FortiClient EMS - Use Cases

Version 6.0.3

December 19, 2018
FortiClient EMS 6.0.3 Use Cases
04-603-530344-20181219

TABLE OF CONTENTS

Use Case: FortiClient Software Management

This use case describes how to use FortiClient EMS for basic central management of FortiClient endpoints when deploying FortiClient to endpoints using AD servers. This scenario requires the following steps:

1. Complete the prerequisites by preparing the AD server and Windows endpoints for deployment. See Prerequisites on page 4.
2. Add endpoints to EMS by adding the AD server to EMS. See Adding endpoints using an Active Directory Domain service on page 4.
3. Create a gateway list. Creating a gateway list is only necessary if connecting Telemetry to FortiGate. See Creating a gateway list on page 6.
4. Create a FortiClient installer. Specify the gateway list (if created) in the installer. See Creating a FortiClient installer on page 7.
5. Create a profile, select the FortiClient installer package, and configure FortiClient features in the profile. See Creating a deployment profile on page 11.
6. Assign the profile to a branch of the AD domain to push the FortiClient installation process on the endpoints. See Assigning the profile to endpoints on page 13.
7. Verify the deployment by monitoring FortiClient connections to FortiClient EMS.
8. When a new FortiClient version is available, create a corresponding installer to deploy the new FortiClient version to endpoints. See Upgrading endpoints to the latest version of FortiClient on page 14.

Prerequisites

To continue with this use case, you must complete the following prerequisite steps. For details, see *Deployment* in the *FortiClient EMS Administration Guide.*:

1. Install and prepare the AD server as follows.
   a. Configure a group policy on the AD server.
   b. Configure required Windows services.
   c. Create deployment rules for Windows firewall.
   d. Configure Windows firewall domain profile settings.
2. Prepare Windows endpoints for deployment as follows:
   a. Configure required Windows services.
   b. Configure Windows firewall to allow certain inbound connections.

Adding endpoints using an Active Directory Domain service

First, you must import the desired endpoints into FortiClient EMS. In this scenario, you will add endpoints using an Active Directory (AD) domain server.

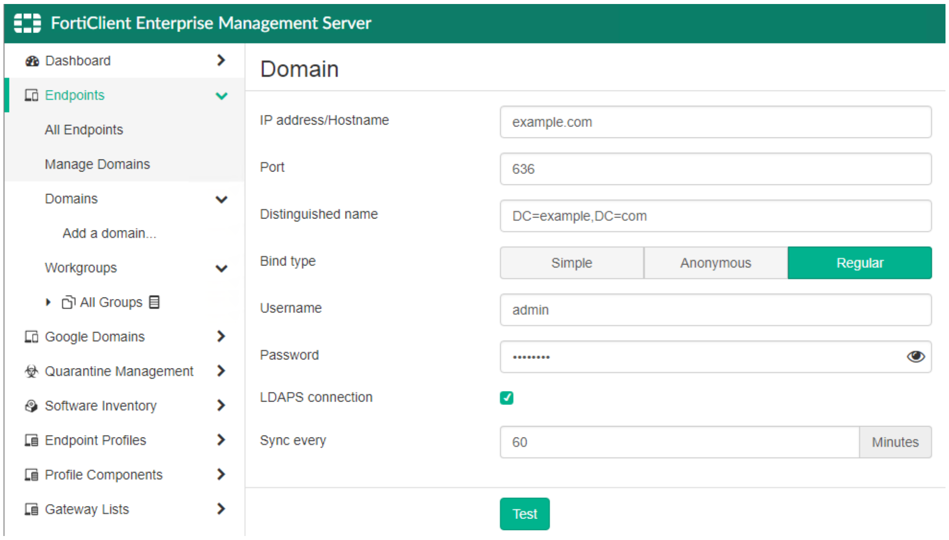
You can also use workgroups to deploy FortiClient software, although you cannot use workgroups to deploy an initial installation of FortiClient to endpoints. After FortiClient is installed on endpoints and endpoints are connected to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints. See the *FortiClient EMS Administration Guide* for details.

Endpoints can be manually imported from an AD server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying endpoints that are part of an AD domain server.

An instructional video on how to add a domain is available in the Fortinet Video Library.

You can add the entire domain or an organizational unit (OU) from the domain.

1. Go to *Endpoints* > *Manage Domains* > *Add*. The *Domain* pane displays.



IP address/Hostname	example.com
Port	636
Distinguished name	DC=example,DC=com
Bind type	Simple / Anonymous / **Regular**
Username	admin
Password	••••••••
LDAPS connection	☑
Sync every	60 Minutes

2. Configure the following options:

IP address/Hostname	Enter the domain's IP address or hostname. In this example, the AD server's hostname is example.com.
Port	Enter the port number. In this example, the port number, 636, is the default value when LDAPS connection is enabled.
Distinguished name	Enter the distinguished name. This field is optional.
Bind type	Select the bind type: *Simple*, *Anonymous*, or *Regular*. In this example, *Regular* was selected.

Username	Enter the username for the AD server.
Password	Enter the user password for the AD server.
Show Password	Turn on and off to show or hide the password.
LDAPS connection	Turn on to enable a secure connection protocol when *Bind Type* is set to *Regular*.
Sync every	Enter the sync schedule between FortiClient EMS and the domain in minutes. In this example, the sync schedule has been configured as 60 minutes.

3. Click *Test* to test the domain settings connection.
4. If the test is successful, select *Save* to save the new domain. If not, correct the information as required, then test the settings again.

After importing endpoints from an AD server, you can edit the endpoints. These changes are not synced back to the AD server.

Creating a gateway list

Next, you can create a gateway list. The gateway list is used to specify what IP addresses or fully qualified domain names (FQDN) and ports endpoints can use to connect FortiClient Telemetry to FortiGate, EMS, or FortiGate and EMS.

You do not need to create a gateway list if using FortiClient EMS without a FortiGate.

You can create a gateway list that contains IP addresses for multiple FortiGate units. FortiClient searches for IP addresses in its subnet in the gateway IP list and connects to the FortiGate in the list that is in the same subnet as the host system.

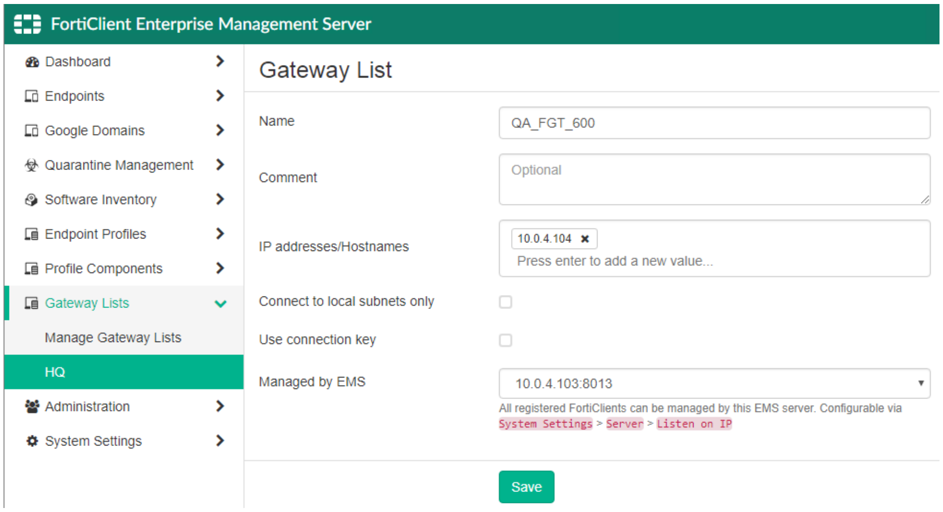
If FortiClient cannot find any FortiGates in its subnet, it attempts to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was configured in the gateway list.

In this example, we will configure a gateway list to facilitate connection between FortiClient and a FortiGate, which has an IP address of 10.0.4.104.

1. Go to *Gateway Lists* > *Manage Gateway Lists*.
2. Click the *Add* button.

3. Configure the following:

Name	Enter the list name. It is recommended to use an easily identifiable name. In this example, the name given is QA_FGT_600, indicating that the FortiGate is running FortiOS 6.0.0 and is used to manage endpoints belonging to employees from the QA organization.
Comment	Enter additional comments. This is optional.
IP addresses/Hostnames	Enter the IP address(es) or hostname(s) of the FortiGate devices. You can also use an FQDN. In this example, the FortiGate's IP address is 10.0.4.104. Press the *Enter* key to add additional IP addresses.
Connect to local subnets only	Enable to only allow connection to local subnets. This is optional and has not been enabled in this example.
Use connection key	Enable the connection key endpoints can use to connect to FortiGate units. This is optional and has not been enabled in this example.
Managed by EMS	Select an option from the dropdown list. Users can configure this IP address in *System Settings > Server*. Endpoints will be managed by this EMS.



Gateway List

Name: QA_FGT_600

Comment: Optional

IP addresses/Hostnames: 10.0.4.104 ✖
Press enter to add a new value...

Connect to local subnets only ☐

Use connection key ☐

Managed by EMS: 10.0.4.103:8013 ▾

All registered FortiClients can be managed by this EMS server. Configurable via `System Settings` > `Server` > `Listen on IP`

4. Click *Save*.

Creating a FortiClient installer

Now you must create a FortiClient installer. You will use this installer to deploy FortiClient to endpoints.

When you create a FortiClient installer to FortiClient EMS, you can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint.

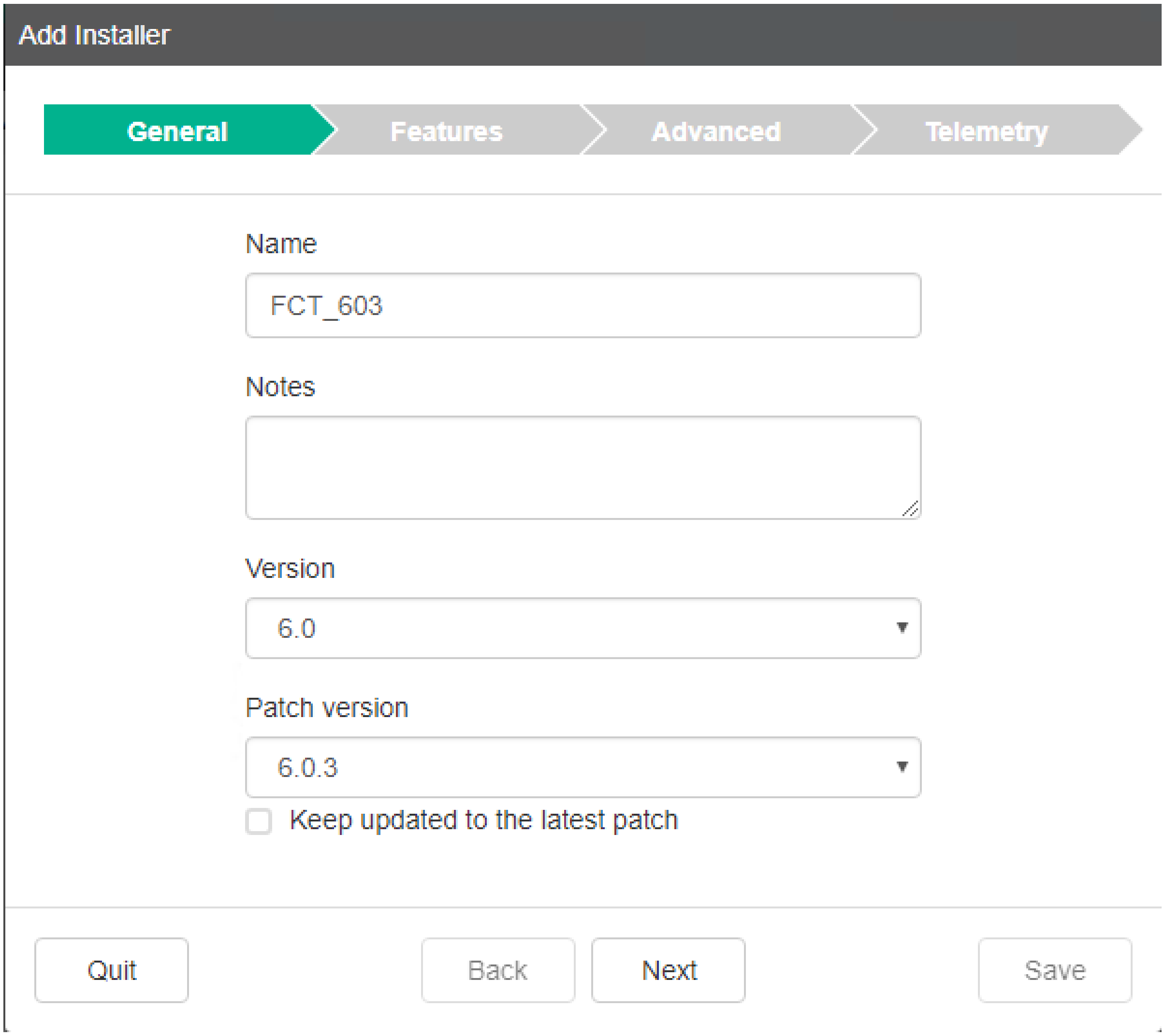
For example, consider that you create an installer that has SSL VPN and IPsec VPN enabled. You then assign the installer to a profile where VPN is disabled. The endpoints that the profile is deployed to will have VPN disabled. At a later time, if you enable VPN on the profile, the endpoints will then have VPN enabled, since it was included in the installer.

When you create a FortiClient installer in FortiClient EMS, an installer for the Windows operating system and an installer for the macOS operating system are added to FortiClient EMS.

After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

1. Go to *Profile Components* > *Manage Installers*.
2. Click *Add*.

3. On the *General* tab, set the following options.



Add Installer

Name: FCT_603

Notes:

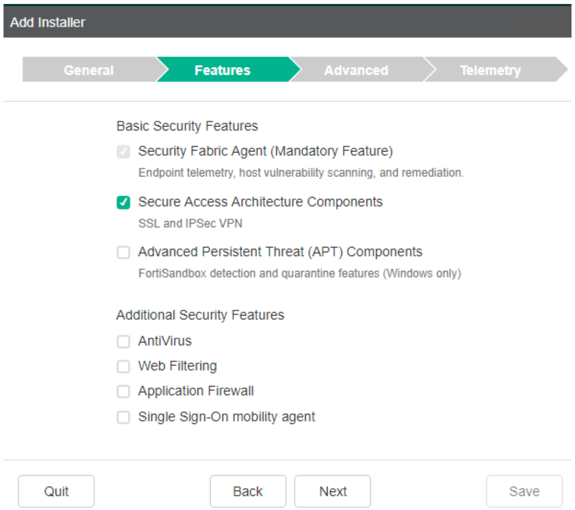
Version: 6.0

Patch version: 6.0.3

□ Keep updated to the latest patch

Name	Enter the FortiClient installer's name. In the example, the installer's name is FCT_603, to indicate that is used to deploy FortiClient 6.0.3.
Notes	Enter any notes about the FortiClient installer. This field is optional.
Version	Select the FortiClient version to install. The example is configured for FortiClient 6.0.
Patch version	Select the specific FortiClient patch version to install. The example is configured for FortiClient 6.0.3.
Keep updated to the latest patch	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint. This is optional and has not been enabled in this example.

4. Click *Next*. On the *Features* tab, you can select which features to include in the installer. In this example, only VPN has been included in addition to Security Fabric Agent, which is enabled by default.



Add Installer

Basic Security Features

☑ Security Fabric Agent (Mandatory Feature)
Endpoint telemetry, host vulnerability scanning, and remediation.

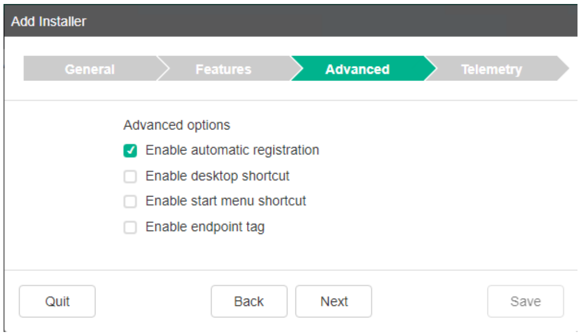
☑ Secure Access Architecture Components
SSL and IPSec VPN

□ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features (Windows only)

Additional Security Features

□ AntiVirus
□ Web Filtering
□ Application Firewall
□ Single Sign-On mobility agent

5. Click *Next*. On the *Advanced* tab, you can set additional options for the installer. In this example, only automatic registration is enabled for the installer. This allows FortiClient to automatically connect Telemetry to EMS or FortiGate after FortiClient is installed on the endpoint.

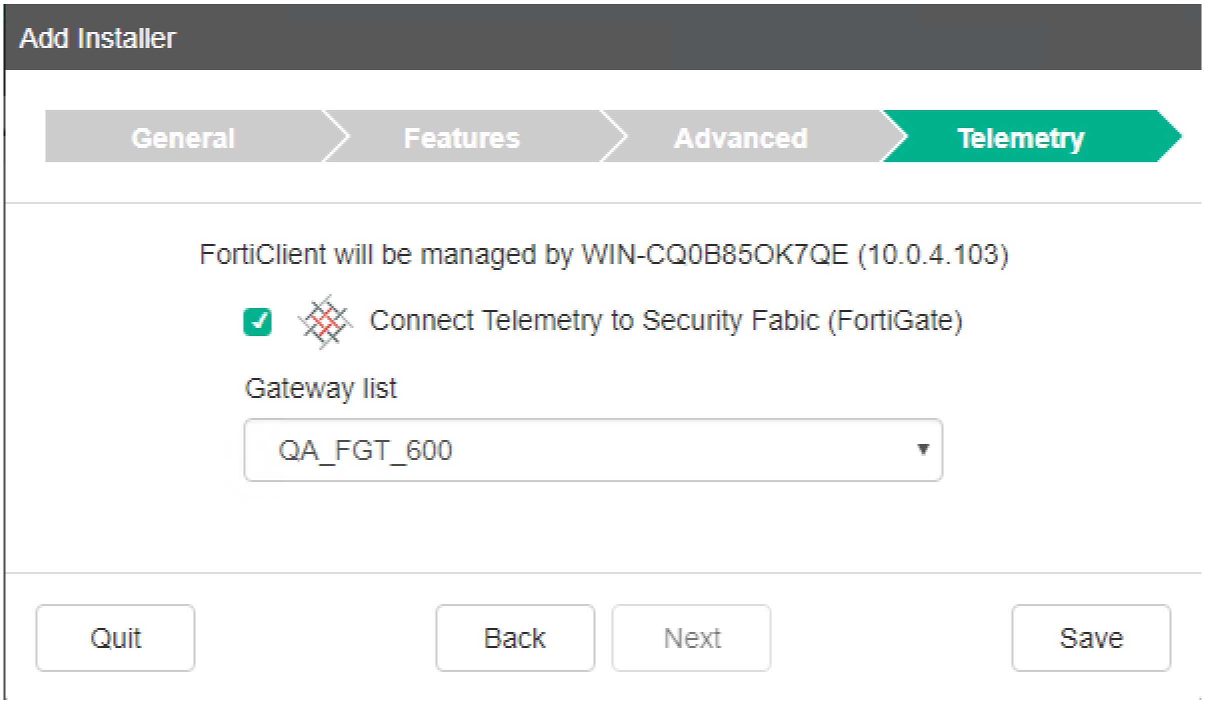


Add Installer

Advanced options

☑ Enable automatic registration
□ Enable desktop shortcut
□ Enable start menu shortcut
□ Enable endpoint tag

6. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the EMS server, which will manage FortiClient once it is installed on the endpoint. In the Gateway list dropdown list, select the gateway list created in Creating a gateway list on page 6. In this example, this is QA_FGT_600.



FortiClient will be managed by WIN-CQ0B85OK7QE (10.0.4.103)

☑ Connect Telemetry to Security Fabic (FortiGate)

Gateway list

QA_FGT_600

7. Click *Save*. The FortiClient installer is added to FortiClient EMS and displays on the *Manage Installers* pane.

Creating a deployment profile

Next, you must create a new profile to deploy FortiClient to endpoints. You will assign the installer created in Creating a FortiClient installer on page 7 to the profile.

When creating a profile to deploy FortiClient, you must create a new profile. You cannot add an installer to the default profile.

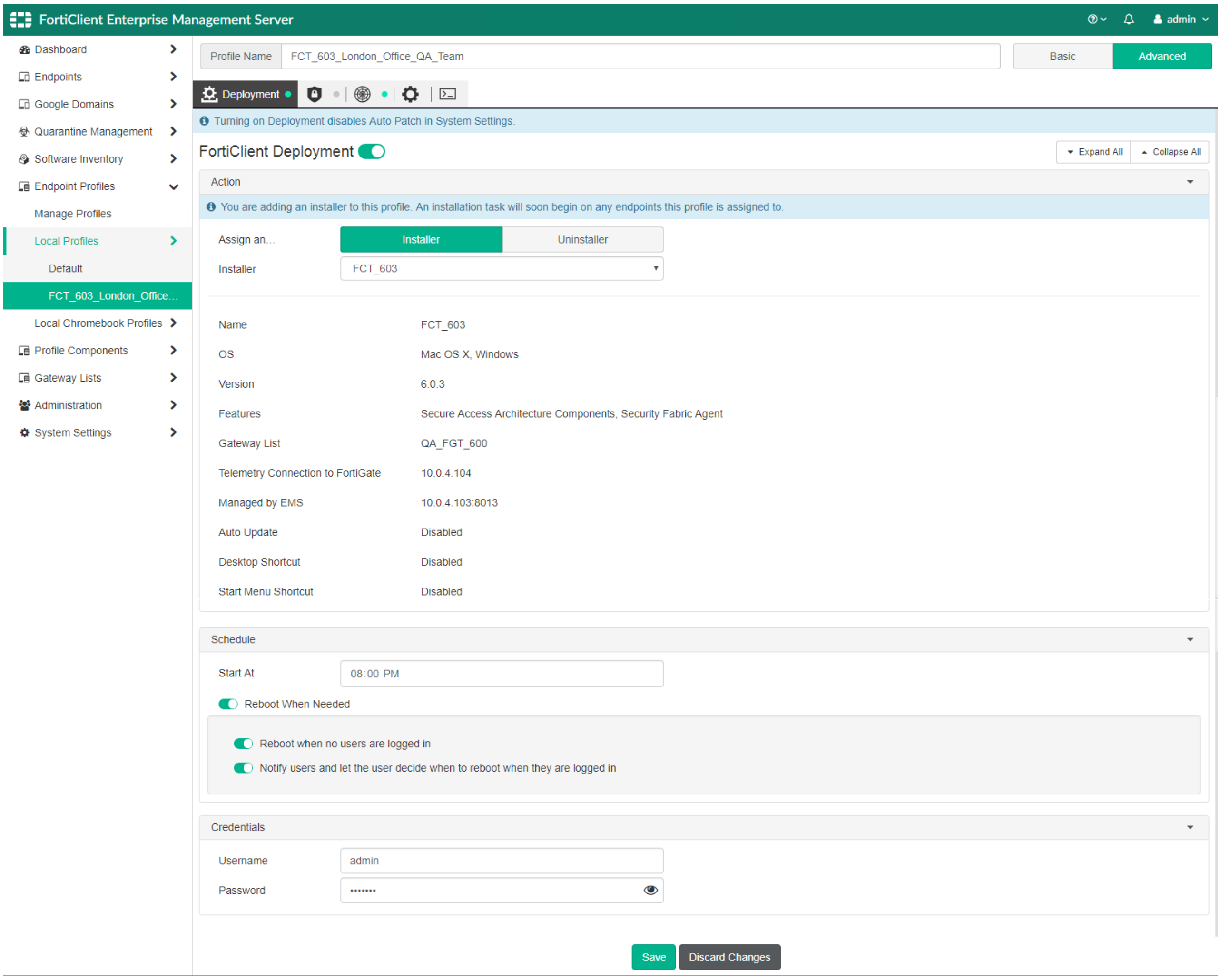
The selected FortiClient installer in a profile controls what tabs are displayed for configuration in the profile. Only the tabs for the features in the selected installer are displayed for configuration in the profile. For example, if the installer includes only the VPN feature, only the *VPN* tab is displayed for you to configure. The *System Settings* tab always displays.

You can disable a feature included in the installer, then enable the feature in the profile later. For example, if the installer includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Filter is installed, but disabled.

1. Go to *Endpoint Profiles* > *Manage Profile*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.
3. Set the following options on the *Deployment* tab:

Action

	Assign an	Click *Installer*.
	Installer	In the *Installer* list, select the FortiClient installer created in Creating a FortiClient installer on page 7. The installer options display.
Schedule		
	Start At	Specify what time to start installing FortiClient on endpoints. In this example, the time is configured for 8:00 PM.
	Reboot When Needed	Enable to reboot the endpoint to install FortiClient when needed.
	Reboot when no users is logged in	Enable to allow the endpoint to reboot without prompt if no endpoint user is logged into FortiClient.
	Notify users and let the user decide when to reboot when they are logged in	Enable to notify the end user if a reboot of the endpoint is needed and allow the user to decide what time to reboot the endpoint. Disable to reboot the endpoint without notifying the user.
Credentials		
	Username	Enter the username to perform deployment on AD. You must enter the admin credentials for the AD in the profile. Enter the appropriate credentials in the profile to assign to the AD. The credentials allow EMS to install FortiClient on endpoints using AD. If the credentials are wrong, the installation fails, and an error displays in EMS.
	Password	Enter the password to perform deployment on AD.



Profile Name: FCT_603_London_Office_QA_Team

Turning on Deployment disables Auto Patch in System Settings.

FortiClient Deployment

Action

You are adding an installer to this profile. An installation task will soon begin on any endpoints this profile is assigned to.

Assign an...: Installer | Uninstaller

Installer: FCT_603

Name	FCT_603
OS	Mac OS X, Windows
Version	6.0.3
Features	Secure Access Architecture Components, Security Fabric Agent
Gateway List	QA_FGT_600
Telemetry Connection to FortiGate	10.0.4.104
Managed by EMS	10.0.4.103:8013
Auto Update	Disabled
Desktop Shortcut	Disabled
Start Menu Shortcut	Disabled

Schedule

Start At: 08:00 PM

Reboot When Needed

Reboot when no users are logged in

Notify users and let the user decide when to reboot when they are logged in

Credentials

Username: admin

Password: •••••••

4. Set the options on the remaining tabs if desired. See the *FortiClient EMS Administration Guide* for details.
5. Click *Save*.

For information on additional profile configuration, see the *FortiClient EMS Administration Guide*.

Assigning the profile to endpoints

After creating the profile, you can assign the profile to the domain or a group within the domain. When you assign the profile to a domain or group, the profile settings are automatically pushed to all endpoints in the specified domain or group.

If you do not assign a profile to a specific domain or group, EMS automatically applies the default profile.

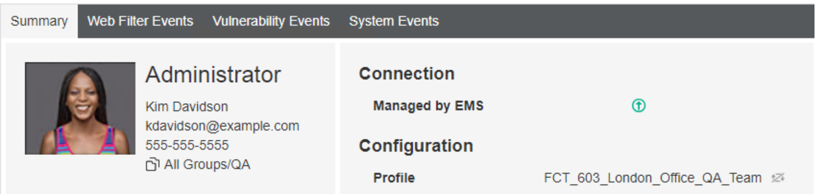
1. Go to *Endpoints*.
2. Right-click a domain or group, select *Assign profile*, then the profile. A confirmation dialog displays.

3. Click *Yes*. The profile is assigned.

Once the profile is assigned to a specified domain or group and the start time configured in Creating a FortiClient installer on page 7 is reached, EMS deploys FortiClient to the endpoints. The profile controls the endpoint's FortiClient configuration. FortiClient connects Telemetry to the FortiGate specified in the gateway list and the EMS server specified in the installer.

After initial deployment of FortiClient, you can use the profile to change the endpoint's FortiClient configuration. To push configuration changes to endpoints, simply make changes to the endpoint's assigned profile. EMS syncs the configuration changes to FortiClient on the endpoint. You can check the *Endpoints* pane to see if the endpoint's synchronization status.

The below shows an endpoint that is not synchronized with the latest profile configuration changes.

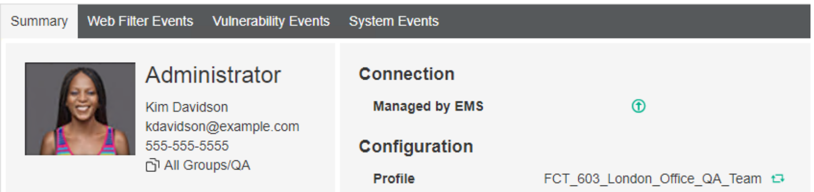


Administrator
Kim Davidson
kdavidson@example.com
555-555-5555
All Groups/QA

Connection
Managed by EMS

Configuration
Profile FCT_603_London_Office_QA_Team

The below shows an endpoint that is synchronized with the latest profile configuration changes.



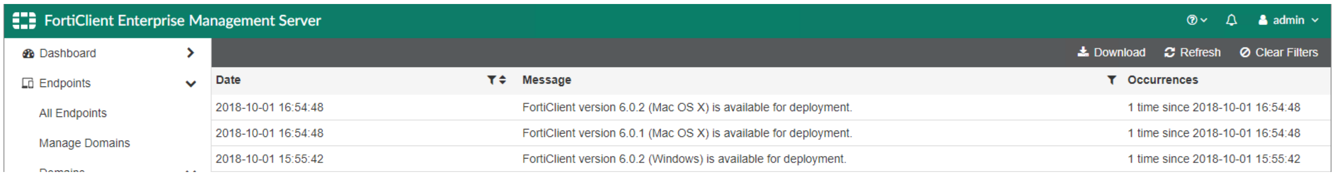
Administrator
Kim Davidson
kdavidson@example.com
555-555-5555
All Groups/QA

Connection
Managed by EMS

Configuration
Profile FCT_603_London_Office_QA_Team

Upgrading endpoints to the latest version of FortiClient

When a new version of FortiClient is available, EMS displays an alert (the bell icon) in the top right-corner of the GUI. The below shows an example of the EMS GUI when new versions of FortiClient (in this case for macOS and Windows) are available.



Date	Message	Occurrences
2018-10-01 16:54:48	FortiClient version 6.0.2 (Mac OS X) is available for deployment.	1 time since 2018-10-01 16:54:48
2018-10-01 16:54:48	FortiClient version 6.0.1 (Mac OS X) is available for deployment.	1 time since 2018-10-01 16:54:48
2018-10-01 15:55:42	FortiClient version 6.0.2 (Windows) is available for deployment.	1 time since 2018-10-01 15:55:42

You can update endpoints to the new version of FortiClient by creating a new installer as described in Creating a FortiClient installer on page 7. You can then edit the assigned endpoint profile's *Deployment* tab to specify the newly created installer:

1. Go to *Endpoint Profiles*, and select the assigned profile.
2. Click *Edit*. The profile settings display in the content pane.
3. On the *Deployment* tab, select the new installer from the *Installer* dropdown list.
4. Edit other settings as desired.
5. Click *Save*.

EMS syncs the profile changes to the affected endpoints, and the new version of FortiClient is installed on them.

Use Case: Fortinet Security Fabric Agent for Your Security Fabric

This use case describes how to deploy Security Fabric Agent (SFA), a key module within FortiClient that integrates endpoints with FortiGate and the Security Fabric. SFA strengthens enterprise security through enhanced endpoint visibility, compliance control, vulnerability scanning, and automated response.

SFA is enabled by default when installing FortiClient and includes components to support the Security Fabric available with FortiGate, such as the following:

Component	Description
FortiClient Telemetry	FortiClient can connect Telemetry to FortiGate and/or EMS. EMS uses the FortiClient Telemetry connection to manage FortiClient endpoints. FortiClient connects Telemetry to FortiGate to participate in the Security Fabric or compliance enforcement.
Vulnerability scanning	Check endpoints for known vulnerabilities. The vulnerability scan results can include: • List of vulnerabilities detected • How many detected vulnerabilities are rated as critical, high, medium, or low threats • Links to more information, including links to the FortiGuard Center FortiClient can detect vulnerabilities for many software.
Vulnerability remediation	After detecting vulnerabilities, FortiClient provides a one-click link to immediately install patches and resolve as many identified vulnerabilities as possible. It also displays a list of patches that require the endpoint user to manually install to resolve outstanding vulnerabilities.

You can use EMS to deploy SFA to endpoints. This scenario requires the following steps:

1. Create a gateway list with the FortiGate IP address. See Creating a gateway list on page 17.
2. Create a FortiClient installer. Specify the gateway list in the installer. See Creating a FortiClient installer on page 18.
3. Create a profile, select the FortiClient installer package, and configure FortiClient features in the profile. See Creating a deployment profile on page 21.
4. Assign the profile to the desired endpoints to push the FortiClient installation process on the endpoints. See Assigning the profile to endpoints on page 23.
5. Verify the endpoints have connected Telemetry to the Security Fabric and to EMS. See Verifying Telemetry connection on page 24.

The procedure above assumes that all desired endpoints have already been imported into EMS. For instructions on how to import endpoints into EMS, see the *FortiClient EMS Administration Guide*.

Creating a gateway list

First, you must create a gateway list in EMS that contains the IP address of a FortiGate that belongs to the Security Fabric. Gateway lists facilitate FortiClient Telemetry connection between FortiClient and the FortiGate. The gateway list is used to specify what IP addresses or fully qualified domain names (FQDN) and ports endpoints can use to connect FortiClient Telemetry to FortiGate, EMS, or FortiGate and EMS.

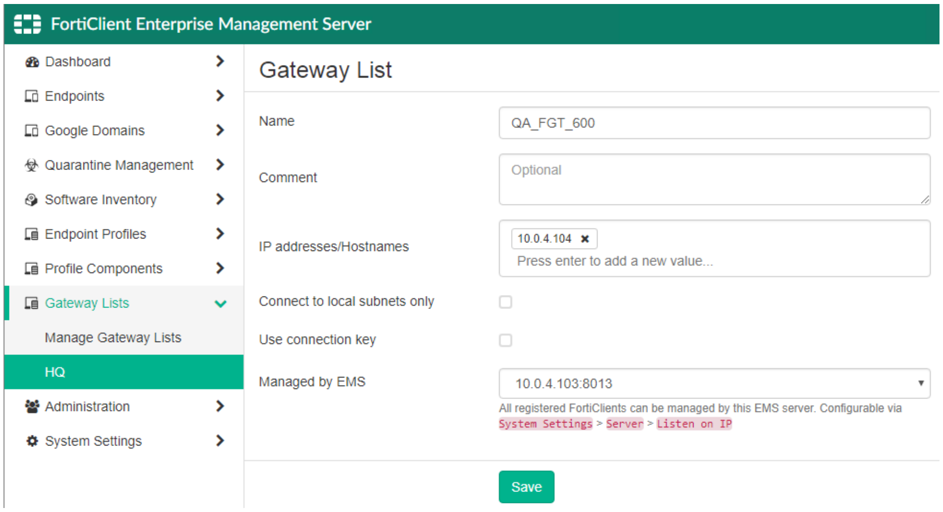
You can create a gateway list that contains IP addresses for multiple FortiGate units. FortiClient searches for IP addresses in its subnet in the gateway IP list and connects to the FortiGate in the list that is in the same subnet as the host system.

If FortiClient cannot find any FortiGates in its subnet, it attempts to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was configured in the gateway list.

In this example, we will configure a gateway list to facilitate connection between FortiClient and a FortiGate, which has an IP address of 10.0.4.104.

1. Go to *Gateway Lists* > *Manage Gateway Lists*.
2. Click the *Add* button.
3. Configure the following:

Name	Enter the list name. It is recommended to use an easily identifiable name. In this example, the name given is QA_FGT_600, indicating that the FortiGate is running FortiOS 6.0.0 and is used to manage endpoints belonging to employees from the QA organization.
Comment	Enter additional comments. This is optional.
IP addresses/Hostnames	Enter the IP address(es) or hostname(s) of the FortiGate devices. You can also use an FQDN. In this example, the FortiGate's IP address is 10.0.4.104. Press the *Enter* key to add additional IP addresses.
Connect to local subnets only	Enable to only allow connection to local subnets. This is optional and has not been enabled in this example.
Use connection key	Enable the connection key endpoints can use to connect to FortiGate units. This is optional and has not been enabled in this example.
Managed by EMS	Select an option from the dropdown list. Users can configure this IP address in *System Settings* > *Server*. Endpoints will be managed by this EMS.



Gateway List

Name: QA_FGT_600

Comment: Optional

IP addresses/Hostnames: 10.0.4.104 ✖ Press enter to add a new value...

Connect to local subnets only ☐

Use connection key ☐

Managed by EMS: 10.0.4.103:8013 ▾

All registered FortiClients can be managed by this EMS server. Configurable via `System Settings` > `Server` > `Listen on IP`

4. Click *Save*.

Creating a FortiClient installer

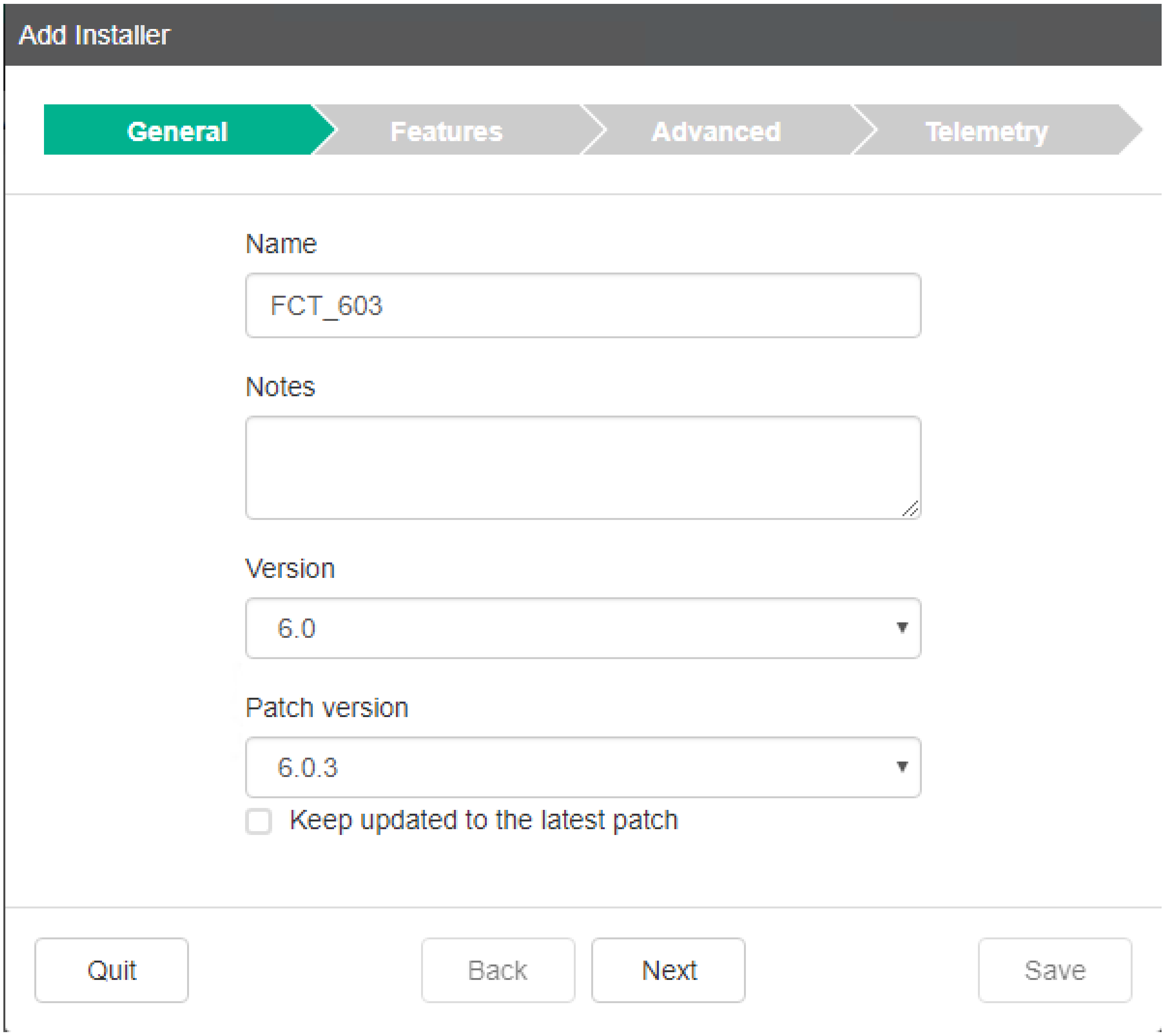
Now you must create a FortiClient installer. You will use this installer to deploy FortiClient with SFA components to endpoints. SFA is enabled by default in the FortiClient installer, as seen in the steps below. Include any other features in the installer as desired.

When you create a FortiClient installer in FortiClient EMS, an installer for the Windows operating system and an installer for the macOS operating system are added to FortiClient EMS.

After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

1. Go to *Profile Components* > *Manage Installers*.
2. Click *Add*.

3. On the *General* tab, set the following options.



Name

FCT_603

Notes

Version

6.0

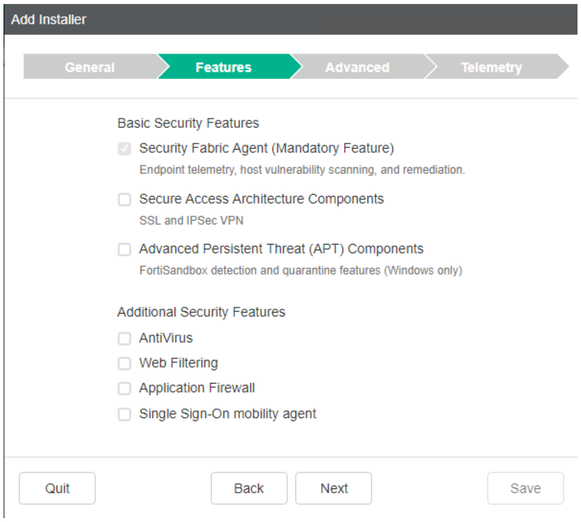
Patch version

6.0.3

□ Keep updated to the latest patch

Name	Enter the FortiClient installer's name. In the example, the installer's name is FCT_603, to indicate that is used to deploy FortiClient 6.0.3.
Notes	Enter any notes about the FortiClient installer. This field is optional.
Version	Select the FortiClient version to install. The example is configured for FortiClient 6.0.
Patch version	Select the specific FortiClient patch version to install. The example is configured for FortiClient 6.0.3.
Keep updated to the latest patch	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint. This is optional and has not been enabled in this example.

4. Click *Next*. On the *Features* tab, you can select which features to include in the installer. In this example, only Security Fabric Agent has been enabled.



Basic Security Features

☑ Security Fabric Agent (Mandatory Feature)
Endpoint telemetry, host vulnerability scanning, and remediation.

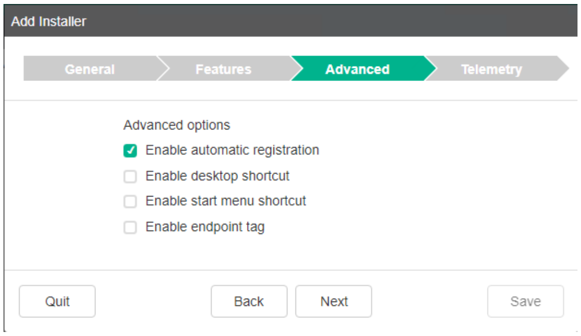
□ Secure Access Architecture Components
SSL and IPSec VPN

□ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features (Windows only)

Additional Security Features

□ AntiVirus
□ Web Filtering
□ Application Firewall
□ Single Sign-On mobility agent

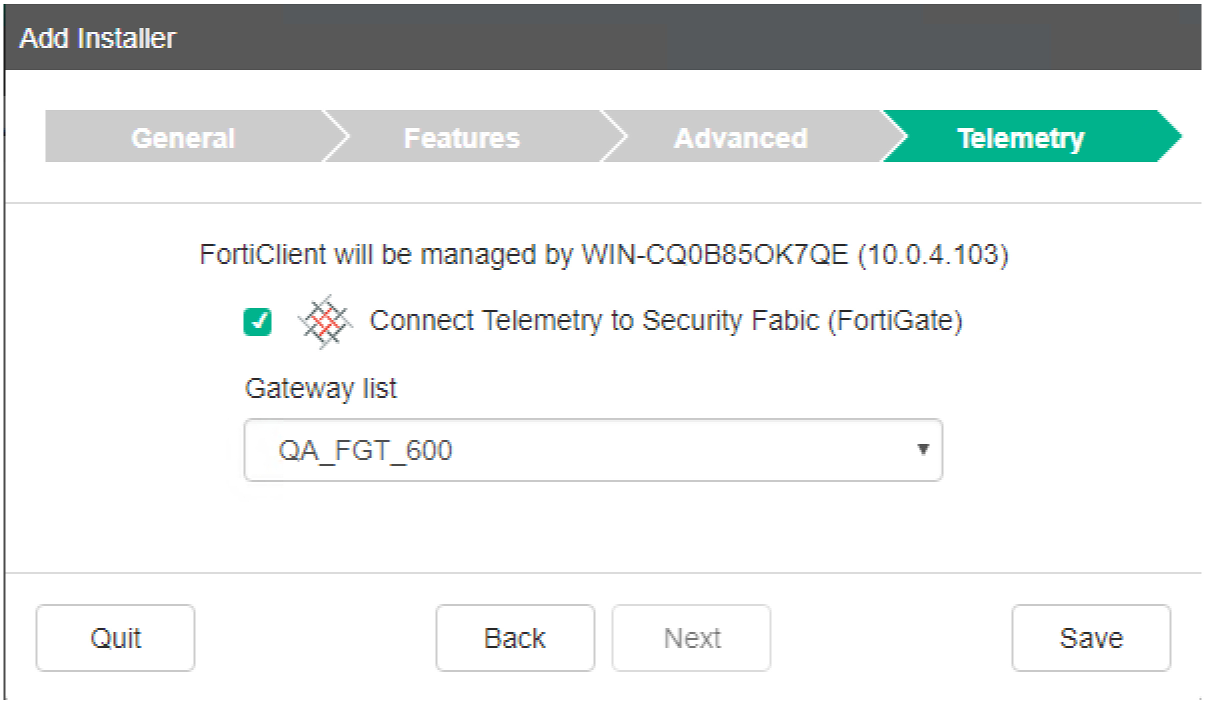
5. Click *Next*. On the *Advanced* tab, you can set additional options for the installer. In this example, only automatic registration is enabled for the installer. This allows FortiClient to automatically connect Telemetry to EMS or FortiGate after FortiClient is installed on the endpoint.



Advanced options

☑ Enable automatic registration
□ Enable desktop shortcut
□ Enable start menu shortcut
□ Enable endpoint tag

6. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the EMS server, which will manage FortiClient once it is installed on the endpoint. In the *Gateway list* dropdown list, select the gateway list created in Creating a gateway list on page 17. In this example, this is QA_FGT_600.



FortiClient will be managed by WIN-CQ0B85OK7QE (10.0.4.103)

☑ Connect Telemetry to Security Fabic (FortiGate)

Gateway list

QA_FGT_600 ▾

7. Click *Save*. The FortiClient installer is added to FortiClient EMS and displays on the *Manage Installers* pane.

For details on configuring other installer options, see the *FortiClient EMS Administration Guide*.

Creating a deployment profile

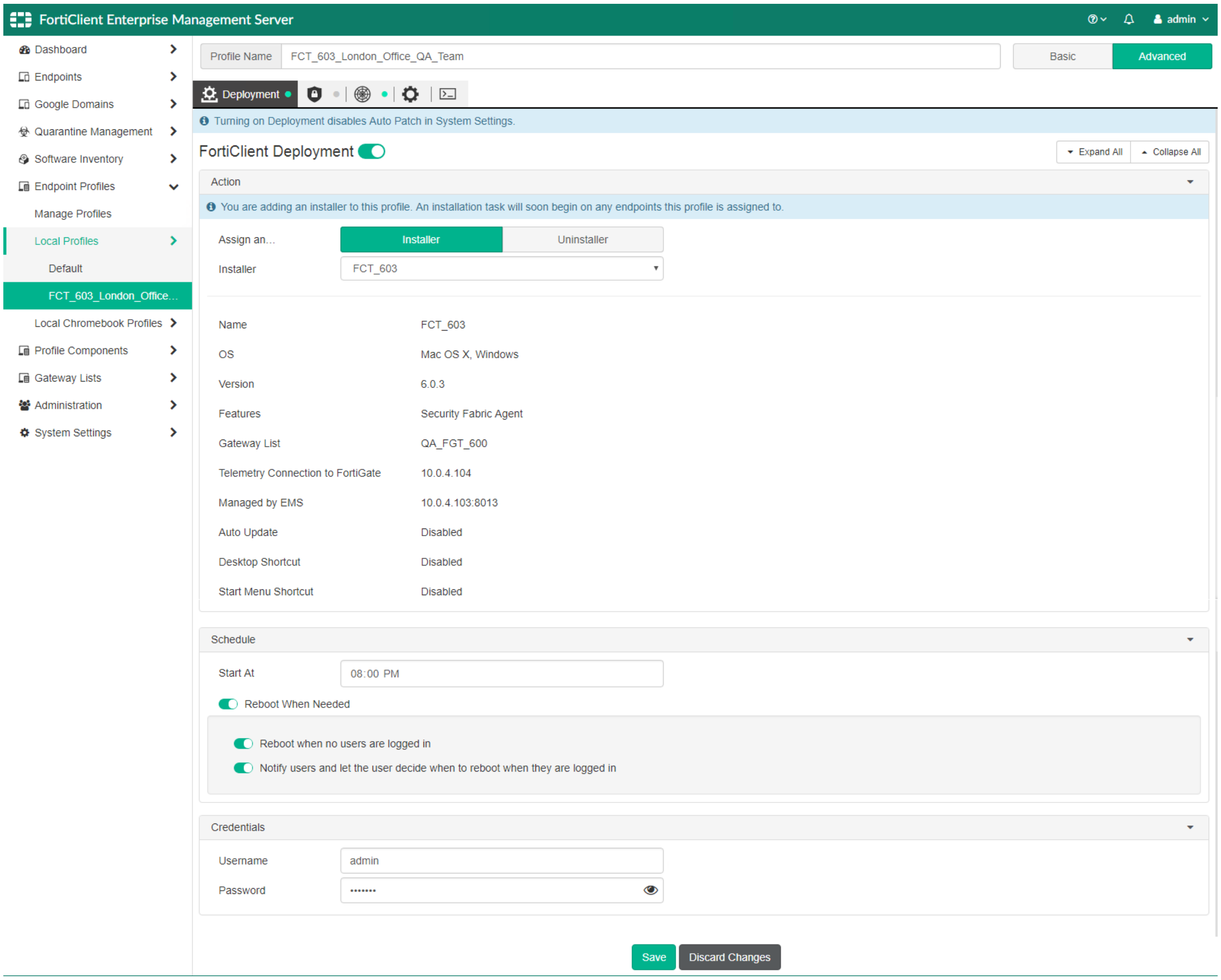
Next, you must create a new profile to deploy FortiClient to endpoints. You will assign the installer created in Creating a FortiClient installer on page 18 to the profile.

When creating a profile to deploy FortiClient, you must create a new profile. You cannot add an installer to the default profile.

1. Go to *Endpoint Profiles* > *Manage Profile*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.
3. Set the following options on the *Deployment* tab:

Action		
	Assign an	Click *Installer*.

	Installer	In the *Installer* list, select the FortiClient installer created in Creating a FortiClient installer on page 18. The installer options display.
Schedule		
	Start At	Specify what time to start installing FortiClient on endpoints. In this example, the time is configured for 8:00 PM.
	Reboot When Needed	Enable to reboot the endpoint to install FortiClient when needed.
	Reboot when no users is logged in	Enable to allow the endpoint to reboot without prompt if no endpoint user is logged into FortiClient.
	Notify users and let the user decide when to reboot when they are logged in	Enable to notify the end user if a reboot of the endpoint is needed and allow the user to decide what time to reboot the endpoint. Disable to reboot the endpoint without notifying the user.
Credentials		
	Username	Enter the username to perform deployment on AD. You must enter the admin credentials for the AD in the profile. Enter the appropriate credentials in the profile to assign to the AD. The credentials allow EMS to install FortiClient on endpoints using AD. If the credentials are wrong, the installation fails, and an error displays in EMS.
	Password	Enter the password to perform deployment on AD.



Profile Name: FCT_603_London_Office_QA_Team

Turning on Deployment disables Auto Patch in System Settings.

FortiClient Deployment (on)

Action

You are adding an installer to this profile. An installation task will soon begin on any endpoints this profile is assigned to.

Assign an...: Installer | Uninstaller

Installer: FCT_603

Name	FCT_603
OS	Mac OS X, Windows
Version	6.0.3
Features	Security Fabric Agent
Gateway List	QA_FGT_600
Telemetry Connection to FortiGate	10.0.4.104
Managed by EMS	10.0.4.103:8013
Auto Update	Disabled
Desktop Shortcut	Disabled
Start Menu Shortcut	Disabled

Schedule

Start At: 08:00 PM

Reboot When Needed (on)

Reboot when no users are logged in (on)

Notify users and let the user decide when to reboot when they are logged in (on)

Credentials

Username: admin

Password: •••••••

4. Set the options on the remaining tabs.
5. Click *Save*.

For information on additional profile configuration, see the *FortiClient EMS Administration Guide*.

Assigning the profile to endpoints

After creating the profile, you can assign the profile to the domain or a group within the domain. When you assign the profile to a domain or group, the profile settings are automatically pushed to all endpoints in the specified domain or group.

If you do not assign a profile to a specific domain or group, EMS automatically applies the default profile.

1. Go to *Endpoints*.
2. Right-click a domain or group, select *Assign profile*, then the profile. A confirmation dialog displays.

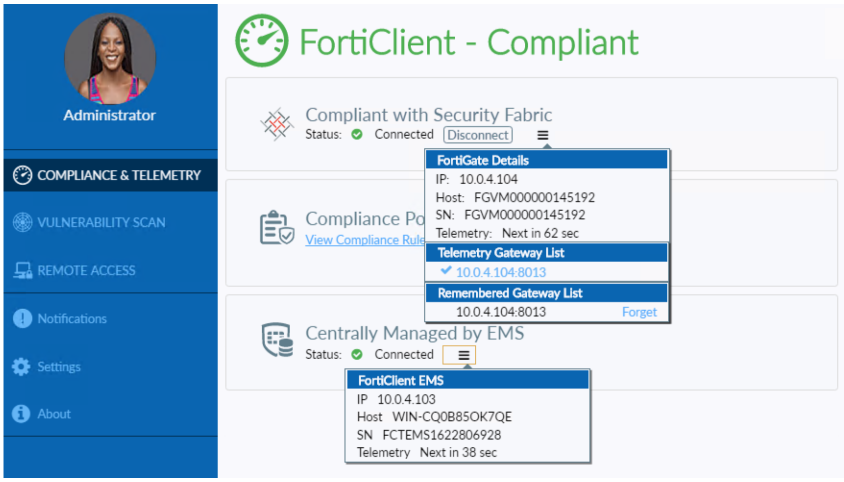
3. Click *Yes*. The profile is assigned.

Once the profile is assigned to a specified domain or group and the start time configured in Creating a FortiClient installer on page 18 is reached, EMS deploys FortiClient to the endpoints. The profile controls the endpoint's FortiClient configuration. FortiClient connects Telemetry to the FortiGate specified in the gateway list and the EMS server specified in the installer.

Verifying Telemetry connection

Now let's verify the Telemetry connection between FortiClient and EMS and between FortiClient and FortiGate in the FortiClient and EMS GUI.

The below shows the FortiClient GUI, which is now connected to both EMS and to the FortiGate at 10.0.4.104. Specifically, the screenshot below shows the *Compliance & Telemetry* tab, which displays the gateway list configured in Creating a gateway list on page 17. FortiClient is also centrally managed by EMS. Note that in this example, FortiClient is shown as compliant with the compliance rules received from FortiGate. For details on compliance, see the *FortiClient Compliance Guide*.



FortiClient - Compliant

Compliant with Security Fabric
Status: ✓ Connected

FortiGate Details
IP: 10.0.4.104
Host: FGVM000000145192
SN: FGVM000000145192
Telemetry: Next in 62 sec

Telemetry Gateway List
✓ 10.0.4.104:8013

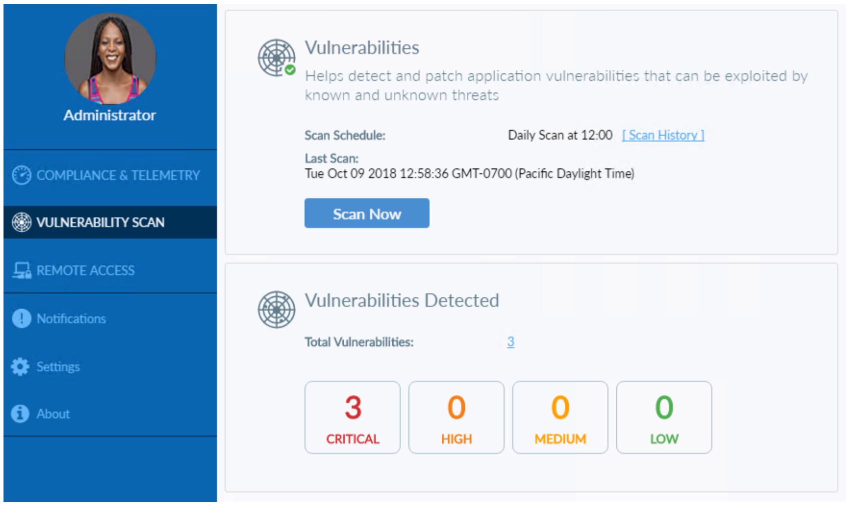
Remembered Gateway List
10.0.4.104:8013

Compliance Po

Centrally Managed by EMS
Status: ✓ Connected

FortiClient EMS
IP 10.0.4.103
Host WIN-CQ0B85OK7QE
SN FCTEMS1622806928
Telemetry Next in 38 sec

In addition to FortiClient Telemetry, SFA also includes Vulnerability Scan components. The below shows a screenshot of the *Vulnerability Scan* tab. The system was last scanned on Tuesday, October 9 at 12:58 and currently has three critical vulnerabilities.



Vulnerabilities

Helps detect and patch application vulnerabilities that can be exploited by known and unknown threats

Scan Schedule: Daily Scan at 12:00 [Scan History]

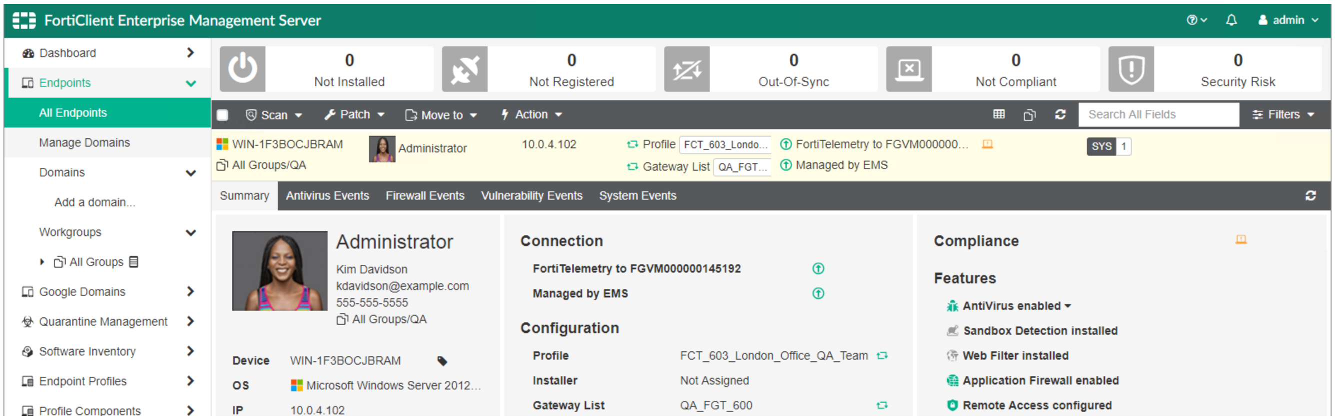
Last Scan:
Tue Oct 09 2018 12:58:36 GMT-0700 (Pacific Daylight Time)

Vulnerabilities Detected

Total Vulnerabilities: 3

3	0	0	0
CRITICAL	HIGH	MEDIUM	LOW

The below shows the EMS GUI when FortiClient is connected to both EMS and FortiGate. In the example, the endpoint is synchronized with the latest profile and gateway list configuration changes from EMS.



0	0	0	0	0
Not Installed	Not Registered	Out-Of-Sync	Not Compliant	Security Risk

WIN-1F3BOCJBRAM Administrator 10.0.4.102 Profile FCT_603_Londo... FortiTelemetry to FGVM000000... SYS 1
All Groups/QA Gateway List QA_FGT... Managed by EMS

Administrator

Kim Davidson
kdavidson@example.com
555-555-5555
All Groups/QA

Device	WIN-1F3BOCJBRAM
OS	Microsoft Windows Server 2012...
IP	10.0.4.102

Connection

FortiTelemetry to FGVM000000145192

Managed by EMS

Configuration

Profile	FCT_603_London_Office_QA_Team
Installer	Not Assigned
Gateway List	QA_FGT_600

Compliance

Features

- AntiVirus enabled
- Sandbox Detection installed
- Web Filter installed
- Application Firewall enabled
- Remote Access configured

Use Case: Enforcing Corporate Security Policies

You can use FortiClient EMS in integrated mode with FortiGate. In this scenario, EMS provides endpoint provisioning, while the FortiGate provides compliance rules to the endpoint. You can use the FortiGate to enforce corporate security policies by:

- Defining compliance rules for endpoint access to the network through FortiGate
- Defining the non-compliance action for FortiGate--that is, how FortiGate handles endpoints that fail to comply with compliance rules

This use case describes how to configure FortiClient compliance rules on FortiOS and shows an example of how non-compliant settings affect an endpoint. Consider the following topics:

1. Create set of compliance rules in FortiOS to send to FortiClient endpoints. See Configuring the FortiClient Compliance Profile in FortiOS on page 26.
2. View received compliance rules in FortiClient and fix non-compliant settings. See Fixing non-compliant settings on page 28.
3. View options available for the compliance rules in FortiOS. See Additional compliance options on page 30.

This use case assumes that FortiClient Telemetry is connected to both EMS and the FortiGate. For details on configuring the FortiClient Telemetry connections, see Use Case: FortiClient Software Management on page 4.

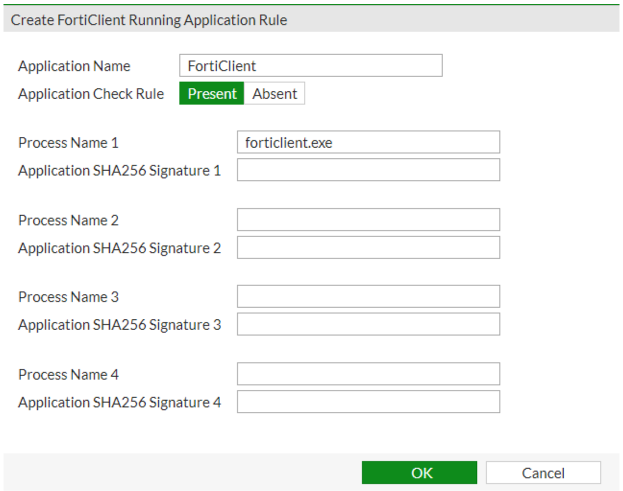
Configuring the FortiClient Compliance Profile in FortiOS

You will configure a FortiClient Compliance Profile in FortiOS. FortiGate provides these compliance rules to the endpoint. In this example, you will configure the profile to do the following:

- Block the endpoint from accessing the network if it has critical or high vulnerabilities
- Warn the endpoint if forticlient.exe is not running. The user can acknowledge and proceed past the warning to access the network.

1. In FortiOS, go to *Security Profiles > FortiClient Compliance*.
2. Create a new profile by selecting the + icon in the upper right corner.
3. In the *Profile Name* field, enter the desired profile name.
4. In the *Assign Profile To* field, select the desired device groups, user groups, and users to assign the profile to. In this example, we are assigning the profile to all Android phones and Windows PCs.
5. Configure the Vulnerability Scan compliance rule:
   a. Enable *Endpoint Vulnerability Scan on FortiClient*.
   b. From the *Vulnerability level* dropdown list, select *High*. This means the non-compliance action will apply to all endpoints with vulnerabilities detected as High or Critical (the only level greater than High).
   c. For the *Non-compliance action*, select *Block*.

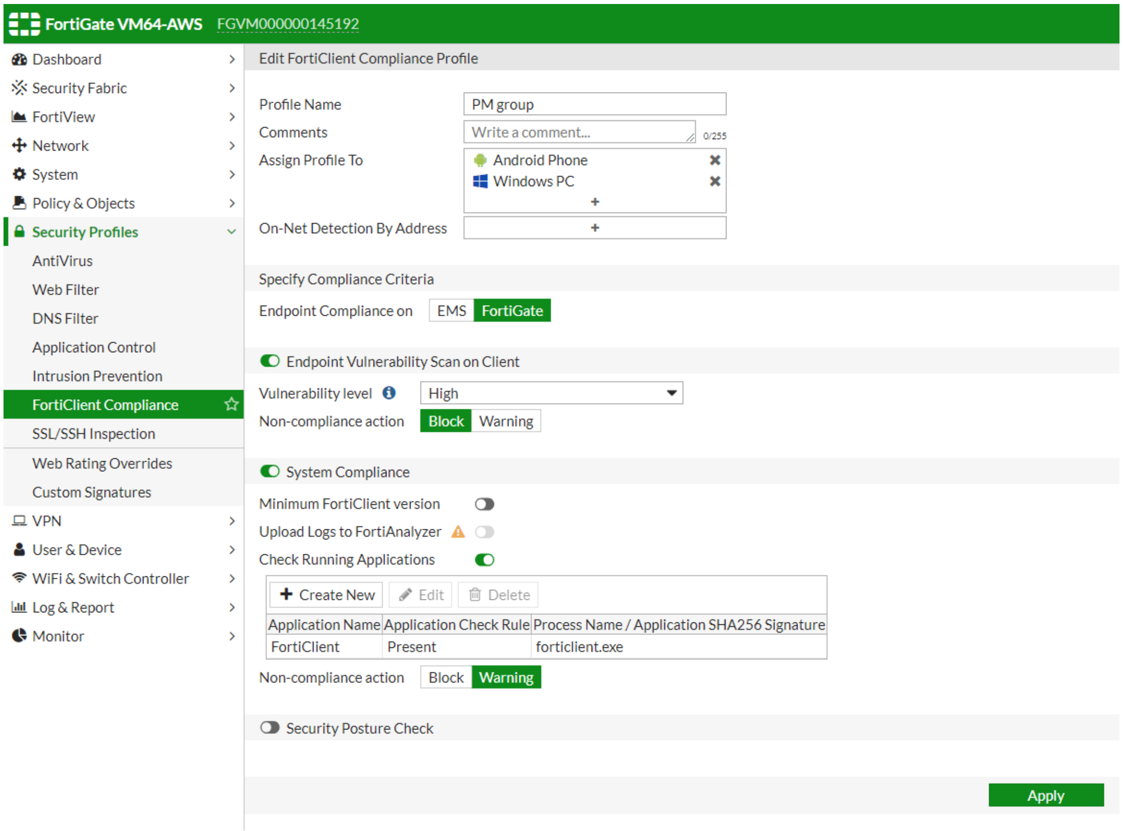
6. Configure the running application compliance rule:
   a. Enable *System Compliance*
   b. Enable *Check Running Applications*.
   c. Click *Create New*.
   d. In the *Application Name* field, enter *FortiClient*.
   e. Ensure that *Application Check Rule* is set to *Present*.
   f. In the *Process Name 1* field, enter *forticlient.exe*.
   g. Click *OK*.



Create FortiClient Running Application Rule

Application Name	FortiClient
Application Check Rule	[✓ Present] Absent
Process Name 1	forticlient.exe
Application SHA256 Signature 1	
Process Name 2	
Application SHA256 Signature 2	
Process Name 3	
Application SHA256 Signature 3	
Process Name 4	
Application SHA256 Signature 4	

7. Click *Apply*.



Edit FortiClient Compliance Profile

Profile Name	PM group
Comments	Write a comment... 0/255
Assign Profile To	Android Phone Windows PC
On-Net Detection By Address	+

Specify Compliance Criteria

Endpoint Compliance on: EMS [✓ FortiGate]

● Endpoint Vulnerability Scan on Client

Vulnerability level: High

Non-compliance action: [✓ Block] Warning

● System Compliance

Minimum FortiClient version ○

Upload Logs to FortiAnalyzer ○

Check Running Applications ●

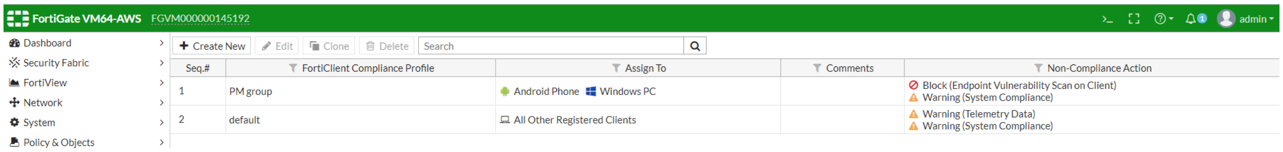
Create New | Edit | Delete

Application Name	Application Check Rule	Process Name / Application SHA256 Signature
FortiClient	Present	forticlient.exe

Non-compliance action: Block [✓ Warning]

○ Security Posture Check

The compliance rule has been created. You can view it in *Security Profiles > FortiClient Compliance*.



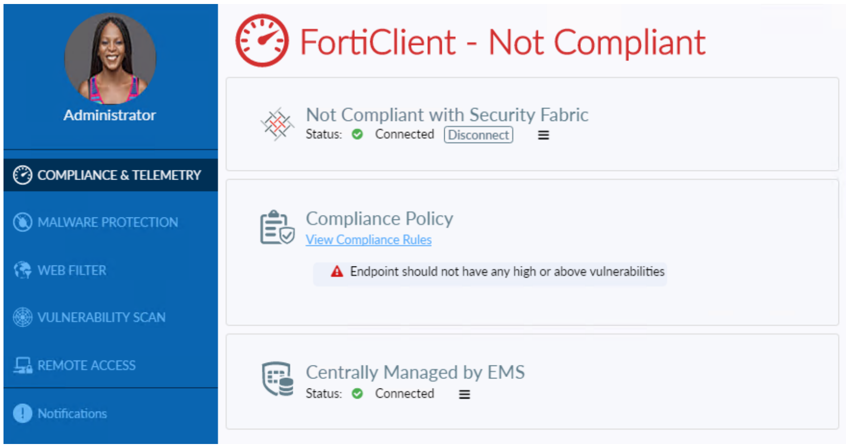
Seq.#	FortiClient Compliance Profile	Assign To	Comments	Non-Compliance Action
1	PM group	Android Phone Windows PC		Block (Endpoint Vulnerability Scan on Client) Warning (System Compliance)
2	default	All Other Registered Clients		Warning (Telemetry Data) Warning (System Compliance)

Fixing non-compliant settings

Now you can go to FortiClient on the endpoint to see the effect of the newly configured compliance rules on the endpoint. The compliance rules take effect with the next Telemetry communication between FortiClient and the FortiGate.

First, let's see the effect of the Vulnerability Scan compliance rule: endpoints must not have any high or critical vulnerabilities. Otherwise, they will be blocked from accessing the network. The example endpoint currently has two critical vulnerabilities, which violates this rule.

In the screenshot, you can see that FortiClient is not compliant with the Security Fabric. In the *Compliance Policy* section, FortiClient also displays the compliance rule it is currently in violation of: the endpoint should not have any high or above vulnerabilities.



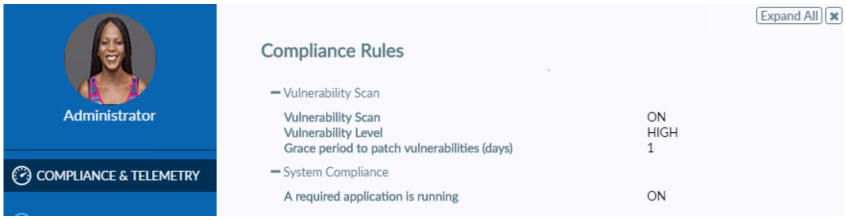
FortiClient - Not Compliant

Not Compliant with Security Fabric
Status: Connected

Compliance Policy
Endpoint should not have any high or above vulnerabilities

Centrally Managed by EMS
Status: Connected

Click *View Compliance Rules* to see more detail about the compliance rules received from FortiGate. This displays all compliance rules, including those that FortiClient is currently compliant with. For the Vulnerability Scan compliance rule, there is a grace period of one day, during which the user is expected to patch the critical and high vulnerabilities. During the grace period, the endpoint is not yet blocked from the network.



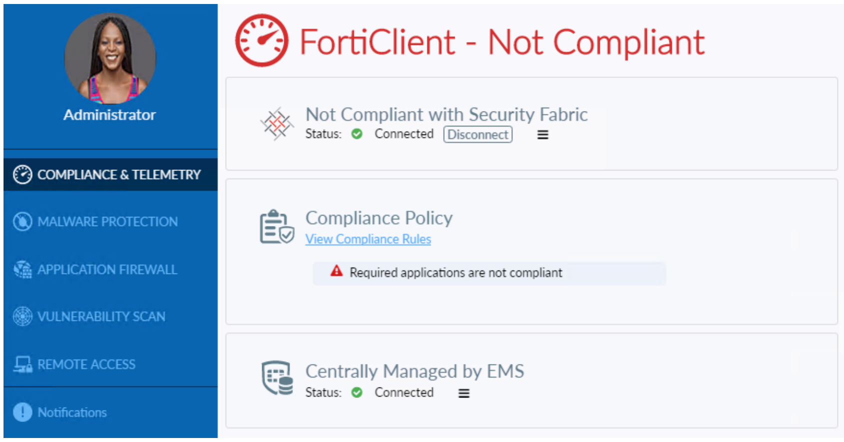
Compliance Rules

− Vulnerability Scan	
Vulnerability Scan	ON
Vulnerability Level	HIGH
Grace period to patch vulnerabilities (days)	1
− System Compliance	
A required application is running	ON

If the grace period passes and the critical and high vulnerabilities have not been patched, the endpoint user is blocked from accessing the network.

For the sake of the example, let's patch the critical and high vulnerabilities on the endpoint. Follow the instructions in Patching endpoint vulnerabilities using EMS. After patching the vulnerabilities, the endpoint is compliant and can access the network.

Now let's consider what happens if the endpoint does not follow the second compliance rule, which is that forticlient.exe must be running. When forticlient.exe is not running on the endpoint, FortiClient displays the following.



FortiClient - Not Compliant

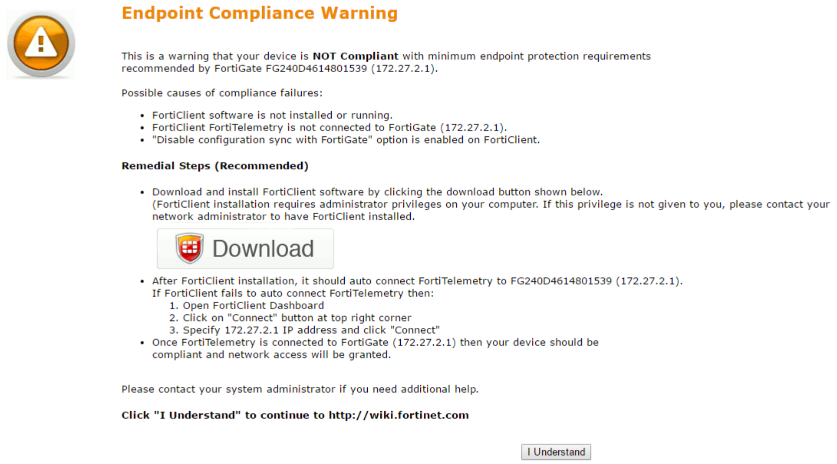
Not Compliant with Security Fabric
Status: Connected

Compliance Policy

Required applications are not compliant

Centrally Managed by EMS
Status: Connected

Since this rule was configured to only warn the user in the case of non-compliance, the user can still access the network without fixing the non-compliant settings. The browser displays the following warning, and the user can click *I Understand* to acknowledge the compliance issue, then proceed. The user can fix the non-compliant settings at a later time.



Endpoint Compliance Warning

This is a warning that your device is **NOT Compliant** with minimum endpoint protection requirements recommended by FortiGate FG240D4614801539 (172.27.2.1).

Possible causes of compliance failures:

- FortiClient software is not installed or running.
- FortiClient FortiTelemetry is not connected to FortiGate (172.27.2.1).
- "Disable configuration sync with FortiGate" option is enabled on FortiClient.

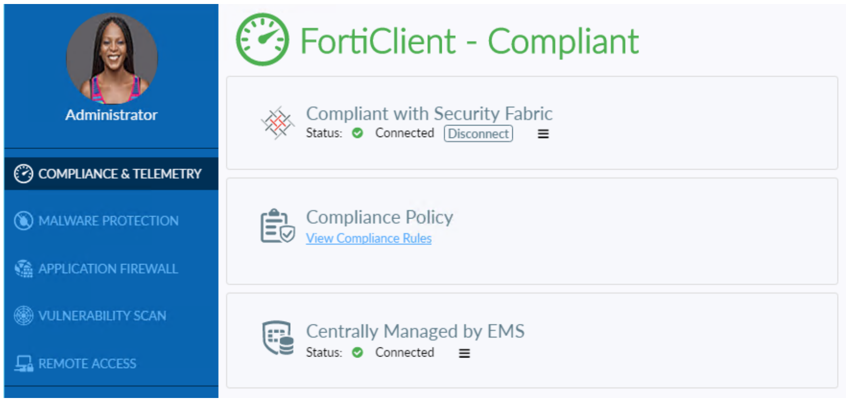
Remedial Steps (Recommended)

- Download and install FortiClient software by clicking the download button shown below. (FortiClient installation requires administrator privileges on your computer. If this privilege is not given to you, please contact your network administrator to have FortiClient installed.
- After FortiClient installation, it should auto connect FortiTelemetry to FG240D4614801539 (172.27.2.1). If FortiClient fails to auto connect FortiTelemetry then:
    1. Open FortiClient Dashboard
    2. Click on "Connect" button at top right corner
    3. Specify 172.27.2.1 IP address and click "Connect"
- Once FortiTelemetry is connected to FortiGate (172.27.2.1) then your device should be compliant and network access will be granted.

Please contact your system administrator if you need additional help.

Click "I Understand" to continue to http://wiki.fortinet.com

When the endpoint is compliant with all compliance rules received from the FortiGate, the FortiClient *Compliance & Telemetry* tab displays the following.



FortiClient - Compliant

Compliant with Security Fabric
Status: Connected

Compliance Policy

Centrally Managed by EMS
Status: Connected

Additional compliance options

Depending on the FortiOS configuration, FortiOS uses one of the following methods to determine endpoint compliance. The first option is only available in FortiOS 6.0.0 and later versions. In both cases, FortiClient must be installed on the endpoint and there must be Telemetry connection between FortiClient and FortiGate.

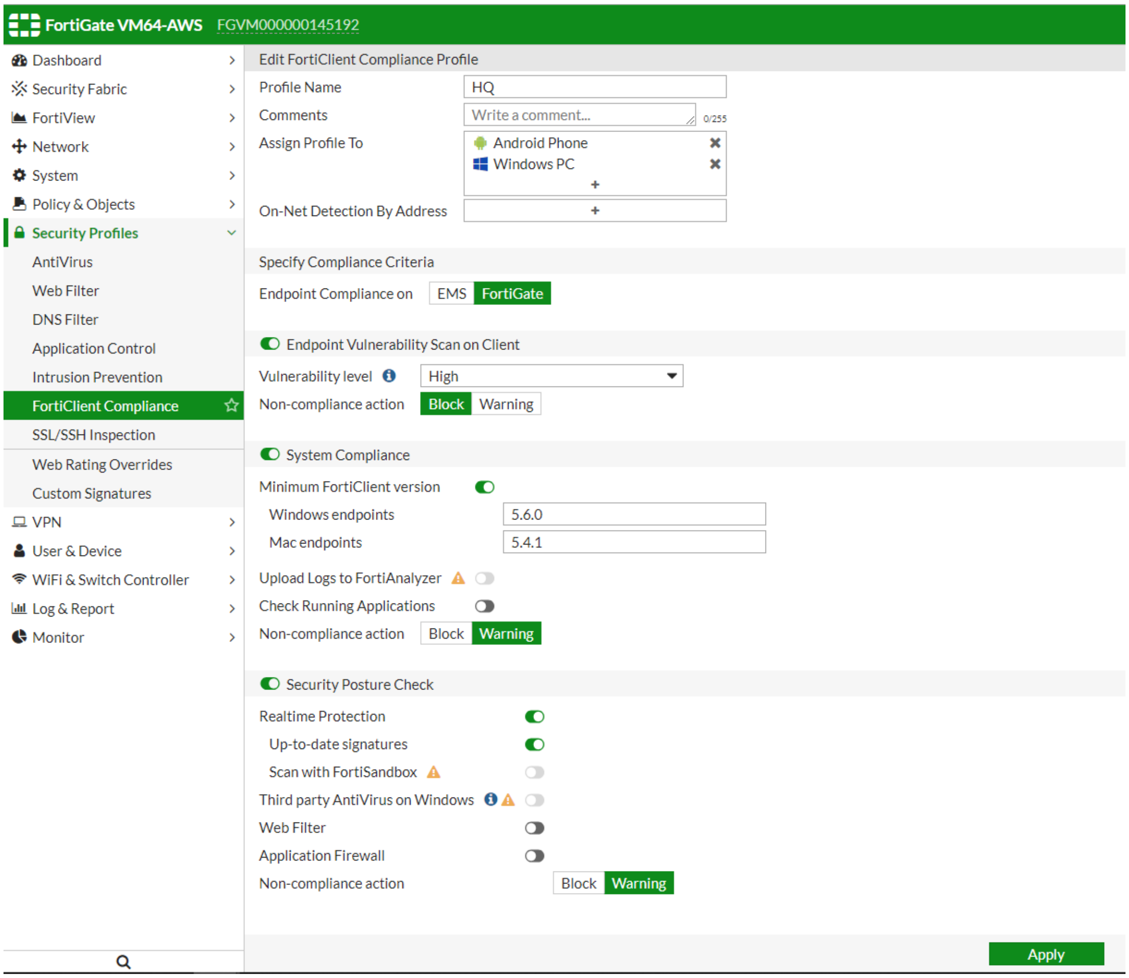
1. An endpoint is considered compliant if its FortiClient is managed by the EMS server authorized in FortiOS.
2. An endpoint is considered compliant if it complies with the specific compliance rules configured in FortiOS. The table below lists the compliance rules administrators can enable or disable in a FortiClient profile.

Option	Description
Endpoint Vulnerability Scan on Client	Endpoints must not have vulnerabilities at or higher than the configured level.
System Compliance	
Minimum FortiClient version	Endpoints must have a FortiClient version installed that is the same or higher than configured. You can set different versions for different operating systems.
Upload Logs to FortiAnalyzer	Endpoints must send the specified logs to FortiAnalyzer. FortiClient must have logging to FortiAnalyzer configured to enable this option.
Check Running Applications	Configure rules for certain applications. You can create a rule for a specific application to be running or not running, and also specify processes and signatures.
Security Posture Check	
Realtime Protection	You can specify that endpoints must have: • Realtime Protection enabled • Signatures must be up-to-date • FortiSandbox scanning must be enabled. FortiClient must have FortiSandbox integration configured to enable this option.

Option		Description
	Third party AntiVirus on Windows	Endpoints must run a specified third party antivirus program.
	Web Filter	Endpoints must have the specified Web Filter profile applied.
	Application Firewall	Endpoints must have the specified Application Control sensor applied.

The below shows another example of a FortiClient compliance profile. The profile is configured as follows:

- Block endpoints with high or critical vulnerabilities from accessing the network
- Warn Windows endpoints that have a FortiClient version earlier than 5.6.0
- Warn endpoints that do not have real-time protection enabled
- Warn endpoints that do not have up-to-date signatures



Edit FortiClient Compliance Profile

Profile Name: HQ

Comments: Write a comment... 0/255

Assign Profile To: Android Phone, Windows PC

On-Net Detection By Address

Specify Compliance Criteria

Endpoint Compliance on: EMS [✓ FortiGate]

Endpoint Vulnerability Scan on Client: ●

Vulnerability level: High

Non-compliance action: [✓ Block] Warning

System Compliance: ●

Minimum FortiClient version: ●

Windows endpoints: 5.6.0

Mac endpoints: 5.4.1

Upload Logs to FortiAnalyzer: ○

Check Running Applications: ○

Non-compliance action: Block [✓ Warning]

Security Posture Check: ●

Realtime Protection: ●

Up-to-date signatures: ●

Scan with FortiSandbox: ○

Third party AntiVirus on Windows: ○

Web Filter: ○

Application Firewall: ○

Non-compliance action: Block [✓ Warning]

Use Case: Migrating EMS to a New Server

To enjoy the latest enhancements to EMS, you must ensure that you are using the latest version of EMS. This procedure describes the process of migrating a production environment from one server to another server.

For this use case, the following is assumed:

- You have full access to the following infrastructure:
  - Current EMS production server (referred to as "Server A")
  - A second server with similar capabilities as the EMS production server (referred to as "Server B")
  - FortiClient endpoints available for testing purposes
- There is network connectivity between the infrastructure components listed above.
- You have configured EMS according to the *FortiClient EMS Administration Guide*.
- Endpoints have FortiClient installed and are currently being managed by Server A.

This use case describes the process of migrating an EMS 6.0.3 production server environment from Server A to Server B. In this example, Server A's IP address is 10.200.200.11, and Server B's IP address is 10.200.200.15. The domain name is ems.example.com.

The procedure is as follows:

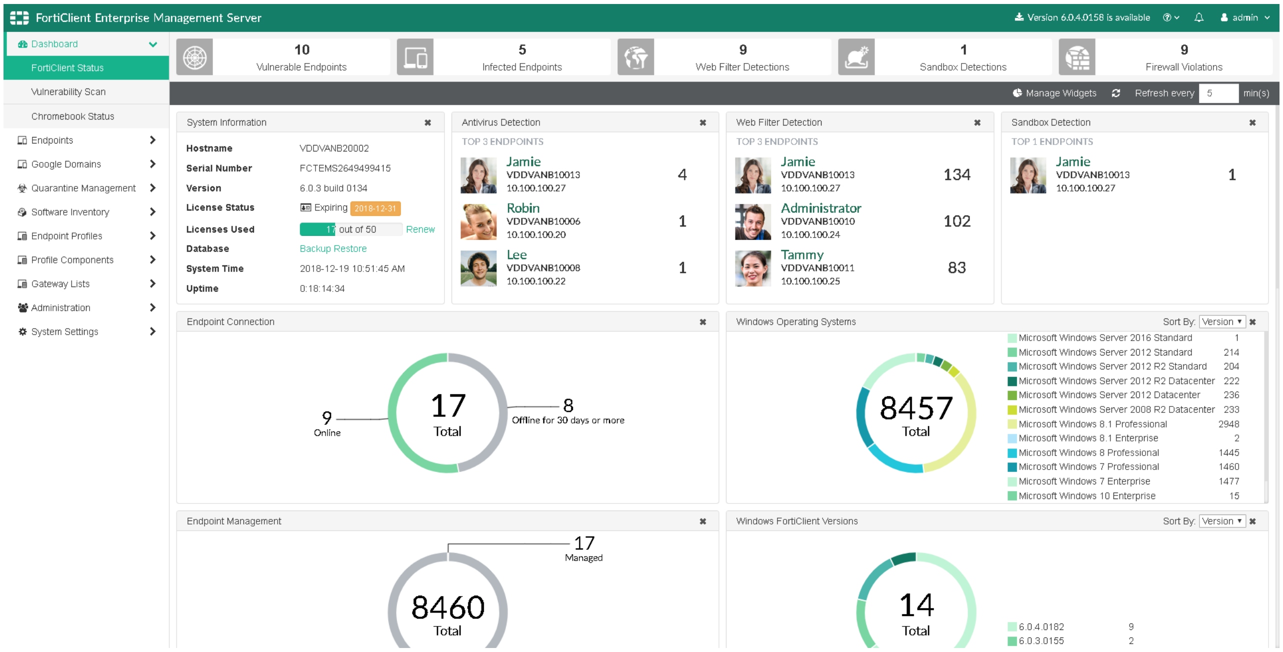
1. Ensure that the prerequisites are met. See Checking the prerequisites on page 32.
2. Install EMS on Server B. See Installing EMS on Server B on page 34.
3. Back up the EMS database from Server A, then restore the database on Server B. Change the configuration as required on Server B. See Backing up and restoring the database on page 34.
4. (Optional) Modify the hosts file on test endpoints so that they connect to Server B. Confirm that Server B is managing the endpoints. See Modifying endpoint hosts files on page 35.
5. Contact Fortinet Customer Service & Support to migrate the EMS license to Server B. See Migrating the EMS license to Server B on page 37.
6. Change the DNS record to redirect all endpoints to Server B. See Changing the DNS record on page 37.
7. Ensure that all endpoints are connected to Server B. See Connecting endpoints to Server B on page 38.

Checking the prerequisites

Ensure that the following prerequisites are met on the EMS servers and on the FortiClient endpoints before proceeding to migrate the EMS server.

EMS servers A and B

- Server A is fully configured and ready to back up its database.



FortiClient Enterprise Management Server

Version 6.0.4.0158 is available · admin

Dashboard
- FortiClient Status
- Vulnerability Scan
- Chromebook Status

Endpoints · Google Domains · Quarantine Management · Software Inventory · Endpoint Profiles · Profile Components · Gateway Lists · Administration · System Settings

10 Vulnerable Endpoints · 5 Infected Endpoints · 9 Web Filter Detections · 1 Sandbox Detections · 9 Firewall Violations

Manage Widgets · Refresh every 5 min(s)

System Information

Hostname	VDDVANB20002
Serial Number	FCTEMS2649499415
Version	6.0.3 build 0134
License Status	Expiring 2018-12-31
Licenses Used	17 out of 50 Renew
Database	Backup Restore
System Time	2018-12-19 10:51:45 AM
Uptime	0:18:14:34

Antivirus Detection – TOP 3 ENDPOINTS

User	Endpoint	IP	Count
Jamie	VDDVANB10013	10.100.100.27	4
Robin	VDDVANB10006	10.100.100.20	1
Lee	VDDVANB10008	10.100.100.22	1

Web Filter Detection – TOP 3 ENDPOINTS

User	Endpoint	IP	Count
Jamie	VDDVANB10013	10.100.100.27	134
Administrator	VDDVANB10010	10.100.100.24	102
Tammy	VDDVANB10011	10.100.100.25	83

Sandbox Detection – TOP 1 ENDPOINTS

User	Endpoint	IP	Count
Jamie	VDDVANB10013	10.100.100.27	1

Endpoint Connection

Windows Operating Systems – Sort By: Version

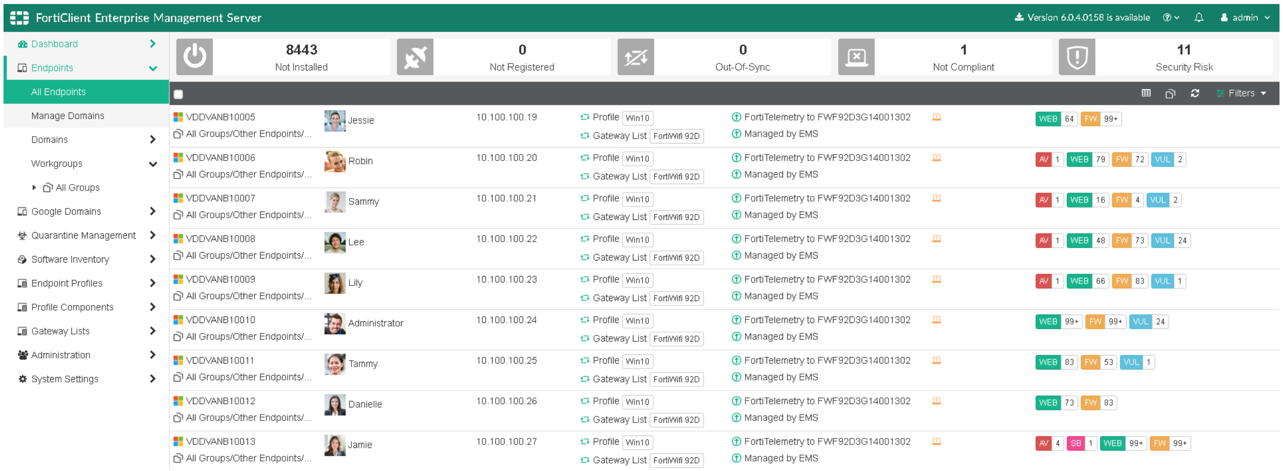
Operating system	Count
Microsoft Windows Server 2016 Standard	1
Microsoft Windows Server 2012 Standard	214
Microsoft Windows Server 2012 R2 Standard	204
Microsoft Windows Server 2012 R2 Datacenter	222
Microsoft Windows Server 2012 Datacenter	236
Microsoft Windows Server 2008 R2 Datacenter	233
Microsoft Windows 8.1 Professional	2948
Microsoft Windows 8.1 Enterprise	2
Microsoft Windows 8 Professional	1445
Microsoft Windows 7 Professional	1460
Microsoft Windows 7 Enterprise	1477
Microsoft Windows 10 Enterprise	15

Endpoint Management

Windows FortiClient Versions – Sort By: Version

Version	Count
6.0.4.0182	9
6.0.3.0155	2

- Server A is currently managing the endpoints that need to be migrated to Server B. Telemetry is functioning normally.



FortiClient Enterprise Management Server

Version 6.0.4.0158 is available · admin

Dashboard · Endpoints
- All Endpoints
- Manage Domains
- Domains
- Workgroups
  - All Groups

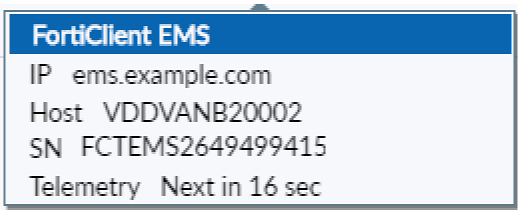
Google Domains · Quarantine Management · Software Inventory · Endpoint Profiles · Profile Components · Gateway Lists · Administration · System Settings

8443 Not Installed · 0 Not Registered · 0 Out-Of-Sync · 1 Not Compliant · 11 Security Risk

Filters

VDDVANB10005 All Groups/Other Endpoints/...	Jessie	10.100.100.19	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G14001302 Managed by EMS	WEB 64 FW 99+
VDDVANB10006 All Groups/Other Endpoints/...	Robin	10.100.100.20	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G14001302 Managed by EMS	AV 1 WEB 79 FW 72 VUL 2
VDDVANB10007 All Groups/Other Endpoints/...	Sammy	10.100.100.21	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G14001302 Managed by EMS	AV 1 WEB 16 FW 4 VUL 2
VDDVANB10008 All Groups/Other Endpoints/...	Lee	10.100.100.22	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G14001302 Managed by EMS	AV 1 WEB 48 FW 73 VUL 24
VDDVANB10009 All Groups/Other Endpoints/...	Lily	10.100.100.23	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G14001302 Managed by EMS	AV 1 WEB 66 FW 83 VUL 1
VDDVANB10010 All Groups/Other Endpoints/...	Administrator	10.100.100.24	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G14001302 Managed by EMS	WEB 99+ FW 99+ VUL 24
VDDVANB10011 All Groups/Other Endpoints/...	Tammy	10.100.100.25	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G14001302 Managed by EMS	WEB 83 FW 53 VUL 1
VDDVANB10012 All Groups/Other Endpoints/...	Danielle	10.100.100.26	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G14001302 Managed by EMS	WEB 73 FW 83
VDDVANB10013 All Groups/Other Endpoints/...	Jamie	10.100.100.27	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G14001302 Managed by EMS	AV 4 SB 1 WEB 99+ FW 99+

- The connection between the Server A and the endpoint has been configured by domain name and not by the EMS server IP address.



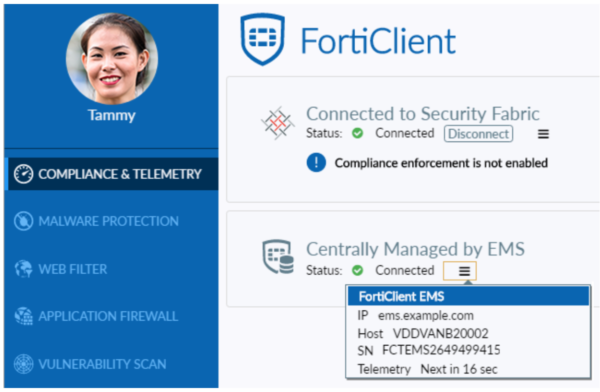
FortiClient EMS

IP	ems.example.com
Host	VDDVANB20002
SN	FCTEMS2649499415
Telemetry	Next in 16 sec

- Server B is ready for further configuration.

FortiClient endpoints

On all desired endpoints, ensure that FortiClient is installed and is being managed by EMS on Server A.



Connected to Security Fabric
Status: Connected Disconnect
Compliance enforcement is not enabled

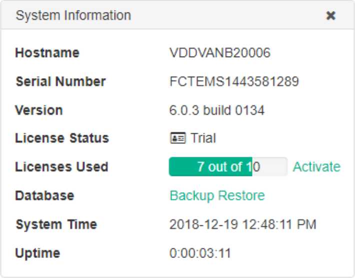
Centrally Managed by EMS
Status: Connected

FortiClient EMS
IP ems.example.com
Host VDDVANB20002
SN FCTEMS2649499415
Telemetry Next in 16 sec

Installing EMS on Server B

Install the same version of EMS that is installed on Server A on Server B. In this example, Server A has EMS 6.0.3 installed. Therefore, you would install EMS 6.0.3 on Server B. For details on how to install EMS, see Installing FortiClient EMS.

When you install EMS on Server B, the free trial license is enabled by default. Keep this trial license for now. You will apply the full license to this server in Migrating the EMS license to Server B on page 37.


System Information

Hostname	VDDVANB20006
Serial Number	FCTEMS1443581289
Version	6.0.3 build 0134
License Status	Trial
Licenses Used	7 out of 10 Activate
Database	Backup Restore
System Time	2018-12-19 12:48:11 PM
Uptime	0:00:03:11

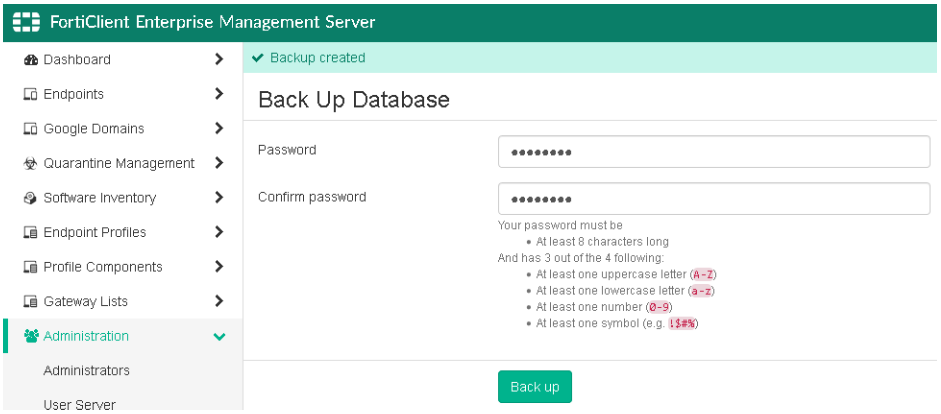
Backing up and restoring the database

You must back up the EMS database from Server A, then restore the database on Server B.

1. Back up the database on Server A:
   a. On Server A, go to *Administration* > *Back up Database*.
   b. Set the following options:

Password	Enter a password for backing up and restoring the database.
Confirm password	Reenter the password to confirm it.

c. Click *Back up*. FortiClient EMS backs up the database.



✓ Backup created

Back Up Database

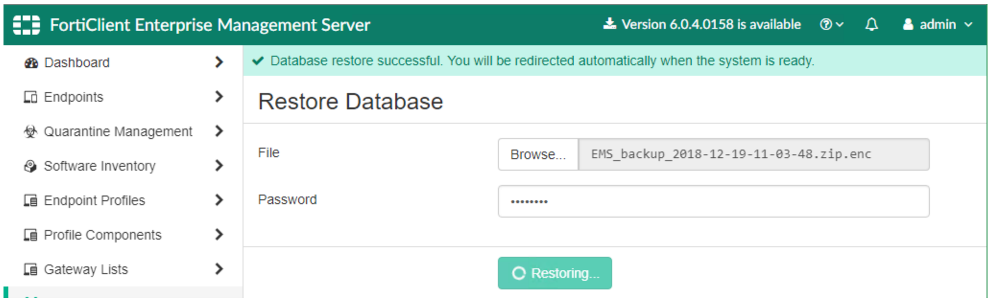
Password ••••••••

Confirm password ••••••••

Your password must be
- At least 8 characters long

And has 3 out of the 4 following:
- At least one uppercase letter (A-Z)
- At least one lowercase letter (a-z)
- At least one number (0-9)
- At least one symbol (e.g. !$#%)

2. Restore the database on Server B:
   a. On Server B, go to *Administration* > *Restore Database*.
   b. Click *Browse*.
   c. Locate the database backup file from Server A, and click *Open*.
   d. In the *Password* box, enter the password used to back up the database.
   e. Click *Restore*. When the database is restored, a message appears. The message instructs you to wait for the restored database to reload.



✓ Database restore successful. You will be redirected automatically when the system is ready.

Restore Database

File EMS_backup_2018-12-19-11-03-48.zip.enc

Password ••••••••

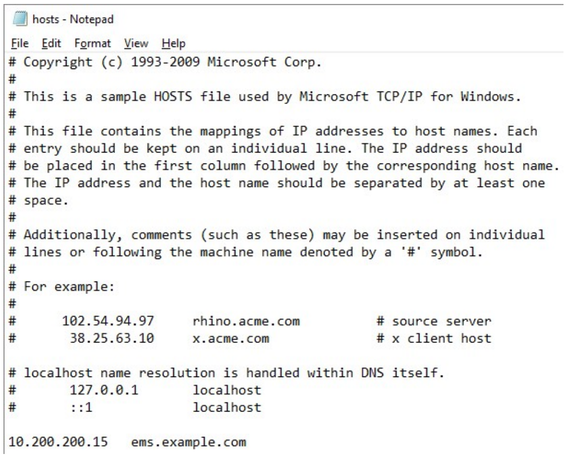
3. Wait for the restored database to be reloaded.
4. Change the configuration as required. For example, you may need to adjust the *Hostname* and *Listen on IP settings* under *System Settings* > *Server*, and verify the Sandbox connection under endpoint profiles.
5. Verify that settings, workgroups, domains, profiles, and so on were loaded correctly after restoring Server A's database on Server B.

Modifying endpoint hosts files

You can modify the hosts file on some test endpoints so that they connect to Server B, then confirm that the endpoints are being managed by Server B. This step is optional.

1. On a test FortiClient endpoint, go to *C:\Windows\System32\drivers\etc* and open the *hosts* file using Notepad as an administrator.

2. At the end of the hosts file, add Server B's IP address and the configured domain name as shown.

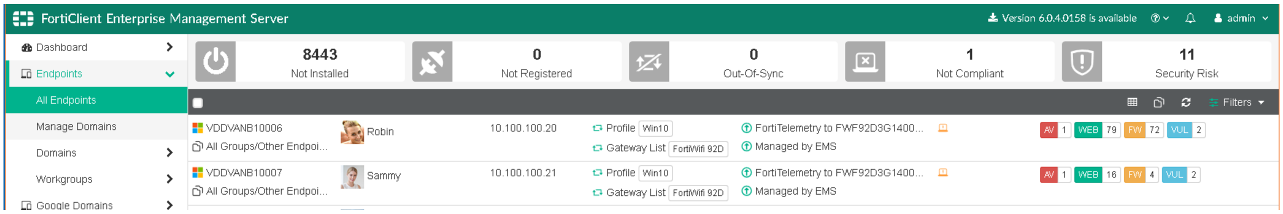


```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

10.200.200.15   ems.example.com
```

3. Save and close the hosts file.
4. Repeat steps 1-3 on additional test endpoints as desired.
5. On Server B, confirm that the test endpoints have connected Telemetry to EMS.

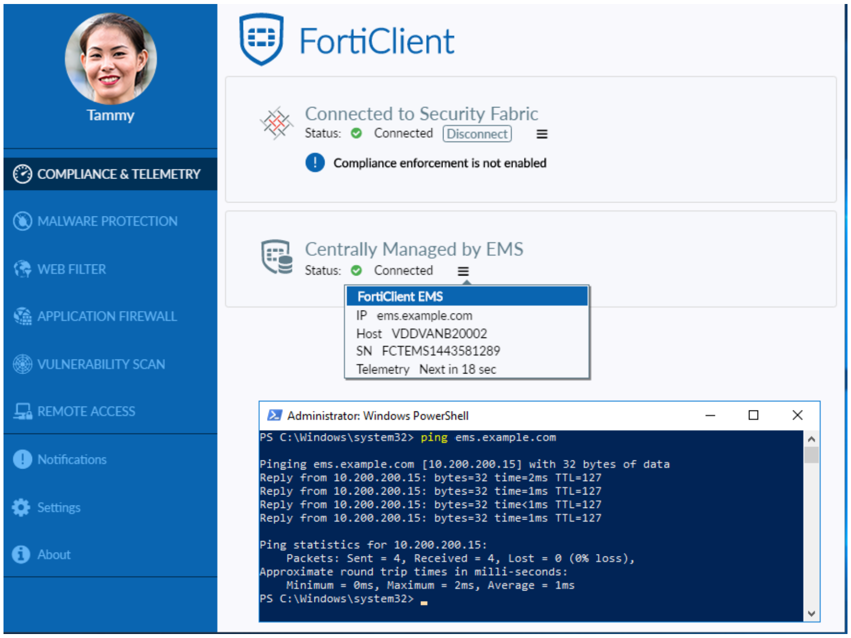


8443 Not Installed | 0 Not Registered | 0 Out-Of-Sync | 1 Not Compliant | 11 Security Risk

VDDVANB10006 — All Groups/Other Endpoi... — Robin — 10.100.100.20 — Profile Win10 — Gateway List FortiWifi 92D — FortiTelemetry to FWF92D3G1400... — Managed by EMS — AV 1 WEB 79 FW 72 VUL 2

VDDVANB10007 — All Groups/Other Endpoi... — Sammy — 10.100.100.21 — Profile Win10 — Gateway List FortiWifi 92D — FortiTelemetry to FWF92D3G1400... — Managed by EMS — AV 1 WEB 16 FW 4 VUL 2

6. On the test endpoints, confirm that a Telemetry connection has been established to EMS on Server B using the domain name.



Connected to Security Fabric
Status: Connected

Compliance enforcement is not enabled

Centrally Managed by EMS
Status: Connected

FortiClient EMS
IP ems.example.com
Host VDDVANB20002
SN FCTEMS1443581289
Telemetry Next in 18 sec

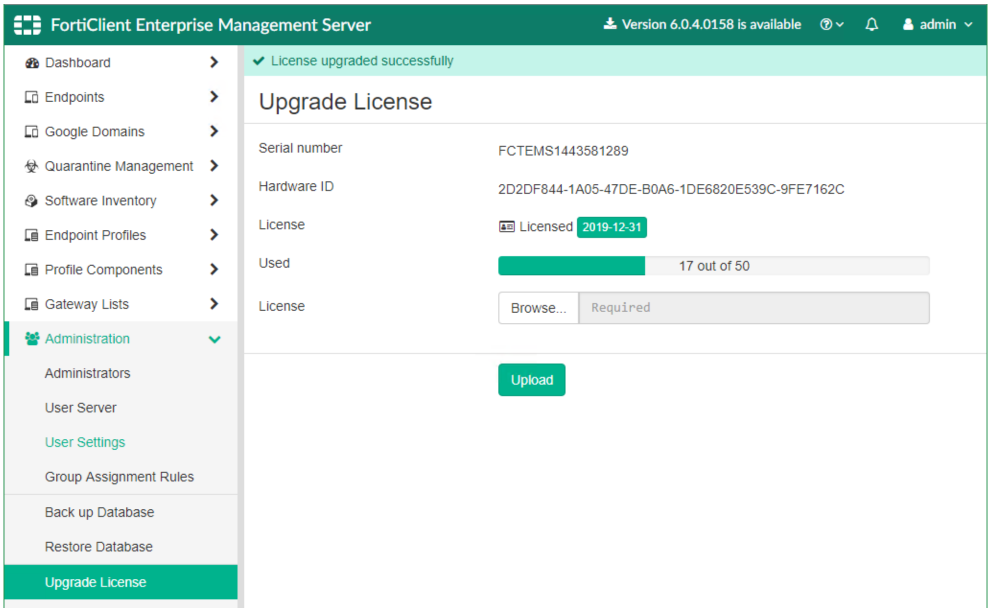
```
PS C:\Windows\system32> ping ems.example.com

Pinging ems.example.com [10.200.200.15] with 32 bytes of data
Reply from 10.200.200.15: bytes=32 time=2ms TTL=127
Reply from 10.200.200.15: bytes=32 time=1ms TTL=127
Reply from 10.200.200.15: bytes=32 time<1ms TTL=127
Reply from 10.200.200.15: bytes=32 time=1ms TTL=127

Ping statistics for 10.200.200.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
PS C:\Windows\system32>
```

Migrating the EMS license to Server B

1. Contact Fortinet Customer Service & Support for assistance in migrating the EMS license.
2. On Server B, go to *Administration* > *Upgrade License* .
3. Click *Browse* and locate the license key file.
4. Click *Upload*.



✓ License upgraded successfully

Upgrade License

Serial number FCTEMS1443581289

Hardware ID 2D2DF844-1A05-47DE-B0A6-1DE6820E539C-9FE7162C

License Licensed 2019-12-31

Used 17 out of 50

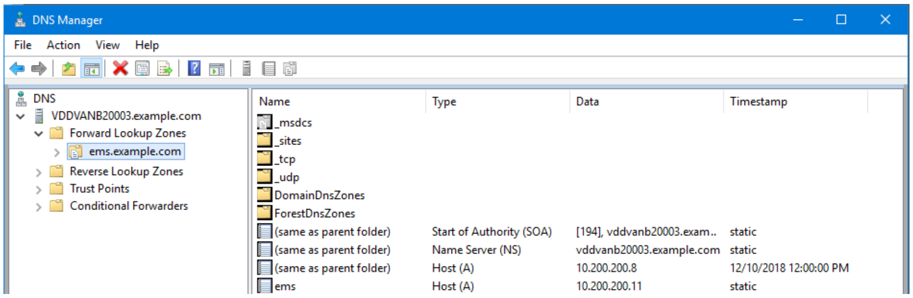
License Required

Changing the DNS record

You must change the EMS DNS record on the enterprise DNS server to redirect all endpoints to Server B.

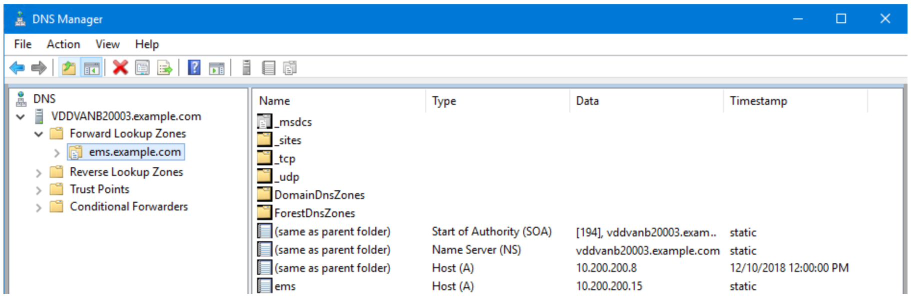
If you encounter any issues during the migration process, return to this step and roll back the EMS DNS record to redirect to Server A, as originally configured.

1. On the enterprise DNS server, open DNS Manager.
2. Under *Forward Lookup Zones*, find the EMS record. The EMS record's *Data* column is populated with Server A's IP address.



Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[194], vddvanb20003.exam..	static
(same as parent folder)	Name Server (NS)	vddvanb20003.example.com	static
(same as parent folder)	Host (A)	10.200.200.8	12/10/2018 12:00:00 PM
ems	Host (A)	10.200.200.11	static

3. Modify the EMS record's *Data* column to point to Server B's IP address.

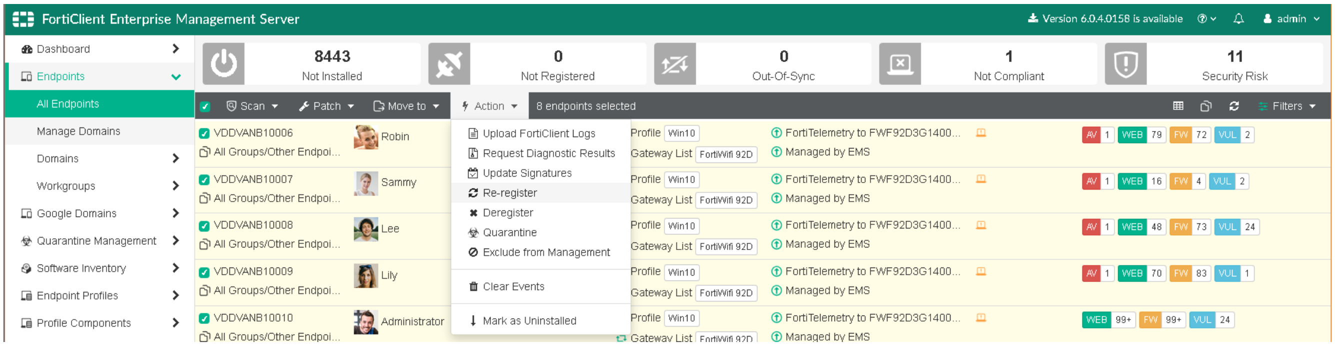


Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[194], vddvanb20003.exam...	static
(same as parent folder)	Name Server (NS)	vddvanb20003.example.com	static
(same as parent folder)	Host (A)	10.200.200.8	12/10/2018 12:00:00 PM
ems	Host (A)	10.200.200.15	static

Connecting endpoints to Server B

It is recommended to flush the endpoints' DNS records to ensure they point to Server B. You can accomplish this by running `ipconfig /flushdns` on the endpoint machines. If this option is not available, reboot the endpoints or wait for the DNS records to update.

The endpoints should now show that they are connected to Server B. However, if there are any issues, reregister the endpoints in EMS on Server B.



☑ VDDVANB10006 All Groups/Other Endpoi...	Robin	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G1400... Managed by EMS	AV 1 WEB 79 FW 72 VUL 2
☑ VDDVANB10007 All Groups/Other Endpoi...	Sammy	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G1400... Managed by EMS	AV 1 WEB 16 FW 4 VUL 2
☑ VDDVANB10008 All Groups/Other Endpoi...	Lee	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G1400... Managed by EMS	AV 1 WEB 48 FW 73 VUL 24
☑ VDDVANB10009 All Groups/Other Endpoi...	Lily	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G1400... Managed by EMS	AV 1 WEB 70 FW 83 VUL 1
☑ VDDVANB10010 All Groups/Other Endpoi...	Administrator	Profile Win10 Gateway List FortiWifi 92D	FortiTelemetry to FWF92D3G1400... Managed by EMS	WEB 99+ FW 99+ VUL 24

Change Log

Date	Change Description
2018-10-24	Initial release.
2018-12-19	Added Use Case: Migrating EMS to a New Server on page 32.