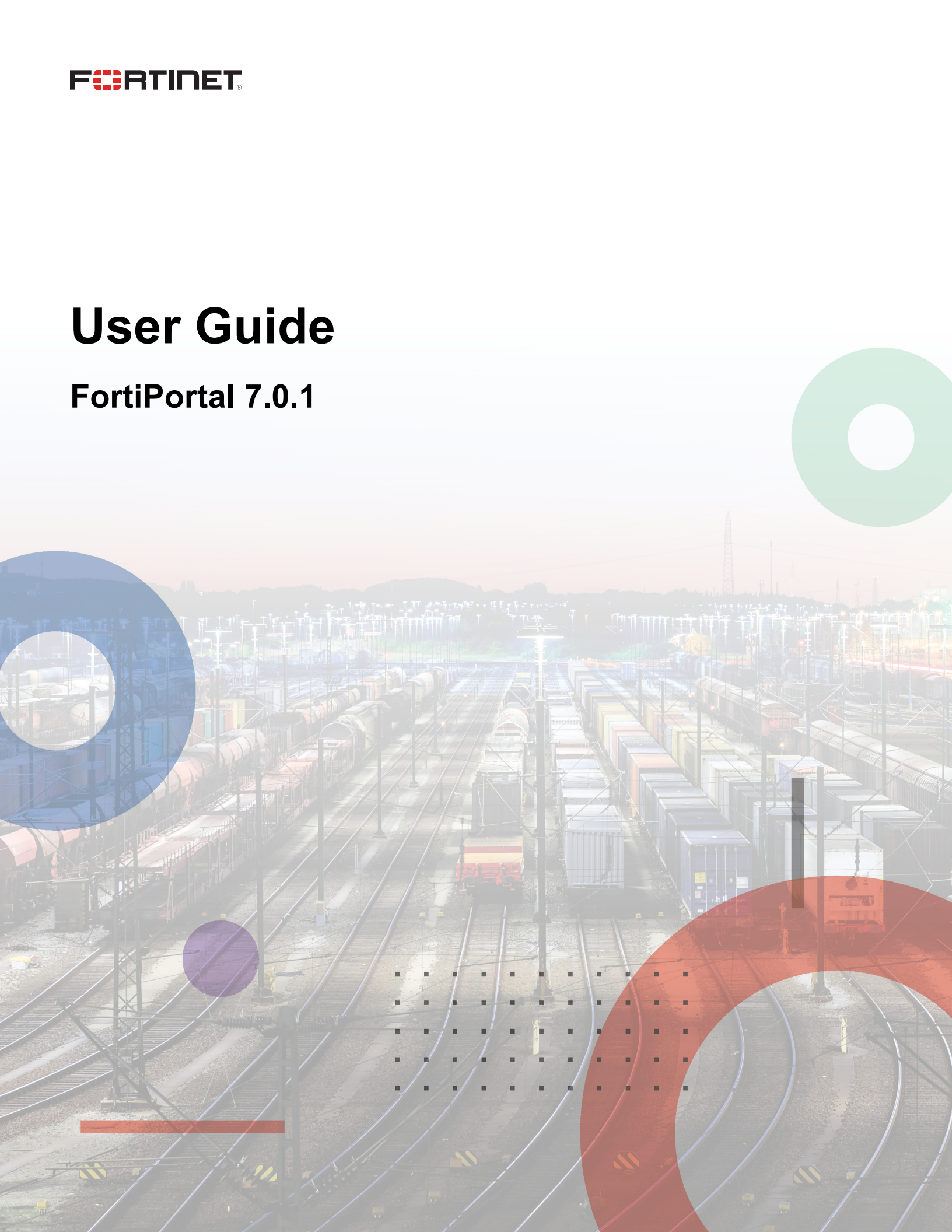


# User Guide

**FortiPortal 7.0.1**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



August 4, 2022

FortiPortal 7.0.1 User Guide

37-701-735200-20220804

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>5</b>
<b>FortiPortal web interface</b> .....	<b>6</b>
<b>Landing page</b> .....	<b>7</b>
<b>Reset password</b> .....	<b>9</b>
<b>Change Password</b> .....	<b>10</b>
<b>Insights</b> .....	<b>11</b>
Dashboard .....	11
Page actions .....	13
Widget actions .....	13
Monitors .....	14
Top Threats .....	15
Top Sources .....	16
Top Destinations .....	17
Policy Hits .....	18
Top Applications .....	19
Top Browsing Users .....	20
Top Website Domains .....	21
VPN .....	22
Health .....	22
Page actions .....	24
Widget actions .....	24
Logs .....	25
Traffic .....	26
Intrusion Prevention .....	28
Sandbox .....	29
Antivirus .....	30
DNS .....	31
Application Control .....	31
Web Filter .....	33
Event .....	35
<b>SD-WAN</b> .....	<b>37</b>
SD-WAN monitoring .....	37
Page actions .....	39
Widget actions .....	41
Configuration .....	42
Page actions .....	43
<b>Security</b> .....	<b>49</b>
Policy .....	50
Page actions .....	50
Configuring policies .....	51
Adding a new firewall policy .....	51
Updating a policy .....	53
Deleting a policy .....	53

Re-installing the policy .....	53
Viewing policy package settings .....	53
Policy data refresh .....	53
Revision backup .....	53
Creating and restoring policy revisions .....	54
Installing policies .....	54
Policy tab column settings .....	55
Policy action .....	55
<b>Firewall objects</b> .....	<b>56</b>
Types of objects .....	56
Page actions .....	60
Configuring firewall objects .....	60
<b>Network</b> .....	<b>77</b>
Page actions .....	77
VPN .....	78
Route .....	81
DHCP .....	82
<b>Switch</b> .....	<b>85</b>
Switch monitoring .....	85
Page actions .....	86
<b>WiFi</b> .....	<b>87</b>
WiFi monitoring .....	87
Page actions .....	88
<b>Reports</b> .....	<b>90</b>
Page actions .....	90
Run Reports actions .....	90
<b>Audit</b> .....	<b>91</b>
Page actions .....	91
<b>Additional Resources</b> .....	<b>92</b>

## Change Log

Date	Change Description
2022-08-04	Initial release.

# FortiPortal web interface

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

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



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

---

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

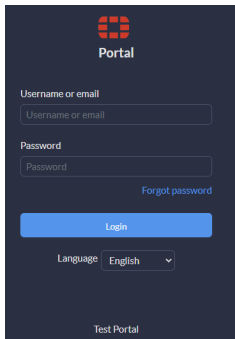
- *Help*—additional window that displays the Help pages
- *Alerts*— window that displays the unread alerts
- *Change Password*—raises a dialog for password change
- *Logout*—log out of the tool

The left pane may contain the following selections:

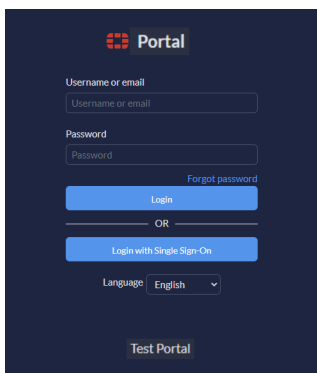
- *Insights*—widgets, monitors, device health, and log related views about the FortiPortal
- *SD-WAN*—SD-WAN related information and configurations
- *Security*—viewing and modifying security policies, firewall objects, and managing virtual private networks (VPNs), static routes, and DHCP servers
- *Switch*—switch monitoring
- *WiFi*—wireless networks monitoring
- *Reports*—lists of available reports
- *Audit*—a log of user activity on the Administrative Web Interface
- *Additional Resources*—page to launch external pages such as a ticketing system

# Landing page

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



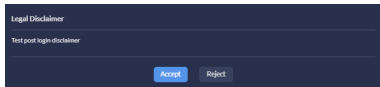
If your service provider has set up SSO authentication, you can log in using the *Login with Single Sign-On* button.



If your service provider has set up disclaimers, the landing page contains a text area for the disclaimer and it appears as follows:



A post-login disclaimer appears once you are successfully authenticated.



You must click *Accept* to access FortiPortal. If you click *Reject*, you are logged out immediately.

---



When a user logs in for the first time, a *Change Password* dialog appears asking the user to change the password.

---

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

---



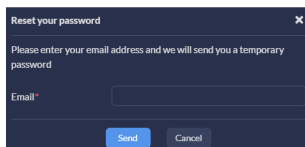
The options in the *Language* dropdown on the login page applies to the login page only.

---



# Reset password

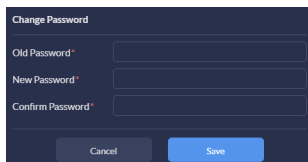
On the Login page, select the *Forgot password* link to display a dialog window:

A dark-themed dialog window titled "Reset your password" with a close button (X) in the top right corner. The text inside reads "Please enter your email address and we will send you a temporary password". Below this is a text input field labeled "Email\*". At the bottom of the dialog are two buttons: "Send" and "Cancel".

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

# Change Password

Selecting the *Change Password* icon (  ) on the banner displays this dialog:



The image shows a dark-themed dialog box titled "Change Password". It contains three input fields: "Old Password\*", "New Password\*", and "Confirm Password\*". At the bottom of the dialog, there are two buttons: "Cancel" and "Save".

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

# Insights

Go to *Insights* to access security event logs views, widgets, monitors, and managed devices status.

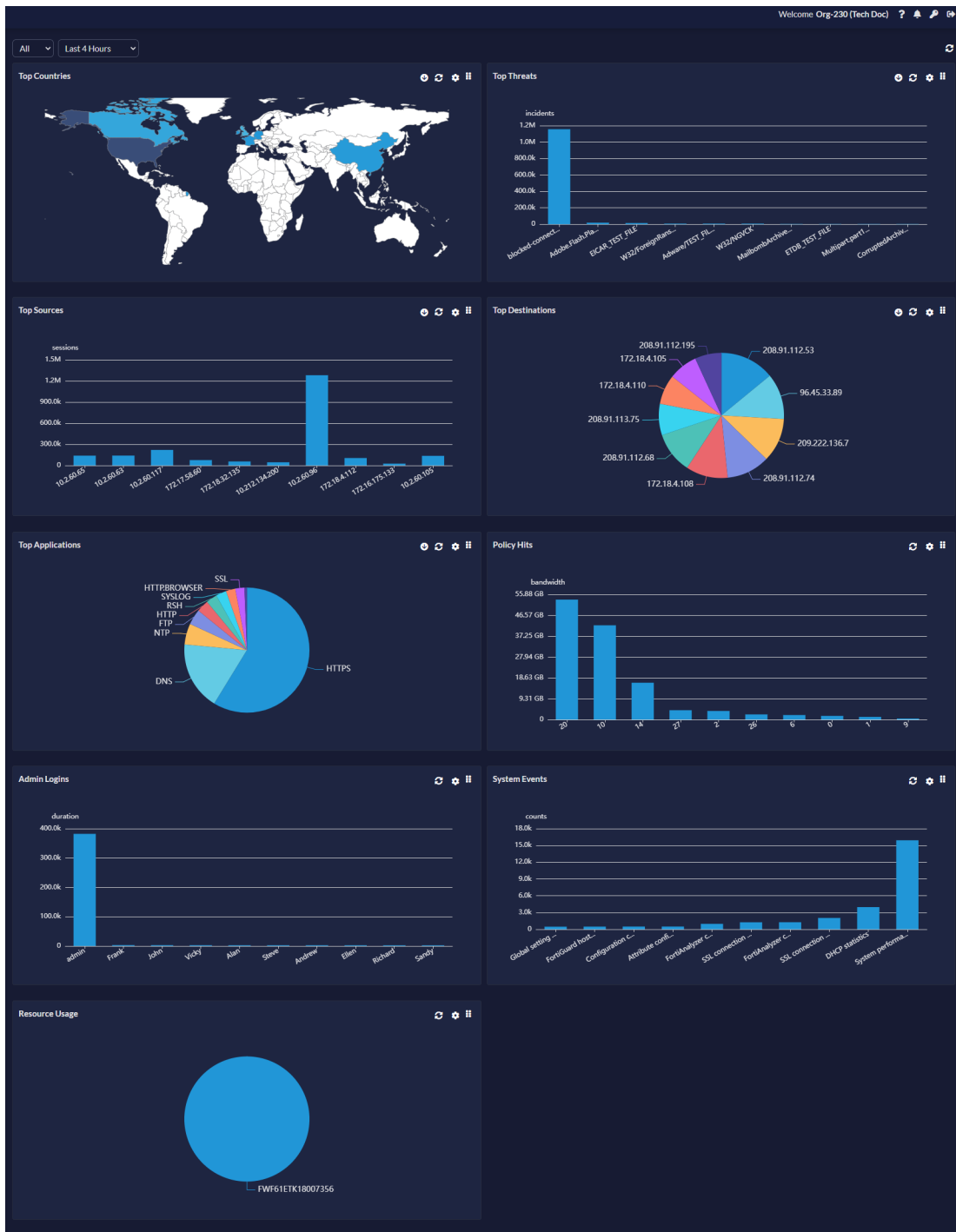
The following tabs are available in *Insight*:

- [Dashboard on page 11](#)
- [Monitors on page 14](#)
- [Health on page 22](#)
- [Logs on page 25](#)

## Dashboard

The *Dashboard* tab displays different views of the security event logs and other information.

The FortiPortal *Dashboard* tab looks like the following:



As shown in the figures, the *Dashboard* tab is organized as a set of widgets.

The following widgets are available:

- *Top Countries*
- *Top Threats*
- *Top Sources*
- *Top Destinations*

- *Top Applications*
- *Policy Hits*
- *Admin Logins*
- *Admin Logins*
- *System Events*
- *Resource Usage*

## Page actions

The following actions are available in the *Dashboard* tab:

- *Scope*—view widget output (All or site)
- *Filter*—filter the data (Last 5 Minutes, Last 30 Minutes, Last 60 Minutes, Last N Minutes, Last 4 Hours, Last 12 Hours, Last N Hours, Last 1 Day, Last 7 Days, Last N Days, Last N Months, or Specify)



When you set the filter to *last N Minutes/Hours/Days/Months*, a search box appears next to *Filter*. Enter a value for *N* and click the *Search* icon to apply this filter.

The widgets for the *Dashboard* tab are updated according to your selection in *Filter* and the value entered in the *N* search box.



Previously selected time range in *Logs*, *Monitors*, or *SD-WAN Monitoring* is automatically applied to the *Dashboard* tab.

You can specify a custom time range and save it as a time selector. The custom time range is preserved between organizations.

- *Refresh*—refresh the data

## Widget actions

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

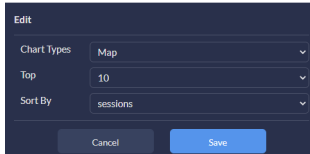
- *Drill-down*—visible in the widgets that support drill-down capability
- *Refresh*—refresh the data
- *action*—edit or delete the widget
- *Drag to reorder*—select and then drag and drop to change the position of a widget in the pane



Hover over the widgets to see additional information.

## Edit actions

Selecting *Edit* in the *action* dropdown opens a window within the widget that 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.

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 a region, traffic, or intrusion prevention (depending on the widget). When you select one of the results, the *Logs* tab opens with a view filtered by that result. The view filter is listed above the table.

Date/Time	Device ID	Action	Source IP	Users	Destination IP	Service	Application	Application Category	Sent Bytes	Received Bytes
2022-03-06 19:49:36	FGVM02TM21013313	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	tcp/8013	unscanned	NaN undefined	NaN undefined
2022-03-06 19:49:56	FGVM02TM21013313	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	tcp/8013	unscanned	NaN undefined	NaN undefined
2022-03-06 19:51:31	FGVM02TM21013313	dns	10.0.0.17.000		8.8.8.8	DNS	DNS	unscanned	NaN undefined	NaN undefined
2022-03-06 19:51:31	FGVM02TM21013313	dns	10.0.0.17.000		8.8.8.8	DNS	DNS	unscanned	NaN undefined	NaN undefined
2022-03-06 19:51:58	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-06 19:52:16	FGVM02TM21013313	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	unscanned	NaN undefined	NaN undefined
2022-03-06 19:52:36	FGVM02TM21013313	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	unscanned	NaN undefined	NaN undefined
2022-03-06 19:53:10	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-06 19:53:29	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-06 19:53:31	FGVM02TM21013313	dns	10.0.0.17.000		8.8.8.8	DNS	DNS	unscanned	NaN undefined	NaN undefined
2022-03-06 19:53:36	FGVM02TM21013313	dns	10.0.0.17.000		8.8.8.8	DNS	DNS	unscanned	NaN undefined	NaN undefined
2022-03-06 19:53:50	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-06 19:54:15	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-06 19:54:35	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-06 19:55:10	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-06 19:55:29	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-06 19:55:31	FGVM02TM21013313	dns	10.0.0.17.000		8.8.8.8	DNS	DNS	unscanned	NaN undefined	NaN undefined
2022-03-06 19:55:36	FGVM02TM21013313	dns	10.0.0.17.000		8.8.8.8	DNS	DNS	unscanned	NaN undefined	NaN undefined
2022-03-06 19:55:50	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-06 19:56:10	FGVM02TM21012080	ip-conn	10.0.0.0		10.0.0.0	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined

## Monitors

The *Monitors* tab in *Insights* displays monitoring information about threats, traffic, and application and websites. It also contains the *VPN* view allowing you to display VPN related information.

The following action buttons are available in the top pane:

- *Top Threats/Top Sources/Top Destinations/Policy Hits/ Top Applications/Top Browsing Users/Top Website Domains/SSL & Dialup IPsec/ Site-to-Site IPsec*—view the following information:
  - *Threats*: Top Threats
  - *Traffic*: Top Sources, Top Destinations, and Policy Hits
  - *Applications & Websites*: Top Applications, Top Browsing Users, and Top Website Domains.
  - *VPN*: SSL & Dialup IPsec and Site-to-Site IPsec
- *Scope*—view output for all sites or select a specific site.
- *Set Filter*—filter the data (last 5 Minutes, last 30 Minutes, last 60 Minutes, last N Minutes, last 4 Hours, last 12 Hours, last N Hours, last 1 Day, last 7 Days, last N Days, last N Months, or specify).



When you set the filter to *last N Minutes/Hours/Days/Months*, a search box appears next to *Set Filter*. Enter a value for *N* and click the *Search* icon to apply this filter.

The widgets and graphs for your monitor are updated according to your selection in *Set Filter* and the value entered in the *N* search box.

---



Previously selected time range in *Dashboard, Logs, or SD-WAN Monitoring* is automatically applied to *Monitors*.

You can specify a custom time range and save it as a time selector. The custom time range is preserved between organizations.

---

- *Refresh*—refresh the data.
- *Sort*—Some columns in the content pane have a sorting feature, allowing you to sort data in ascending or descending order.

For some of the tabs, a dropdown list at the bottom allows for selecting the number of entries to display per page. Also, some tabs have an additional *Search* bar.

When available, you can use < and > buttons on the bottom right for page navigation, or you can select the page number directly to go to the page.

For information on individual monitors, see:

- [Top Threats on page 15](#)
- [Top Sources on page 16](#)
- [Top Destinations on page 17](#)
- [Policy Hits on page 18](#)
- [Top Applications on page 19](#)
- [Top Browsing Users on page 20](#)
- [Top Website Domains on page 21](#)
- [VPN on page 22](#)

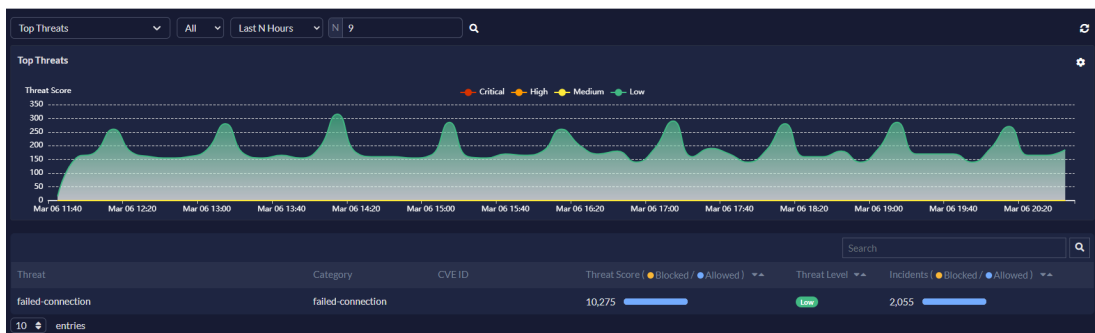
## Top Threats

The *Top Threats* tab in *Insights > Monitors* displays the threat information. It contains Virus/Intrusion Prevention information similar to *Top Threats* in FortiAnalyzer.

The following incidents are considered threats:

- Risk applications detected by application control
- Intrusion incidents detected by IPS
- Malicious web sites detected by web filtering
- Malware/botnets detected by antivirus

The figure below shows the *Top Threats* tab:



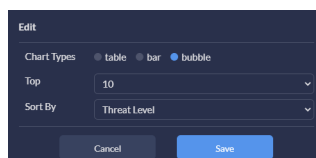
The content pane displays the threats, category, CVE ID, threat score (blocked and allowed), threat level, and the number of incidents.

Hover over the graph to see the threat information.

**To edit the top threats chart:**

1. Go to *Settings* (\*) > *Edit* to edit the top threats chart.

The figure below shows the *Edit* pane:



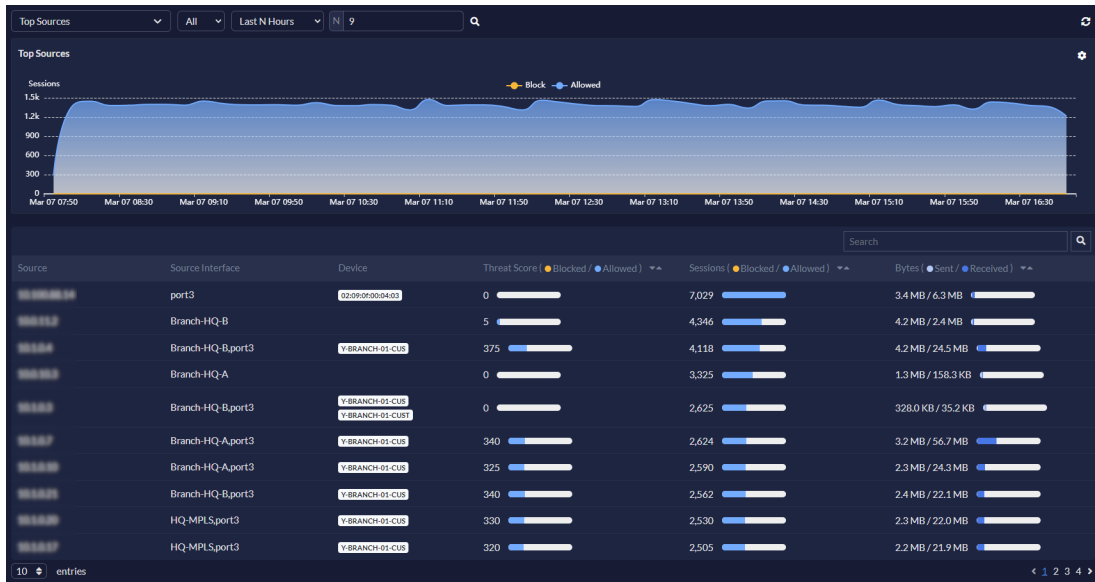
The *Edit* pane allows you to select from three different chart types: table, bar, or bubble. For the bar and bubble chart types, you can select the top 10, 15, or 20 threats to display and sort them by *Threat Level*, *Threat Score*, or *Incidents*.

## Top Sources

The *Top Sources* tab in *Insights* > *Monitors* displays the highest network traffic by source IP address, source interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).

The figure below shows the *Top Sources* tab:



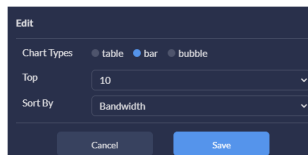


Hover over the graph to see the sessions information.

### To edit the top sources chart:

1. Go to **Settings** (⚙) > **Edit** to edit the top sources chart.

The figure below shows the *Edit* pane:

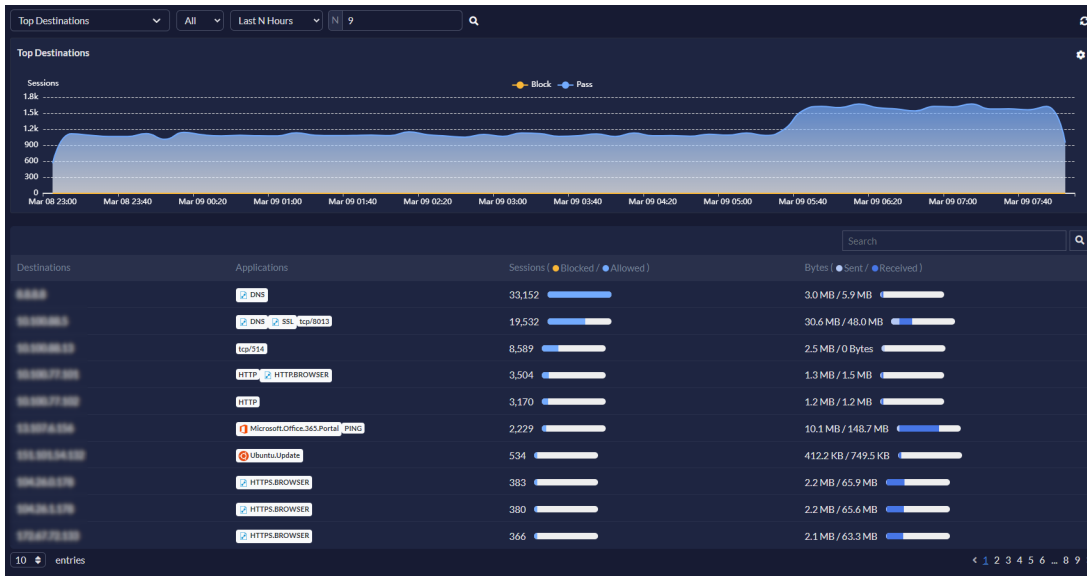


The *Edit* pane allows you to select from three different chart types: table, bar, or bubble. For the bar and bubble chart types, you can select the top 10, 15, or 20 sources to display and sort them by *Bandwidth*, *Sessions*, or *Threat Score*.

## Top Destinations

The *Top Destinations* tab in *Insights > Monitors* displays top destinations from recent network traffic by bandwidth or sessions.

The figure below shows the *Top Destinations* tab:



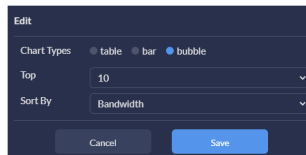
The content pane displays destination IP address, applications, sessions (blocked and allowed), and bytes (sent and received).

Hover over the graph to see the sessions information.

**To edit the top destinations chart:**

1. Go to *Settings* (\*) > *Edit* to edit the top destinations chart.

The figure below shows the *Edit* pane:



The *Edit* pane allows you to select from three different chart types: table, bar, or bubble. For the bar and bubble chart types, you can select the top 10, 15, or 20 sources to display and sort them by *Bandwidth* or *Sessions*.

## Policy Hits

The *Policy Hits* tab in *Insights* > *Monitors* displays top policy hits from recent traffic.

The figure below shows the *Policy Hits* tab:



The content pane displays the following:

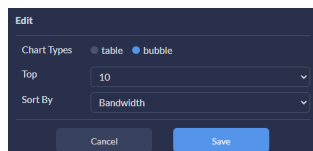
- policy and its type
- source and destination interface
- device name
- VDOM
- hit count
- bytes (sent and received)
- last used (date and time)

Hover over the graph to see the bandwidth information.

### To edit the policy hits chart:

1. Go to *Settings* (\*) > *Edit* to edit the policy hits chart.

The figure below shows the *Edit* pane:



The *Edit* pane allows you to select from either the table or the bubble chart type. For the bubble chart, you can select the top 10, 15, or 20 policies to display and sort them by *Bandwidth* or *Counts*.

## Top Applications

The *Top Applications* tab in *Insights* > *Monitors* displays the top applications used on the network, including application name, category, risk level, number of clients, sessions (blocked and allowed), and bytes (sent and received).

The figure below shows the *Top Applications* tab:

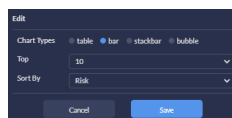


Hover over the graph to see the sessions information.

**To edit the top applications chart:**

1. Go to *Settings* (\*) > *Edit* to edit the top applications chart.

The figure below shows the *Edit* pane:



The *Edit* pane allows you to select from four different chart types: table, bar, stackbar, or bubble. For the bar and bubble chart types, you can select top 10, 15, or 20 applications and sort them by *Bandwidth*, *Risk*, or *Sessions*. Also, the stackbar chart type allows you to select the top 5 or 10 applications. The stackbar chart can be sorted by *Bandwidth* or *Sessions*.

## Top Browsing Users

The *Top Browsing Users* tab in *Insights* > *Monitors* displays top browsing users from recent traffic.

The figure below shows the *Top Browsing Users* tab:



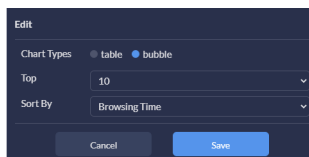
The content pane displays source, group, the number of sites visited, browsing time, and bytes (sent and received).

Hover over the graph to see the bandwidth information.

**To edit the top browsing user chart:**

1. Go to *Settings* (⚙) > *Edit* to edit the top browsing user chart.

The figure below shows the *Edit* pane:

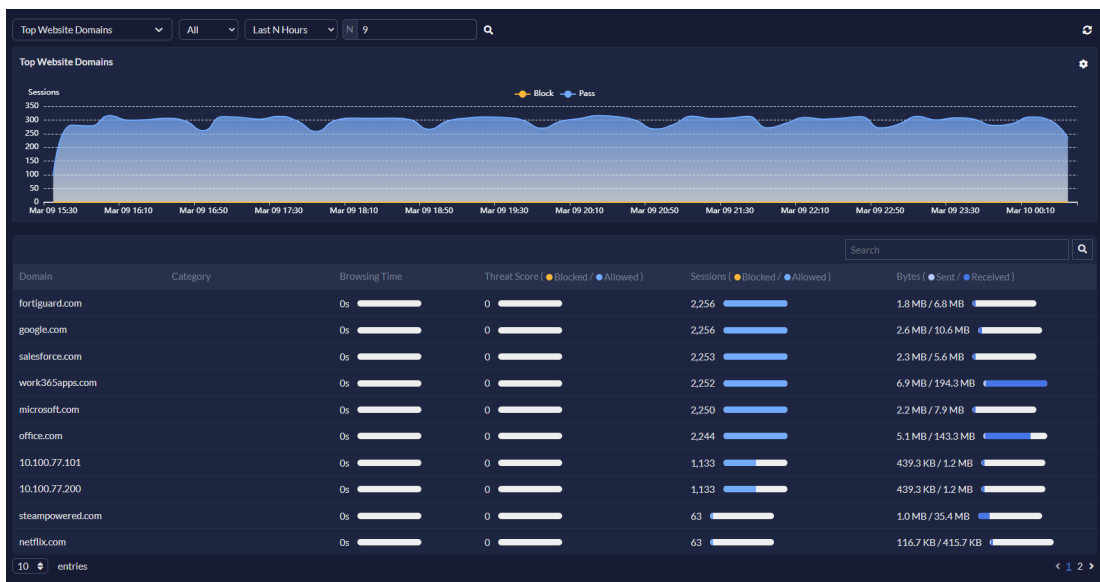


The *Edit* pane allows you to select from either the table or the bubble chart type. For the bubble chart, you can select the top 10, 15, or 20 users to display and sort them by *Browsing Time* or *Bandwidth*.

## Top Website Domains

The *Top Website Domains* tab in *Insights* > *Monitors* displays top website domains from recent traffic.

The figure below shows the *Top Website Domains* tab:



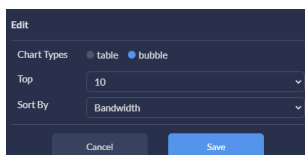
The content pane displays the domain name, category, browsing time, threat score, sessions, and bandwidth.

Hover over the graph to see the sessions information.

**To edit the top website domains chart:**

1. Go to *Settings* (⚙) > *Edit* to edit the top website domains.

The figure below shows the *Edit* pane:



The *Edit* pane allows you to select either the table or the bubble chart type. For the bubble chart, you can select the top 10, 15, or 20 website domains to display and sort them by *Bandwidth*, *Sessions*, or *Threat Score*.

## VPN

The *SSL & Dialup IPsec* and *Site-to-Site IPsec* tabs in *Insights > Monitors* display the VPN related information, allowing users to monitor *SSL & Dialup IPsec* and *Site-to-Site IPsec*.

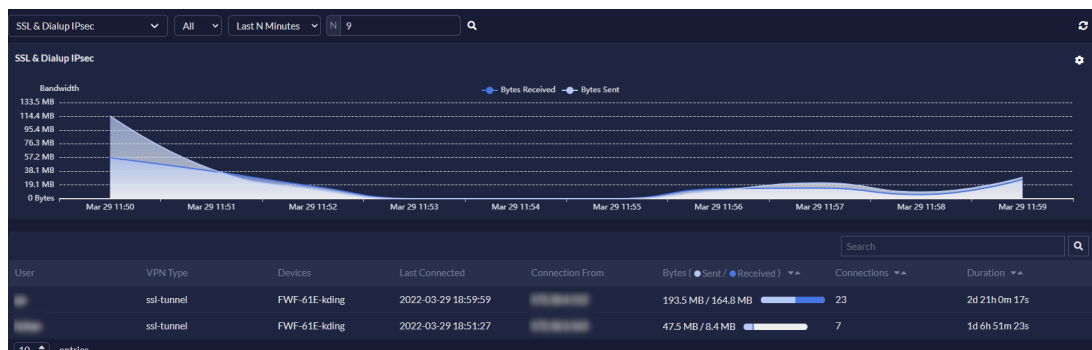
It gives the following details:

- VPN users
- Connection time
- Connecting location
- Duration

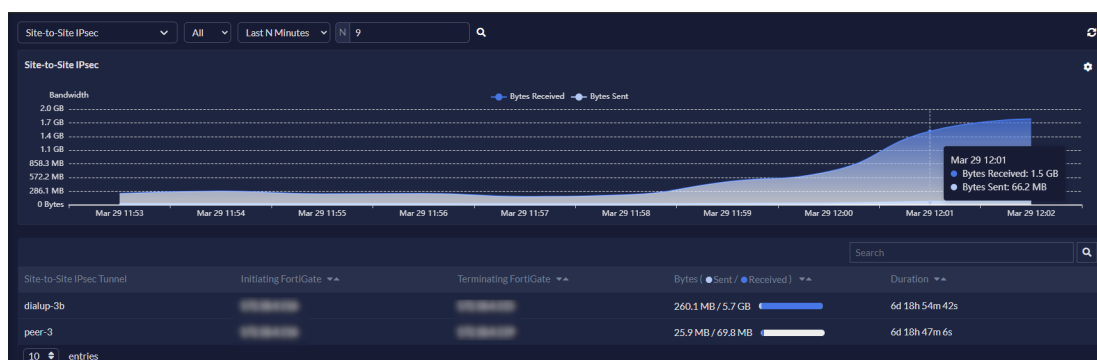
### To open the VPN view:

1. Go to *Insights > Monitors*.
2. From the dropdown menu at the top, under *VPN*, select *SSL & Dialup IPsec* or *Site-to-Site IPsec*.  
The figures below show examples of the *VPN* view:

#### SSL & Dialup IPsec



#### Site to Site IPsec



Hover over the graphs to see information on bandwidth.

## Health

The *Health* tab displays the managed devices status summary that you can use to access the device health.

The tab includes device monitoring view for devices within each site.

By default, *Site* view is selected.

The *Health* (site view) tab looks like the following:

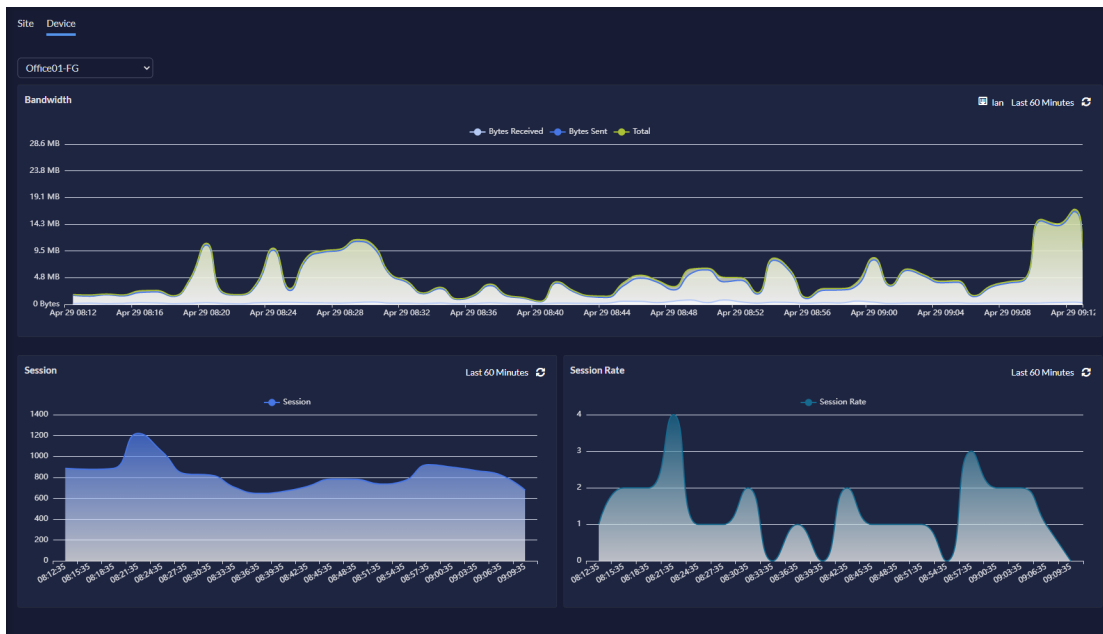


As shown in the figure, the *Health* tab is organized as a set of widgets.

The following widgets are available:

- *Uptime*
- *Network Configuration Status*
- *Policy & Object Status*
- *Top CPU Load*
- *Top Memory Usage*
- *Top Number of Sessions*

The *Device* view looks like the following:



The following widgets are available:

- **Bandwidth**: Displays bandwidth graphs for non-SD-WAN-enabled devices. You can view bandwidth for individual interfaces along with options to select historical data, such as last 60 minutes, last 1 day, and last 7 days.



For the **Bandwidth** widget to display, you must enable monitoring bandwidth on the FortiGate port by using the following CLI commands:

```
config system interface
  edit <name> # name of the FortiGate interface
    set monitor-bandwidth enable
  next
end
```

- **Session**
- **Session Rate**

## Page actions

The following actions are available in the *Device Health* tab:

- **View**—choose the type of view (*Site* or *Device*)
- **Scope**—view widget output for a site or a device depending on the selected *View*
- **Refresh**—refresh the data

## Widget actions

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

- **Interface**—select an interface



- *Filter*—filter the data (Last 1 Minute, Last 10 Minutes, Last 30 Minutes, Last 60 Minutes, Last 12 Hours, or Last 1 Day, or Last 7 days)

Some or all of the filter options are available for a widget.

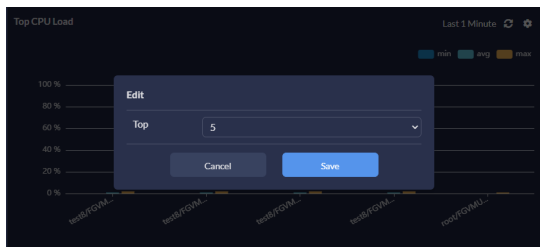
- *Refresh*—refresh the data
- *action*—edit the widget



Hover over the widgets to see additional information.  
Clicking some of the widgets open a table view with the related information.

## Edit actions

Selecting *Edit* in the *action* dropdown opens a window within the widget that allows you to select the top N results.



## Logs

The *Logs* tab in *Insights* 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 in the top pane:

- *Traffic/Intrusion Prevention/Sandbox/Antivirus/DNS/Application Control/Web Filter/Event*—view the event logs grouped by:
  - Application
  - Attack
  - Sandbox
  - Antivirus
  - Domain names
  - Application control
  - Web filter
  - Event
- *Scope*—view output for all sites or select a specific site.
- *Set Filter*—filter the data (Last 5 minutes, Last 30 minutes, Last 60 minutes, Last N minutes, Last 4 hours, Last 12 hours, Last N hours, Last 1 day, Last 7 days, Last N days, Last N months, or Specify).



When you set the filter to *last N Minutes/Hours/Days/Months*, a search box appears next to *Set Filter*. Enter a value for *N* and click the *Search* icon to apply this filter.

The table for your log is updated according to your selection in *Set Filter* and the value entered in the *N* search box.



Previously selected time range in *Dashboard*, *Monitors*, or *SD-WAN Monitoring* is automatically applied to *Logs*.

You can specify a custom time range and save it as a time selector. The custom time range is preserved between organizations.

- *Export to CSV*—export the log view information as a CSV file.
- *Refresh*—refresh the data.
- *Add Filter*—add a filter to narrow down the search.



Double-click a field in any *View* table to add the field as a filter. You can combine multiple filters to narrow down your search.

- *Settings*—opens the *Column Settings* dialog. Select columns from the list to display.
- *Sort*—Some columns have a sorting feature, allowing you to sort data in ascending or descending order.

A dropdown list at the bottom allows for selecting the number of entries to display per page.

You can use < and > buttons on the bottom right for page navigation, or you can select the page number directly to go to the page.

The following tabs provide different views of the data:

- *Traffic*—arranged by application. See [Traffic on page 26](#).
- *Intrusion Prevention*—arranged by attack. See [Intrusion Prevention on page 28](#).
- *Sandbox*—arranged by sandbox. See [Sandbox on page 29](#).
- *Antivirus*—arranged by antivirus. See [Antivirus on page 30](#).
- *DNS*—arranged by domain names. See [DNS on page 31](#).
- *Application Control*—arranged by application control. See [Application Control on page 31](#).
- *Web Filter*—arranged by web filters. See [Web Filter on page 33](#).
- *Event*—arranged by events. See [Event on page 35](#).

## Traffic

The *Traffic* tab in *Insights > Logs* displays event logs grouped by application.

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

Date/Time	Device ID	Action	Source IP	Users	Destination IP	Service	Application	Application Category	Sent Bytes	Received Bytes
2022-03-09 07:54:08	FGVM02TM21012080	timeout	192.168.1.100		192.168.1.100	HTTP	Citrix.Services	Collaboration	60 Bytes	0 Bytes
2022-03-09 07:54:08	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	132 Bytes	206 Bytes
2022-03-09 07:54:08	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	120 Bytes	348 Bytes
2022-03-09 07:54:08	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	120 Bytes	348 Bytes
2022-03-09 07:54:08	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	128 Bytes	378 Bytes
2022-03-09 07:54:08	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	128 Bytes	378 Bytes
2022-03-09 07:54:08	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	120 Bytes	164 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	accept	192.168.1.100		192.168.1.100	NTP	NTP	Network.Service	76 Bytes	76 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	67 Bytes	122 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	67 Bytes	131 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	close	192.168.1.100		192.168.1.100	tcp/8013	tcp/8013	unknown	180 Bytes	132 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	130 Bytes	262 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	130 Bytes	262 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	130 Bytes	412 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	130 Bytes	412 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	timeout	192.168.1.100		192.168.1.100	HTTPS	HTTPS	unknown	60 Bytes	0 Bytes
2022-03-09 07:54:13	FGVM02TM21012080	accept	192.168.1.100		8.8.8.8	DNS	DNS	Network.Service	132 Bytes	206 Bytes
2022-03-09 07:54:18	FGVM02TM21012080	server-rst	192.168.1.100		192.168.1.100	tcp/8013	SSL_TLSv1.3	Network.Service	4.3 KB	7.3 KB
2022-03-09 07:54:18	FGVM02TM21012080	ip-conn	192.168.1.100		192.168.1.100	tcp/8013	SSL_TLSv1.3	Network.Service	NaN undefined	NaN undefined
2022-03-09 07:54:21	FGVM02TM21012080	close	192.168.1.100		192.168.1.100	HTTP	HTTPBROWSER	Web.Client	394 Bytes	744 Bytes

Select **Add Filter** to apply a filter. Once you select a filter from the filters dropdown, enter the details in the box that appears. You can add multiple filters to narrow down your search. Alternatively, double-click a field to add it as a filter.

Select the **Settings** (⚙️) icon on the right of the content pane to open the **Column Settings** dialog, and select a new column to display.

Select the **n** button to see more traffic related information for this device.



## Intrusion Prevention

The *Intrusion Prevention* tab in *Insights > Logs* displays event logs grouped by attack.

The following figure shows an example of the *Intrusion Prevention* tab:

Date/Time	Device ID	Source IP	Destination IP	Action	Service	Count
2022-03-29 12:21:10	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	HTTP	1
2022-03-29 12:21:10	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	HTTP	1
2022-03-29 12:21:10	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	HTTP	1
2022-03-29 12:21:10	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	HTTP	1
2022-03-29 12:21:10	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	HTTP	1
2022-03-29 12:21:10	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	HTTP	1
2022-03-29 12:21:10	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	PING	1
2022-03-29 12:21:12	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	HTTP	1
2022-03-29 12:21:12	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	HTTP	1
2022-03-29 12:21:12	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	HTTP	1
2022-03-29 12:21:12	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	HTTP	1
2022-03-29 12:21:12	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	PING	1
2022-03-29 12:21:12	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	PING	1
2022-03-29 12:21:12	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	PING	1
2022-03-29 12:21:13	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	tcp/45099	1
2022-03-29 12:21:13	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	PING	1
2022-03-29 12:21:13	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	PING	1
2022-03-29 12:21:13	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	PING	1
2022-03-29 12:21:14	FWF61ETK18007356	192.168.1.100	192.168.1.1	detected	HTTP	1
2022-03-29 12:21:14	FWF61ETK18007356	192.168.1.100	192.168.1.1	dropped	HTTP	1

Select **Add Filter** to apply a filter. Once you select a filter from the filters dropdown, enter the details in the box that appears. You can add multiple filters to narrow down your search. Alternatively, double-click a field to add it as a filter.

Select the **Settings** (⚙️) icon on the right of the content pane to open the **Column Settings** dialog, and select a new column to display.

Select the **n** button to see more intrusion prevention related information for this device.

Category	Field	Value
Security	Level	alert
	Source	
Source	Device ID	FWF61ETK18007356
	Device Name	FWF-61E-ldfmg
	IP	192.168.1.100
	Interface	switch
Destination	Port	48312
	UEBA Endpoint ID	101337
	UEBA User ID	7201
	Endpoint ID	101
Action	Firewall Action	detected
	Policy ID	2
Threat	Attack ID	10372
	Attack	ACL Server Directory Traversal
	Direction	outgoing
	Incident Serial No.	1446790717
Others	Reference	https://fortiguard.fortinet.com/encyclopedial/ps/10372
	Severity	low
General	Log ID	16384
	Session ID	101940028
	Virtual Domain	root
	End User ID	3
Application	Endpoint ID	101
	hostname	212.47.2.77
	IP	212.47.2.77
	Interface	wan1
Type	Port	80
	Profile	default
	Protocol	6
	Service	HTTP
Sub-Type	Sub-Type	ips
	Type	utm
Date/Time	Date/Time	19:43:09
	Device Time	2022-03-29 19:43:09
	Time Stamp	2022-03-29 12:43:09
	logser	502000000

## Sandbox

The **Sandbox** tab in **Insights > Logs** displays event logs grouped by sandbox.

Select *Add Filter* to apply a filter. Once you select a filter from the filters dropdown, enter the details in the box that appears. You can add multiple filters to narrow down your search. Alternatively, double-click a field to add it as a filter.

Select the *Settings* (⚙️) icon on the right of the content pane to open the *Column Settings* dialog, and select a new column to display.

When you select one of the entries in the table, the sandbox view works like the Intrusion Prevention view.

## Antivirus

The *Antivirus* tab in *Insights > Logs* displays event logs grouped by antivirus.

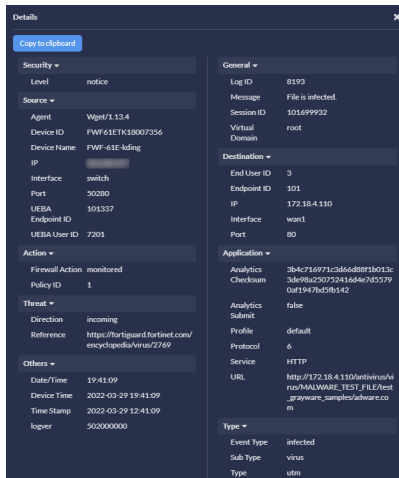
The following figure shows an example of the *Antivirus* tab:

Date/Time	Device ID	Action	Service	Source IP	Destination IP
2022-03-29 12:24:30	FWF61ETK18007356	monitored	HTTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:30	FWF61ETK18007356	monitored	HTTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:30	FWF61ETK18007356	monitored	HTTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:30	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:30	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:30	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	monitored	HTTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	monitored	HTTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:31	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:33	FWF61ETK18007356	monitored	HTTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:33	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:33	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:33	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:33	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:33	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1
2022-03-29 12:24:33	FWF61ETK18007356	blocked	FTP	192.168.1.1	192.168.1.1

Select *Add Filter* to apply a filter. Once you select a filter from the filters dropdown, enter the details in the box that appears. You can add multiple filters to narrow down your search. Alternatively, double-click a field to add it as a filter.

Select the *Settings* (⚙️) icon on the right of the content pane to open the *Column Settings* dialog, and select a new column to display.

Select the ⓘ button to see more antivirus related information for this device.



## DNS

The *DNS* tab in *Insights > Logs* displays event logs grouped by domain names.

Select *Add Filter* to apply a filter. Once you select a filter from the filters dropdown, enter the details in the box that appears. You can add multiple filters to narrow down your search. Alternatively, double-click a field to add it as a filter.

Select the *Settings* (⚙️) icon on the right of the content pane to open the *Column Settings* dialog, and select a new column to display.

Select the  button to see more DNS related information for this domain name.

## Application Control

The *Application Control* tab in *Insights > Logs* displays event logs grouped by application control.

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

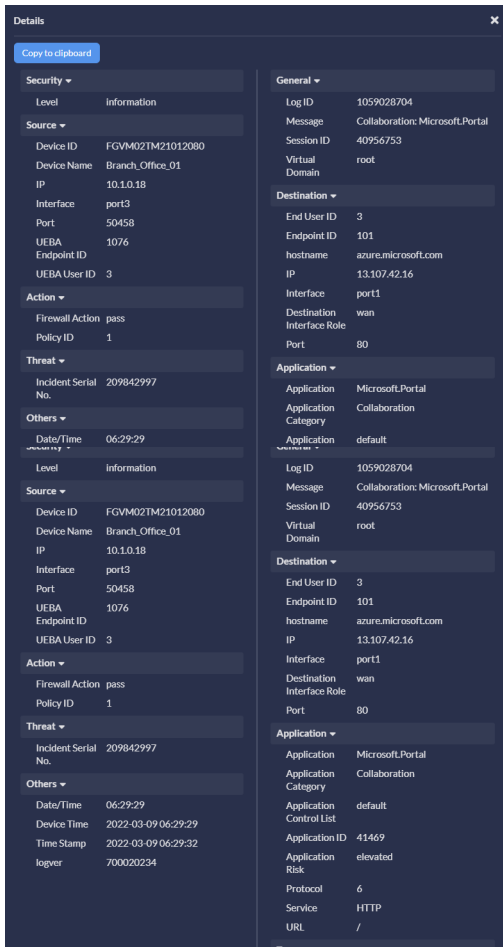
Date/Time	Level	Device ID	Source IP	Destination Port	Destination IP	Service	Application Control List	Application Category	Application	Action	Hostname
2022-03-09 06:29:27	Information	FGVM02TM21012080	10.100.77.101	80	10.100.77.101	HTTP	default	Collaboration	Microsoft.Office:365:Portal	pass	www.office.cor
2022-03-09 06:29:27	Information	FGVM02TM21012080	10.100.77.200	443	10.100.77.200	SSL	default	Business	Salesforce	pass	www.salesfor
2022-03-09 06:29:27	Information	FGVM02TM21012080	10.100.77.200	80	10.100.77.200	HTTP	default	Business	Salesforce	pass	www.salesfor
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	8013	10.100.77.200	SSL	default	Network.Service	SSL_TLSv1.3	pass	
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	8013	10.100.77.200	SSL	default	Network.Service	SSL	pass	
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	80	10.100.77.200	HTTP	default	Web.Client	HTTPBROWSER	pass	10.100.77.101
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	80	10.100.77.200	HTTP	default	Web.Client	HTTPBROWSER	pass	10.100.77.200
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	443	10.100.77.200	SSL	default	Web.Client	HTTPS.BROWSER	pass	www.work365
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	443	10.100.77.200	SSL	default	Network.Service	SSL	pass	www.work365
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	80	10.100.77.200	HTTP	default	Web.Client	HTTPBROWSER	pass	www.work365
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	443	10.100.77.200	SSL	default	Collaboration	Microsoft:Portal	pass	azure.microsof
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	80	10.100.77.200	HTTP	default	Collaboration	Microsoft:Portal	pass	azure.microsof
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	80	10.100.77.200	HTTP	default	Collaboration	Citrix:Services	pass	
2022-03-09 06:29:32	Information	FGVM02TM21012080	10.100.77.200	443	10.100.77.200	SSL	default	Collaboration	Microsoft.Office:365:Portal	pass	www.office.cor
2022-03-09 06:29:47	Information	FGVM02TM21012080	10.100.77.200	123	10.100.77.200	NTP	default	Network.Service	NTP	pass	
2022-03-09 06:29:47	Information	FGVM02TM21012080	10.100.77.200	123	10.100.77.200	NTP	default	Network.Service	NTP	pass	
2022-03-09 06:29:47	Information	FGVM02TM21012080	10.100.77.200	123	10.100.77.200	NTP	default	Network.Service	NTP	pass	
2022-03-09 06:29:47	Information	FGVM02TM21012080	10.100.77.200	123	10.100.77.200	NTP	default	Network.Service	NTP	pass	
2022-03-09 06:29:47	Information	FGVM02TM21012080	10.100.77.200	123	10.100.77.200	NTP	default	Network.Service	NTP	pass	
2022-03-09 06:29:47	Information	FGVM02TM21012080	10.100.77.200	123	10.100.77.200	NTP	default	Network.Service	NTP	pass	

Select **Add Filter** to apply a filter. Once you select a filter from the filters dropdown, enter the details in the box that appears. You can add multiple filters to narrow down your search. Alternatively, double-click a field to add it as a filter.

Select the **Settings** (⚙️) icon on the right of the content pane to open the **Column Settings** dialog, and select a new column to display.

Select the ⓘ button to see more application control related information for this device.





## Web Filter

The *Web Filter* tab in *Insights > Logs* displays event logs grouped by web filters.

The following figure shows an example of the *Web Filter* tab:

Date/Time	Device ID	Source IP	Destination IP	Service	Hostname	Action	URL
2022-03-29 12:30:12	FWF61ETK18007356			http	show.buzzcity.net	passthrough	/show.php
2022-03-29 12:30:12	FWF61ETK18007356			HTTP	141.101.115.20	passthrough	/site_url=http://www.google.com/admin/admin.php?ipstest
2022-03-29 12:30:12	FWF61ETK18007356			http	mlog.hildo.com	passthrough	/c.gif
2022-03-29 12:30:12	FWF61ETK18007356			http	203.151.183.208	passthrough	/mobileoc.music.fc.qq.com/M500002FPV0k48xuz.mp3
2022-03-29 12:30:12	FWF61ETK18007356			http	203.151.183.208	passthrough	/mobileoc.music.fc.qq.com/M5000049RL0j4Qoajb.mp3
2022-03-29 12:30:12	FWF61ETK18007356			http	pebed.dnagg	passthrough	/
2022-03-29 12:30:12	FWF61ETK18007356			http	mlog.hildo.com	passthrough	/c.gif
2022-03-29 12:30:12	FWF61ETK18007356			http	203.151.183.193	passthrough	/fcgi-bin/getpush
2022-03-29 12:30:12	FWF61ETK18007356			http	93.190.141.73	passthrough	/news/index.php
2022-03-29 12:30:12	FWF61ETK18007356			http	203.151.183.208	passthrough	/mobileoc.music.fc.qq.com/M5000049RL0j4Qoajb.mp3
2022-03-29 12:30:12	FWF61ETK18007356			http	mlog.hildo.com	passthrough	/c.gif
2022-03-29 12:30:12	FWF61ETK18007356			http	74.125.200.139	passthrough	/generate_204
2022-03-29 12:30:12	FWF61ETK18007356			http	api.share.mob.com	passthrough	/log4
2022-03-29 12:30:12	FWF61ETK18007356			http	weather.smarttechnology365.org	passthrough	/weather
2022-03-29 12:30:12	FWF61ETK18007356			http	169.51.65.146	passthrough	/dlina.aspx
2022-03-29 12:30:12	FWF61ETK18007356			http	149.154.64.60	passthrough	/locator.php
2022-03-29 12:30:12	FWF61ETK18007356			http	mlog.hildo.com	passthrough	/c.gif
2022-03-29 12:30:12	FWF61ETK18007356			http	locker.data.kamobile.net	passthrough	/c/
2022-03-29 12:30:12	FWF61ETK18007356			http	c.data.mob.com	passthrough	/c/data
2022-03-29 12:30:13	FWF61ETK18007356			http	d2e24t2jgcnor2.webhostid.com	passthrough	/secure/checkUser_id=cb031741-f2be-4f61-8441-89ba43505efb&uc=20141114&subId=20141114/ytd&version=1.0.5577.20076&implementation_id=browsersafeguard-rockettab-spligot-ytd&block_host=False&reg=False&redirectms=True&ResponseCode=200&ContentType=text/html&f

Select **Add Filter** to apply a filter. Once you select a filter from the filters dropdown, enter the details in the box that appears. You can add multiple filters to narrow down your search. Alternatively, double-click a field to add it as a filter.

Select the **Settings** (⚙️) icon on the right of the content pane to open the **Column Settings** dialog, and select a new column to display.

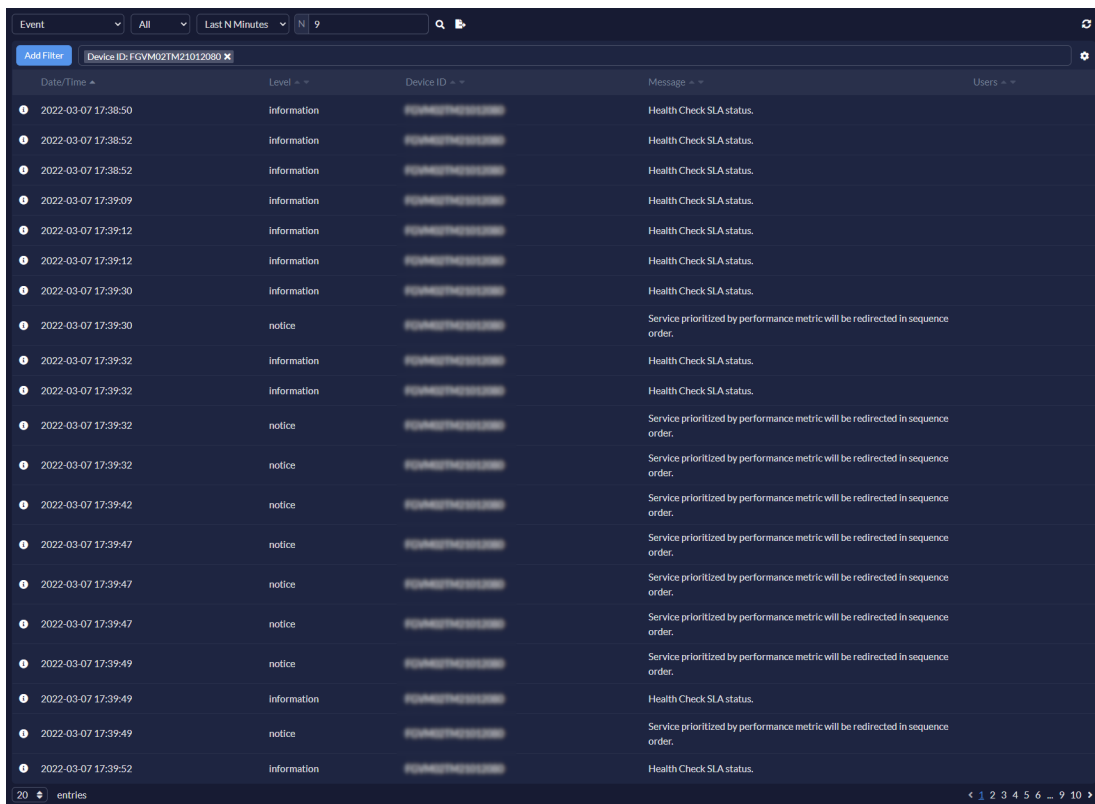
Select **ℹ️** the button to see more web filter related information for this device.



## Event

The *Event* tab in *Insights > Logs* displays event logs grouped by events.

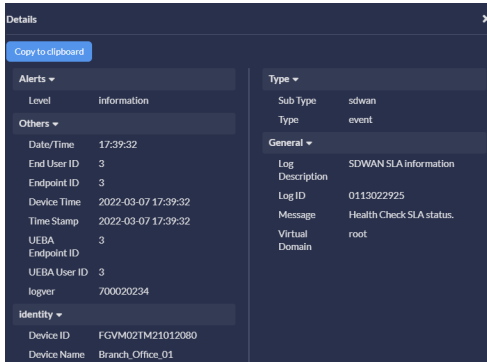
The following figure shows an example of the *Event* tab:



Select *Add Filter* to apply a filter. Once you select a filter from the filters dropdown, enter the details in the box that appears. You can add multiple filters to narrow down your search. Alternatively, double-click a field to add it as a filter.

Select the *Settings* (⚙️) icon on the right of the content pane to open the *Column Settings* dialog, and select a new column to display.

Select the ⓘ button to see more event related information for this device.



# SD-WAN

Go to *SD-WAN* for SD-WAN related information.

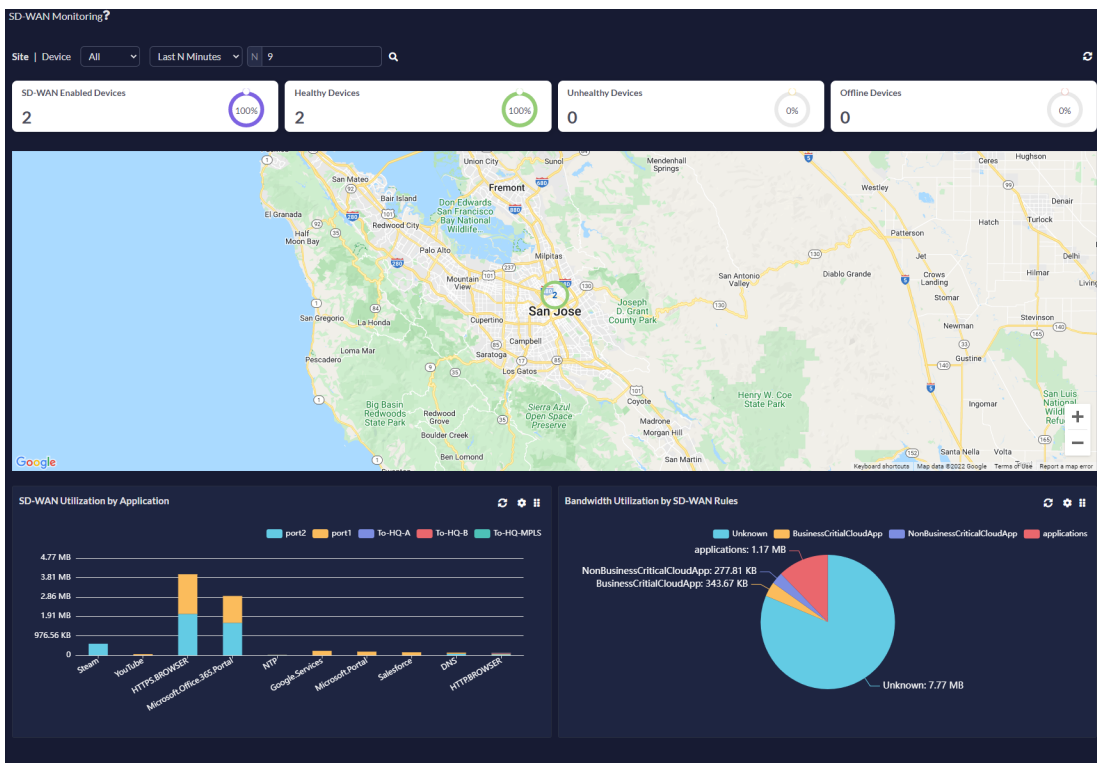
- [SD-WAN monitoring on page 37](#)— allows you to check the performance of the SD-WAN interfaces using a set of widgets, and it contains widgets from SD-WAN device monitoring and the log-based SD-WAN monitor.
- [Configuration on page 42](#)— allows you to view and create *SD-WAN Templates*, *Interface Members*, *Performance SLA*, and *SD-WAN Rules*.

## SD-WAN monitoring

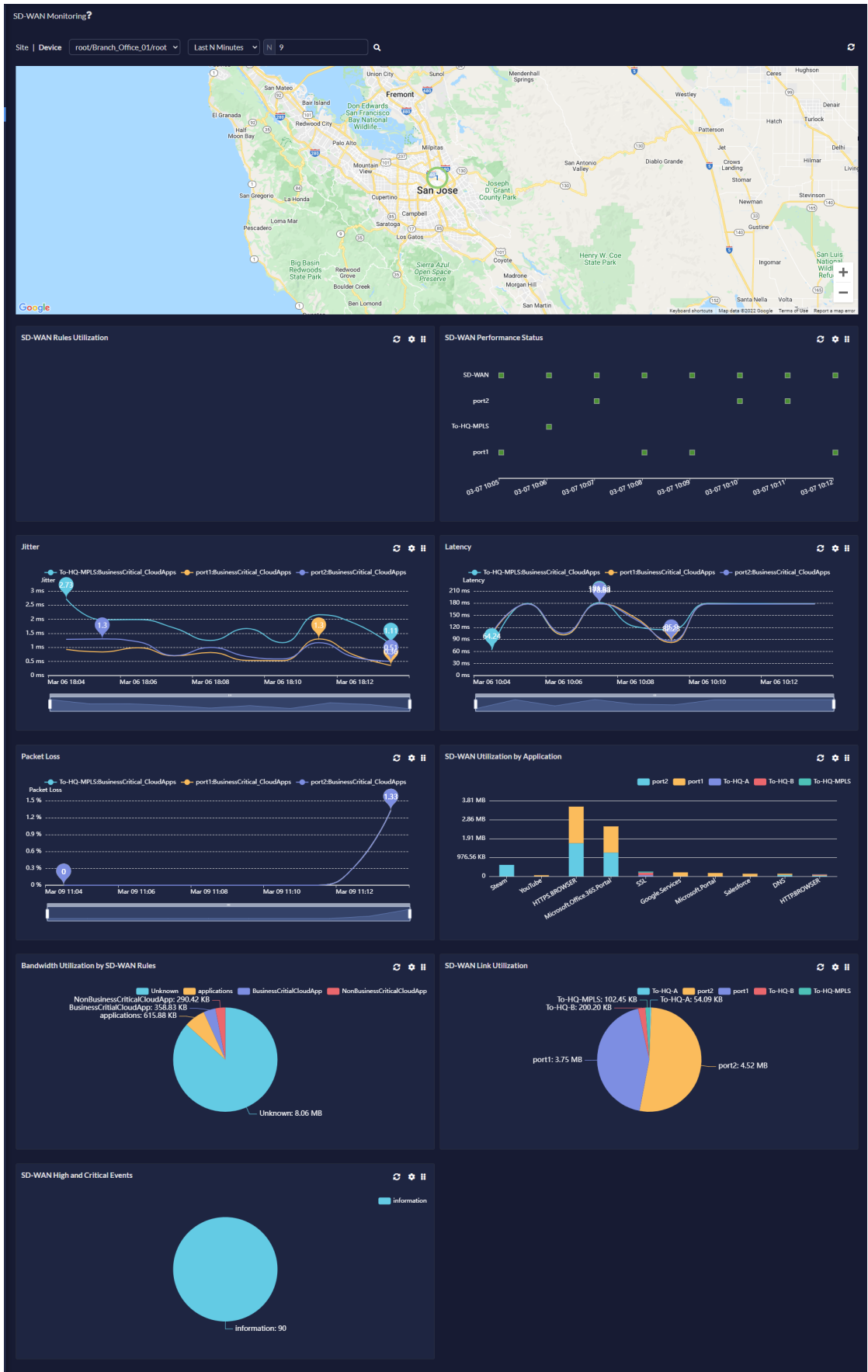
The *Monitoring* tab in *SD-WAN* consolidates SD-WAN related information.

By default, *Site* view is selected.

The *SD-WAN Monitoring* tab (site view) looks like the following:



The *Device* view looks like the following:



As shown in the figures, the *SD-WAN Monitoring* tab is organized as a set of widgets.

At the top, the following widgets are available:

- *SD-WAN Enabled Devices*
- *Healthy Devices*
- *Unhealthy Devices*
- *Offline Devices*

The following additional widgets are available:

- *SD-WAN Rules Utilization*
- *SD-WAN Performance Status*
- Link Health: *Jitter, Latency, and Packet Loss*
- *SD-WAN Utilization by Application*
- *Bandwidth Utilization by SD-WAN Rules*
- *SD-WAN Link Utilization*
- *SD-WAN High and Critical Events*

## Page actions

The following actions are available on the *SD-WAN Monitoring* tab:

- *View*—choose the type of view (*Site* or *Device*)
- *Scope*—view widget output (*All* or a site)  
The *Scope* option is only available for *Site* view.
- *Device*—use the dropdown to view widget output for a device  
The *Device* option is only available for *Device* view.
- *Filter*—filter the data (Last 5 Minutes, Last 30 Minutes, Last 60 Minutes, Last N Minutes, Last 4 Hours, Last 12 Hours, Last N Hours, Last 1 Day, Last 7 Days, Last N Days, Last N Months, or Specify)



When you set the filter to *last N Minutes/Hours/Days/Months*, a search box appears next to *Filter*. Enter a value for *N* and click *Search* to apply this filter.

The widgets and graphs for your monitor are updated according to your selection in *Filter* and the value entered in the *N* search box.

---



Previously selected time range in *Dashboard, Logs, and Monitors* is automatically applied to *SD-WAN Monitoring*.

You can specify a custom time range and save it as a time selector. The custom time range is preserved between organizations.

---



You can zoom in and out of the map by rotating the wheel, or use the + or - buttons to zoom in and out respectively.

---

## SD-WAN Status

Click the devices in the map to open the *SD-WAN Status* window containing performance related information in a table.

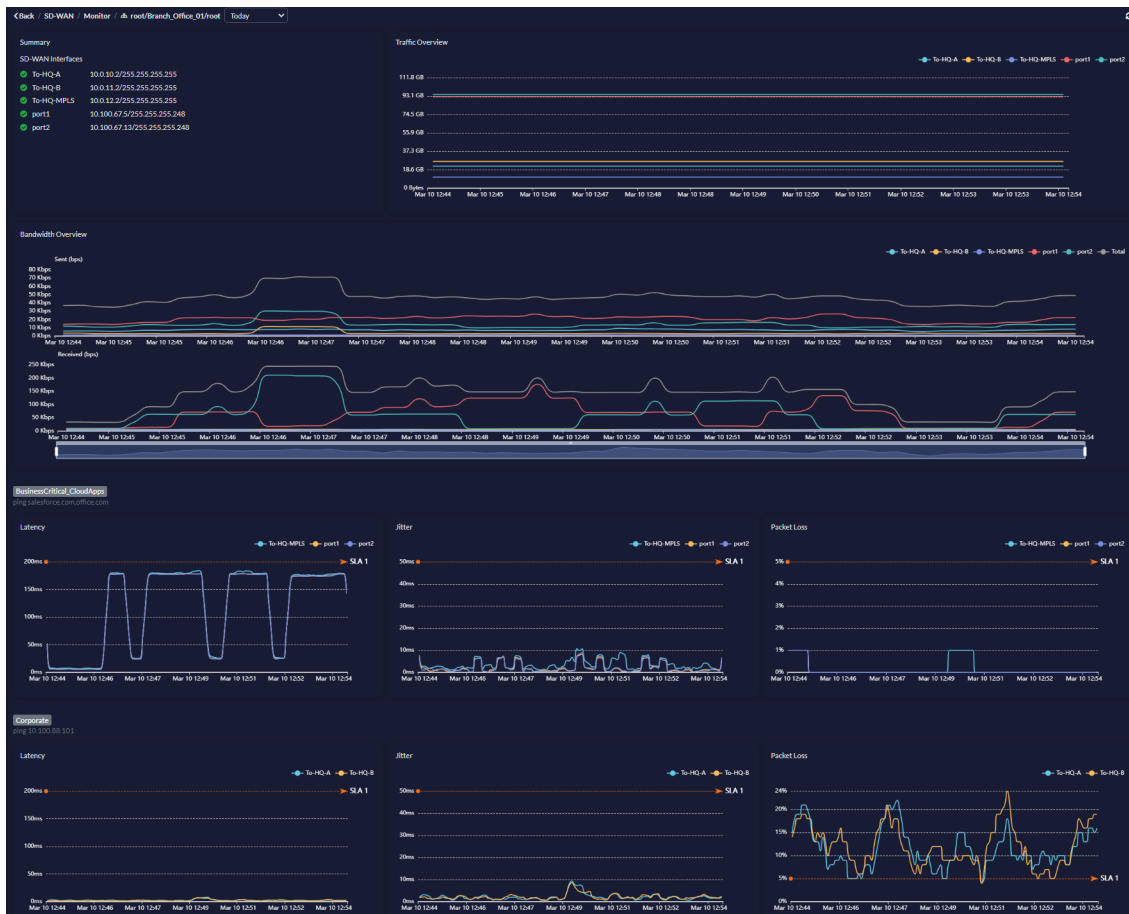
The screenshot shows the 'SD-WAN Status' window with a search bar and a table of performance metrics. The table has columns for Device, Interface, Performance SLA, Jitter (ms), Latency (ms), Packet Loss (%), Session, Bandwidth (Tx), and Bandwidth (Rx). The data is organized into two main sections for 'root/branch.Office.01/root' and 'root/branch.Office.02/root'.

Device	Interface	Performance SLA	Jitter (ms)	Latency (ms)	Packet Loss (%)	Session	Bandwidth (Tx)	Bandwidth (Rx)	
root/branch.Office.01/root			3.46	3.30	6%				
To-HQ-A	Corporate								
	LinkA		2.07	1.62	0%	6	8.21 Kbps	6.75	
	shortcut		2.23	2.07	0%				
To-HQ-B	Corporate		3.57	3.30	8%	9	2.43 Kbps	4.16	
	shortcut		0.68	1.01	0%				
To-HQ-MPLS	BusinessCritical_CloudApps		2.15	174.06	0%	3	1.31 Kbps	3.39	
	BusinessCritical_CloudApps		1.61	174.85	0%				
	port1	NonBusinessCritical_CloudApp	1.64	53.20	3%	16	23.03 Kbps	89.39	
	port2	BusinessCritical_CloudApps		0.81	174.25	0%			
		NonBusinessCritical_CloudApp		1.33	53.15	0%	4	13.49 Kbps	64.21
	root/branch.Office.02/root			1.46	1.37	0%	6	2.71 Kbps	3.39
To-HQ-A	shortcut								
	shortcut		1.23	1.13	0%	2	659 kbps	1.70	
To-HQ-B	BusinessCritical_CloudApps		2.20	179.61	0%	9	2.09 Kbps	5.03	
	Corporate		0.41	0.65	0%				
To-HQ-MPLS	BusinessCritical_CloudApps		0.78	177.93	0%				
	NonBusinessCritical_CloudApp		0.69	52.88	0%	12	9.10 Kbps	7.42	
	port1	BusinessCritical_CloudApps		0.58	177.66	0%			
		NonBusinessCritical_CloudApp		0.57	52.72	0%	12	5.58 Kbps	5.56

In the *SD-WAN Status* window, select a device to open the *Monitoring* dashboard.

- *Summary*
- *Traffic Overview*
- *Bandwidth Overview*: Total bandwidth and bandwidth per interface.
- Link health: *Jitter*, *Latency*, and *Packet Loss*.





Use the *Set Filter* dropdown available at the top of the *Monitoring* dashboard to filter the data (Today, Last 1 day, Last 1 week, Last 1 month, or Specify).

## Widget actions

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

- *Refresh*— refresh the data
- *action*—edit the widget
- *Drag to reorder*—select and then drag and drop to change the position of a widget in the pane



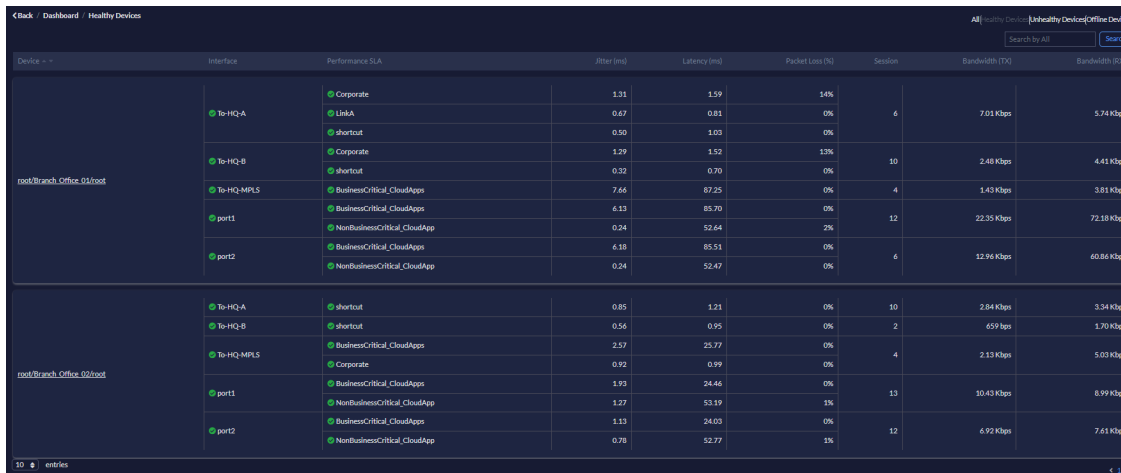
Hover over the widgets to see additional information.

## Edit actions

Selecting *Edit* in the *action* dropdown opens a window within the widget that allows you to select the top N results.

## Top Widgets

The widgets at the top (*SD-WAN Enabled Devices*, *Healthy Devices*, *Unhealthy Devices*, and *Offline Devices*) display performance related information in a table when clicked. This is same as the *SD-WAN Status* window that appears when devices are accessed from the map. See [SD-WAN Status on page 40](#).



Device	Interface	Performance SLA	jitter (ms)	Latency (ms)	Packet Loss (%)	Session	Bandwidth (TX)	Bandwidth (RX)	
root/Branch_Office_01/root	To-HQ-A	Corporate	1.31	1.59	14%				
	To-HQ-A	LinkA	0.67	0.81	0%	6	7.01 Kbps	5.74 Kbps	
		shortcut		0.50	1.03	0%			
	To-HQ-B	Corporate	1.29	1.52	13%	10	2.48 Kbps	4.41 Kbps	
		shortcut		0.32	0.70	0%			
	To-HQ-MPLS	BusinessCritical_CloudApps	7.66	87.25	0%	4	1.43 Kbps	3.81 Kbps	
		NonBusinessCritical_CloudApp		6.13	85.70	0%	12	22.35 Kbps	72.18 Kbps
part2	BusinessCritical_CloudApps		0.24	32.64	7%				
	NonBusinessCritical_CloudApp		6.18	85.51	0%	6	12.96 Kbps	40.86 Kbps	
root/Branch_Office_02/root	To-HQ-A	shortcut	0.85	1.21	0%	10	2.84 Kbps	3.34 Kbps	
	To-HQ-B	shortcut	0.56	0.95	0%	2	659 kbps	1.70 Kbps	
		BusinessCritical_CloudApps		2.57	25.77	0%			
	To-HQ-MPLS	Corporate	0.92	0.99	0%	4	2.13 Kbps	5.03 Kbps	
		BusinessCritical_CloudApps		1.93	24.46	0%			
	part1	NonBusinessCritical_CloudApp		1.27	53.19	1%	13	10.43 Kbps	8.99 Kbps
		BusinessCritical_CloudApps		1.13	24.03	0%			
part2	BusinessCritical_CloudApps		0.78	52.77	1%	12	6.93 Kbps	7.43 Kbps	
	NonBusinessCritical_CloudApp								

Selecting a device opens the *Monitoring* dashboard.



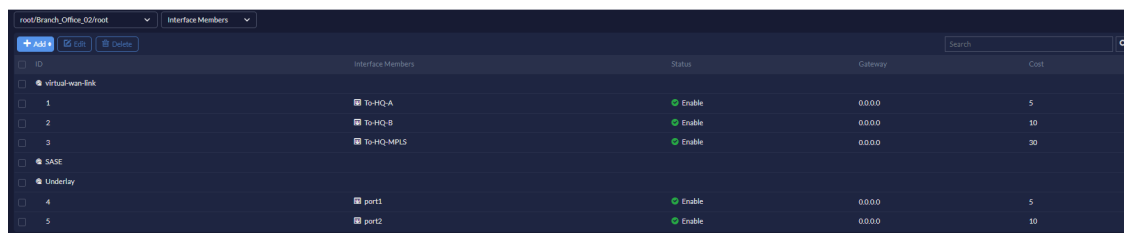
From the top-right, select *All/Healthy Devices/Unhealthy Devices/Offline Devices* to display related information in the table.

## Configuration

Go to the *Configuration* tab in *SD-WAN* and from the dropdown select devices under:

- *Central Management*—to create SD-WAN templates.
- *Per Device*—to create *Interface Members*, *Performance SLA*, and *SD-WAN Rules*.

The *Configuration* tab looks like the following:



ID	Interface Members	Status	Gateway	Cost
1	To-HQ-A	Enable	0.0.0.0	5
2	To-HQ-B	Enable	0.0.0.0	10
3	To-HQ-MPLS	Enable	0.0.0.0	30
4	part1	Enable	0.0.0.0	5
5	part2	Enable	0.0.0.0	10



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

See [Page actions on page 43](#).

## Page actions

The following actions are available in the *Configuration* tab:

- *Devices*—select devices in *Central Management* to create SD-WAN templates or *Per Device* to create Interface members, Performance SLA, and SD-WAN rules.
- *SD-WAN Templates/Interface Members/Performance SLA/SD-WAN Rules*—select *SD-WAN Templates*, *Interface Members*, *Performance SLA*, or *SD-WAN Rules* depending on the option selected in *Devices*.
- *Add/Create*—select to create new *SD-WAN Templates*, *SD-WAN Member*, *SD-WAN Zone*, *Performance SLA*, and *SD-WAN Rules*.



Per device SD-WAN members and zones can be created when *Interface Members* is selected.

---

- *Edit*—select to edit an SD-WAN template, interface member, performance SLA, and SD-WAN rule.
- *Delete*—select to delete an SD-WAN template, interface member, performance SLA, and SD-WAN rule.
- *Assign to Device*—assign an SD-WAN template to a device.
- *Move*—move an SD-WAN rule.
- *Search*—enter text to search in the content pane.
- *Sort*—some columns in the content pane have a sorting feature, allowing you to sort data in ascending or descending order.

A dropdown list at the bottom allows for selecting the number of entries to display per page.

## SD-WAN Templates

Select *SD-WAN Templates* from the dropdown in the *SD-WAN > Configuration* tab to define an SD-WAN for an ADOM.

### To add an SD-WAN Template:

1. Select *Configuration* in *SD-WAN*.
2. Ensure that a device under *Central Management* is selected.
3. Select *SD-WAN Templates* in the dropdown.
4. Select *Create*.

5. Enter values in the relevant fields.

Settings	Guidelines
Name	Enter a name for the new template.
Description	Enter a description for the new template.
Status	Select <i>enable</i> to enable the SD-WAN status.
Interface Members	Define which physical FortiPortal interfaces belong to the SD-WAN. <a href="#">Interfaces belonging to the SD-WAN template on page 44.</a>
Performance SLA	Define a new performance service level agreement (SLA). <a href="#">Define a performance SLA on page 45.</a>
SD-WAN Rule	Define SD-WAN rules to control how sessions are distributed to physical interfaces in the SD-WAN. <a href="#">Define SD-WAN rules on page 46.</a>

6. Click *Submit*.

### Interfaces belonging 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.

In the *Interface Members* pane in *SD-WAN > Configuration > SD-WAN Template*, the following actions are available:

- *Create*—define a new interface member or SD-WAN zone
- *Edit*—edit an interface member or SD-WAN zone
- *Delete*—delete an interface member or SD-WAN zone

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

1. After step 4 in [To add an SD-WAN Template: on page 43](#), in the *Interface Members* pane, select *SD-WAN Member* from the *Create* dropdown.
2. In the *Create New SD-WAN Interface Members* dialog, enter values in the relevant fields.

Settings	Guidelines
Sequence Number	Member sequence number. The range is 0-4294967295.
Interface Member	Enter a name for the interface member.
SD-WAN Zone	From the dropdown, select an SD-WAN zone.
Gateway IP	Enter the IPv4 address of the default gateway for this interface.
Cost	More traffic is directed to interfaces with higher costs. The cost field must be 0 or more.
Status	Toggle <i>On</i> or <i>Off</i> to enable or disable the SD-WAN status.
Priority	Assign interfaces a priority based on the priority assigned to the interface.

3. Click *Submit*.

**To create a new SD-WAN zone:**

1. After step 4 in [To add an SD-WAN Template: on page 43](#), in the *Interface Members* pane, select *SD-WAN Zone* from the *Create* dropdown.
2. In the *Create New SD-WAN Zone* dialog:
  - a. Enter a name for the SD-WAN zone.
  - b. Add interface members to it from the *Interface Members* dropdown.
3. Click *Submit*.

**Define a performance SLA**

Use the *Performance SLA* pane in *SD-WAN > Configuration > SD-WAN Template* to configure SLA management.

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

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

**To add a new performance SLA:**

1. After step 4 in [To add an SD-WAN Template: on page 43](#), select *Create* in the *Performance SLA* pane.
2. In the *Create New Performance SLA* dialog, enter values in the relevant fields.

Settings	Guidelines
Name	Enter a name for the performance SLA.
IP Version	From the dropdown, select either IPv4 or IPv6.
Probe Mode	Select <i>Active</i> , <i>Passive</i> , or <i>Prefer Passive</i> probe mode.
Protocol	Protocol used to determine if the FortiPortal unit can communicate with the server. Select <i>HTTP</i> , <i>Ping</i> , <i>TCPECHO</i> , <i>TWAMP</i> , or <i>UDP ECHO</i> .
Health Check Server	Select a health check server.
Participants	<i>All SD-WAN Members</i> or <i>Specify</i> the SD-WAN members.
Enable Probe Packets	Toggle <i>On</i> or <i>Off</i> sending probe packets.
<b>SLA</b>	
Select <i>Create</i> , enter values in the relevant fields, and click <i>Submit</i> .	
Latency Threshold	Latency for SLA to make decision in milliseconds. The default is 5; the range is 0 - 1000000.
Jitter Threshold	Jitter for SLA to make decision in milliseconds. The default is 5; the range is 0 - 1000000.
Packet Loss Threshold	Packet loss for SLA to make decision in percentage. The default is 0; the range is 0 -100.
<b>Link Status</b>	

Settings	Guidelines
Interval	Status check interval, which is the time between attempting to connect to the server, in seconds (1 - 3600, default = 5).
Failure Before Inactive	Number of failures before server is considered lost (1 - 10, default = 5).
Restore Link After	Number of successful responses received before the server is considered recovered (1 - 10, default = 5).
<b>Action When Inactive</b>	
Update Static Route	Toggle <i>On</i> or <i>Off</i> updating the static route.
Update Cascade Interface	Toggle <i>On</i> or <i>Off</i> updating the cascade interface.

3. Click *Submit*.

### Define SD-WAN rules

Use the *SD-WAN Rule* pane in *SD-WAN > Configuration > SD-WAN Template* to configure SD-WAN rules or priority rules to control how sessions are distributed to physical interfaces in the SD-WAN.

In the *SD-WAN Rule* pane, the following actions are available:

- *Create*—define an SD-WAN rule
- *Edit*—edit an existing SD-WAN rule
- *Delete*—delete an existing SD-WAN rule
- *Move*—move an SD-WAN rule

### To add a new SD-WAN rule:

1. After step 4 in [To add an SD-WAN Template: on page 43](#), select *Create* in the *SD-WAN Rule* pane.
2. In the *Create New SD-WAN Rules* dialog, enter values in the relevant fields.

Settings	Guidelines
Name	Enter a priority rule name.
IP Version	From the dropdown, select either IPv4 or IPv6.
<b>Source</b>	
Source Address	Select the source addresses from the list.
User(s)	Select the users from the list.
User Groups	Select the user groups from the list.
<b>Destination</b>	
Select <i>Address</i> to use destination addresses or select <i>Internet Service</i> to use destination Internet services.	
Address	Available if <i>Destination</i> is set to <i>Address</i> . Select the destination addresses from the list.

Settings	Guidelines
Route Tag	Available if <i>Destination</i> is set to <i>Address</i> . Available when route tags are defined for BGP route-map.
Protocol	Available if <i>Destination</i> is set to <i>Address</i> . Select <i>TCP</i> , <i>UDP</i> , <i>ANY</i> , or <i>Specify</i> . If you select <i>Specify</i> , enter the protocol number, type of service, and bit mask.
Type of Service Bit Mask	Type of service evaluated bits. This value determines which bits in the IP header's TOS field are significant.
Type of Service	Type of service bit pattern.
Internet Service	Available if <i>Destination</i> is set to <i>Internet Service</i> . Select the Internet services from the list.
Internet Service Group	Available if <i>Destination</i> is set to <i>Internet Service</i> . Select the Internet service groups from the list.
Custom Internet Service	Available if <i>Destination</i> is set to <i>Internet Service</i> . Select the custom Internet services from the list.
Application	Available if <i>Destination</i> is set to <i>Internet Service</i> . Select the applications from the list.
Application Group	Available if <i>Destination</i> is set to <i>Internet Service</i> . Select the application groups from the list.
<b>Outgoing Interfaces</b>	
Strategy	Select <i>Manual</i> , <i>Best Quality</i> , <i>Lowest Cost (SLA)</i> , or <i>Maximize Bandwidth (SLA)</i> .
Interface Preference	Set interface preference order when multiple eligible links have the same cost.

3. Click *Submit*.

## Per Device Interface Members

### To add a new interface member per device:

1. Select *Configuration* in *SD-WAN*.
2. Ensure that a device under *Per Device* is selected.
3. Select *Interface Members* from the dropdown.
4. In *Add*, select *SD-WAN Member* or *SD-WAN Zone*.
5. Enter values in the relevant fields in [To define which physical interfaces belong to the SD-WAN template: on page 44](#) for *SD-WAN Member* and in [To create a new SD-WAN zone: on page 45](#) for *SD-WAN Zone*.
6. Click *Save*.

## Per Device Performance SLA

### To add a new performance SLA per device:

1. Select *Configuration* in *SD-WAN*.
2. Ensure that a device under *Per Device* is selected.
3. Select *Performance SLA* from the dropdown.
4. Select *Create*.
5. Enter values in the relevant fields in [To add a new performance SLA: on page 45](#).
6. Click *Save*.

## Per Device SD-WAN Rules

### To add a new SD-WAN rule per device:

1. Select *Configuration* in *SD-WAN*.
2. Ensure that a device under *Per Device* is selected.
3. Select *SD-WAN Rules* from the dropdown.
4. Select *Create*.
5. Enter values in the relevant fields in [To add a new SD-WAN rule: on page 46](#).
6. Click *Save*.



# Security

Go to *Security* to access policy, firewall objects, and network related settings.

The following tabs are available in *Security*:

- [Policy on page 50](#)
- [Firewall objects on page 56](#)
- [Network on page 77](#)

# Policy

Go to *Policy* to view policies grouped by type.

Use the *Policy Package* dropdown to open a new window that displays devices.



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

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile	Protocol Options	Log	NAT	Comments
1	Out Overlay Traf	port1	Undefay	BOL_LAN	BOL_Guest	all	always	ALL	Accept	default	default	Log All Sessions	Enabled	
2	Out Overlay Traff	port1	virtual-wan-lin	BOL_LAN	BOL_Guest	all	always	ALL	Accept	default	default	Log All Sessions	Disabled	
3	In Overlay Traffic	virtual-wan-lin	port3	all	BOL_LAN	always	ALL	ALL	Accept	default	default	Log All Sessions	Disabled	
4	Traffic-To-FortiNA	FWAC_Isolatio	port7	all	all	always	ALL	ALL	Accept	no-inspection	default	Log All Sessions	Disabled	
5	antispoam_to_U	antispoam	Undefay	all	all	always	ALL	ALL	Accept	no-inspection	default	Log All Sessions	Enabled	
6	unboarding_to_U	unboarding	Undefay	all	all	always	ALL	ALL	Accept	no-inspection	default	Log All Sessions	Enabled	
7	bypass-webfilter	antispoam_off	Undefay	all	BOL_BFW	always	ALL	ALL	Accept	no-inspection	default	Log All Sessions	Disabled	
8	antispoam_off_to_U	antispoam_off	Undefay	all	all	always	ALL	ALL	Accept	block_yahoo.co	default	Log All Sessions	Enabled	
Implicit / Total: 1														
-	Implicit Deny	any	any	all	all	always	all	all	Deny			No Log	Disabled	

The page includes a dropdown list of policy packages at the top. When you select an entry, the content pane displays the policy data associated with that entry.



When a policy package is assigned to a device in FortiManager but never installed, FortiPortal does not show the policy package.

A policy package is displayed in FortiPortal, given that it has been installed or modified in FortiManager.



FortiPortal now supports FortiManager policies with consolidated firewall mode enabled.

## Page actions

The following actions are available in the *Policy* tab:

- 
- *Policy Package*—from the dropdown, select a policy package to display.
  - *Policy type*—from the dropdown, select a policy type to display for the selected policy package.
  - *View*—view settings that affect all policies in a package. See [Viewing policy package settings on page 53](#).
  - *Refresh*—refresh the policy information. See [Policy data refresh on page 53](#).
  - *Policy Revisions*—opens the *Policy Revisions* window. See [Creating and restoring policy revisions on page 54](#).
  - *Install*—opens the *Policy Install* window. See [Installing policies on page 54](#).
  - *Export to CSV*—export policy package information as a CSV file.
  - *Create*—create a new policy. See [Configuring policies on page 51](#).
  - *Edit*—edit a selected policy. See [Configuring policies on page 51](#).
  - *Delete*—delete selected policies.
  - *Action*—enable/disable or move a selected policy. See [Policy action on page 55](#).
  - *Column Settings*—use the dropdown to select what columns to display in the *Policy* tab. See [Policy tab column settings on page 55](#).
  - *Search*—use the search bar to look for a policy based on object name, IP address or a portion of the IP address.
- 



You can also look for policies based on port numbers within the service objects or objects found in groups or nested groups.

---

## Configuring policies

Go to *Policy* to create and edit policies.

---



Your service provider can grant write access to your policies. If so, you are enabled to create/edit/delete, enable/disable, and change the order of the policies.

If not, FortiPortal displays a warning message and restricts the data in the Policy page to read-only.

---

## Adding a new firewall policy

1. Go to *Policy*.
2. Select a policy package where this policy is created and *Firewall Policy* in *Policy type*.
3. Select *Create* to create a new policy.  
The *Create Firewall Policy* window opens.

4. In the *Create Firewall Policy* window, enter the following information:

Settings	Guidelines
Name	Name for the policy.
Incoming Interface	From the dropdown, select one or more incoming interfaces.
Outgoing Interface	From the dropdown, select one or more outgoing interfaces.
Source Internet Service	Enable/disable the source internet service, then select services. This option is only available for IPv4 policies.
IPv4 Source Address	Select the IPv4 source addresses. This option is only available when <i>Source Internet Service</i> is disabled.
Source User	Select source users.
Source User Group	Select source user groups.
FSSO Groups	Select the FSSO groups added via Fortinet Single Sign-On.
Destination Internet Service	Enable/disable the destination internet service, then select services. This option is only available for IPv4 policies.
IPv4 Destination Address	Select to add one or more address objects. This option is only available when <i>Destination Internet Service</i> is disabled.
Service	Select services and service groups. This option is only available when <i>Destination Internet Service</i> is disabled.
Schedule	Select one entry from the dropdown.
Action	Accept or deny.
<b>Disclaimer Options</b>	
Display Disclaimer	Enable disclaimer for this type of traffic.
Customize Message	From the dropdown, select a customized message. This option is only available if <i>Display Disclaimer</i> is enabled.
<b>Logging Options</b>	
Log Violation Traffic	Enable to create a log for each denied packet.
Generate Logs when Session Starts	Enable to generate logs when the session starts.
<b>Advanced</b>	
WCCP	Enable Web Cache Communication Protocol (WCCP).
Exempt from Captive Portal	Select to exempt from the captive portal.
Comments	Optionally, enter a comment for the policy.

5. Click **Save**.

---

## Updating a policy

**To update a policy:**

1. Select a policy and then select *Edit*.
2. Modify the relevant fields and select *Save*.

## Deleting a policy

**To delete a policy:**

1. Select policies in the list and then select *Delete*.

## Re-installing the policy

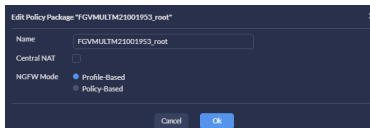
**To reinstall the policy:**

1. After you create or edit a policy, select *Install* to view the installation targets.
2. Select the device and then select *Install* to install the policy packages to the assigned device.

## Viewing policy package settings

Policy packages are listed at the top of the *Policy* tab in the *Policy Package* dropdown.

To check settings that affect all policies in a package, click the *View* icon after selecting a policy package from the dropdown.



The Policy Package dialog 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*.

---

## 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).

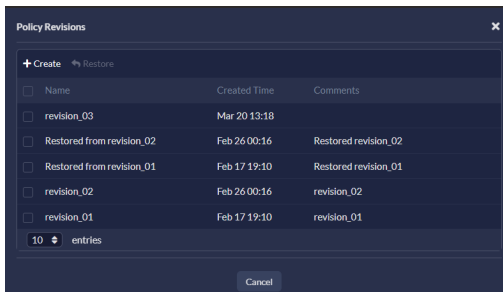
Observe the following restrictions:

- Organization must be part of only one ADOM.
- No other organization can be part of that ADOM.

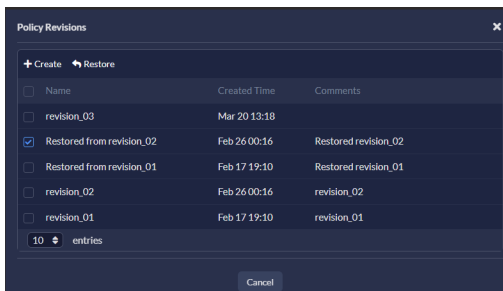
## Creating and restoring policy revisions

Select *Policy Revisions* to open the *Policy Revisions* window.

Select *Create* to define a backup of the current policy and object data. If one exists, the *Policy Revisions* window provides details.



To restore the backup, select the entry, and then select *Restore*.

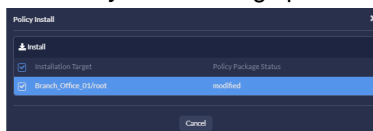


## Installing policies

You can install or reinstall policy packages from *Policy > Install*.

**To install a policy package:**

1. Go to the *Policy* tab.
2. Select the policy package in the *Policy Package* dropdown and select *Install*.
3. The *Policy Install* dialog opens.



4. Select one or more devices from the list.
5. Click *Install*.  
The progress bar on the *Policy Install* dialog shows the status of the installation.

6. Once the policy package is installed, click *Finish*.

## Policy tab column settings

To display selected columns in the *Policy* tab:

1. In the *Column Settings* dropdown:
  - a. Select the columns you want to display and clear the columns you want to hide.



Select *Reset to default* to reset the column display.

## Policy action

After selecting a policy, select *Action* to enable, disable, or move policies.



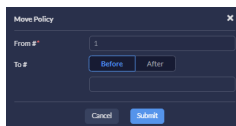
A disabled policy is marked with a red x sign before it in the Seq.# column.

#	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profile	Log	NAT	Comments
1	aaa@11111	wsp-root	any	all	not-test	always	ALL_ICMP BGP CVSFSERVER	Accept	no-inspection	Log Security Events	Enabled	
x 2	testtest12345w w3	any	lan	test ipfs.google-play	all	always	ALL	Accept	default	Log All Sessions	Enabled	55123
3	test2324	lan	wan2	all	all	always	ALL	Accept	no-inspection	Log All Sessions	Enabled	

## Moving a policy

To change the order of the policies:

1. Select the policy in the list and then select *Move* from the *Action* dropdown. The system opens a dialog box, showing the policy ID of the selected policy.



2. Select the option of *Before* or *After*.
3. Enter the target Policy ID.



Enter the ID, not the sequence number.

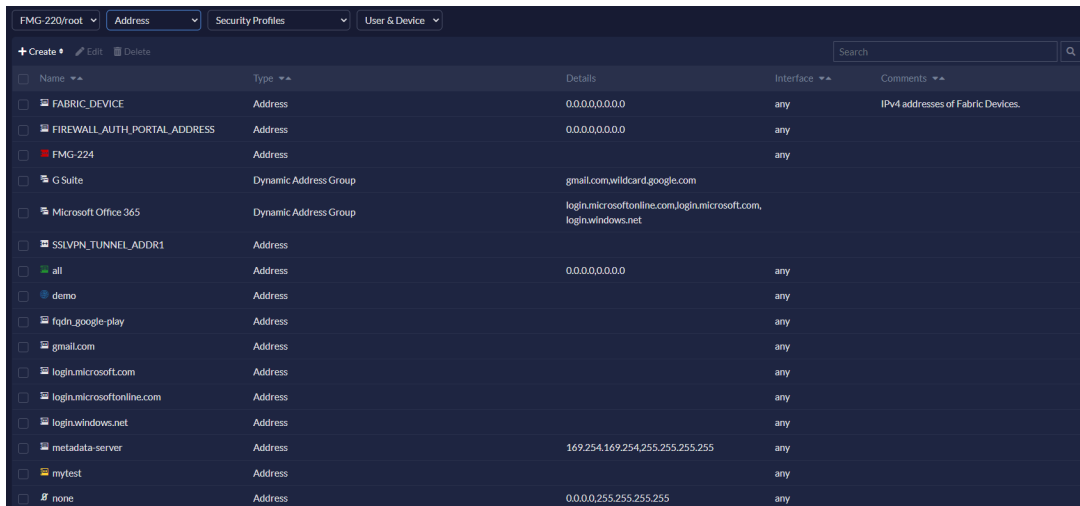
4. Click *Submit*. The system moves the selected policy to before/after the target.

## Firewall objects

The *Firewall objects* tab provides a view of the objects that are defined in the FortiManager devices. Firewall objects include items such as addresses, schedule, services, and virtual IP(s).

You can also set up security profiles, user, and user groups.

You can use an object in more than one policy to avoid repeating data in multiple places.



The screenshot shows the FortiManager interface for the 'Address' tab. At the top, there are dropdown menus for 'FMG:220/root', 'Address', 'Security Profiles', and 'User & Device'. Below these are buttons for 'Create', 'Edit', and 'Delete', and a search bar. The main area is a table with columns: Name, Type, Details, Interface, and Comments. The table lists various objects such as FABRIC\_DEVICE, FIREWALL\_AUTH\_PORTAL\_ADDRESS, FMG-224, G Suite, Microsoft Office 365, SSLVPN\_TUNNEL\_ADDR1, all, demo, fqdn\_google-play, gmail.com, login.microsoft.com, login.microsoftonline.com, login.windows.net, metadata-server, mytest, and # none.

Name	Type	Details	Interface	Comments
FABRIC_DEVICE	Address	0.0.0.0,0.0.0.0	any	IPV4 addresses of Fabric Devices.
FIREWALL_AUTH_PORTAL_ADDRESS	Address	0.0.0.0,0.0.0.0	any	
FMG-224	Address		any	
G Suite	Dynamic Address Group	gmail.com,wildcard.google.com		
Microsoft Office 365	Dynamic Address Group	login.microsoftonline.com,login.microsoft.com,login.windows.net		
SSLVPN_TUNNEL_ADDR1	Address			
all	Address	0.0.0.0,0.0.0.0	any	
demo	Address		any	
fqdn_google-play	Address		any	
gmail.com	Address		any	
login.microsoft.com	Address		any	
login.microsoftonline.com	Address		any	
login.windows.net	Address		any	
metadata-server	Address	169.254.169.254,255.255.255.255	any	
mytest	Address		any	
# none	Address	0.0.0.0,255.255.255.255	any	

Dropdown menus at the top lets you access the firewall objects. When you select an object in the dropdown menu, the content pane displays the data associated with that object. This data is displayed for the selected ADOM. You can select a different ADOM using the ADOM dropdown list.

## Types of objects

The page displays the following object categories:

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

## Firewall Objects

Firewall objects are components of the firewall that go together like interlocking building blocks. Firewall objects can be configured once and then reused. They assist in making the administration of the firewall unit easier and more intuitive.

Firewall objects include address, schedule, service and virtual IP.

### 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 groups, which defines a group of related addresses.



Address firewall objects list looks like the following:

Name	Type	Details	Interface	Comments
FABRIC_DEVICE	Address	0.0.0.0/0.0.0.0	any	IPv4 addresses of Fabric Devices.
FIREWALL_AUTH_PORTAL_ADDRESS	Address	0.0.0.0/0.0.0.0	any	
G Suite	Dynamic Address Group	gmail.com,wildcard.google.com		
Microsoft Office 365	Dynamic Address Group	login.microsoftonline.com,login.microsoft.com,login.windows.net		
SSLVPN_TUNNEL_ADDR1	Address		any	
all	Address	0.0.0.0/0.0.0.0	any	
gmail.com	Address		any	
login.microsoft.com	Address		any	
login.microsoftonline.com	Address		any	
login.windows.net	Address		any	
metadata-server	Address	169.254.169.254,255.255.255.255	any	
none	Address	0.0.0.0,255.255.255.255	any	
wildcard.dropbox.com	Address		any	
wildcard.google.com	Address		any	

## Schedule

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

Schedule firewall objects list looks like the following:

Name	Type	Details
always	Recurring Schedule	SMTWTFSS 00:00-00:00
default-darrp-optimize	Recurring Schedule	SMTWTFSS 01:30-01:30
none	Recurring Schedule	-----00:00-00:00

## 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/SCTP*—address and destination port range
- *ICMP*—type and code

Service firewall objects list looks like the following:

Name	Type	Details	Comments	Created Time	Last Modified
ALL	General	IP/0		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
ALL_TCP	General	TCP/1-65535		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
ALL_UDP	General	UDP/1-65535		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
ALL_ICMP	General	ICMP / ANY		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
ALL_ICMP6	General	ICMP6 / ANY		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
GRE	Tunneling	IP/47		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
GTP	Uncategorized	UDP/2123,2152,3386		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
AH	Tunneling	IP/51		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
ESP	Tunneling	IP/50		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
AOL	Uncategorized	TCP/5190-5194		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
BGP	Network Services	TCP/179		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
DHCP	Network Services	UDP/67-68		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
DNS	Network Services	TCP/53, UDP/53		2022-04-22 17:36:24	admin/2022-04-22 17:36:24

## Virtual IP

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

FortiPortal supports the following Virtual IP object types:

- *Virtual IP*—uses static NAT to map a range of external addresses to an internal address range
- *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 features protecting the network from threats are together known as security profiles.

The following security profiles are supported on FortiPortal:

- Antivirus Profile
- Intrusion Prevention Profile
- Local Category
- Web Rating Overrides
- Web Filter Profile
- Application Control

## Antivirus Profile

Use the Antivirus profile to detect and identify viruses.

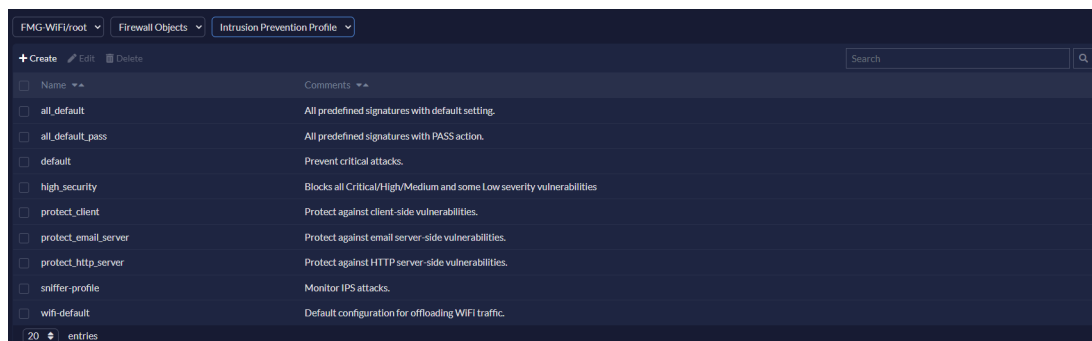
Antivirus security profiles list looks like the following:

Name	Comments
default	Scan files and block viruses.
sniffer-profile	Scan files and monitor viruses.
wifi-default	Default configuration for offloading WiFi traffic.

## Intrusion Prevention Profile

Use intrusion prevention profiles to protect your network against hacking and attempts to exploit vulnerabilities.

Intrusion prevention profiles list looks like the following:



The screenshot shows the FortiPortal interface for the 'Intrusion Prevention Profile' section. It features a table with columns for Name, Comments, and a search bar. The table lists several profiles with their respective descriptions.

Name	Comments
all_default	All predefined signatures with default setting.
all_default_pass	All predefined signatures with PASS action.
default	Prevent critical attacks.
high_security	Blocks all Critical/High/Medium and some Low severity vulnerabilities
protect_client	Protect against client-side vulnerabilities.
protect_email_server	Protect against email server-side vulnerabilities.
protect_http_server	Protect against HTTP server-side vulnerabilities.
sniffer-profile	Monitor IPS attacks.
wifi-default	Default configuration for offloading WIFI traffic.

## 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.

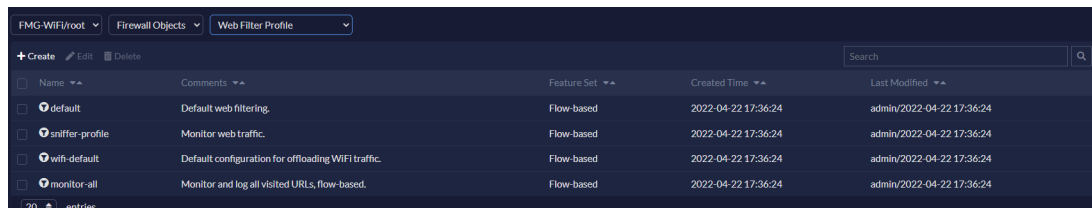
## Web Rating Overrides (security profile introduced with FortiPortal 1.2.0)

Use a *Web Rating Override* object to override the rating for a URL.

## Web Filter Profile

Set up a web filter profile to protect or limit user activity on the web.

The web filter security profiles list looks like the following:



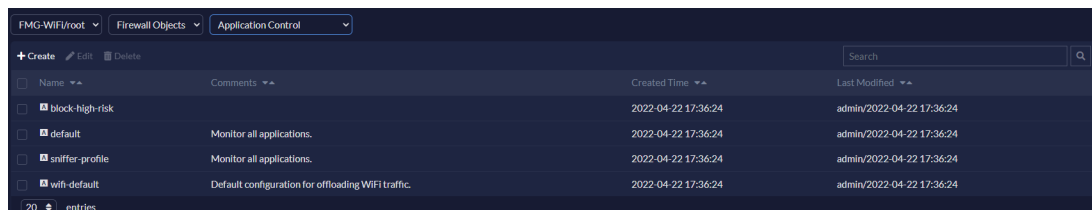
The screenshot shows the FortiPortal interface for the 'Web Filter Profile' section. It features a table with columns for Name, Comments, Feature Set, Created Time, and Last Modified. The table lists several profiles with their respective descriptions and settings.

Name	Comments	Feature Set	Created Time	Last Modified
default	Default web filtering.	Flow-based	2022-04-22 17:36:24	admin/2022-04-22 17:36:24
sniffer-profile	Monitor web traffic.	Flow-based	2022-04-22 17:36:24	admin/2022-04-22 17:36:24
wifi-default	Default configuration for offloading WIFI traffic.	Flow-based	2022-04-22 17:36:24	admin/2022-04-22 17:36:24
monitor-all	Monitor and log all visited URLs, flow-based.	Flow-based	2022-04-22 17:36:24	admin/2022-04-22 17:36:24

## Application Control

Use application control to detect network traffic and control application communication.

The application control security profiles list looks like the following:



The screenshot shows the FortiPortal interface for the 'Application Control' section. It features a table with columns for Name, Comments, Created Time, and Last Modified. The table lists several profiles with their respective descriptions and settings.

Name	Comments	Created Time	Last Modified
block-high-risk		2022-04-22 17:36:24	admin/2022-04-22 17:36:24
default	Monitor all applications.	2022-04-22 17:36:24	admin/2022-04-22 17:36:24
sniffer-profile	Monitor all applications.	2022-04-22 17:36:24	admin/2022-04-22 17:36:24
wifi-default	Default configuration for offloading WIFI traffic.	2022-04-22 17:36:24	admin/2022-04-22 17:36:24

---

## User & Device

Security policies may allow access to specified users and user groups only.

### User

A user is a user account consisting of username, password, and in some cases other information, configured on the firewall unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group.

You can create local users (accounts stored on the firewall unit), see [Configuring a user](#).

### Two-factor authentication

Two-factor authentication methods, including FortiToken, provide additional security.

### User Group

A user group is a list of user identities. To add or edit a user group, see [Configuring a user group](#).



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

---

## Page actions

The following actions are available on the *Firewall Objects* tab:

- *ADOM*—select an ADOM from the dropdown to display related firewall objects.
- *Type*—select a firewall object type from the dropdown.
- *Security Profiles*—select a security profile from the dropdown.
- *Create*—select to create a firewall object or a security profile.
- *Edit*—edit a selected firewall object or a security profile.
- *Delete*—delete selected firewall objects or a security profile.
- *Search*—search a firewall object or a security profile.
- *Sort*—Some columns in the content pane have a sorting feature, allowing you to sort data in ascending or descending order.
- *Show x entries*— set the number of entries per page (20 or 50).

## Configuring firewall objects

- [Configuring an address](#)
- [Configuring an address group](#)
- [Configuring a schedule](#)
- [Configuring a service](#)

- 
- [Configuring a virtual IP](#)
  - [Configuring an Antivirus profile](#)
  - [Configuring an intrusion prevention profile](#)
  - [Configuring a local category](#)
  - [Configuring a web rating override](#)
  - [Configuring a web filter profile](#)
  - [Configuring application control](#)
  - [Configuring a user](#)
  - [Configuring a user group](#)
- 



Address and address group firewall objects support IPv6 addresses.

---

### **To configure an address:**

1. Go to *Security > Firewall Objects*.
2. Select *Address* in the firewall object type dropdown.
3. In the *Create* dropdown, select *Address* to open the *Create Address* dialog.

4. In the *Create Address* dialog, enter the following information:

Settings	Guidelines
Name	Required. Enter a name for the address.
Color	From the dropdown, select a color option.
Type	Required. Select a type from the following options in the dropdown: <ul style="list-style-type: none"> <li>• <i>Subnet</i> (default)</li> <li>• <i>IP Range</i></li> <li>• <i>FQDN</i></li> <li>• <i>Geography</i></li> <li>• <i>Dynamic</i></li> <li>• <i>Device (MAC Address)</i></li> </ul>
Sub Type	Required. Select a subtype from the following options in the dropdown: <ul style="list-style-type: none"> <li>• <i>ClearPass</i> (default)</li> <li>• <i>Fabric Connector Address</i></li> <li>• <i>FortiNAC Tag</i></li> <li>• <i>FortiVoice Tag</i></li> <li>• <i>Fortinet Single Sign-On</i></li> <li>• <i>Switch Controller NAC Policy Tag</i></li> </ul> <p><b>Note:</b> This option is only available when the <i>Type</i> is <i>Dynamic</i>.</p>
IP/Netmask	Required. Enter the IP address and the netmask. <b>Note:</b> This option is only available when the <i>Type</i> is <i>Subnet</i> .
IP Range	Required. Enter the IP address range. <b>Note:</b> This option is only available when the <i>Type</i> is <i>IP Range</i> .
FQDN	Required. Enter the Fully Qualified Domain Name (FQDN). <b>Note:</b> This option is only available when the <i>Type</i> is <i>FQDN</i> .
Geography/Region	Required. Select a country/territory from the dropdown. <b>Note:</b> This option is only available when the <i>Type</i> is <i>Geography</i> .
SPT(System Posture Token)	Required. Select an SPT from the following options in the dropdown: <ul style="list-style-type: none"> <li>• <i>Checkup</i> (default)</li> <li>• <i>Healthy</i></li> <li>• <i>Infected</i></li> <li>• <i>Quarantine</i></li> <li>• <i>Transient</i></li> <li>• <i>Unknown</i></li> </ul> <p><b>Note:</b> This option is only available when the <i>Sub Type</i> is <i>Clear Pass</i>.</p>
Fabric Connector Address	Required. From the dropdown, select a <i>Fabric Connector Address</i> . <b>Note:</b> This option is only available when the <i>Sub Type</i> is <i>Fabric Connector Address</i> .

Settings	Guidelines
Fortinet Single Sign-On (FSSO)	Required. From the dropdown, select an FSSO option. <b>Note:</b> This option is only available when the <i>Sub Type</i> is Fortinet Single Sign-On (FSSO).
MAC Address	Select +, and enter the MAC addresses. <b>Note:</b> This option is only available when the <i>MAC Address Scope</i> is <i>single</i> .
Interface	Required. From the dropdown, select an interface.
Static route configuration	Enable static route configuration. <b>Note:</b> This option is not available when the <i>Type</i> is <i>Geography, Dynamic, or Device (MAC Address)</i> .
Comments	Enter comments about the address.

5. Click **Save**.

#### To configure an address group:

1. Go to *Security > Firewall Objects*.
2. Select *Address* in the firewall object type dropdown.
3. In the *Create* dropdown, select *Address Group* to open the *Create Address Group* dialog.
4. In the *Create Address Group* dialog, enter the following information:

Settings	Guidelines
Name	Required. Enter a name for the address group.
Color	From the dropdown, select a color option.
Members	Required. From the dropdown, select an address.
Comments	Enter comments about the address group.

5. Click **Save**.

#### To configure a schedule:

1. Go to *Security > Firewall Objects*.
2. Select *Schedule* in the firewall object type dropdown.
3. Select *Create* to open the *Create New Schedule* dialog.

4. In the *Create New Schedule* dialog, enter the following information:

Settings	Guidelines
Type	Select either <i>One Time Schedule</i> or <i>Recurring Schedule</i> .
Name	Required. Enter a name for the schedule.
Color	From the dropdown, select a color option.
Start Time	Enter a start date (MM/DD/YYYY) and time. Alternatively, select the calendar icon and then select the date of your choice. Similarly, select the clock icon to select a time. <b>Note:</b> The date option is only available when the <i>Type</i> is <i>One Time Schedule</i> .
End Time	Enter the end date (MM/DD/YYYY) and time. Alternatively, select the calendar icon and then select the date of your choice. Similarly, select the clock icon to select a time. <b>Note:</b> The date option is only available when the <i>Type</i> is <i>One Time Schedule</i> .
Days	Select days of the week the schedule applies. <b>Note:</b> This option is only available when the <i>Type</i> is <i>Recurring Schedule</i> .
All Day	Select the option if the schedule applies all day. <b>Note:</b> This option is only available when the <i>Type</i> is <i>Recurring Schedule</i> .
Pre-expiration event log	Select to create an event log <i>Number of days before the End Time</i> . <b>Note:</b> This option is selected by default and only available when the <i>Type</i> is <i>One Time Schedule</i> .
Number of days before	Enter the number of days (default = 3). <b>Note:</b> This option is only available when the <i>Type</i> is <i>One Time Schedule</i> and <i>Pre-expiration event log</i> is selected.


5. Click **Save**.

#### To configure a service:

1. Go to *Security > Firewall Objects*.
2. Select *Service* in the firewall object type dropdown.
3. Select *Create* to open the *Create Service* dialog.



4. In the *Create Service* dialog, enter the following information:

Settings	Guidelines
Name	Enter a name for the service.
Comments	Enter comments about the service.
Color	Required. From the dropdown, select a color.
Show in Service list	Enable to display the service in the service list. <b>Note:</b> This option is enabled by default.
Category	From the dropdown, select a category from the following options: <ul style="list-style-type: none"> <li>• <i>Uncategorized</i> (default)</li> <li>• <i>Authentication</i></li> <li>• <i>Email</i></li> <li>• <i>File Access</i></li> <li>• <i>General</i></li> <li>• <i>Network Services</i></li> <li>• <i>Remote Access</i></li> <li>• <i>Tunneling</i></li> <li>• <i>VoIP, Messaging, &amp; Other Application</i></li> <li>• <i>Web Access</i></li> <li>• <i>Web Proxy</i></li> </ul>
Protocol Type	Select a protocol type: <ul style="list-style-type: none"> <li>• <i>TCP/UDP/SCTP</i>—address and destination port range (default).</li> <li>• <i>ICMP</i>—type and code</li> <li>• <i>IP</i>—IP protocol number</li> </ul>
Address	Select either <i>IP Range</i> or <i>FQDN</i> and then enter the IP address range or the FQDN. <b>Note:</b> This option is only available when the <i>Protocol Type</i> is <i>TCP/UDP/SCTP</i> .
Destination Port	From the dropdown, select <i>TCP</i> , <i>UDP</i> , or <i>SCTP</i> protocol type and enter a port range.
	<div style="text-align: center;">  </div> <p>Select + to add multiple destination ports and ranges. Select the <i>Delete</i> (✖) icon to remove a destination port.</p>
	<b>Note:</b> This option is only available when the <i>Protocol Type</i> is <i>TCP/UDP/SCTP</i> .
Type	Enter the type number. <b>Note:</b> This option is only available when the <i>Protocol Type</i> is <i>ICMP</i> .
Code	Enter the code number. <b>Note:</b> This option is only available when the <i>Protocol Type</i> is <i>ICMP</i> .
Protocol Number	Enter the protocol number.

**Note:** This option is only available when the *Protocol Type* is *IP*.

5. Click *Save*.

#### To configure a virtual IP:

1. Go to *Security > Firewall Objects*.
2. Select *Virtual IP* in the firewall object type dropdown.
3. Select *Create* to open the *Create Service* dialog.

4. In the *Create New VirtualIP* dialog, enter the following information:

Settings	Guidelines
Type	Select either <i>Virtual IP</i> or <i>Virtual IP Group</i> . <b>Note:</b> By default, <i>Virtual IP</i> is selected.
Name	Required. Enter a name for the virtual IP or the virtual IP group.
comment	Enter comments about the virtual IP or the virtual IP group.
Color	From the dropdown, select a color.
Members	From the dropdown, select members. <b>Note:</b> This option is only available if the <i>Type</i> is <i>Virtual IP Group</i> .
<b>Firewall/Network Options</b>	
Interface	From the dropdown, select an interface.
Type	Select either <i>Static NAT</i> or <i>FQDN</i> . <b>Note:</b> By default, <i>Static NAT</i> is selected.
External IP Address/Range	Required. Enter the public IP address or range.
Mapped IPV4 Address/Range	Required. Enter the IPv4 address or range the traffic is directed to. <b>Note:</b> This option is only available when the type is <i>Static NAT</i> .
Mapped Address	From the dropdown, select a mapped address. <b>Note:</b> This option is only available when the type is <i>FQDN</i> .
Port Forwarding	Enable/disable port forwarding. <b>Note:</b> This option is disabled by default.
Protocol	Select from the following protocols: <ul style="list-style-type: none"> <li>• <i>TCP</i> (default)</li> <li>• <i>UDP</i></li> <li>• <i>SCTP</i></li> <li>• <i>ICMP</i></li> </ul> <b>Note:</b> This option is only available when <i>Port Forwarding</i> is enabled.
External Service Port	Required. Enter the range of the external interface ports. <b>Note:</b> This option is only available when <i>Port Forwarding</i> is enabled and the protocol is not <i>ICMP</i> .
Map to IPv4 Port	Required. Enter the range of the listening ports. <b>Note:</b> This option is only available when <i>Port Forwarding</i> is enabled and the protocol is not <i>ICMP</i> .
Enable ARP Reply	Select to enable Address Resolution Protocol (ARP) replies. <b>Note:</b> This option is enabled by default.

5. Click *Save*.

---

**To configure an Antivirus profile:**

1. Go to *Security > Firewall Objects*.
2. Select *Antivirus Profile* from the *Security Profiles* dropdown.
3. Select *Create* to create an Antivirus profile.

4. In the *Create Antivirus Profile* dialog, enter the following information:

Settings	Guidelines
Name	Enter a name for the Antivirus profile.
Comments	Enter comments about the Antivirus profile.
AntiVirus scan	Enable Antivirus scan. <b>Note:</b> The profile must be inspecting at least one protocol to enable the option.
Feature set	Set the inspection mode: <ul style="list-style-type: none"> <li>• <i>Flow-based</i>: Scanning takes a snapshot of content packets and uses pattern matching to identify security threats in the content (default).</li> <li>• <i>Proxy-based</i>: Scanning reconstructs content passing through the firewall unit and inspects the content for security threats.</li> </ul>
Inspection Protocols	Enable any of the following protocols: <ul style="list-style-type: none"> <li>• <i>HTTP</i></li> <li>• <i>SMTP</i></li> <li>• <i>POP3</i></li> <li>• <i>IMAP</i></li> <li>• <i>FTP</i></li> <li>• <i>CIFS</i></li> </ul>
<b>apt.protection.options</b>	
Treat Windows Executables in Email Attachments as Viruses	Enable to treat all Windows executable files in email attachments as viruses. <b>Note:</b> By default, <i>Treat Windows Executables in Email Attachments as Viruses</i> is disabled.
Include Mobile Malware Protection	Enable to include mobile malware protection. <b>Note:</b> By default, <i>Include Mobile Malware Protection</i> is enabled.
Send Files to FortiSandbox Appliance for Inspection	Choose from the following options: <ul style="list-style-type: none"> <li>• <i>None</i>: Do not send files to FortiSandbox (default).</li> <li>• <i>Suspicious Files Only</i>: Send suspicious files to FortiSandbox.</li> <li>• <i>All Supported Files</i>: Send all supported files to FortiSandbox.</li> </ul>
<b>Virus Outbreak Prevention</b>	
Use FortiGuard Outbreak Prevention Database	Enable. Block or monitor FortiGuard outbreak prevention database. <b>Note:</b> By default, <i>Use FortiGuard Outbreak Prevention Database</i> is disabled.
Use External Malware Block List	Enable. Block or monitor external malware block list. <b>Note:</b> By default, <i>Use External Malware Block List</i> is disabled.

5. Click **Save**.

## To configure an intrusion prevention profile:

1. Go to *Security > Firewall Objects*.
2. Select *Intrusion Prevention Profile* from the *Security Profiles* dropdown.
3. Select *Create* to create an intrusion prevention profile.
4. In the *Create New IPS Sensor* dialog, enter the following information:

Settings	Guidelines
Name	Required. Enter a name for the IPS Sensor.
Comments	Enter comments about the IPS Sensor.
Block malicious URLs	Select to block malicious URLs.
Scan Outgoing Connections to Botnet Sites	Choose from the following options: <ul style="list-style-type: none"> <li>• <i>Block</i>: Scan and block outgoing connections to Botnet sites.</li> <li>• <i>Disable</i>: Disable scanning outgoing connections to Botnet sites (default).</li> <li>• <i>Monitor</i>: Monitor outgoing connections to Botnet sites.</li> </ul>

5. Select *Create* to add an IPS signature filter to the IPS sensor.




To edit an IPS signature filter, select an IPS signature filter from the list and then select *Edit*.



When editing an IPS signature filter, the fields are the same as when creating it.



Use the search box to look for an IPS signature filter.

6. In the *Create IPS Signature Filter* dialog, enter the following information:

Settings	Guidelines
Type	Select either <i>Filter</i> (default) or <i>Signature</i> type. <b>Note:</b> When the <i>Type</i> is <i>Signature</i> , you can select a signatures from the list and click <i>Save</i> .
	 <p>Use the <i>Search</i> bar to look for a signature.</p>
Action	From the dropdown, select one of the following actions: <ul style="list-style-type: none"> <li>• <i>Default</i> (default)</li> <li>• <i>Allow</i></li> <li>• <i>Monitor</i></li> <li>• <i>Block</i></li> <li>• <i>Reset</i></li> <li>• <i>Quarantine</i>: Enter the duration of the quarantine, and click <i>Save</i>.</li> </ul>

Settings	Guidelines
Packet Logging	Enable or disable packet logging.
Status	Enable, disable, or set the status as default.
Filter	Select <i>Edit IPS Filter</i> to edit an IPS filter, enter the following information as shown in <b>Edit IPS Filter</b> .
	 <p>Alternatively, from the list, select a preconfigured IPS filter and click <i>Save</i>.</p>
	 <p>Use the <i>Search</i> bar to look for an IPS filter.</p>

### Edit IPS Filter

Severity	From the dropdown, select severity levels: <ul style="list-style-type: none"> <li>• <i>critical</i></li> <li>• <i>High</i></li> <li>• <i>Medium</i></li> <li>• <i>Low</i></li> <li>• <i>Info</i></li> </ul>
Target	From the dropdown, select <i>client</i> and/or <i>server</i> .
Protocol	From the dropdown, select protocols.
OS	From the dropdown, select OS: <ul style="list-style-type: none"> <li>• <i>bsd</i></li> <li>• <i>Linux</i></li> <li>• <i>MacOS</i></li> <li>• <i>Other</i></li> <li>• <i>Solaris</i></li> <li>• <i>Windows</i></li> </ul>
Application	From the dropdown, select applications.

7. Click *Save* to save changes to the IPS filter.
8. Click *Save* to save changes to the IPS signature filter.
9. Click *Save* to save changes to the IPS sensor.

### To configure a local category:

1. Go to *Security > Firewall Objects*.
2. Select *Local Category* from the *Security Profiles* dropdown.
3. Select *Create* to create a new local category.

4. In the *Create Local Category* dialog, enter the category description.
5. Click *Save*.

**To configure a web rating override:**


1. Go to *Security > Firewall Objects*.
2. Select *Web Rating Overrides* from the *Security Profiles* dropdown.
3. Select *Create* to create a new web rating override.
4. In the *Create Web Rating Overrides* dialog, enter the following information:

Settings	Guidelines
URL	Required. Enter the URL of a web site.
Status	Enable the web rating override.
Category	Select from the following categories: <ul style="list-style-type: none"> <li>• <i>All Categories</i> (default)</li> <li>• <i>Potentially Liable</i></li> <li>• <i>Adult/Mature Content</i></li> <li>• <i>Bandwidth Consuming</i></li> <li>• <i>Security Risk</i></li> <li>• <i>General Interest- Personal</i></li> <li>• <i>General Interest- Business</i></li> <li>• <i>Unrated</i></li> <li>• <i>Local Categories</i></li> </ul>
Sub Category	Required. Select a sub category for the selected category.
Comments	Enter comments about the web rating override.

5. Click *Save*.

**To configure a web filter profile:**

1. Go to *Security > Firewall Objects*.
2. Select *Web Filter Profile* from the *Security Profiles* dropdown.
3. Select *Create* to create a new web filter profile.
4. In the *Create Web Filter profile* dialog, enter the following information:

Settings	Guidelines
Name	Enter a name for the web filter.
Comments	Enter comments about the web filter.
Category Based Filter	Enable and select FortiGuard category based filters from the list.
	<div style="text-align: center;">  <p>Use the search bar to look for a category based filter.</p> </div>



## Settings

## Guidelines

For the selected category, select from the following actions:

- *Allow*: Allow selected category.
- *Monitor*: Monitor selected category.
- *Block*: Block selected category.
- *Warning*: Select to open the *Filter* dialog.

Enter the *Warning Interval*, select from the *Available User Groups* dropdown, and click *Save*.

- *Authenticate*: Select to open the *Filter* dialog.

Enter the *Warning Interval*, select from the *Available User Groups* dropdown, and click *Save*.

- *Disable*: Disable selected category.

### Static URL Filter

Block invalid URLs

Enable to block invalid URLs.

**Note:** This option is disabled by default.

URL Filter

Enable and then select *Create* to create a URL filter. Enter the information as shown in **To create a URL filter**, and click *Save*.



To edit a URL filter, select a URL filter from the list and then select *Edit*.

When editing a URL filter, the fields are the same as when creating it.



Use the *Search* bar to look for URLs and narrow down the search by using criteria.

You can filter results based on prefix/suffix wildcards.

Block malicious URLs discovered by sandbox

Enable blocking malicious URLs discovered by FortiSandbox.

**Note:** This option is disabled by default.

### Rating Options

Allow websites when a rating error occurs

Enable to allow websites when a rating error has occurred.

**Note:** This option is disabled by default.

Rate URLs by domain and IP Address

Enable to rate URLs by domain and IP address.

**Note:** This option is disabled by default.

### Proxy Options

HTTP POST Action

Select whether the HTTP Post action is *Normal* or *Block*.

HTTP POST is the command used by your browser when you send information, such as a form you have filled-out or a file you are uploading, to a web server.

Settings	Guidelines
Remove Cookies	Enable to remove cookies. <b>Note:</b> This option is disabled by default.


**To create a URL filter:**

URL	Enter the URL.
Type	Select a type from the following: <ul style="list-style-type: none"> <li>• <i>Simple</i> (default)</li> <li>• <i>Regular Expression</i></li> <li>• <i>Wildcard</i></li> </ul>
Action	Select an action from the following: <ul style="list-style-type: none"> <li>• <i>Exempt</i> (default)</li> <li>• <i>Block</i></li> <li>• <i>Allow</i></li> <li>• <i>Monitor</i></li> </ul>
Status	<i>Enable</i> (default) or <i>Disable</i> .

5. Click **Save**.

**To configure application control:**

1. Go to *Security > Firewall Objects*.
2. Select *Application Control* from the *Security Profiles* dropdown.
3. Select *Create* to create a new application control.
4. In the *Create Application Control* dialog, enter the following information:

Settings	Guidelines
Name	Required. Enter a name for the application control.
Comments	Enter comments about the application control.
Category	For each category, select from the following actions: <ul style="list-style-type: none"> <li>• <i>Monitor</i> (default)</li> <li>• <i>Allow</i></li> <li>• <i>Block</i></li> <li>• <i>Quarantine</i>: Enter the quarantine duration, and click <b>Save</b>.</li> <li>• <i>Traffic Shaping</i>: Select <i>Shaper</i> and <i>Shaper Reverse</i>, and click <b>Save</b>.</li> </ul>
Application and Filter Overrides	Select <i>Create</i> to create application and filter overrides.
	
<p>To edit application and filter overrides, select an application and filter overrides from the list and then select <i>Edit</i>.</p> <p>When editing an application and filter overrides, the fields are the same as when creating it.</p>	

## Settings

## Guidelines



Use the *Search* bar to look for overrides.

### To edit application and filter overrides:

#### Type

Select either *Application* (default) or *Filter*.

**Note:** When the *Type* is *Application*, you can select preconfigured signatures from the list, select *Use selected signatures*, and click *Save*.



Use the *Search* bar to look for signatures.

#### Action

From the dropdown, select an action:

- *Monitor* (default)
- *Allow*
- *Block*
- *Quarantine*: Enter the duration of the quarantine, and click *Save*.

#### Category

Select a category or select *Category* to select all options.

**Note:** This option is only available when the *Type* is *Filter*.

#### Popularity

Order of popularity.

**Note:** This option is only available when the *Type* is *Filter*.

#### Technology

Select a technology or select *Technology* to select all options.

**Note:** This option is only available when the *Type* is *Filter*.

#### Behavior

Select a behavior or select *Behavior* to select all options.

**Note:** This option is only available when the *Type* is *Filter*.

#### Vendor

Select a vendor or select *Vendor* to select all options.

**Note:** This option is only available when the *Type* is *Filter*.

#### Protocols

Select a protocol select *Protocol* to select all options.

**Note:** This option is only available when the *Type* is *Filter*.

#### Risk

Select risk level or select *Risk* to select all options.

**Note:** This option is only available when the *Type* is *Filter*.

5. Click *Save* to save overrides.
6. Click *Save* to save the application control.

### To configure a user:

1. Go to *Security > Firewall Objects*.
2. Select *User* from the *User & Device* dropdown.

3. Select *Create* to create a user.
4. In the *Create User* dialog, enter the following information:

Settings	Guidelines
User Name	Required. Enter a name for the user.
Disable	Enable to disable the user.
Password	Enter the password.
<b>Contact Information</b>	
Email	Enter the email address.
Two-factor Authentication	Select from the following: <ul style="list-style-type: none"> <li>• <i>Disable</i></li> <li>• <i>FortiToken</i>: From the dropdown, select a FortiToken. See <a href="#">FortiToken</a>.</li> <li>• <i>Email based two-factor authentication</i>. See <a href="#">Email based two-factor authentication on page 76</a>.</li> </ul>

5. Click *Save*.

## 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 our 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.

## Email based two-factor authentication


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.

### To configure a user group

1. Go to *Security > Firewall Objects*.
2. Select *User Groups* from the *User & Device* dropdown.
3. Select *Create* to create a user group.
4. In the *Create User group* dialog, enter the following information:

Settings	Guidelines
Name	Enter a name for the user group.
Type	Select either <i>Firewall</i> or <i>FSSO/SSO Connectors</i> .
Members	From the dropdown, select users to be added as members.
Remote Groups	Select <i>Create</i> to create a remote group for the user group. From the <i>Remote Server</i> dropdown, select a remote server, and click <i>Save</i> .
	 To edit a remote group, select a remote group from the list and then select <i>Edit</i> . When editing a remote group, the fields are the same as when creating it.
	<b>Note:</b> This option is only available when the <i>Type</i> is <i>Firewall</i> .

5. Click *Save*.

## Network

Use the *Network* tab for the following:

- Configure IPSec phase 1 and phase 2. See [VPN on page 78](#).
- Define static routes. See [Route on page 81](#).
- Set up DHCP servers. See [DHCP Server on page 83](#).



Use the first dropdown at the top to select the correct VDOM or firewall device.

## Page actions

The following actions are available in the *Network* tab:

- *Create*—configure IPSec phase 1/ IPSec phase 2 configurations, static routes, and DHCP servers
- *Edit*—change an existing IPSec phase 1/ IPSec phase 2 configurations, static routes, and DHCP servers

- **Delete**—delete an IPSec phase-1/ IPSec phase-2 configurations, static routes, and DHCP servers
- **Search**—enter text to search for in the table
- **Sort**—Some columns have a sorting feature, allowing you to sort data in ascending or descending order
- **Show x Entries**—use the drop-down menu to set the number of entries to display (20 or 50)

## VPN

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

Gateway Name	Gateway IP	Mode	Encryption Algorithm	Interface
<input checked="" type="checkbox"/> Branch-HQ-A	0.0.0.0		AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1	port1
<input type="checkbox"/> Branch-HQ-B	0.0.0.0		AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1	port5
<input type="checkbox"/> HQ-MPLS	0.0.0.0		AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1	port6
<input type="checkbox"/> FortiDEMO	0.0.0.0	Main	AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1	port4

Use the *VPN* dropdown menu to configure VPNs.

## Configuring VPNs

Use the *VPN* dropdown 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.



When creating a new IPSec interface, FortiPortal now checks whether the normalization interface exists or not using the IPSec interface name:

- If the interface exists, FortiPortal creates a dynamic mapping for the targeted firewall device/VDOM.
- Otherwise, FortiPortal creates both the normalization interface and the dynamic mapping.

When deleting an IPSec interface, FortiPortal removes the dynamic mapping from the normalization interface.

## Creating an IPSec phase-1 or phase-2 configuration

1. Select *IPSec Phase 1* or *IPSec Phase 2* from the *VPN* dropdown menu.
2. Select *Create*.
3. Enter values in the relevant fields and select *Save*. See [IPSec phase-1 fields on page 79](#) and [IPSec phase-2 fields on page 80](#).
4. Select *Save*.

## Updating an IPSec phase-1 or phase-2 configuration

1. Select *IPSec Phase 1* or *IPSec Phase 2* from the *VPN* dropdown menu.
2. Select a configuration and then select *Edit*.

3. Update the values that have changed.
4. Select *Save*.

## Deleting an IPsec phase-1 or phase-2 configuration

1. Select *IPsec Phase 1* or *IPsec Phase 2* from the *VPN* dropdown menu.
2. Select configurations and then select *Delete*.

## IPsec phase-1 fields

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

Settings	Guidelines
Name	Required. Type a name for this Phase-1 configuration. The value is a string with a maximum of 15 characters.
Comments	Type an optional description. The value is a string with a maximum of 255 characters.
Remote Gateway	Required. Select <i>Static IP Address</i> , <i>Dialup user</i> , or <i>Dynamic DNS</i> .
IP Address	Required if you select <i>Static IP Address</i> as the <i>Remote Gateway</i> . Type the IPv4 address.
Dynamic DNS	Optional if you select <i>Dynamic DNS</i> as the <i>Remote Gateway</i> . Type the fully qualified domain name.
Local Interface	Required. Select an interface from the dropdown or select <i>any</i> .
Mode	Required. Select <i>Main</i> or <i>Aggressive</i> for the phase-1 mode.
Authentication Method	Required. Select <i>Pre-shared Key</i> or <i>Signature</i> for the authentication method.
Pre-shared Key	If <i>Pre-shared Key</i> is selected as the <i>Authentication Method</i> , 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.
Certificate Name	If <i>Signature</i> is selected as the <i>Authentication Method</i> , this field is required. Select a certificate from the dropdown.
Peer Options	If the <i>Mode</i> is <i>Aggressive</i> , or <i>Signature</i> is selected as the <i>Authentication Method</i> , this field is available but optional. Select <i>Any peer id</i> , <i>One peer id</i> , <i>Peer certificate</i> , or <i>Peer certificate group</i> .
Peer id	If <i>One peer id</i> is selected in <i>Peer Options</i> , 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.

Settings	Guidelines
Peer Certificate	If <i>Peer certificate</i> is selected in <i>Peer Options</i> , this field is available but optional. From the dropdown, select a peer certificate.
Peer Certificate Group	If <i>Peer certificate group</i> is selected in <i>Peer Options</i> , this field is available but optional. From the dropdown, select a peer certificate group.
<b>Advanced...(XAUTH, NAT-traversal, DPD)</b>	
P1 Proposal	Select the encryption and authentication algorithms. You can select more than one from the dropdown.

## IPSec phase-2 fields

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

Settings	Guidelines
Tunnel Name	Required. Type a name for this Phase-2 configuration. The value is a string with a maximum of 35 characters.
Phase 1	Required. Select an IPSec Phase-1 configuration.
<b>Advanced</b>	
Diffie-Hellman Groups	Required. Select one or more of the following Diffie-Hellman (DH) groups: 1,2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 27, 28, 29, 30, 31, and 32. At least one of the DH group settings on the remote peer or client must match one the selections on the firewall unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode. By default, 5 and 14 are selected.
Key Life	Required. Select the PFS key life. Select <i>Seconds</i> , <i>KBytes</i> , or <i>Both</i> . <ul style="list-style-type: none"> <li>If <i>Seconds</i> is selected, type the number of seconds. The default is 43200. The value range is 120-172800.</li> <li>If <i>KBytes</i> is selected, type the number of KB. The default is 5120. The value range is 5120-4294967295.</li> <li>If <i>Both</i> is selected, type the number of seconds and the number of KB.</li> </ul>
DHCP-IPsec	Optional. The default is deselected.
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.
<b>Quick Mode Selector</b>	
Local Address	Select <i>Subnet</i> , <i>IP Range</i> , <i>Static IP Address</i> , or <i>Named Address</i> . <ul style="list-style-type: none"> <li>If <i>Subnet</i> is selected, enter an IP address and netmask.</li> </ul>



Settings	Guidelines
	<ul style="list-style-type: none"> <li>If <i>IP Range</i> is selected, enter the first IP address and the last IP address in the range.</li> <li>If <i>Static IP Address</i> is selected, enter an IPv4 address.</li> <li>If <i>Named Address</i> is selected, select from the drop-down list.</li> </ul>
Remote Address	Select <i>Subnet</i> , <i>IP Range</i> , <i>Static IP Address</i> , or <i>Named Address</i> . <ul style="list-style-type: none"> <li>If <i>Subnet</i> is selected, enter an IP address and netmask.</li> <li>If <i>IP Range</i> is selected, enter the first IP address and the last IP address in the range.</li> <li>If <i>Static IP Address</i> is selected, enter an IPv4 address.</li> <li>If <i>Named Address</i> is selected, select from the drop-down list.</li> </ul>
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.

## Route

The *Route* dropdown on the *Security > Network* tab displays a list of static routes.

Gateway Name	Gateway IP	Mode	Encryption Algorithm	Interface
<input checked="" type="checkbox"/> Branch-HQ-A	0.0.0.0		AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1	port1
<input type="checkbox"/> Branch-HQ-B	0.0.0.0		AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1	port5
<input type="checkbox"/> HQ-MPLS	0.0.0.0		AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1	port6
<input type="checkbox"/> FortiDEMO	0.0.0.0	Main	AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1	port4

## Configuring static routes

### Adding a new static route

1. Select *Static Route* from the *Route* dropdown.
2. Select *Create* to create a new static route.
3. Enter values in the relevant fields. See [Static route fields on page 82](#).
4. Select *Save*.

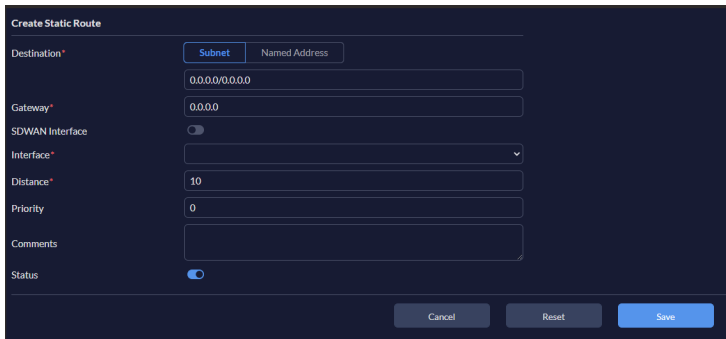
### Updating a static route

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

## Deleting a static route

1. Select *Static Route* from the *Route* dropdown.
2. Select a static route and then select *Delete*.

## Static route fields



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

Settings	Guidelines
Destination	Required. Select <i>Subnet</i> or <i>Named Address</i> for the destination type. <ul style="list-style-type: none"><li>• If <i>Subnet</i> is selected, enter destination IP address and netmask.</li><li>• If <i>Named Address</i> is selected, select from the dropdown.</li></ul>
Gateway	Required. Enter an IPv4 address for the next hop. <b>Note:</b> This options is not available when <i>SD-WAN Interface</i> is enabled.
SDWAN Interface	Enable SD-WAN interface.
SDWAN Zones	From the dropdown, select an SD-WAN zone. <b>Note:</b> This options is available when <i>SD-WAN Interface</i> is enabled.
Interface	Required. Select the network interface that connects to the gateway from the dropdown. <b>Note:</b> This options is not available when <i>SD-WAN Interface</i> is enabled.
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. <b>Note:</b> This options is not available when <i>SD-WAN Interface</i> is enabled.
Comments	Optional. Enter a description of the static route. The value is a string with a maximum of 255 characters.
Status	Enable or disable the static route.

## DHCP

The *System* dropdown in the *Security > Network* tab allows you to add, update, or delete a DHCP server. See [Add, update, or delete a DHCP server](#).

## DHCP Server

You can add, update, and delete DHCP servers.

### Adding a DHCP server

1. Select *DHCP Server* from the *System* dropdown.
2. Select *Create* to create a new DHCP server.
3. Enter values in the relevant fields. See [DHCP server fields on page 83](#).
4. Select *Save*.

### Updating a DHCP server

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

### Deleting a DHCP server

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

### DHCP server fields

The screenshot shows a configuration dialog for a DHCP server. The fields are as follows:

- Interface: bbb
- DHCP status: Enabled
- IP Range: +
- Netmask: 0.0.0.0
- Default gateway: Same as Interface IP
- DNS server: Same as System DNS
- DNS server 1: 0.0.0.0
- DNS server 2: 0.0.0.0
- DNS server 3: 0.0.0.0
- DNS server 4: 0.0.0.0
- Lease time: 604800 second(s)

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

Settings	Guidelines
Interface	From the dropdown, select an interface.
DHCP status	Enable/disable DHCP status. <b>Note:</b> By default, the DHCP status is enabled.

Settings	Guidelines
IP Range	DHCP IP address range. The IP range of each DHCP server must match the network address range. See <a href="#">Configure an IP range on page 84</a> .
Netmask	Netmask assigned by the DHCP server.
Default Gateway	Select either <i>Same as Interface IP</i> (default) or <i>Specify</i> . When <i>Specify</i> selected, enter the default gateway IP address assigned by the DHCP server.
DNS server	Options for assigning DNS servers to DHCP clients: <ul style="list-style-type: none"> <li>• <i>Same as System DNS</i>—Clients are assigned the configured DNS servers of the firewall.</li> <li>• <i>Same as Interface IP</i>—The IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.</li> <li>• <i>Specify</i>—Specify up to four DNS servers in the DHCP server configuration (default).</li> </ul>
DNS Server1	DNS server 1. <b>Note:</b> This option is only available when the <i>DNS server</i> is <i>Specify</i> .
DNS Server2	DNS server 2. <b>Note:</b> This option is only available when the <i>DNS server</i> is <i>Specify</i> .
DNS Server3	DNS server 3. <b>Note:</b> This option is only available when the <i>DNS server</i> is <i>Specify</i> .
DNS Server4	DNS server 3. <b>Note:</b> This option is only available when the <i>DNS server</i> is <i>Specify</i> .
Lease time	Set the time after which the assigned IP address expires, in seconds. The default is 604800.

## Configure an IP range

1. In *IP Range*, select + to add a new IP address range.
2. In the *IP Range* field, enter the IP range.

# Switch

Use the *Switch* tab for the following:

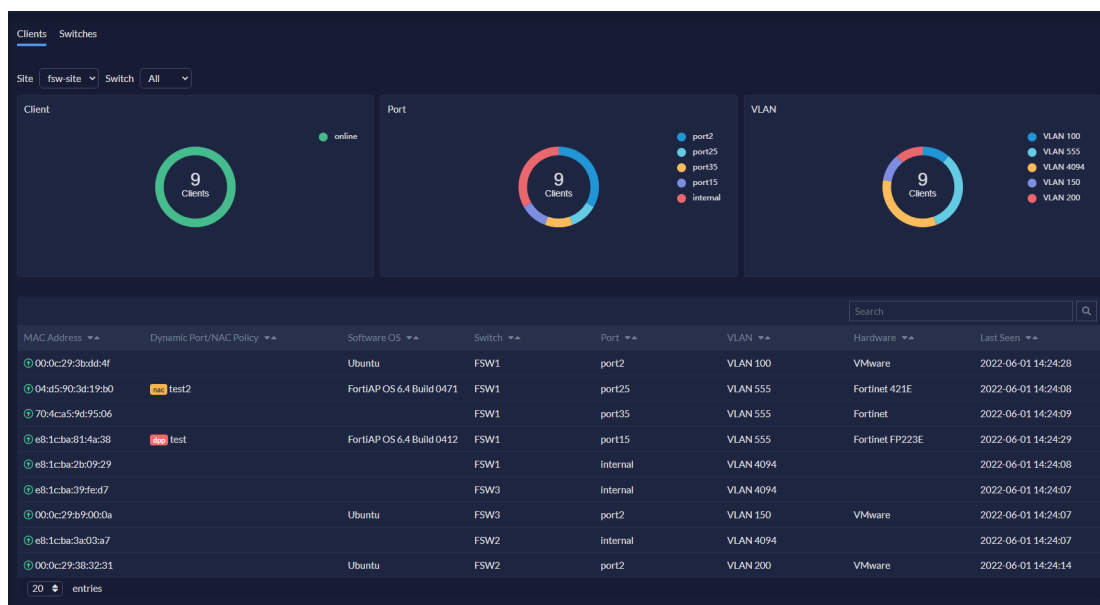
- Monitor switches and clients. See [Switch monitoring on page 85](#).

## Switch monitoring

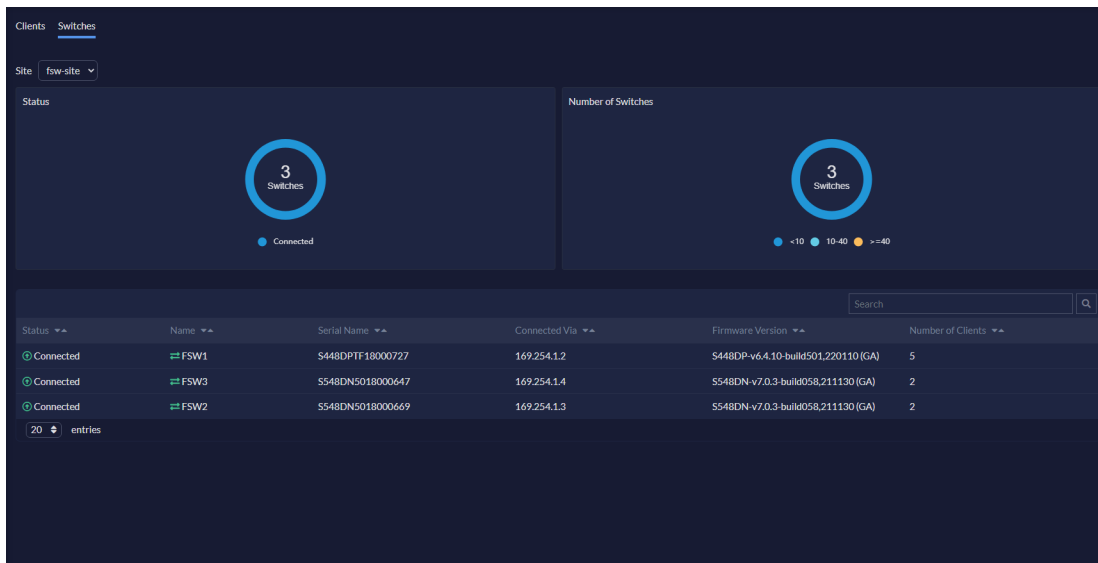
The *Monitoring* tab in *Switch* displays switches available in a site and their major properties. It also displays all the switch clients with their properties including software OS, ports, and last seen status.

The *Switch monitoring* tab looks like the following:

### Clients view



### Switches view



The following widgets are available:

- *Client*
- *Port*
- *VLAN*
- *Status*
- *Number of Switches*

## Page actions

The following actions are available on the *Switch Monitoring* tab:

- *Site*—from the dropdown, select a site
- *Switch*—from the dropdown, select a FortiSwitch  
The *Switch* dropdown is only available in the *Clients* view
- *Search*—look for a particular switch or a client.
- *Sort*—allows you to sort some columns in ascending or descending order
- *Show x entries*—set the number of entries per page (20 or 50)

# WiFi

Use the *WiFi* tab for the following:

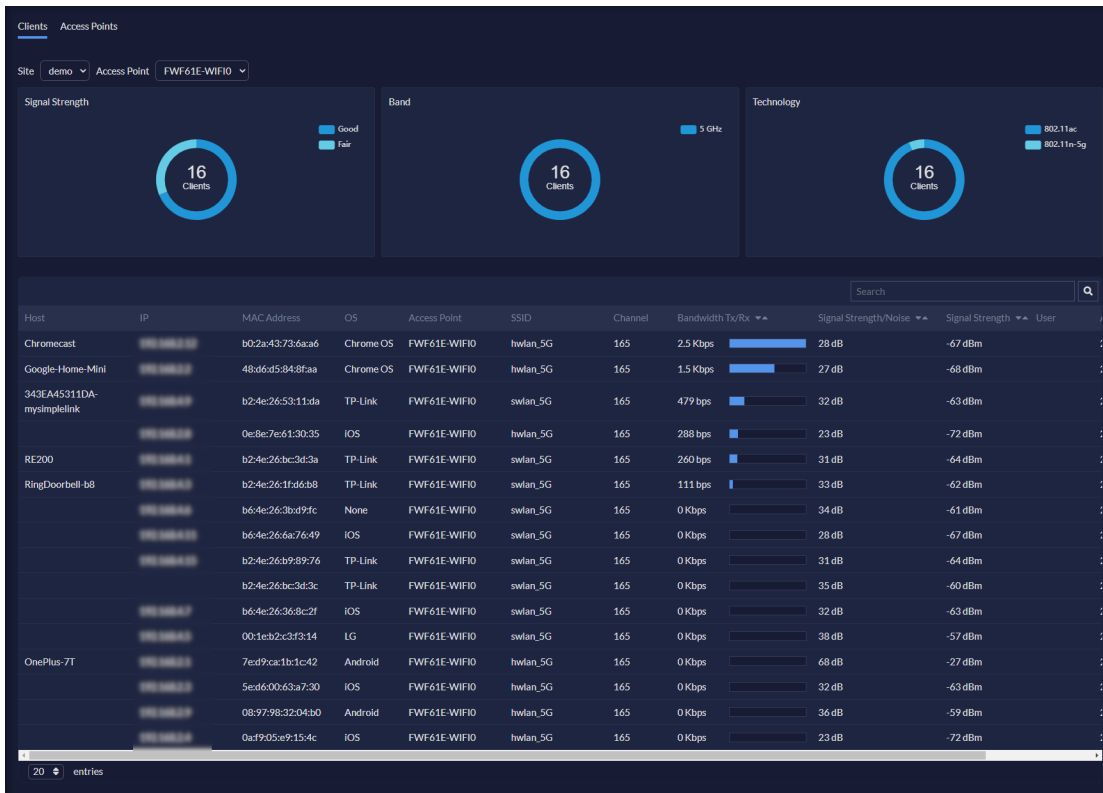
- Monitor and drill-down on APs and their clients. See [WiFi monitoring on page 87](#).

## WiFi monitoring

The *Monitoring* tab in *WiFi* displays Access Points (APs) available in a site and their major properties. It also displays all the AP clients with their properties including signal strength, Signal-to-Noise Ratio (SNR), and the connection status.

The *WiFi monitoring* tab looks like the following:

### Clients view



### Access Points view



The following widgets are available:

- *Signal Strength*
- *Band*
- *Technology*
- *Status*
- *2.4 GHz Radio Channel Utilization*
- *5 GHz Radio Channel Utilization*
- *Channel*
- *Type*

## Page actions

The following actions are available on the *WiFi Monitoring* tab:

- *Site*—from the dropdown, select a site
- *Access Point*—from the dropdown, select an access point  
The *Access Point* dropdown is only available in the *Clients* view
- *Search*—look for a particular access point by name or *SSIDs*  
Similarly, look for a client by *Host*, *IP*, *MAC Address*, or the *OS*
- *Sort*—*Bandwidth Tx/Rx*, *Clients*, *Signal Strength/Noise*, and *Signal Strength* columns have a sorting feature, allowing you to sort data in ascending or descending order
- *Show x entries*—set the number of entries per page (20 or 50)

## Drill-down capability

You can click on an access point or an AP client in the table to see additional information including a list of interfering SSIDs for an access point and traffic details from FortiAnalyzer for an AP client.

Access point drill-down



Access Point - FP223E5518015121

Base MAC Address: e8:1c:ba:81:4a:38  
 Status: ● Connected  
 Country: CA  
 IPv4 Address: 192.168.1.149  
 Uptime: 9 d 19 hr 32 min 15 sec  
 Version: FP223E-v6.4-build0412  
 Radio 1 - 2.4 GHz: ● Interfering SSIDs ● Clients ● Channel Utilization

**Interfering SSIDs**

SSID	AP BSSID	Channel	Signal
	8a:d8:1b:3e:41:a2	4	-79 dBm
swlan_base	08:60:6e:bb:37:d0	6	-57 dBm
bc-wifi	3c:37:86:fa:d1:13	7	-87 dBm
lalagoon2	84:d8:1b:3e:2a:ca	4	-79 dBm
lalagoon2	84:d8:1b:3e:41:a2	4	-75 dBm
swlan_ext	b0:4e:26:bc:3d:3b	6	-55 dBm

10 entries

Close

### AP client drill-down

Client - b6:4e:26:30:5d:71

MAC Address: b6:4e:26:30:5d:71  
 SSID: swlan\_5G  
 Access Point: FP223E5518015121  
 Channel: 44  
 Association Time: 2022-04-28 20:16:34  
 IP Address: 192.168.1.7  
 VLAN: 0  
 MIMO: 1x1  
 Status: ● Signal Strength/Noise ● Signal Strength ● Band

Deassociate

**Traffic Details**

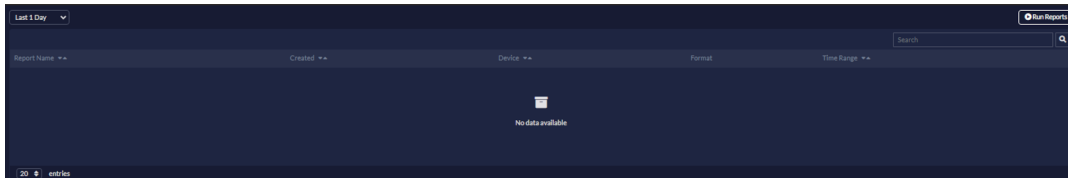
Date/Time	Source	Destination IP	Service	Application	Action
20:16:00	fe80::8d:e68f:970::9b0	:::16	icmp6/143/0	icmp6/143/0	accept

10 entries

Close

# Reports

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



## Page actions

This tab contains the following actions:

- *Set Filter*—filter the data ((Last 1 Day, Last 1 Week, or Last 1 Month)
- *Run Reports*—opens a window to specify the report to be run
- *Search*—text search by report name
- *Show x entries*—sets the number of entries that are displayed (20 or 50)

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

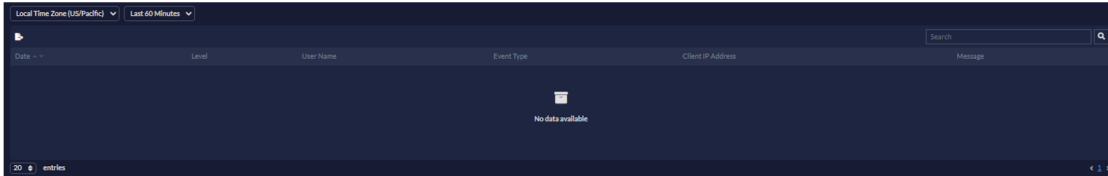
## Run Reports actions

The *Report to be Executed* window contains the following selections:

Settings	Guidelines
Report Duration	Duration of data included in the report: Today, Yesterday, Last 7 Days, or Last 14 Days.
Reports	From the dropdown, select reports.
Device	From the dropdown, select devices.

# Audit

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

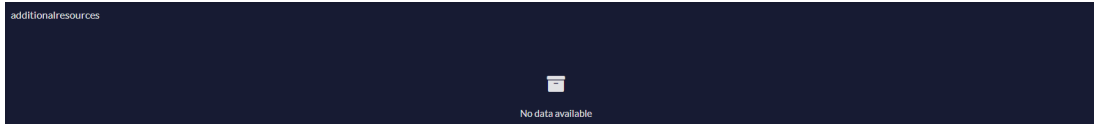


## Page actions

- *Time zone*—use the dropdown to set the time zone to *Local Time Zone (US/Pacific)* or *GMT Time Zone*
- *Filter*—set the duration of the logs to display (*Last 60 Minutes*, *Last 1 Day*, *Last 1 Week*, or *Specify*)
- *Export to CSV*—export the audit log list as a Comma-Separated Value (CSV) file
- *Search*—use any column to search the audit log list by level, user name, event type, client IP address, or message
- *Show x entries*—use the dropdown to set the number of entries to display
- *Sort*—allows you to sort the log list ascending or descending order of date.

## 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.





[www.fortinet.com](http://www.fortinet.com)

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.