd2) : ssl.vd2	
ssl.vd3		FGVM010000110244 (vd3) : ssl.vd3	
ssl.vd4		FGVM010000110244 (vd4) : ssl.vd4	
test port			
Zone (1)			
test		FGVM010000110244 (root) : Test,Test 123 FGVM010000110244 (root) : port1 FGVM010000110244 (root) : Test,Test 123	test

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 choose a different ADOM using the pull-down selector above the main panel.

Types of Objects

The page displays the following object categories:

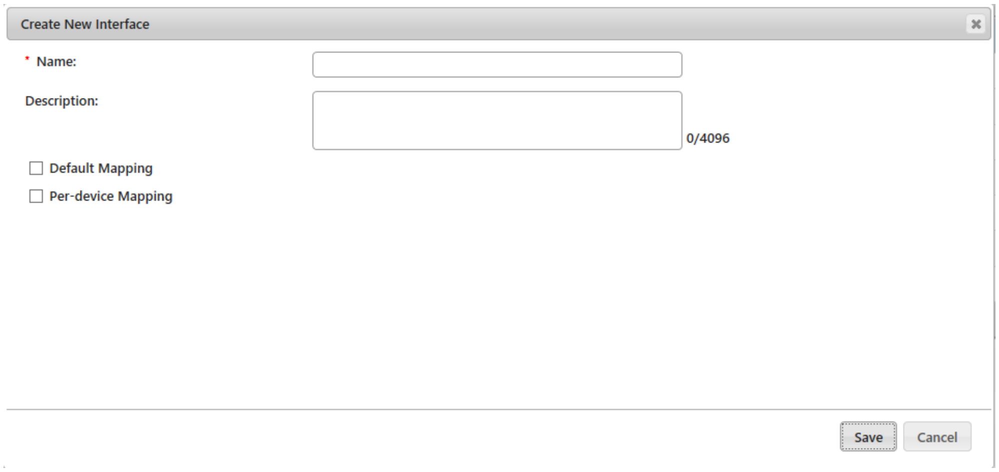
- Zone/Interface
- Firewall Objects
- Security Profiles
- User & Device

These objects are described in the following sections.

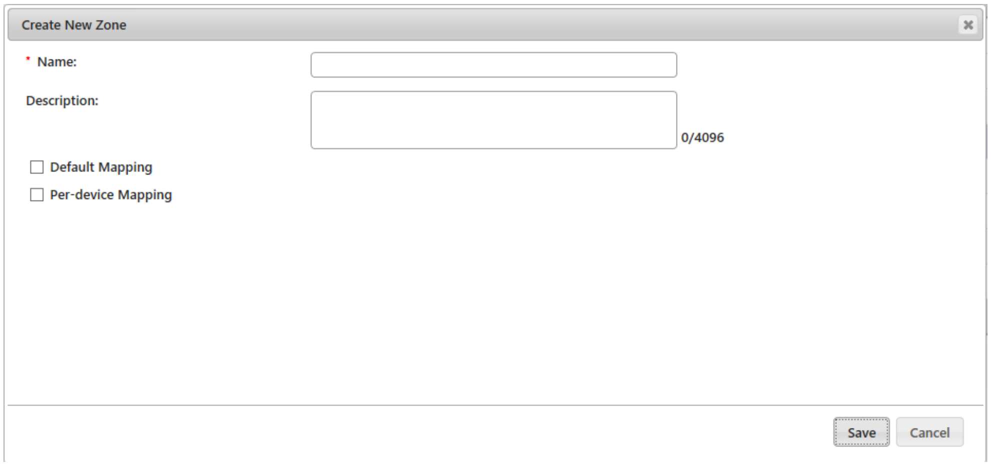
Zone/Interface

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 5.6 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):

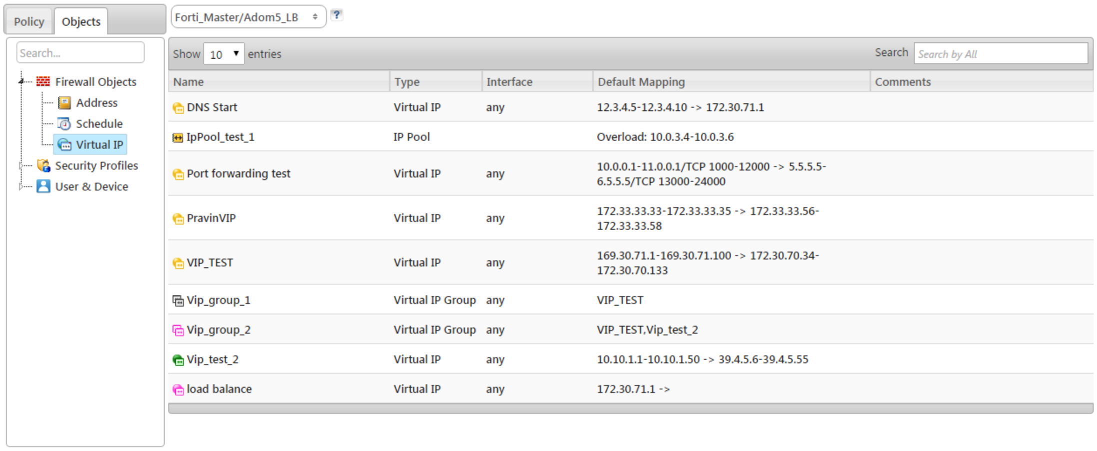
- **IP -** IP protocol number
- **TCP/UDP/SCP -** source and destination port range

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:



Name	Type	Interface	Default Mapping	Comments
DNS Start	Virtual IP	any	12.3.4.5-12.3.4.10 -> 172.30.71.1	
IpPool_test_1	IP Pool		Overload: 10.0.3.4-10.0.3.6	
Port forwarding test	Virtual IP	any	10.0.0.1-11.0.0.1/TCP 1000-12000 -> 5.5.5.5-6.5.5.5/TCP 13000-24000	
PravinVIP	Virtual IP	any	172.33.33.33-172.33.33.35 -> 172.33.33.56-172.33.33.58	
VIP_TEST	Virtual IP	any	169.30.71.1-169.30.71.100 -> 172.30.70.34-172.30.70.133	
Vip_group_1	Virtual IP Group	any	VIP_TEST	
Vip_group_2	Virtual IP Group	any	VIP_TEST,Vip_test_2	
Vip_test_2	Virtual IP	any	10.10.1.1-10.10.1.50 -> 39.4.5.6-39.4.5.55	
load balance	Virtual IP	any	172.30.71.1 ->	

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 an FPC:

- Antivirus Profile
- Application Sensor
- Data Leak Prevention Sensor
- Email Filter Profile
- IPS Sensor
- Web Filter Profile

- Local Category
- Rating Overrides

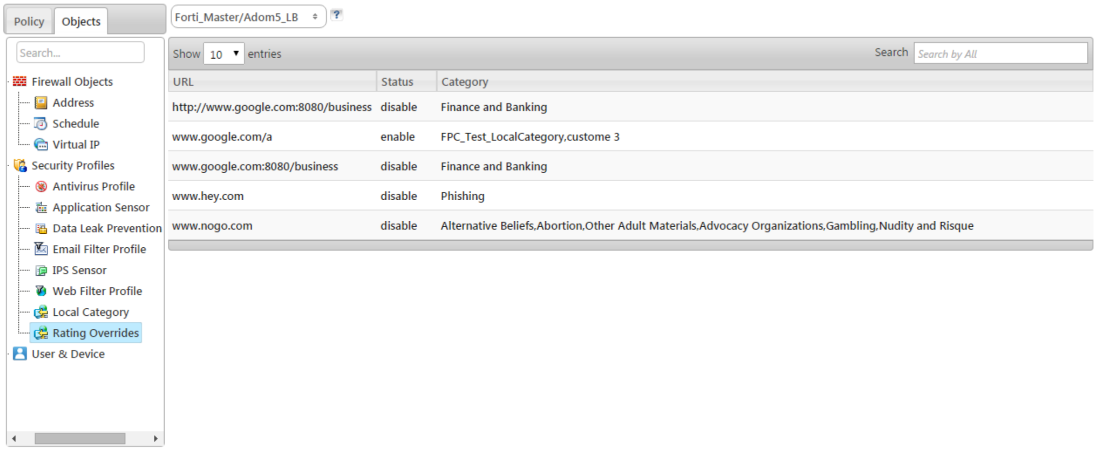
Local Category (security profile introduced with FPC 1.2.0)

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

Rating Overrides (security profile introduced with FPC 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:



URL	Status	Category
http://www.google.com:8080/business	disable	Finance and Banking
www.google.com/a	enable	FPC_Test_LocalCategory,custome 3
www.google.com:8080/business	disable	Finance and Banking
www.hey.com	disable	Phishing
www.nogo.com	disable	Alternative Beliefs,Abortion,Other Adult Materials,Advocacy Organizations,Gambling,Nudity and Risque

User & Device

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

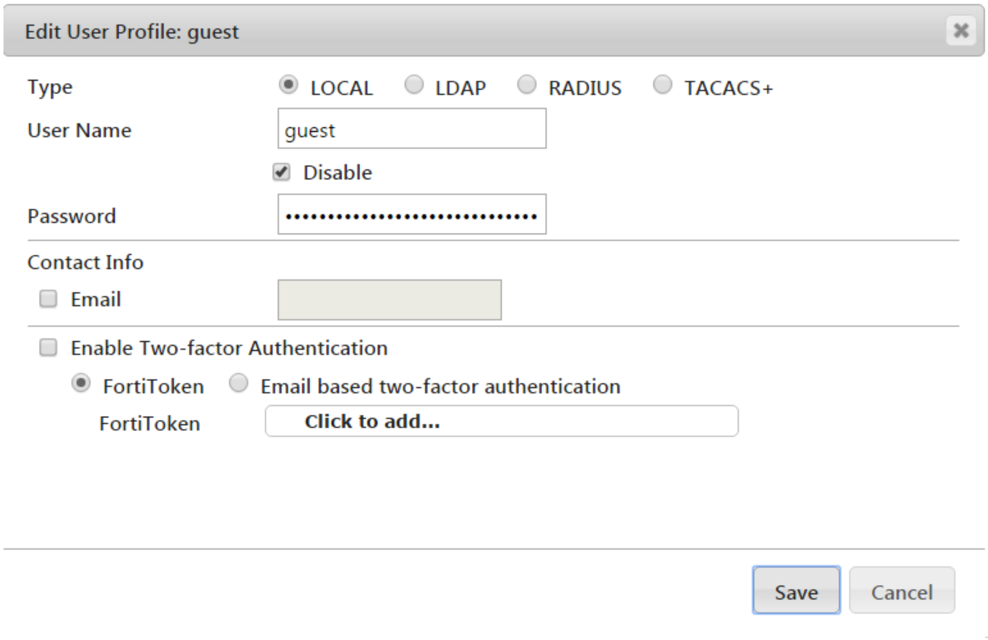
For additional information about users and user groups, refer to FortiOS Handbook: Authentication.

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.

You can also enable two-factor authentication using FortiAuthenticator.

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



Edit User Profile: guest

Type ● LOCAL ○ LDAP ○ RADIUS ○ TACACS+

User Name: guest

☑ Disable

Password: ••••••••••••••••••••••••••••••

Contact Info

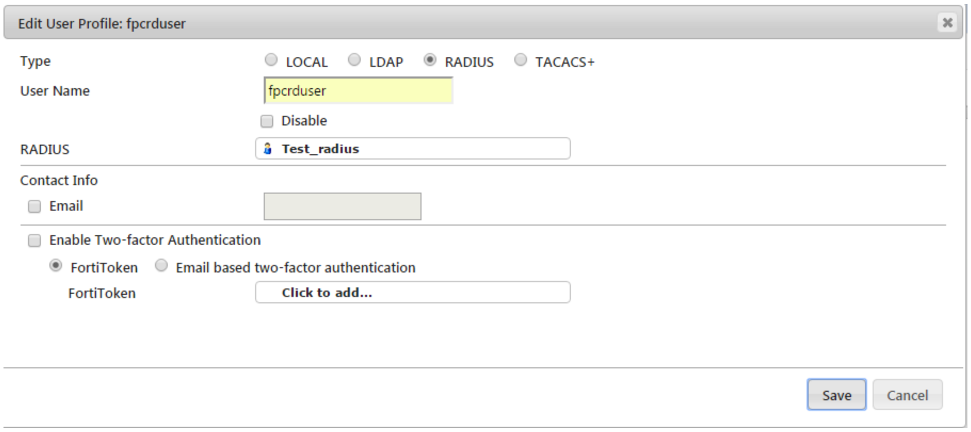
□ Email

□ Enable Two-factor Authentication

● FortiToken ○ Email based two-factor authentication

FortiToken: Click to add...

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



Edit User Profile: fpcrduser

Type ○ LOCAL ○ LDAP ● RADIUS ○ TACACS+

User Name: fpcrduser

□ Disable

RADIUS: Test_radius

Contact Info

□ Email

□ Enable Two-factor Authentication

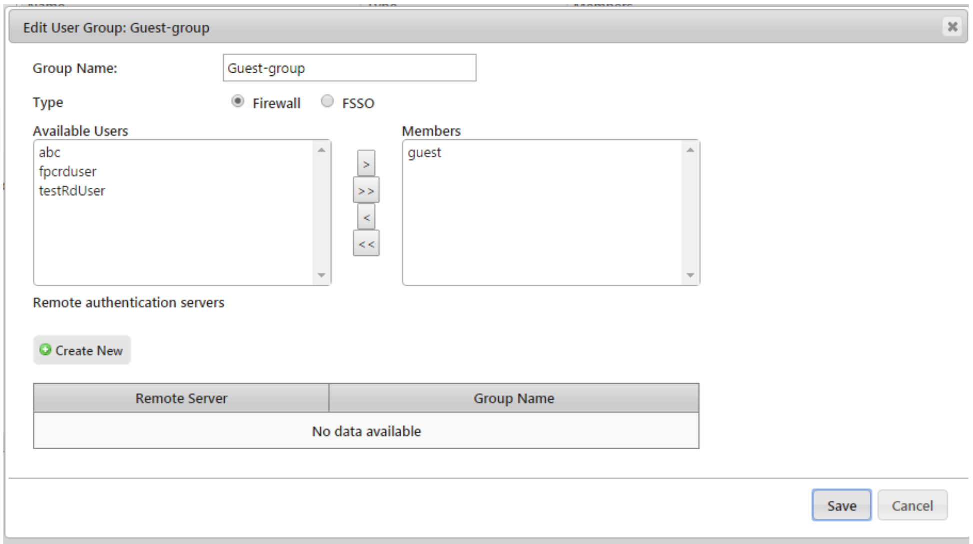
● FortiToken ○ Email based two-factor authentication

FortiToken: Click to add...

User Group

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

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



Edit User Group: Guest-group

Group Name: Guest-group

Type ● Firewall ○ FSSO

Available Users: abc, fpcrduser, testRdUser

Members: guest

Remote authentication servers

Remote Server	Group Name
No data available	

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 click **Save**.

Updating an Object

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

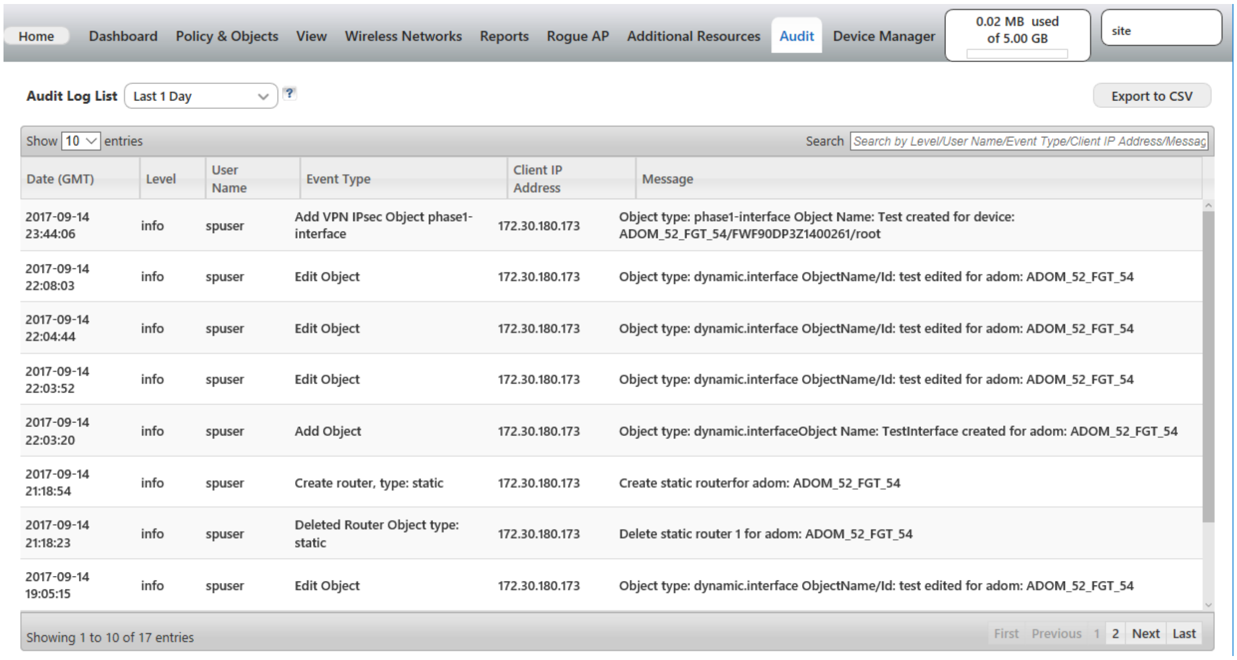
Deleting an Object

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

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

Audit

The Audit tab displays an log of user activity on the Administrative Web Interface:



Audit Log List: Last 1 Day

Show 10 entries

Search: Search by Level/User Name/Event Type/Client IP Address/Messag

Date (GMT)	Level	User Name	Event Type	Client IP Address	Message
2017-09-14 23:44:06	info	spuser	Add VPN IPsec Object phase1-interface	172.30.180.173	Object type: phase1-interface Object Name: Test created for device: ADOM_52_FGT_54/FWF90DP3Z1400261/root
2017-09-14 22:08:03	info	spuser	Edit Object	172.30.180.173	Object type: dynamic.interface ObjectName/Id: test edited for adom: ADOM_52_FGT_54
2017-09-14 22:04:44	info	spuser	Edit Object	172.30.180.173	Object type: dynamic.interface ObjectName/Id: test edited for adom: ADOM_52_FGT_54
2017-09-14 22:03:52	info	spuser	Edit Object	172.30.180.173	Object type: dynamic.interface ObjectName/Id: test edited for adom: ADOM_52_FGT_54
2017-09-14 22:03:20	info	spuser	Add Object	172.30.180.173	Object type: dynamic.interfaceObject Name: TestInterface created for adom: ADOM_52_FGT_54
2017-09-14 21:18:54	info	spuser	Create router, type: static	172.30.180.173	Create static routerfor adom: ADOM_52_FGT_54
2017-09-14 21:18:23	info	spuser	Deleted Router Object type: static	172.30.180.173	Delete static router 1 for adom: ADOM_52_FGT_54
2017-09-14 19:05:15	info	spuser	Edit Object	172.30.180.173	Object type: dynamic.interface ObjectName/Id: test edited for adom: ADOM_52_FGT_54

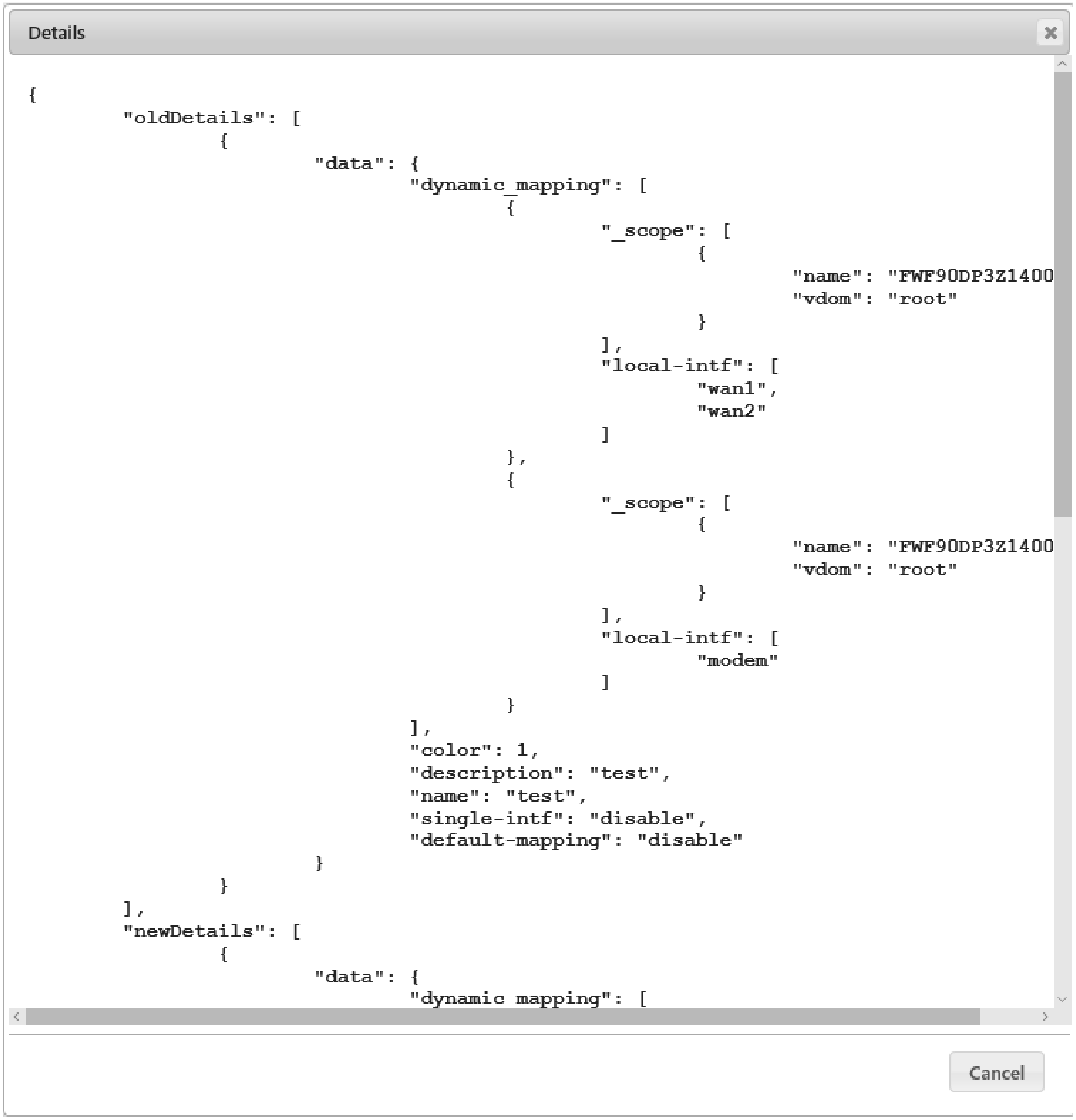
Showing 1 to 10 of 17 entries

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

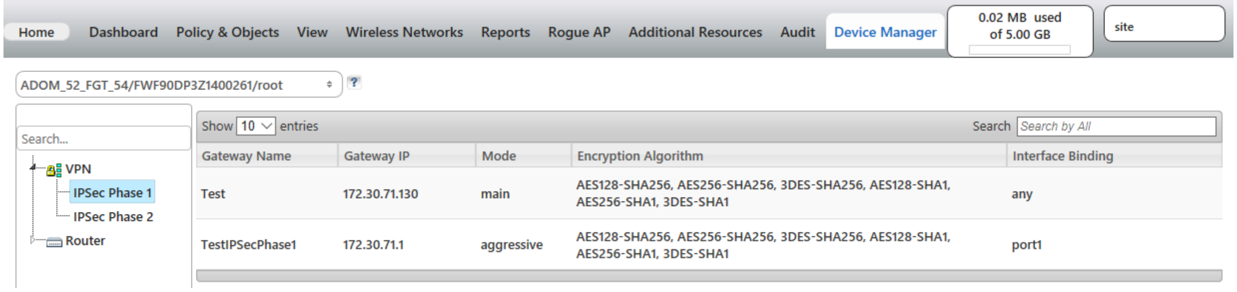
When you click the **Message** field for an **Edit Customer** audit entry, the system opens a pop-up window to display the details of the change. The details window shows the original ("oldDetails") and new ("newDetails") field values:



```
{
        "oldDetails": [
                {
                        "data": {
                                "dynamic_mapping": [
                                        {
                                                "_scope": [
                                                        {
                                                                "name": "FWF90DP3Z1400
                                                                "vdom": "root"
                                                        }
                                                ],
                                                "local-intf": [
                                                        "wan1",
                                                        "wan2"
                                                ]
                                        },
                                        {
                                                "_scope": [
                                                        {
                                                                "name": "FWF90DP3Z1400
                                                                "vdom": "root"
                                                        }
                                                ],
                                                "local-intf": [
                                                        "modem"
                                                ]
                                        }
                                ],
                                "color": 1,
                                "description": "test",
                                "name": "test",
                                "single-intf": "disable",
                                "default-mapping": "disable"
                        }
                }
        ],
        "newDetails": [
                {
                        "data": {
                                "dynamic mapping": [
```

VPNs

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



Gateway Name	Gateway IP	Mode	Encryption Algorithm	Interface Binding
Test	172.30.71.130	main	AES128-SHA256, AES256-SHA256, 3DES-SHA256, AES128-SHA1, AES256-SHA1, 3DES-SHA1	any
TestIPSecPhase1	172.30.71.1	aggressive	AES128-SHA256, AES256-SHA256, 3DES-SHA256, AES128-SHA1, AES256-SHA1, 3DES-SHA1	port1

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:

- **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 click **Save**. See "IPSec Phase-1 fields" on page 37 and "IPSec Phase-2 fields" on page 39.
4. Click **Save**.

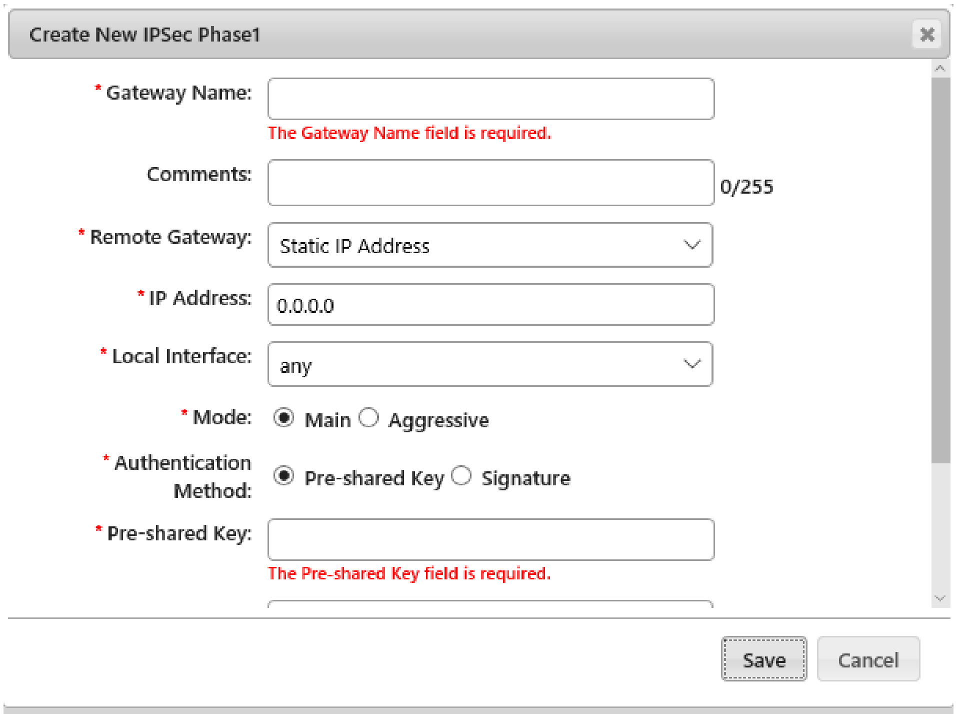
Updating an IPSec Phase-1 or Phase-2 configuration

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. Click **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



Create New IPSec Phase1

* Gateway Name:

The Gateway Name field is required.

Comments: 0/255

* Remote Gateway: Static IP Address

* IP Address: 0.0.0.0

* Local Interface: any

* Mode: ● Main ○ Aggressive

* Authentication Method: ● Pre-shared Key ○ Signature

* Pre-shared Key:

The Pre-shared Key field is required.

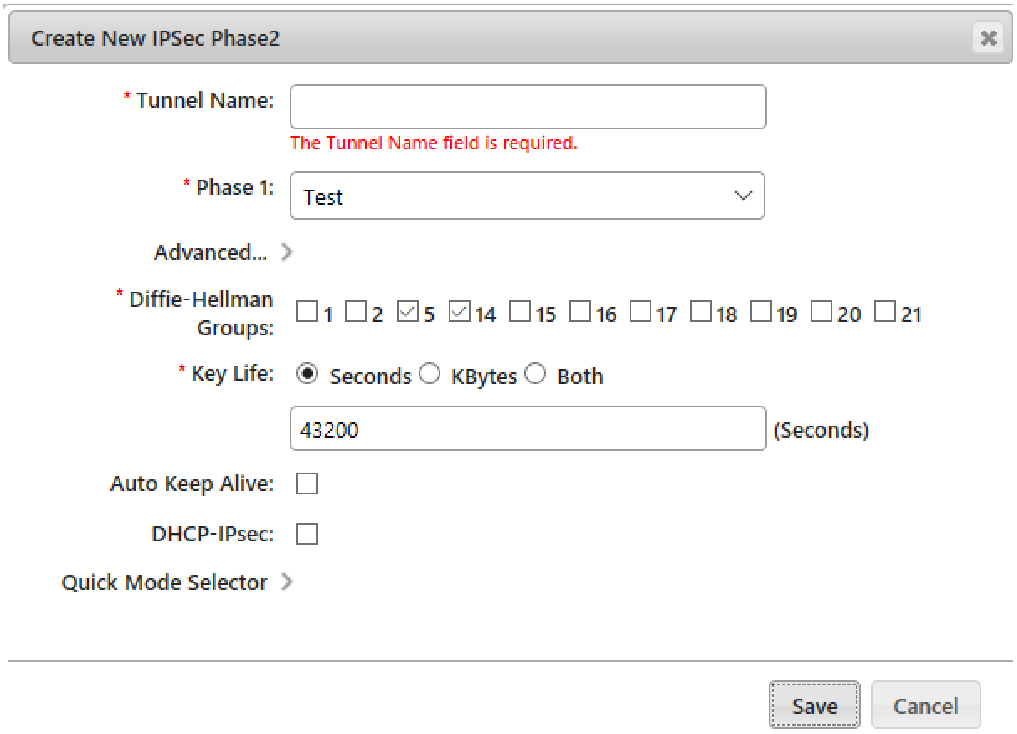
The Create New IPSec Phase1 and Edit IPSec Phase1 forms contain the following fields:

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

Settings	Guidelines
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.
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.

Settings	Guidelines
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



Create New IPSec Phase2

* Tunnel Name:	 The Tunnel Name field is required.
* Phase 1:	Test
Advanced... >	
* Diffie-Hellman Groups:	□1 □2 ☑5 ☑14 □15 □16 □17 □18 □19 □20 □21
* Key Life:	● Seconds ○ KBytes ○ Both 43200 (Seconds)
Auto Keep Alive:	□
DHCP-IPsec:	□
Quick Mode Selector >	

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

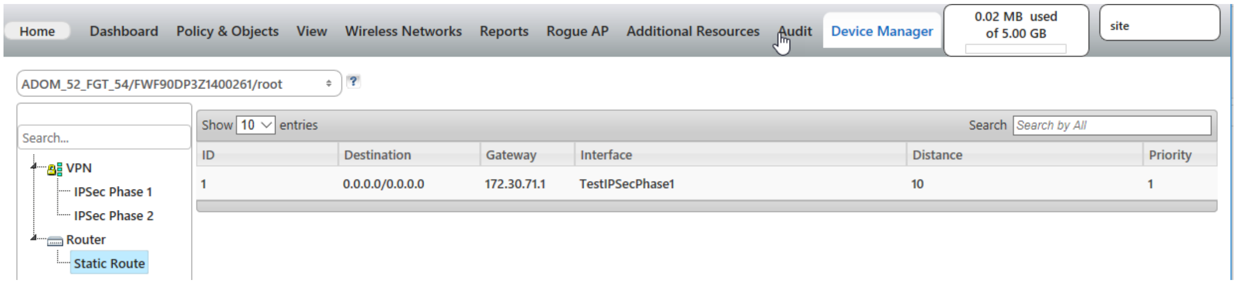
Settings	Guidelines
Tunnel Name	Required. Type a name for this Phase-2 configuration. The value is a string with a maximum of 35 characters.
Phase 1	Required. Select an IPSec Phase-1 configuration.
Advanced	

Settings	Guidelines
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	
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.

Settings	Guidelines
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.

Routes

The Router tree under the Device Manager tab displays a list of static routes.



ID	Destination	Gateway	Interface	Distance	Priority
1	0.0.0.0/0.0.0.0	172.30.71.1	TestIPSecPhase1	10	1

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 and click **Save**. See "Static route fields" on page 43.
4. Click **Save**.

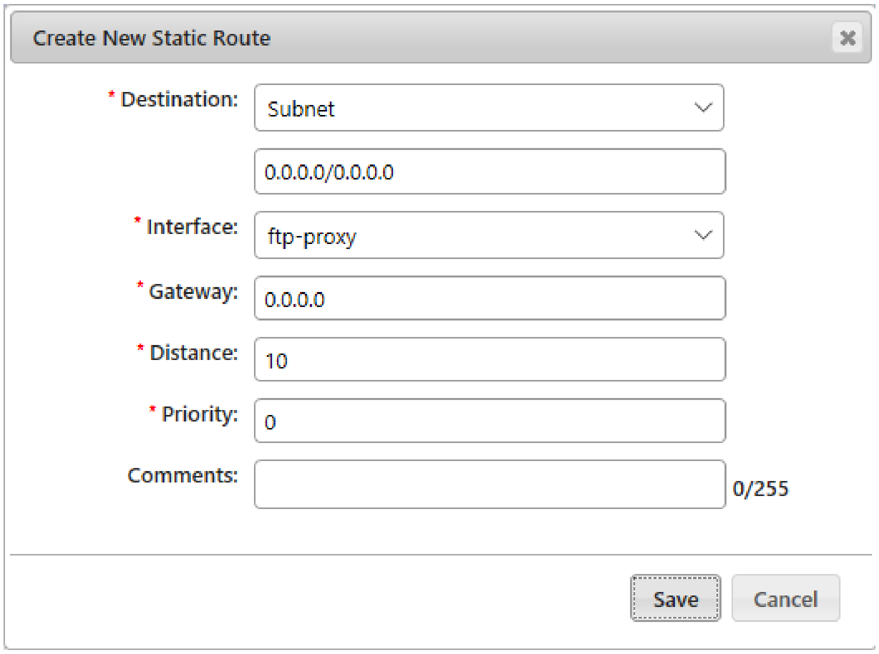
Updating a static route

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. Click **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



Create New Static Route

* Destination:	Subnet
	0.0.0.0/0.0.0.0
* Interface:	ftp-proxy
* Gateway:	0.0.0.0
* Distance:	10
* Priority:	0
Comments:	0/255

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

Settings	Guidelines
Destination	Required. Select **Subnet** or **Named Address** for the destination. • If **Subnet** is selected, enter an IP address and netmask. • If **Named Address** is selected, select 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	Enter an optional description. The value is a string with a maximum of 255 characters.

High Performance Network Security