Micro-FortiGuard Server for FortiClient - Administration Guide

Version 6.0.3

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 COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

December 12, 2018
Micro-FortiGuard Server for FortiClient 6.0.3 Administration Guide
02-603-504219-20181102

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-	Initial release.

Introduction

Micro-FortiGuard Server for FortiClient is a local update server for FortiClient endpoints. FortiClient can receive software and signature updates locally from Micro-FortiGuard Server for FortiClient instead of reaching out to FortiGuard Distribution Server, helping save WAN bandwidth. It is recommended that organizations with more than 5000 FortiClient endpoints use Micro-FortiGuard Server for FortiClient to receive local updates.

Micro-FortiGuard Server for FortiClient feature support for FortiClient endpoints includes:

- FortiClient software updates
- WebFilter
- Antivirus signature, application control, and vulnerability database updates

This document contains the following sections:

- Device Firmware and Security Updates on page 6
- System Settings on page 15

Device Firmware and Security Updates

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your Micro-FortiGuard Server for FortiClient system and itsFortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS), which update the FortiGuard services on your Micro-FortiGuard Server for FortiClient system on a regular basis so that your Micro-FortiGuard Server for FortiClient system is protected against the latest threats.

To view and configure these services, go to *FortiGuard Server > Settings*.

In FortiGuard Management, you can configure the Micro-FortiGuard Server for FortiClient system to act as a local FDS, or use a web proxy server to connect to the FDN. Micro-FortiGuard Server for FortiClient systems acting as a local FDS synchronize their FortiGuard service update packages with the FDN, then provide FortiGuard these updates and look up replies to your private network's devices. The local FDS provides a faster connection, reducing Internet connection load and the time required to apply frequent updates to many devices.

FortiGuard Management also includes firmware revision management. To view and configure firmware options, go to *FortiGuard Server > Firmware Images*.

Before you can use your Micro-FortiGuard Server for FortiClient system as a local FDS, you must:

- Register your devices with Fortinet Customer Service & Support and enable the FortiGuard service licenses. See your device documentation for more information on registering your products.
- Enable and configure the Micro-FortiGuard Server for FortiClient system's built-in FDS. For more information, see Configuring network interfaces on page 21.
- Connect the Micro-FortiGuard Server for FortiClient system to the FDN.
  The Micro-FortiGuard Server for FortiClient system must retrieve service update packages from the FDN before it can redistribute them to FortiClient agents. For more information, see Connecting the built-in FDS to the FDN on page 8.
- Configure each FortiClient endpoint to use the Micro-FortiGuard Server for FortiClient system's built-in FDS as their override server.

This section contains the following topics:

- Settings
- Package Management
- Query Server Management
- Firmware images

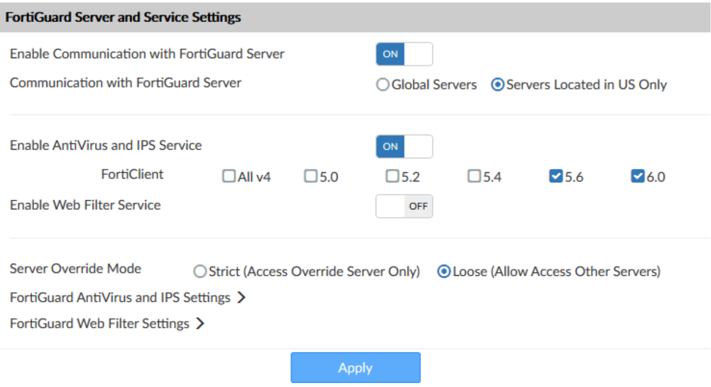
For information on current security threats, virus and spam sample submission, and FortiGuard service updates available through the FDN, including antivirus, IPS, web filtering, and email filtering, see the FortiGuard Center website, https://fortiguard.com.

Settings

FortiGuard Server > Settings provides a central location for configuring and enabling your Micro-FortiGuard Server for FortiClient system's built-in FDS as an FDN override server.

By default, this option is enabled. After configuring FortiGuard and configuring your devices to use the Micro-FortiGuard Server for FortiClient system as their FortiGuard server, you can view overall and per device statistics on FortiGuard service benefits.

To operate in a closed network, disable communication with the FortiGuard server. See Operating as an FDS in a Closed Network on page 13.



FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server: ON

Communication with FortiGuard Server: ○ Global Servers ● Servers Located in US Only

Enable AntiVirus and IPS Service: ON

FortiClient: □ All v4 □ 5.0 □ 5.2 □ 5.4 ☑ 5.6 ☑ 6.0

Enable Web Filter Service: OFF

Server Override Mode: ○ Strict (Access Override Server Only) ● Loose (Allow Access Other Servers)

FortiGuard AntiVirus and IPS Settings >

FortiGuard Web Filter Settings >

Apply

Enable communication with FortiGuard servers.	When toggled *OFF*, you must manually upload packages, databases, and licenses to your Micro-FortiGuard Server for FortiClient. See Operating as an FDS in a Closed Network on page 13.
Communication with FortiGuard Server	Select *Servers Located in the US Only* to limit communication to FortiGuard servers located in the USA. Select *Global Servers* to communicate with servers anywhere.
Enable Antivirus and IPS Service	Toggle *ON* to enable antivirus and intrusion protection service. When on, select what versions of *FortiClient* to download updates for.
Enable Web Filter and Services	Toggle *ON* to enable web filter services. When uploaded to Micro-FortiGuard Server for FortiClient, the Web Filter database version is displayed.
Server Override Mode	Select *Strict (Access Override Server Only)* or *Loose (Allow Access Other Servers)* override mode.
FortiGuard Antivirus and IPS Settings	Configure antivirus and IPS settings. See FortiGuard antivirus and IPS settings on page 7.
FortiGuard Web Filter Settings	Configure web filter settings. See FortiGuard web filter settings on page 8.

FortiGuard antivirus and IPS settings

In this section you can enable settings for FortiGuard Antivirus and IPS settings. The following settings are available:

Use Override Server Address for FortiClient	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries. To override the default server for updating FortiClient device's FortiGuard services, see Overriding default IP addresses and ports on page 9.

Scheduled Regular Updates	Configure when packages are updated without manually initiating an update request. To schedule regular service updates, see Scheduling updates on page 10.
Advanced	Enables logging of service updates.

FortiGuard web filter settings

In this section you can enable settings for FortiGuard Web Filter.

The following settings are available:

Connection to FortiGuard Distribution Server(s)	Configure connections for overriding the default built-in FDS or web proxy server for web filter and email filter settings. To override an FDS server for web filter services, see Overriding default IP addresses and ports on page 9. To enable web filter service updates using a web proxy server, see Enabling updates through a web proxy on page 9.
Use Override Server Address	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries.
Use Web Proxy	Configure the Micro-FortiGuard Server for FortiClient system's built-in FDS to connect to the FDN through a web proxy. IPv4 and IPv6 are supported. To enable updates using a web proxy, see Enabling updates through a web proxy on page 9.
Polling Frequency	Configure how often polling is done.
Log Settings	Configure logging of FortiGuard server update, and web filtering events. • *Log FortiGuard Server Update Events*: enable or disable • *FortiGuard Web Filtering*: Choose from *Log URL disabled*, *Log non-URL events*, and *Log all URL lookups*.

Connecting the built-in FDS to the FDN

When you enable the built-in FDS and initiate an update either manually or by a schedule, the Micro-FortiGuard Server for FortiClient system attempts to connect to the FDN.

If all connection attempts to the server list fail, the connection status will be *Disconnected*.

If the connection status remains *Disconnected*, you may need to configure the Micro-FortiGuard Server for FortiClient system's connection to the FDN by overriding the default IP address and/or port.

After establishing a connection with the FDN, the built-in FDS can receive FortiGuard service update packages from the FDN.

To enable the built-in FDS:

1. Go to *FortiGuard Server* > *Settings*.
2. Enable the types of FDN services that you want to provide through your Micro-FortiGuard Server for FortiClient system's built-in FDS.
3. Click *Apply*.
   The built-in FDS attempts to connect to the FDN.

If the built-in FDS is unable to connect, you may need to enable the selected services on a network interface. For more information, see Configuring network interfaces on page 21.

If you still cannot connect to the FDN, check routes, DNS, and any intermediary firewalls or NAT devices for policies that block necessary FDN ports and protocols.

See the *FortiOS HandBook: Security Fabric* document in the Fortinet Document Library at http://docs.fortinet.com/fortigate/admin-guides for more information.

Enabling updates through a web proxy

If the Micro-FortiGuard Server for FortiClient system's built-in FDS must connect to the FDN through a web (HTTP or HTTPS) proxy, you can specify the IP address and port of the proxy server.

If the proxy requires authentication, you can also specify a user name and password.

To enable updates to the Micro-FortiGuard Server for FortiClient system through a proxy:

1. Go to *FortiGuard Server* > *Settings*.
2. Expand *FortiGuard Web Filter Settings*.
3. Toggle *ON* beside *Use Web Proxy* and enter the IP address and port number of the proxy.
4. If the proxy requires authentication, enter the user name and password.
5. Click *Apply*.
   If the FDN connection status is *Disconnected*, the Micro-FortiGuard Server for FortiClient system is unable to connect through the web proxy.

Overriding default IP addresses and ports

The Micro-FortiGuard Server for FortiClient device's built-in FDS connects to the FDN servers using default IP addresses and ports. You can override these defaults if you want to use a port or specific FDN server that is different from the default.

To override default IP addresses and ports:

1. Go to *FortiGuard Server* > *Settings*.
2. Expand *FortiGuard Antivirus and IPS Settings* or *FortiGuard Web Filter Settings*, as required.
3. Toggle *On* beside *Use Override Server Address*.
4. Enter the IP address and/or port number.

5. Click *Apply*.
   If the FDN connection status remains disconnected, the Micro-FortiGuard Server for FortiClient system is unable to connect with the configured override.

FDN port numbers and protocols

Both the built-in FDS and devices use certain protocols and ports to successfully request and receive updates from the FDN or override server. Any intermediary proxies or firewalls must allow these protocols and ports, or the connection will fail.

After connecting to the FDS, you can verify connection status on the FortiGuard Management page. For more information about connection status, see Connecting the built-in FDS to the FDN on page 8.

Scheduling updates

Keeping the built-in FDS up-to-date is important to provide current FortiGuard update packages and rating lookups to requesting devices. This is especially true as new viruses, malware, and spam sources pop-up frequently. By configuring a scheduled update, you are guaranteed to have a recent version of database updates.

A Micro-FortiGuard Server for FortiClient system acting as an FDS synchronizes its local copies of FortiGuard update packages with the FDN when it is scheduled to poll or update its local copies of update packages.

If the network is interrupted when the FortiManager system is downloading a large file, it downloads all files again when the network resumes.

To schedule antivirus and IPS updates:

1. Go to *FortiGuard Server* > *Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*; see FortiGuard antivirus and IPS settings on page 7.
3. In *Polling Frequency*, select the number of hours and minutes of the polling interval.
4. Click *Apply*.

To schedule Web Filtering polling:

1. Go to *FortiGuard* > *Settings*.
2. Click the arrow to expand *FortiGuard Web Filter Settings*.
3. In *Polling Frequency*, select the number of hours and minutes of the polling interval.
4. Click *Apply*.

Package Management

Antivirus and IPS signature packages are managed in *FortiGuard Server* > *Package Management*.

The following information is displayed:

Refresh	Select to refresh the table.

Show Used Object Only	Clear to show all package information. Select to show only relevant package information.
Search	Use the search field to find a specific object in the table.
Seq.#	The sequence number.
Object Name	The name of the object.
Object Type	The type of object for the package.
Package Received	The name of the package.
Latest Version (Release Date/Time)	The package version.
Size	The size of the package.
To Be Deployed Version	The package version that is to be deployed. Select *Change* to change the version.
Update History	Select the icon to view the package update history.

Deployed version

To change the to be deployed version of a received packaged, click *Change* in the *To Be Deployed Version* column for the package.

The *Change Version* dialog box is displayed, allowing you to select an available version from the dropdown list.

Update history

When you click the *Update History* button for a package, the *Update History* pane is displayed for the package.

It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.

Query Server Management

Web filter database packages are managed in *FortiGuard Server > Query Server Management*.

The following information is displayed:

Refresh	Select to refresh the table.
Search	Use the search field to find a specific entry in the table.
History	The record of received packages.
Package Received	The name of the received package.
Latest Version (Release Date/Time)	The latest version of the received package.
Size	The size of the package.
Update History	Click to view the package update history.

Update history

When you click the *Update History* button for a package, the *Update History* pane is displayed for the package.

It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.

Firmware images

Go to *FortiGuard Servers > Firmware Images* to manage the firmware images stored on the Micro-FortiGuard Server for FortiClient device. You can download only the images that are needed from the FDS systems.

The following information is available:

Column Settings	Change the displayed columns, or reset them to the default view.
Search	Use the search field to find a specific entry in the table.
Seq.#	The sequence number.
Object ID	
Object Version	
Build	
Type	The installer type, either light or full.
Version	The version of the firmware.
Platform	The platform of the firmware image.
Local	
Download/Delete	Download the firmware image from the FDS if it is available. If the firmware images has already been downloaded, then delete the firmware image from the FortiManager device.

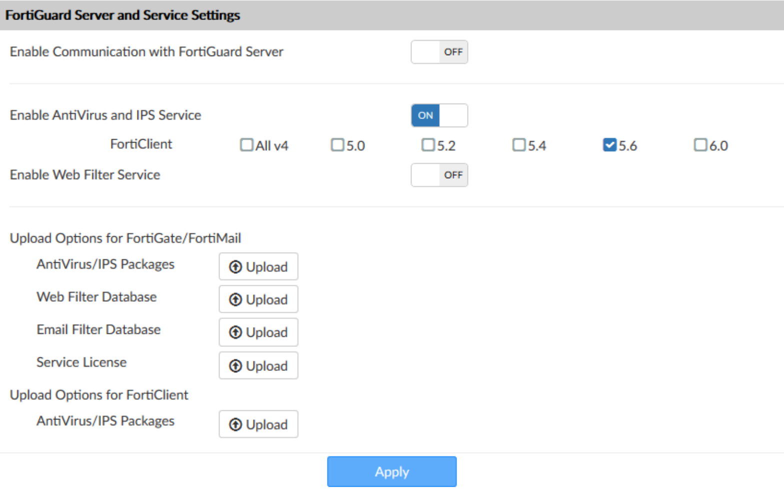
Operating as an FDS in a Closed Network

The Micro-FortiGuard Server for FortiClient can be operated as a local FDS server when it is in a closed network with no internet connectivity.

Without a connection to a FortiGuard server, update packages and licenses must be manually downloaded from support, and then uploaded to the Micro-FortiGuard Server for FortiClient.

As databases can be large, we recommend uploading them using the CLI. See Uploading packages with the CLI on page 14.

Go to *FortiGuard Server* > *Settings* to configure Micro-FortiGuard Server for FortiClient as a local FDS server and to upload update packages and license.



FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server: OFF

Enable AntiVirus and IPS Service: ON

FortiClient: □ All v4 □ 5.0 □ 5.2 □ 5.4 ☑ 5.6 □ 6.0

Enable Web Filter Service: OFF

Upload Options for FortiGate/FortiMail

- AntiVirus/IPS Packages: Upload
- Web Filter Database: Upload
- Email Filter Database: Upload
- Service License: Upload

Upload Options for FortiClient

- AntiVirus/IPS Packages: Upload

Enable Communication with FortiGuard Servers	Toggle *OFF* to disable communication with the FortiGuard servers.
Enable Antivirus and IPS Service	Toggle *ON* to enable antivirus and intrusion protection service. When on, select what versions of *FortiClient* to download updates for.
Enable Web Filter Services	This option is not functional.
Upload Options for FortiGate/FortiMail	
AntiVirus/IPS Packages	Select to upload antivirus and IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer, or drag and drop the file onto the dialog box. Click *OK* to upload the package to Micro-FortiGuard Server for FortiClient.
Web Filter Database	This option is not functional.
Email Filter Database	This option is not functional.

Service License	This option is not functional.
Upload Options for FortiClient	
AntiVirus/IPS Packages	Select to upload the FortiClient AntiVirus/IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer, or drag and drop the file onto the dialog box. Click *OK* to upload the package to Micro-FortiGuard Server for FortiClient.

Uploading packages with the CLI

Packages and licenses can be uploaded using the CLI. This should be used when the packages being uploaded are large, like database packages.

To upload packages and license files using the CLI:

1. If not already done, disable communications with the FortiGuard server and enable a closed network with the following CLI commands:
```
config fmupdate publicnetwork
   set status disable
end
```
2. Upload an update package or license:
   a. Load the package or license file to an FTP, SCP, or TFTP server
   b. Run the following CLI command:
```
execute fmupdate {ftp | scp | tftp} import <av-ips | fct-av | url | spam |
     file-query | license-fgt | license-fct | custom-url | domp> <remote_file>
     <ip> <port> <remote_path> <user> <password>
```

System Settings

System Settings allows you to manage system options for your Micro-FortiGuard Server for FortiClient device.

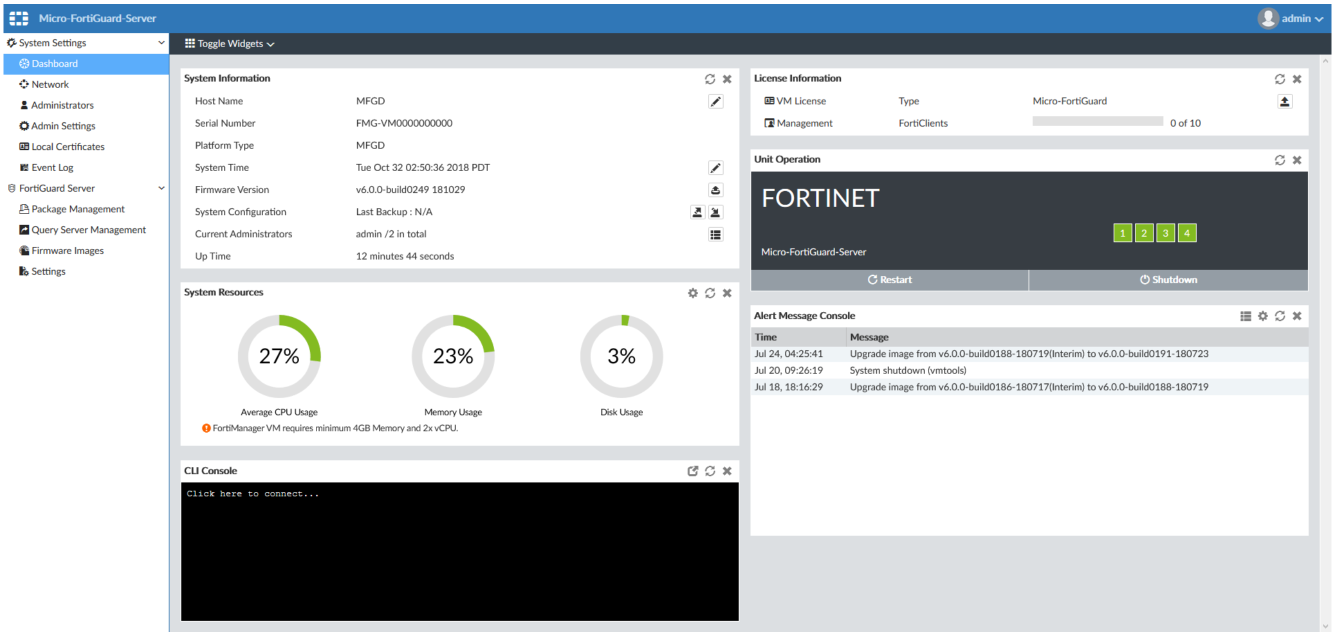
Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the GUI page to access these options.

This section contains the following topics:

- Dashboard on page 15
- Network on page 20
- Managing administrator accounts on page 23
- Global administration settings on page 27
- Certificates on page 30
- Event Log on page 33

Dashboard

The *Dashboard* contains widgets that provide performance and status information and enable you to configure basic system settings. The dashboard also contains a CLI widget that lets you use the command line through the GUI.



System Information

Host Name	MFGD
Serial Number	FMG-VM0000000000
Platform Type	MFGD
System Time	Tue Oct 32 02:50:36 2018 PDT
Firmware Version	v6.0.0-build0249 181029
System Configuration	Last Backup : N/A
Current Administrators	admin /2 in total
Up Time	12 minutes 44 seconds

System Resources

FortiManager VM requires minimum 4GB Memory and 2x vCPU.

CLI Console

```
Click here to connect...
```

License Information

VM License	Type	Micro-FortiGuard	
Management	FortiClients		0 of 10

Unit Operation

Alert Message Console

Time	Message
Jul 24, 04:25:41	Upgrade image from v6.0.0-build0188-180719(Interim) to v6.0.0-build0191-180723
Jul 20, 09:26:19	System shutdown (vmtools)
Jul 18, 18:16:29	Upgrade image from v6.0.0-build0186-180717(Interim) to v6.0.0-build0188-180719

The following widgets are available:

Widget	Description
System Information	Displays basic information about the FortiManager system, such as up time and firmware version. For more information, see System Information widget on page 17. From this widget you can manually update the FortiManager firmware to a different release. For more information, see Updating the system firmware on page 19.
System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see System Resources widget on page 19.
License Information	Displays license status and how many endpoints of the supported maximum are connected to the Micro-FortiGuard Server for FortiClient. See License Information widget on page 20. From this widget you can manually upload a license to increase the maximum number of endpoints that can be connected.
Unit Operation	Graphically displays the status of each port. The port name indicates its status by its color. Green indicates the port is connected. Grey indicates there is no connection. Hover the cursor over the ports to view a pop-up that displays the full name of the interface, the IP address and netmask, the link status, the speed of the interface, and the amounts of sent and received data.
CLI Console	Opens a terminal window that enables you to configure the Micro-FortiGuard Server for FortiClient unit using CLI commands directly from the GUI, without making a separate Telnet, SSH, or local console connection to access the CLI. When using the widget, you are logged in with the same administrator account that you used to access the GUI. You can enter commands by typing them, or you can copy and paste commands into or out of the console. Click *Detach* in the widget toolbar to open the widget in a separate window. **Note:** The *CLI Console* widget requires that your web browser support JavaScript.
Alert Message Console	Displays log-based alert messages for both the Micro-FortiGuard Server for FortiClient unit itself and connected devices. Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget and the refresh interval. To view a complete list of alert messages, click *Show More* from the widget toolbar. The widget will show the complete list of alerts. To clear the list, click *Delete All Messages*. Click *Show Less* to return to the regular view.

Customizing the dashboard

The Micro-FortiGuard Server for FortiClient system dashboard can be customized. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized. It can also be viewed in full screen by selecting the full screen button on the far right side of the toolbar.

Action	Steps
Move a widget	Move the widget by clicking and dragging its title bar, then dropping it in its new location
Add a widget	Select *Toggle Widgets* from the toolbar, then select the name widget you need to add.
Delete a widget	Click the *Close* icon in the widget's title bar.
Customize a widget	For widgets with an edit icon, you can customize the widget by clicking the Edit icon and configuring the settings.
Reset the dashboard	Select *Toggle Widgets* > *Reset to Default* from the toolbar. The dashboards will be reset to the default view.

System Information widget

The following information is available on this widget:

Host Name	The identifying name assigned to this Micro-FortiGuard Server for FortiClient unit. Click the edit host name button to change the host name. For more information, see Changing the host name on page 17.
Serial Number	The serial number of the Micro-FortiGuard Server for FortiClient unit. The serial number is unique to the Micro-FortiGuard Server for FortiClient unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Platform Type	Displays the Micro-FortiGuard Server for FortiClient platform type.
System Time	The current time on the Micro-FortiGuard Server for FortiClient internal clock. Click the edit system time button to change system time settings. For more information, see Configuring the system time on page 18.
Firmware Version	The version number and build number of the firmware installed on the Micro-FortiGuard Server for FortiClient unit. To update the firmware, you must download the latest version from the Customer Service & Support website at https://support.fortinet.com. Click the update button, then select the firmware image to load from the local hard disk or network volume. For more information, see Updating the system firmware on page 19.
Current Administrators	The number of administrators currently logged in. Click the current session list button to view the session details for all currently logged in administrators.
Up Time	The duration of time the Micro-FortiGuard Server for FortiClient unit has been running since it was last started or restarted.

Changing the host name

The host name of the Micro-FortiGuard Server for FortiClient unit is used in several places.

- It appears in the *System Information* widget on the dashboard.
- It is used in the command prompt of the CLI.

The *System Information* widget and the `get system status` CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed.

To change the host name:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the edit host name button next to the *Host Name* field.
3. In the *Host Name* box, type a new host name.
   The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
4. Click the checkmark to change the host name.

Configuring the system time

You can either manually set the Micro-FortiGuard Server for FortiClient system time or configure the Micro-FortiGuard Server for FortiClient unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

For many features to work the Micro-FortiGuard Server for FortiClient system time must be accurate.

To configure the date and time:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the edit system time button next to the *System Time* field.
3. Configure the following settings to either manually configure the system time, or to automatically synchronize the Micro-FortiGuard Server for FortiClient unit’s clock with an NTP server:

System Time	The date and time according to the Micro-FortiGuard Server for FortiClient unit’s clock at the time that this pane was loaded or when you last clicked the *Refresh* button.
Time Zone	Select the time zone in which the Micro-FortiGuard Server for FortiClient unit is located and whether or not the system automatically adjusts for daylight savings time.
Update Time By	Select *Set time* to manually set the time, or *Synchronize with NTP Server* to automatically synchronize the time.
Set Time	Manually set the data and time.
Select Date	Set the date from the calendar or by manually entering it in the format: YYYY/MM/DD.

Select Time	Select the time.
Synchronize with NTP Server	Automatically synchronize the date and time.
Sync Interval	Enter how often, in minutes, the device should synchronize its time with the NTP server. For example, entering 1440 causes the Fortinet unit to synchronize its time once a day.
Server	Enter the IP address or domain name of an NTP server. Click the plus icon to add more servers. To find an NTP server that you can use, go to http://www.ntp.org.

4. Click the checkmark to apply your changes.

Updating the system firmware

To take advantage of the latest features and fixes, the Micro-FortiGuard Server for FortiClient firmware can be updated.

Before you can download firmware updates for your Micro-FortiGuard Server for FortiClient unit, you must first register your Micro-FortiGuard Server for FortiClient unit with Customer Service & Support. For details, go to https://support.fortinet.com/ or contact Customer Service & Support.

To update the Micro-FortiGuard Server for FortiClient firmware:

1. Download the firmware (the `.out` file) from the Customer Service & Support website, https://support.fortinet.com/.
2. Go to *System Settings* > *Dashboard*.
3. In the *System Information* widget, in the *Firmware Version* field, click *Upgrade Firmware*. The *Firmware Upload* dialog box opens.
4. Drag and drop the file onto the dialog box, or click *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal and then click *Open*.
5. Click *OK*. Your device will upload the firmware image and you will receive a confirmation message noting that the upgrade was successful.

   Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

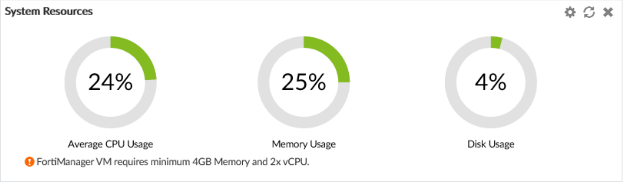
   ```
   execute restore image {ftp | tftp} <file path to server> <IP of server>
         <username on server> <password>
   ```

6. Refresh the browser and log back into the device.

System Resources widget

The *System Resources* widget displays the usage status of the CPUs, memory, and hard disk. You can view system resource information in real-time or historical format, as well as average or individual CPU usage.

Warning messages are displayed if the amount of memory or the number of CPUs assigned are too low.



FortiManager VM requires minimum 4GB Memory and 2x vCPU.

To toggle between real-time and historical data, click *Edit* in the widget toolbar, select *Historical* or *Real-time*, edit the other settings as required, then click *OK*.

To view individual CPU usage, from the Real-Time display, click on the CPU chart. To go back to the standard view, click the chart again.

License Information widget

The *License Information* widget displays the number of devices connected to the Micro-FortiGuard Server for FortiClient.

VM License	VM license information and status. Click the upload license button to upload a new license file and increase the maximum number of endpoints that can be connected. The **Duplicate** status appears when users try to upload a license that is already in use. Additionally, the following message will be displayed in the Notifications: *Duplicate License has been found! Your VM license will expire in XX hours (Grace time: 24 hours)* Users will have 24 hours to upload a valid license before the duplicate license is blocked.
Management	The total number of connected FortiClient endpoints out of the total number of endpoint licenses.

Network

The network settings are used to configure ports for the Micro-FortiGuard Server for FortiClient unit. You should also specify what port and methods that an administrators can use to access the Micro-FortiGuard Server for FortiClient unit. If required, static routes can be configured.

The default port for Micro-FortiGuard Server for FortiClient units is port 1. It can be used to configure one IP address for the Micro-FortiGuard Server for FortiClient unit, or multiple ports can be configured with multiple IP addresses for improved security.

You can configure administrative access in IPv4 or IPv6 and include settings for HTTPS, HTTP, PING, SSH, TELNET, SNMP, and Web Service.

You can prevent unauthorized access to the GUI by creating administrator accounts with trusted hosts. With trusted hosts configured, the administrator can only log in to the GUI when working on a computer with the trusted host as defined in the administrator account. For more information, see Trusted hosts on page 26 and Managing administrator accounts on page 23.

Configuring network interfaces

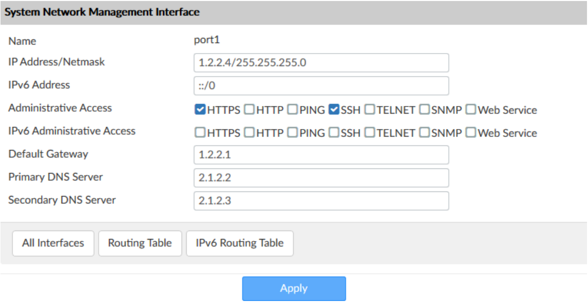
Endpoints can receive updates from any of the interfaces. The DNS servers must be on the networks to which the Micro-FortiGuard Server for FortiClient unit connects, and should have two different IP addresses.

The following port configuration is recommended:

- Use port 1 for endpoint connections, and disable unneeded services on it, such as SSH, TELNET, Web Service, and so on.
- Use a second port for administrator access, and enable HTTPS, Web Service, and SSH for this port. Leave other services disabled.

To configure port 1:

1. Go to *System Settings > Network*. The *System Network Management Interface* pane is displayed.



System Network Management Interface

Name	port1
IP Address/Netmask	1.2.2.4/255.255.255.0
IPv6 Address	::/0
Administrative Access	☑HTTPS □HTTP □PING ☑SSH □TELNET □SNMP □Web Service
IPv6 Administrative Access	□HTTPS □HTTP □PING □SSH □TELNET □SNMP □Web Service
Default Gateway	1.2.2.1
Primary DNS Server	2.1.2.2
Secondary DNS Server	2.1.2.3

2. Configure the following settings for *port1*, then click *Apply* to apply your changes.

Name	Displays the name of the interface.
IP Address/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address associated with this interface.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
Default Gateway	The default gateway associated with this interface.
Primary DNS Server	The primary DNS server IP address.
Secondary DNS Server	The secondary DNS server IP address.

To configure additional ports:

1. Go to *System Settings > Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Configure the settings as required.
4. Click *OK* to apply your changes.

The port name, default gateway, and DNS servers cannot be changed from the *Edit System Interface* pane. The port can be given an alias if needed.

Disabling ports

Ports can be disabled to prevent them from accepting network traffic

To disable a port:

1. Go to *System Settings* > *Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. In the *Status* field, click *Disable*
4. Click *OK* to disable the port.

Changing administrative access

Administrative access defines the protocols that can be used to connect to the Micro-FortiGuard Server for FortiClient through an interface. The available options are: HTTPS, HTTP, PING, SSH, TELNET, SNMP, and Web Service.

To change administrative access:

1. Go to *System Settings* > *Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Select one or more access protocols for the interface for IPv4 and IPv6, if applicable.
4. Click *OK* to apply your changes.

Static routes

Static routes can managed from the routing tables for IPv4 and IPv6 routes.

The routing tables can be accessed by going to *System Settings* > *Network* and clicking *Routing Table* and *IPv6 Routing Table*.

To add a static route:

1. From the IPv4 or IPv6 routing table, click *Create New* in the toolbar. The *Create New Network Route* pane opens.
2. Enter the destination IP address and netmask, or IPv6 prefix, and gateway in the requisite fields.
3. Select the network interface that connects to the gateway from the dropdown list.
4. Click *OK* to create the new static route.

To edit a static route:

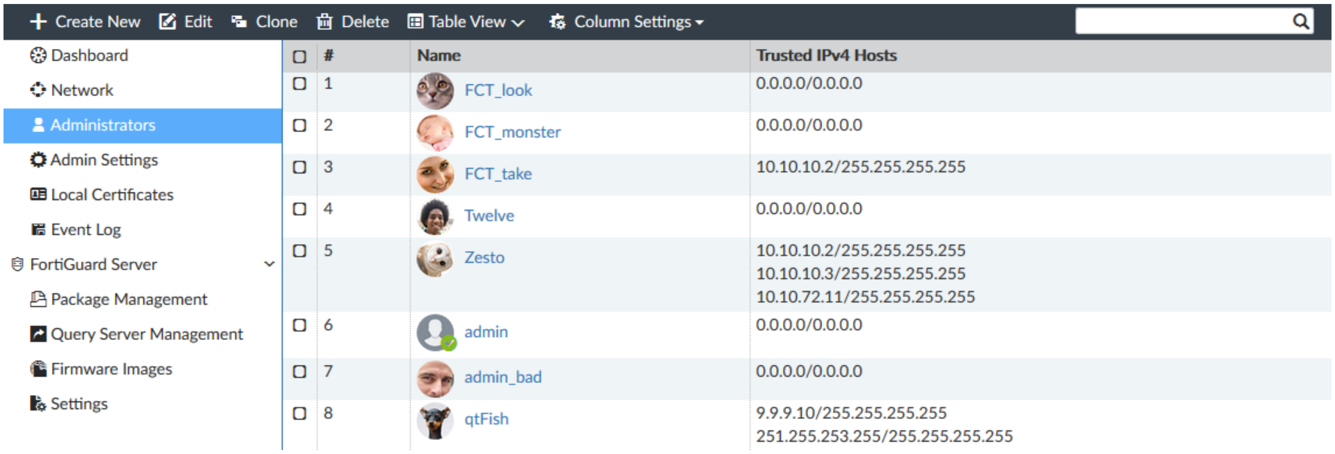
1. From the IPv4 or IPv6 routing table: double-click on a route, right-click on a route then select *Edit* from the pop-up menu, or select a route then click *Edit* in the toolbar. The *Edit Network Route* pane opens.
2. Edit the configuration as required. The route ID cannot be changed.
3. Click *OK* to apply your changes.

To delete a static route or routes:

1. From the IPv4 or IPv6 routing table, right-click on a route then select *Delete* from the pop-up menu, or select a route or routes then click *Delete* in the toolbar.
2. Click *OK* in the confirmation dialog box to delete the selected route or routes.

Managing administrator accounts

Go to *System Settings > Administrator* to view the list of administrators and manage administrator accounts.



□	#	Name	Trusted IPv4 Hosts
□	1	FCT_look	0.0.0.0/0.0.0.0
□	2	FCT_monster	0.0.0.0/0.0.0.0
□	3	FCT_take	10.10.10.2/255.255.255.255
□	4	Twelve	0.0.0.0/0.0.0.0
□	5	Zesto	10.10.10.2/255.255.255.255 10.10.10.3/255.255.255.255 10.10.72.11/255.255.255.255
□	6	admin	0.0.0.0/0.0.0.0
□	7	admin_bad	0.0.0.0/0.0.0.0
□	8	qtFish	9.9.9.10/255.255.255.255 251.255.253.255/255.255.255.255

The following options are available:

Create New	Create a new administrator. See Creating administrators on page 24.
Edit	Edit the selected administrator. See Editing administrators on page 25.
Clone	Clone the selected administrator.
Delete	Delete the selected administrator or administrators. See Deleting administrators on page 25.
Table View/Tile View	Change the view of the administrator list. Table view shows a list of the administrators in a table format. Tile view shows a separate card for each administrator in a grid pattern.
Column Settings	Change the displayed columns.
Search	Search the administrators.

Change Password	Change the selected administrator's password. This option is only available from the right-click menu. See Editing administrators on page 25.

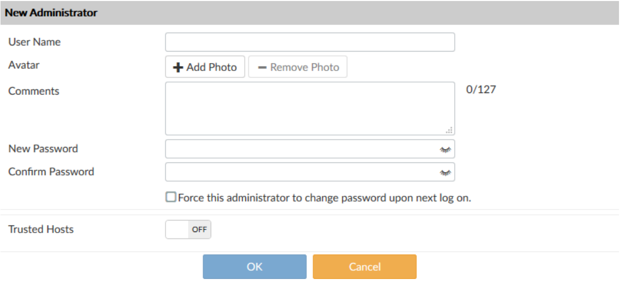
The following information is shown:

Seq.#	The sequence number.
Name	The name the administrator uses to log in.
Comments	Comments about the administrator account. This column is hidden by default.
Trusted IPv4 Hosts	The IPv4 trusted host(s) associated with the administrator. See Trusted hosts on page 26.
Trusted IPv6 Hosts	The IPv6 trusted host(s) associated with the administrator. See Trusted hosts on page 26. This column is hidden by default.

Creating administrators

To create a new administrator:

1. Go to *System Settings > Administrators*.
2. In the toolbar, click *Create New* to display the *New Administrator* pane.



3. Configure the following settings, and then click *OK* to create the new administrator.

User Name	Enter the name of the administrator will use to log in.
Avatar	Apply a custom image to the administrator. Click *Add Photo* to select an image already loaded to the Micro-FortiGuard Server for FortiClient, or to load an new image from the management computer. If no image is selected, the avatar will use the first letter of the user name.
Comments	Optionally, enter a description of the administrator, such as their role, location, or the reason for their account.
New Password	Enter the password.
Confirm Password	Enter the password again to confirm it.
Force this administrator to change password upon next log on.	Force the administrator to change their password the next time that they log in to the Micro-FortiGuard Server for FortiClient.

	This option is only available if *Password Policy* is enabled in *Admin Settings*. See Password policy on page 29.
Trusted Hosts	Optionally, turn on trusted hosts, then enter their IP addresses and netmasks. Up to ten IPv4 and ten IPv6 hosts can be added. See Trusted hosts on page 26 for more information.

Editing administrators

The administrator's name cannot be edited. An administrator's password can be changed using the right-click menu.

To edit an administrator:

1. Go to *System Settings > Administrators*.
2. Double-click on an administrator, right-click on an administrator and then select *Edit* from the menu, or select the administrator then click *Edit* in the toolbar. The *Edit Administrator* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To change an administrator's password:

1. Go to *System Settings > Administrators*.
2. Right-click on an administrator and select *Change Password* from the menu. The *Change Password* dialog box opens.
3. Enter the new password for the administrator in the *New Password* and *Confirm Password* fields.
4. Select *OK* to change the administrator's password.

The current administrator's password can also be changed from the admin menu in the GUI banner.

Deleting administrators

You cannot delete an administrator that is currently logged in to the device.

The *admin* administrator can only be deleted using the CLI.

To delete an administrator or administrators:

1. Go to *System Settings > Administrators*.
2. Select the administrator or administrators you need to delete.

3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the administrator or administrators.

To delete an administrator using the CLI:

1. Open a CLI console and enter the following command:

```
config system admin user
   delete <username>
end
```

Trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative permissions. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the Micro-FortiGuard Server for FortiClient unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply to both the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.

If you set trusted hosts and want to use the Console Access feature of the GUI, you must also set 127.0.0.1/255.255.255.255 as a trusted host.

Monitoring administrators

The *Admin Session List* lets you view a list of administrators currently logged in to the Micro-FortiGuard Server for FortiClient unit.

To view logged in administrators:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button. The *Admin Session List* opens in the widget.
   The following information is available:

User Name	The name of the administrator account. Your session is indicated by *(current)*.
IP Address	The IP address where the administrator is logging in from. This field also displays the logon type (GUI, jsconsole, SSH, or telnet).
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).

Disconnecting administrators

Administrators can be disconnected from the Micro-FortiGuard Server for FortiClient unit from the *Admin Session List*.

To disconnect administrators:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button. The *Admin Session List* opens in the widget.
3. Select the administrator or administrators you need to disconnect.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
   The selected administrators will be automatically disconnected from the Micro-FortiGuard Server for FortiClient device.

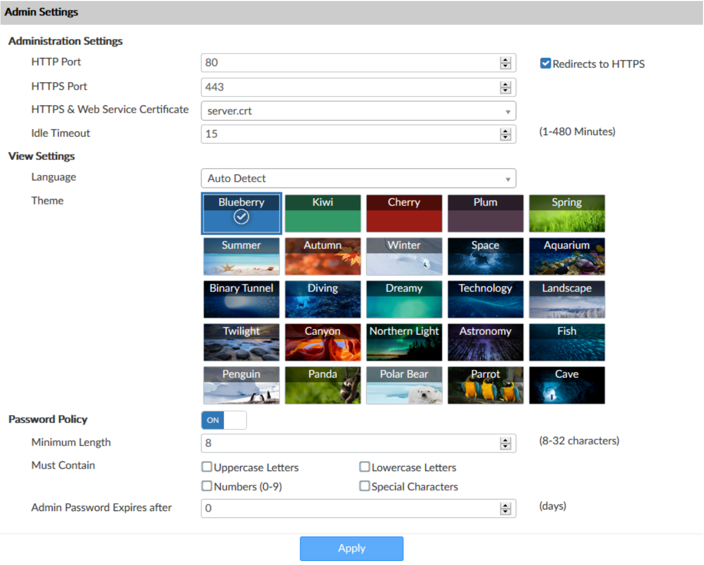
Global administration settings

The administration settings page provides options for configuring global settings for administrator access to the Micro-FortiGuard Server for FortiClient device. Settings include:

- Ports for HTTPS and HTTP administrative access
  To improve security, you can change the default port configurations for administrative connections to the Micro-FortiGuard Server for FortiClient. When connecting to the Micro-FortiGuard Server for FortiClient unit when the port has changed, the port must be included, such as `https://<ip_address>:<port>`. For example, if you are connecting to the Micro-FortiGuard Server for FortiClient unit using port 8080, the URL would be `https://192.168.1.99:8080`. When you change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is unique.
- Idle timeout settings
  By default, the GUI disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the GUI if the management computer is left unattended.
- GUI language
  The language the GUI uses. For best results, you should select the language used by the management computer.
- GUI theme
  The default color theme of the GUI is *Blueberry*. You can choose another color or an image.
- Password policy
  Enforce password policies for administrators.

To configure the administration settings:

1. Go to *System Settings > Admin Settings*.



Admin Settings

Administration Settings

HTTP Port: 80 ☑ Redirects to HTTPS

HTTPS Port: 443

HTTPS & Web Service Certificate: server.crt

Idle Timeout: 15 (1-480 Minutes)

View Settings

Language: Auto Detect

Theme: Blueberry ✓

Password Policy: ON

Minimum Length: 8 (8-32 characters)

Must Contain: □ Uppercase Letters □ Lowercase Letters □ Numbers (0-9) □ Special Characters

Admin Password Expires after: 0 (days)

2. Configure the following settings as needed, then click *Apply* to save your changes to all administrator accounts:

Administration Settings		
	HTTP Port	Enter the TCP port to be used for administrative HTTP access. Default: 80. Select *Redirect to HTTPS* to redirect HTTP traffic to HTTPS.
	HTTPS Port	Enter the TCP port to be used for administrative HTTPS access. Default: 443.
	HTTPS & Web Service Server Certificate	Select a certificate from the dropdown list.
	Idle Timeout	Enter the number of minutes an administrative connection can be idle before the administrator must log in again, from 1 to 480 (8 hours). See Idle timeout on page 30 for more information.
View Settings		
	Language	Select a language from the dropdown list. See GUI language on page 30 for more information.
	Theme	Select a theme for the GUI. The selected theme is not applied until you click *Apply*, allowing to you to sample different themes. Default: Blueberry.
Password Policy		Click to enable administrator password policies. See Password policy on page 29 and Password lockout and retry attempts on page 29 for more information.
	Minimum Length	Select the minimum length for a password, from 8 to 32 characters. Default: 8.
	Must Contain	Select the types of characters a password must contain.
	Admin Password Expires after	Select the number of days a password is valid for, after which it must be changed.

Password policy

You can enable and configure password policy for the Micro-FortiGuard Server for FortiClient.

To configure the password policy:

1. Go to *System Settings* > *Admin Settings*.
2. Click to enable *Password Policy*.
3. Configure the following settings, then click *Apply* to apply to password policy.

Minimum Length	Specify the minimum number of characters that a password must be, from 8 to 32. Default: 8.
Must Contain	Specify the types of characters a password must contain: uppercase and lowercase letters, numbers, and/or special characters.
Admin Password Expires after	Specify the number of days a password is valid for. When the time expires, an administrator will be prompted to enter a new password.

Password lockout and retry attempts

By default, the number password retry attempts is set to three, allowing the administrator a maximum of three attempts at logging in to their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts and the default wait time before the administrator can try to enter a password again can be customized. Both settings can be configured using the CLI.

To configure the lockout duration:

1. Enter the following CLI commands:

```
config system global
   set admin-lockout-duration <seconds>
end
```

To configure the number of retry attempts:

1. Enter the following CLI commands:

```
config system global
   set admin-lockout-threshold <failed_attempts>
end
```

Example

To set the lockout threshold to one attempt and set a five minute duration before the administrator can try to log in again, enter the following CLI commands:

```
config system global
   set admin-lockout-duration 300
   set admin-lockout-threshold 1
end
```

GUI language

The GUI supports multiple languages, including:

- English
- Simplified Chinese
- Traditional Chinese
- Japanese
- Korean

By default, the GUI language is set to *Auto Detect*, which automatically uses the language used by the management computer. If that language is not supported, the GUI defaults to English. For best results, you should select the language used by the operating system on the management computer.

To change the GUI language:

1. Go to *System Settings* > *Admin Settings*.
2. Under the *View Settings*, In the *Language* field, select a language, or *Auto Detect*, from the dropdown list.
3. Click *Apply* to apply the language change.

Idle timeout

To ensure security, the idle timeout period should be short. By default, administrative sessions are disconnected if no activity takes place for five minutes. This idle timeout is recommended to prevent anyone from using the GUI on a PC that was logged in to the GUI and then left unattended. The idle timeout period can be set from 1 to 480 minutes.

To change the idle timeout:

1. Go to *System Settings* > *Admin Settings*.
2. Change the *Idle Timeout* period as required.
3. Click *Apply*.

Certificates

The Micro-FortiGuard Server for FortiClient generates a certificate request based on the information you entered to identify the Micro-FortiGuard Server for FortiClient unit. After you generate a certificate request, you can download the request to a management computer and then forward the request to a CA.

Local certificates are issued for a specific server, or website. Generally they are very specific, and often for an internal enterprise network.

Local certificates

The Micro-FortiGuard Server for FortiClient unit generates a certificate request based on the information you enter to identify the Micro-FortiGuard Server for FortiClient unit. After you generate a certificate request, you can download the request to a computer that has management access to the Micro-FortiGuard Server for FortiClient unit and then forward the request to a CA.

The certificate window also enables you to export certificates for authentication, importing, and viewing.

The Micro-FortiGuard Server for FortiClient has two default local certificate: *Fortinet_Local* and *Fortinet_Local2*.

You can manage local certificates from the *System Settings > Local Certificates* page. Some options are available in the toolbar and some are also available in the right-click menu.

Creating a local certificate

To create a certificate request:

1. Go to *System Settings > Local Certificates*.
2. Click *Create New* in the toolbar. The *Generate Certificate Signing Request* pane opens.
3. Enter the following information as required, then click *OK* to save the certificate request:

Certificate Name	The name of the certificate.
Subject Information	Select the ID type from the dropdown list: • *Host IP*: Select if the unit has a static IP address. Enter the public IP address of the unit in the *Host IP* field. • *Domain Name*: Select if the unit has a dynamic IP address and subscribes to a dynamic DNS service. Enter the domain name of the unit in the *Domain Name* field. • *Email*: Select to use an email address. Enter the email address in the *Email Address* field.
Optional Information	
Organization Unit (OU)	The name of the department. You can enter a series of OUs up to a maximum of 5. To add or remove an OU, use the plus (+) or minus (-) icons.
Organization (O)	Legal name of the company or organization.
Locality (L)	Name of the city or town where the device is installed.
State/Province (ST)	Name of the state or province where the FortiGate unit is installed.
Country (C)	Select the country where the unit is installed from the dropdown list.
E-mail Address (EA)	Contact email address.
Subject Alternative Name	Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma.

	A name can be: • e-mail address • IP address • URI • DNS name (alternatives to the Common Name) • directory name (alternatives to the Distinguished Name) You must precede the name with the name type. Examples: • IP:1.1.1.1 • email:test@fortinet.com • email:my@other.address • URI:http://my.url.here/
Key Type	The key type can be *RSA* or *Elliptic Curve*.
Key Size	Select the key size from the dropdown list: *512 Bit*, *1024 Bit*, *1536 Bit*, or *2048 Bit*. This option is only available when the key type is *RSA*.
Curve Name	Select the curve name from the dropdown list: *secp256r1* (default), *secp384r1*, or *secp521r1*. This option is only available when the key type is *Elliptic Curve*.
Enrollment Method	The enrollment method is set to *File Based*.

Importing local certificates

To import a local certificate:

1. Go to *System Settings* > *Local Certificates*.
2. Click *Import* in the toolbar or right-click and select *Import*. The *Import* dialog box opens.
3. Enter the following information as required, then click *OK* to import the local certificate:

Type	Select the certificate type from the dropdown list: *Local Certificate*, *PKCS #12 Certificate*, or *Certificate*.
Certificate File	Click *Browse...* and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
Key File	Click *Browse...* and locate the key file on the management computer, or drag and drop the file onto the dialog box. This option is only available when *Type* is *Certificate*.
Password	Enter the certificate password. This option is only available when *Type* is *PKCS #12 Certificate* or *Certificate*.
Certificate Name	Enter the certificate name. This option is only available when *Type* is *PKCS #12 Certificate* or *Certificate*.

Deleting local certificates

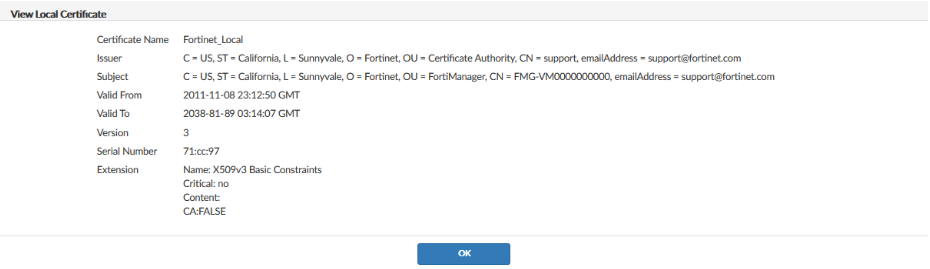
To delete a local certificate or certificates:

1. Go to *System Settings* > *Local Certificates*.
2. Select the certificate or certificates you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected certificate or certificates.

Viewing details of local certificates

To view details of a local certificate:

1. Go to *System Settings* > *Local Certificates*.
2. Select the certificates that you would like to see details about, then click *View Certificate Detail* in the toolbar or right-click menu. The *View Local Certificate* page opens.



Certificate Name	Fortinet_Local
Issuer	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com
Subject	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN = FMG-VM0000000000, emailAddress = support@fortinet.com
Valid From	2011-11-08 23:12:50 GMT
Valid To	2038-81-89 03:14:07 GMT
Version	3
Serial Number	71:cc:97
Extension	Name: X509v3 Basic Constraints Critical: no Content: CA:FALSE

3. Click *OK* to return to the local certificates list.

Downloading local certificates

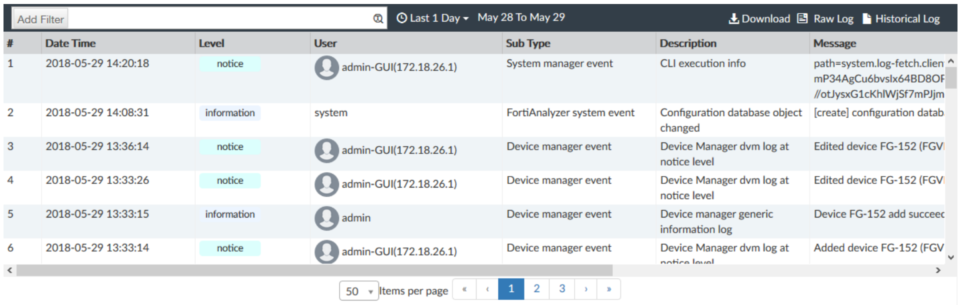
To download a local certificate:

1. Go to *System Settings* > *Local Certificates*.
2. Select the certificate that you need to download.
3. Click *Download* in the toolbar, or right-click and select *Download*, and save the certificate to the management computer.

Event Log

The *Event Log* pane provides an audit log of actions made by users on Micro-FortiGuard Server for FortiClient. It allows you to view log messages that are stored in memory or on the internal hard disk drive. You can use filters to search the messages and download the messages to the management computer.

Go to *System Settings* > *Event Log* to view the local log list.



#	Date Time	Level	User	Sub Type	Description	Message
1	2018-05-29 14:20:18	notice	admin-GUI(172.18.26.1)	System manager event	CLI execution info	path=system.log-fetch.clien mP34AgCu6bvslx64BD8OF //otJysxG1cKhlWjSf7mPJjm
2	2018-05-29 14:08:31	information	system	FortiAnalyzer system event	Configuration database object changed	[create] configuration datab
3	2018-05-29 13:36:14	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Edited device FG-152 (FGV
4	2018-05-29 13:33:26	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Edited device FG-152 (FGV
5	2018-05-29 13:33:15	information	admin	Device manager event	Device manager generic information log	Device FG-152 add succeec
6	2018-05-29 13:33:14	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Added device FG-152 (FGV

The following options are available:

Add Filter	Filter the event log list based on the log level, user, sub type, or message. See Event log filtering on page 35.
Last...	Select the amount of time to show from the available options, or select a custom time span or any time.
Download	Download the event logs in either CSV or the normal format to the management computer.
Raw Log / Formatted Log	Click on *Raw Log* to view the logs in their raw state. Click *Formatted Log* to view them in the formatted into a table.
Historical Log	Click to view the historical logs list.
Back	Click the back icon to return to the regular view from the historical view.
View	View the selected log file. This option is also available from the right-click menu, or by double-clicking on the log file. This option is only available when viewing historical event logs.
Delete	Delete the selected log file. This option is also available from the right-click menu. This option is only available when viewing historical event logs.
Clear	Clear the selected file of logs. This option is also available from the right-click menu. This option is only available when viewing historical event logs.
Type	Select the type from the dropdown list: • *Event Log* • *FDS Upload Log*: Select the device from the dropdown list. • *FDS Download Log*: Select the service (*FDS*, or *FCT*) from the *Service* dropdown list, select the event type (*All Event*, *Push Update*, *Poll Update*, or *Manual Update*) from the *Event* dropdown list, and then click *Go* to browse the logs. This option is only available when viewing historical logs.
Search	Enter a search term to search the historical logs. This option is only available when viewing historical event logs.
Pagination	Browse the pages of logs and adjust the number of logs that are shown per page.

The following information is shown:

#	The log number.
Date Time	The date and time that the log file was generated.
Level	The log level: Debug Information Notification Warning Error Critical Alert Emergency
User	The user that the log message relates to.
Sub Type	The log sub-type.
Description	A description of the event.
Message	Log message details.

Event log filtering

The event log can be filtered using the *Add Filter* box in the toolbar.

To filter FortiView summaries using the toolbar:

1. Specify filters in the *Add Filter* box.
    - Regular Search: In the selected summary view, click in the *Add Filter* box, select a filter from the dropdown list, then type a value. Click NOT to negate the filter value. You can add multiple filters at a time, and connect them with an "or".
    - Advanced Search: Click the *Switch to Advanced Search* icon at the right end of the *Add Filter* box to switch to advanced search mode. In this mode, you type in the whole search criteria (log field names and values). Click the *Switch to Regular Search* icon to return to regular search.
2. Click *Go* to apply the filter.