FortiClient & FortiClient EMS - New Features Guide

Version 6.2.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/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: techdoc@fortinet.com

December 19, 2019
FortiClient & FortiClient EMS 6.2.2 New Features Guide
04-622-548127-20191219

TABLE OF CONTENTS

Expanding Fabric family

Managing endpoints with FortiClient Cloud

With FortiClient Cloud, you can manage up to 500 endpoints with a simplified cloud infrastructure created and managed by Fortinet. Using FortiClient Cloud provides you with the opportunity to focus on your endpoint management needs rather than infrastructure configuration and maintenance.

You can execute EMS functions from the cloud-based EMS. You must complete the following steps to create a cloud-based EMS instance under your FortiCloud user account:

1. Register a FortiCloud premium subscription to your FortiCloud account.
2. Register a FortiClient license contract for management by FortiClient Cloud to your FortiCloud account.

⚠ You must register the FortiCloud premium subscription before you can register FortiClient endpoint licenses.

If you attempt to register the endpoint license before the FortiCloud premium subscription, you will not be able to deploy FortiClient & FortiClient EMS Cloud from this FortiCloud account.

This section provides the following information about FortiClient Cloud:

- Requirements on page 4
- Differences between FortiClient Cloud and on-premise EMS on page 5
- Deploying FortiClient Cloud on page 6
- Adding a new invitation for a deployment package on page 7
- Adding a secondary admin account on page 7
- Adding a FortiClient deployment package on page 8
- Installing FortiClient on an endpoint and registering to FortiClient Cloud on page 10

Requirements

The following items are required before you can initialize your FortiClient Cloud instance:

Requirement	Description
FortiCloud account with premium subscription	Create a FortiCloud account if you do not have one and register a FortiCloud premium subscription to this account. Launching FortiClient Cloud requires a primary FortiCloud account with a premium subscription. A primary FortiCloud account with a premium subscription can invite other users to launch FortiClient Cloud. Each FortiCloud account that will access FortiClient Cloud must be registered with its own FortiCloud premium subscription. You must register the FortiCloud premium subscription before registering any endpoint licensing; otherwise, you cannot deploy FortiClient Cloud.

Requirement	Description
Licensing	A license for each endpoint that will be managed using FortiClient Cloud. Purchase one of the following FortiClient license types from Fortinet: • Fabric Agent with Endpoint Protection • Sandbox Cloud When registering the license contract, you must specify that the endpoints will be managed using FortiClient Cloud, as described in Deploying FortiClient Cloud on page 6. Registering a Fabric Agent license for FortiClient Cloud management does not support all features supported for on-premise EMS. See Differences between FortiClient Cloud and on-premise EMS on page 5 for the list of supported features.
Internet access	You must have Internet access to create a FortiClient Cloud instance.
Browser	Device with a browser to access FortiClient Cloud.

FortiClient Cloud only supports FortiClient 6.2.1 and later versions.

Differences between FortiClient Cloud and on-premise EMS

FortiClient Cloud does not currently support the following features. To use these features, use an on-premise EMS instead of FortiClient Cloud:

- Active Directory (AD) integration
- Chromebook management

In addition to the removal of GUI elements that relate to AD integration and Chromebook management, the following lists screens and features that have been modified from what is available in on-premise EMS

GUI pane	Modification
Dashboard	*System Information* widget shows FortiCare account organization name and EMS node ID.
Manage Installers > Deployment Packages	• Deployment packages have an expiry date. After this date, users cannot use this deployment package to install FortiClient. • The *Manage Installers > Deployment Packages* page displays a download link. You can directly download the .zip file that contains the FortiClient installer using this link. • Each deployment package contains an invitation code. • Automatic registration is enabled by default for each deployment package.

GUI pane	Modification
Compliance Verification	*Fabric Device Monitor* is not available.
Administration	• Shows users imported from the FortiCare account. • *Administrators* page only allows changing a user's role. • *Administrators* page displays a *Primary User* column.
System Settings	• *Server* only displays the *DHCP onnet/offnet* and *Sign software packages* options. • *FortiGuard* does not have the option to use FortiManager for software and signature updates.

Deploying FortiClient Cloud

This section explains how to deploy FortiClient Cloud. This section assumes that you have already purchased the desired subscription licenses for your deployment from a Fortinet partner or reseller and received your license activation codes.

You can create only one EMS instance in the Cloud per FortiCloud account with premium subscription.

To deploy FortiClient Cloud:

You must register the FortiCloud premium subscription as described in step 1 before you can register FortiClient endpoint licenses as described in step 2.

If you attempt to register the endpoint license before the FortiCloud premium subscription, you will not be able to deploy FortiClient Cloud from this FortiCloud account.

1. Register the FortiCloud premium subscription contract (FC-15-CLDPS-219-02-DD) to your FortiCloud account:
    a. On the Customer Service & Support site, go to *Asset* > *Register/Activate*.
    b. In the *Specify Registration Code* field, enter your license activation code and select *Next* to continue registering the product.
    c. Enter your details in the other fields and complete the registration. This is a yearly subscription.
2. Register the FortiClient endpoint licenses for management by FortiClient Cloud:
    a. On the Customer Service & Support site, go to *Asset* > *Register/Activate*.
    b. In the *Specify Registration Code* field, enter your license activation code and select *Next* to continue registering the product.
    c. On the *Specify Fortinet Registration Information* screen, select the *Used for Cloud Purpose* checkbox.
    d. Enter your details in the other fields and complete the registration.

You may need to wait a few minutes for the cloud instance to initialize before you can proceed to step 2 or 3.

3. Access FortiClient Cloud in one of the following ways:
   a. Access FortiClient Cloud from FortiCare.
   b. Access FortiClient Cloud from the FortiClient Cloud portal:
      i. In a browser, go to the FortiClient Cloud portal.
      ii. Log in with your FortiCloud credentials.
   c. Access FortiClient Cloud from the link included in the welcome email.

Adding a new invitation for a deployment package

Users can connect to FortiClient Cloud without an IP address or FQDN by using an invitation. FortiClient Cloud offers two invitation types: individual, which can be used once; and bulk, which can be used multiple times. FortiClient Cloud displays how many times an invitation has been used to register an endpoint in the *Use Count* column on the *Invitations* page. The *Expiry Date* column displays the date until the invitation can be used to connect to FortiClient Cloud.

To add a new invitation for a deployment package:

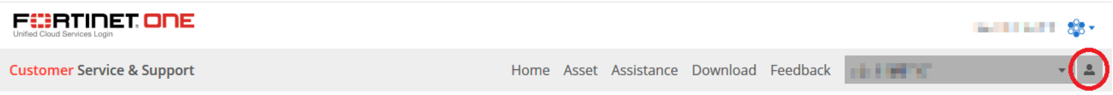
1. Go to *Invitations*.
2. Select an existing invitation code for the desired deployment package.
3. Click *Add*.
4. To send the code to a single recipient, select *Individual*. Otherwise, select *Bulk*.
5. If desired, select *Send email notifications*.
6. In the *Email recipients* field, enter the email addresses of the desired end users.
7. If desired, enable *Send SMS notifications*.
8. In the *Expiry date* field, set the expiry date. Click *Save*. You will see a new invitation code for the deployment package.

Adding a secondary admin account

The FortiClient Cloud primary administrator (the user who created the FortiClient Cloud instance) can add secondary administrators from their FortiCare account. You cannot create a user directly in the FortiClient Cloud GUI. FortiClient Cloud pulls users from the primary administrator's FortiCare account.

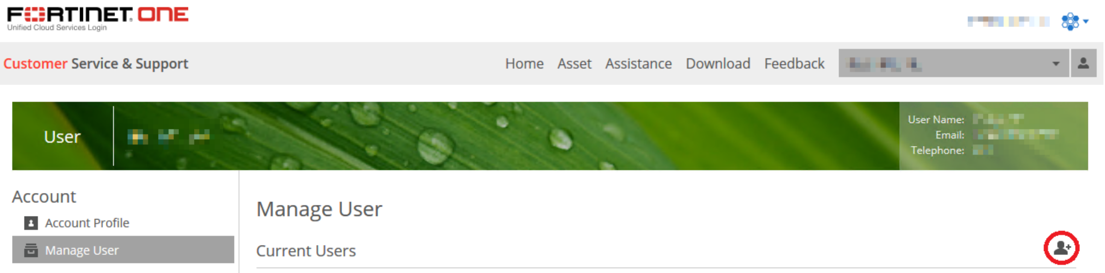
To create a secondary admin account:

1. Log in to Fortinet Service & Support with your FortiCloud account.
2. Click the account icon in the top-right corner.



3. Select *Manage User*.

4. Click the *Add User* icon.

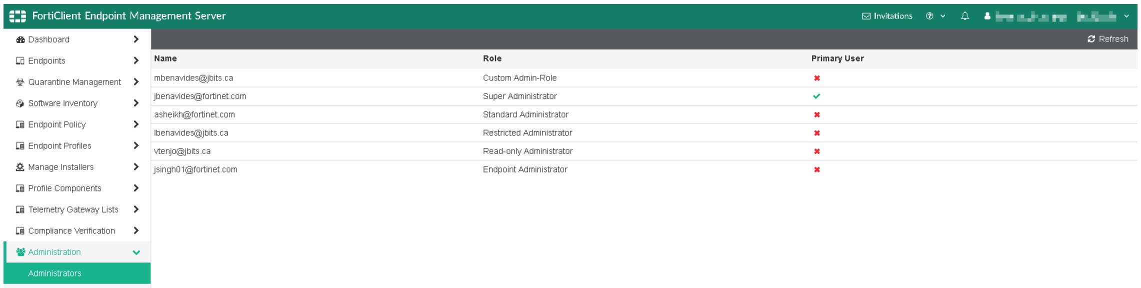


User Name: [redacted]
Email: [redacted]
Telephone: [redacted]

Manage User

Current Users

5. Enter the user information as required. If the new user does not have a FortiCare account, they must create one. Click *Save*. A user added on this page becomes visible on the FortiClient Cloud GUI in *Administrators* and can log in to FortiClient Cloud with their FortiCloud account. These users have limited permissions.



Name	Role	Primary User
mbenavides@jbits.ca	Custom Admin-Role	✖
jbenavides@fortinet.com	Super Administrator	✓
asheikh@fortinet.com	Standard Administrator	✖
lbenavides@jbits.ca	Restricted Administrator	✖
vtenjo@jbits.ca	Read-only Administrator	✖
jsingh01@fortinet.com	Endpoint Administrator	✖

Adding a FortiClient deployment package

To add a deployment package:

1. Go to *Manage Installers > Deployment Packages*.
2. Click *Add*.
3. On the *Version* tab, set the following options:

Installer Type	Use an official FortiClient installer or a custom FortiClient installer. See the *FortiClient EMS Administration Guide* for details on uploading a custom installer.
Release	Select the FortiClient release version to install.
Patch	Select the specific FortiClient patch version to install.
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.
Custom installer	Select the desired custom FortiClient installer.

4. Click *Next*. On the *General* tab, set the following options:

Name	Enter the FortiClient deployment package's name.
Expiry Date	Enter this deployment package's expiry date. After this date, users cannot use this deployment package to install FortiClient.
Notes	(Optional) Enter any notes about the FortiClient deployment package.

5. Click *Next*. On the *Features* tab, set the following options:

Security Fabric Agent	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scan enabled.
Secure Access Architecture Components	Install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package.
Advanced Persistent Threat (APT) Components	Install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient deployment package. Includes FortiSandbox detection and quarantine features.
Additional Security Features	Enable any of the following features: • AntiVirus • Web Filtering • Application Firewall • Single Sign-On (SSO) mobility agent Disable to exclude features from the FortiClient deployment package.

6. Click *Next*. On the *Advanced* tab, set the following options:

Enable automatic registration	Configure FortiClient to automatically connect Telemetry to FortiClient after FortiClient installs on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to FortiClient.
Enable desktop shortcut	Configure the FortiClient deployment package to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Configure the FortiClient deployment package to create a Start menu shortcut on the endpoint.
Enable Installer ID	Configure an installer ID. Select an existing installer ID or enter a new installer ID. If creating an installer ID, select a group path or create a new group in the *Group Path* field. FortiClient automatically groups endpoints according to installer ID group assignment rules.
Enable Endpoint Profile	Select an endpoint profile to include in the installer. EMS applies the profile to the endpoint once it has installed FortiClient. This option is necessary if it is required to have certain security features enabled prior to contact with EMS, or if users require VPN connection to connect to EMS.

7. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the FortiClient server, which will manage FortiClient once it is installed on the endpoint. Also configure the following option:

Enable telemetry connection to Security Fabric (FortiGate)	Enable this option, and select the name of the gateway list to use. The gateway list defines the IP address for the FortiGate. If you have not created a gateway list, this option is not available. See *FortiClient EMS Administration Guide* for details on configuring a gateway list.

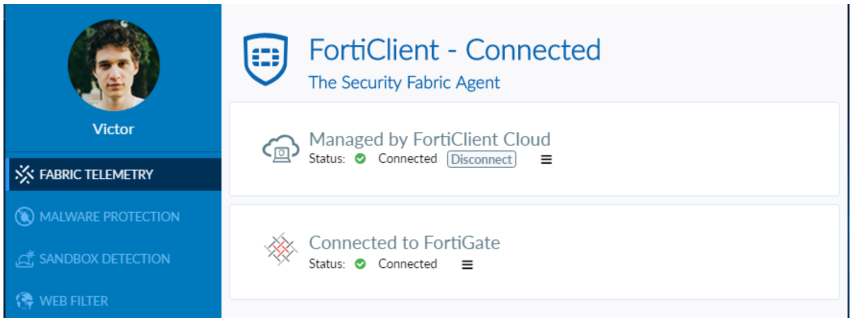
8. Click *Finish*. The FortiClient deployment package is added to FortiClient and displays on the *Manage Installers > Deployment Packages* pane. The deployment package may include .exe (32-bit and 64-bit), .msi, and .dmg files depending on the configuration.

Installing FortiClient on an endpoint and registering to FortiClient Cloud

To install FortiClient on an endpoint:

When installing FortiClient on an endpoint from a deployment package created in FortiClient Cloud, the administrator carries out some actions, while the endpoint user carries out others.

1. (Administrator) In EMS, go to *Manage Installers* > *Deployment Packages*. Note the invitation code for the desired deployment package.
2. (Administrator) Go to *Invitations*.
3. (Administrator) Select the invitation code that was noted in step 2. Click *Edit*.
4. (Administrator) To send the code to a single recipient, select *Individual*. Otherwise, select *Bulk*.
5. (Administrator) In the *Email recipients* field, enter the email addresses of the desired end users.
6. (Administrator) If desired, enable *Send SMS notifications*.
7. (Administrator) If desired, in the *Expiry date* field, set the expiry date. Click *Save*.
8. (End user) Click the FortiClient download link in the invitation email or text message that you received. Extract and run the installer file.
9. (End user) Your FortiClient should automatically register to FortiClient Cloud after installation. If your FortiClient did not automatically register to FortiClient Cloud, use the instructions below to register to FortiClient Cloud.



To register to FortiClient Cloud:

You can use the following instructions to register to FortiClient Cloud in one of the following scenarios:

- If you want to register a FortiClient Linux, iOS, or Android endpoint to FortiClient Cloud. Since you cannot create a deployment package for these operating systems in EMS, this is the only way to register these endpoints to FortiClient Cloud.
- If you did not follow the instructions above to install FortiClient on your endpoint, such as if you downloaded a publicly available FortiClient deployment package.
- If you followed the installation instructions above, but your FortiClient did not automatically register to FortiClient Cloud after installation.

1. Enter the invitation code in the *Join FortiClient Cloud* field on the *Fabric Telemetry* tab in FortiClient. Your EMS administrator should have provided the code to you.
2. Click *Connect*. FortiClient is now managed by FortiClient Cloud.

New compliance verification rule types

EMS 6.2.2 introduces new compliance verification rule types. If an endpoints satisfies a rule, EMS places the endpoint into a group with other endpoints that satisfy the rule. The new rule types are:

- AD Group
- AntiVirus Software
- Sandbox Detection
- Windows Security (only available for Windows endpoints)
- User Identity

Configuring a compliance verification rule set remains similar to earlier versions of EMS. See the *FortiClient EMS 6.2.2 Administration Guide*.

AD Group

An endpoint that belongs to an AD domain may belong to numerous AD groups. You can configure a compliance verification rule that applies tags to endpoints based on what AD group(s) they belong to.

AntiVirus Software

You can configure an AntiVirus Software rule to consist of the following criteria:

- AV Software is installed and running
- AV signature is up-to-date

AV software can include:

- FortiClient AV
- Third-party AV software
- Windows Defender

Sandbox Detection

The Sandbox Detection rule type has one criterion: Sandbox detected malware on the endpoint in the last seven days.

Windows Security

You can configure a Windows Security rule to consist of the following criteria:

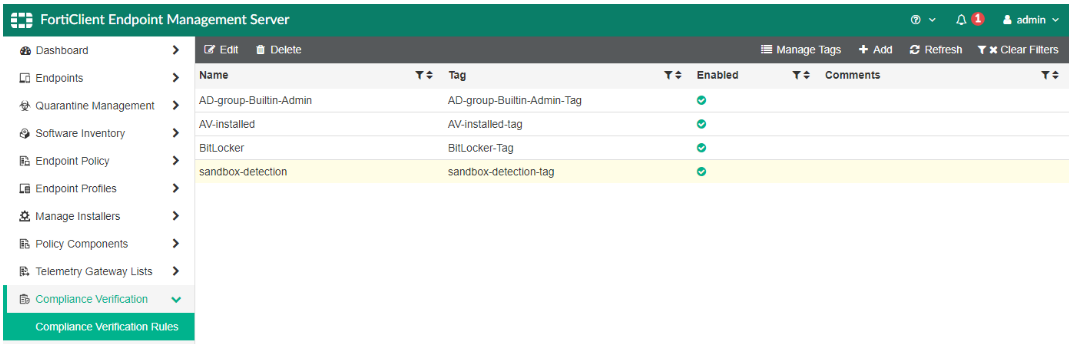
- Windows Defender is enabled
- Bitlocker Disk Encryption is enabled
- Exploit Guard is enabled
- Application Guard is enabled
- Windows Firewall is enabled

Application Guard is only available for Windows 10.

Results

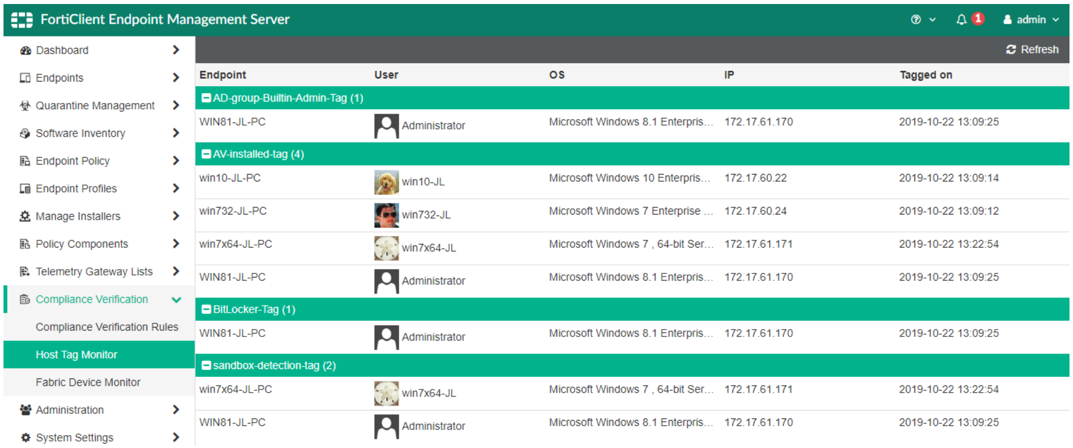
The example shows a rule configured for each new rule type:

Name	Description
AD-group-Builtin-Admin	AD group rule that tags endpoints where the logged-in user is a member of the BuiltIn/Administrators AD group
AV-installed	AntiVirus Software rule that tags endpoints where AV software is installed and running
BitLocker	Windows Security rule that tags endpoints where Bitlocker Disk Encryption is enabled
sandbox-detection	Sandbox Detection rule that tags endpoints where Sandbox detected malware in the last seven days.



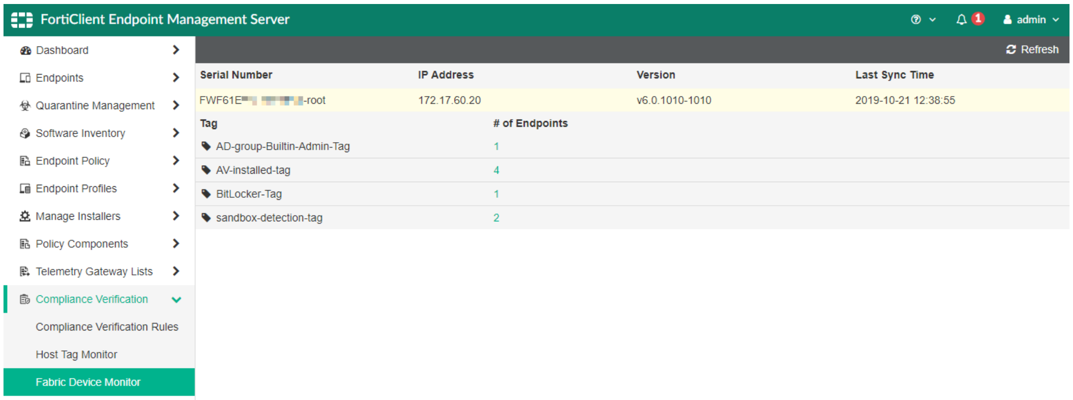
Name	Tag	Enabled	Comments
AD-group-Builtin-Admin	AD-group-Builtin-Admin-Tag	✓	
AV-installed	AV-installed-tag	✓	
BitLocker	BitLocker-Tag	✓	
sandbox-detection	sandbox-detection-tag	✓	

Go to *Compliance Verification* > *Host Tag Monitor*. You can view each tag and the endpoints grouped by each tag:



Endpoint	User	OS	IP	Tagged on
AD-group-Builtin-Admin-Tag (1)				
WIN81-JL-PC	Administrator	Microsoft Windows 8.1 Enterpris...	172.17.61.170	2019-10-22 13:09:25
AV-installed-tag (4)				
win10-JL-PC	win10-JL	Microsoft Windows 10 Enterpris...	172.17.60.22	2019-10-22 13:09:14
win732-JL-PC	win732-JL	Microsoft Windows 7 Enterprise ...	172.17.60.24	2019-10-22 13:09:12
win7x64-JL-PC	win7x64-JL	Microsoft Windows 7 , 64-bit Ser...	172.17.61.171	2019-10-22 13:22:54
WIN81-JL-PC	Administrator	Microsoft Windows 8.1 Enterpris...	172.17.61.170	2019-10-22 13:09:25
BitLocker-Tag (1)				
WIN81-JL-PC	Administrator	Microsoft Windows 8.1 Enterpris...	172.17.61.170	2019-10-22 13:09:25
sandbox-detection-tag (2)				
win7x64-JL-PC	win7x64-JL	Microsoft Windows 7 , 64-bit Ser...	172.17.61.171	2019-10-22 13:22:54
WIN81-JL-PC	Administrator	Microsoft Windows 8.1 Enterpris...	172.17.61.170	2019-10-22 13:09:25

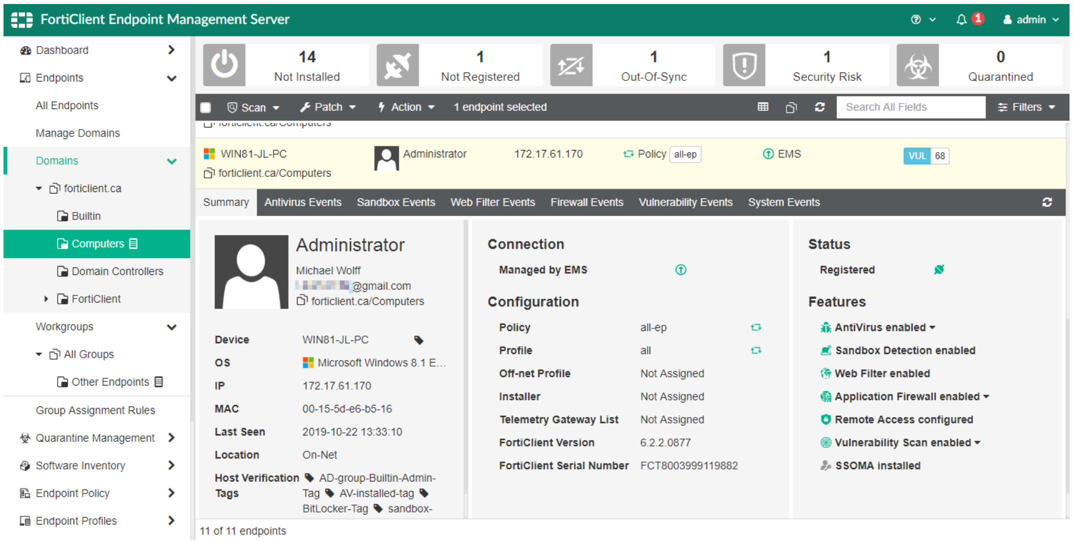
Go to *Compliance Verification* > *Fabric Device Monitor*. You can view all FortiGates that are connected to EMS using the FSSO protocol, the tags shared with the FortiGate, and the number of endpoints in each tag group.



Serial Number	IP Address	Version	Last Sync Time
FWF61E[redacted]-root	172.17.60.20	v6.0.1010-1010	2019-10-21 12:38:55

Tag	# of Endpoints
AD-group-Builtin-Admin-Tag	1
AV-installed-tag	4
BitLocker-Tag	1
sandbox-detection-tag	2

Go to *Endpoints* and view the details for a tagged endpoint. *Host Verification Tags* displays the tags that EMS has applied to the endpoint.



WIN81-JL-PC forticlient.ca/Computers | Administrator | 172.17.61.170 | Policy all-ep | EMS | VUL 68

Administrator
Michael Wolff
[redacted]@gmail.com
forticlient.ca/Computers

Device	WIN81-JL-PC
OS	Microsoft Windows 8.1 E...
IP	172.17.61.170
MAC	00-15-5d-e6-b5-16
Last Seen	2019-10-22 13:33:10
Location	On-Net
Host Verification Tags	AD-group-Builtin-Admin-Tag AV-installed-tag BitLocker-Tag sandbox-

Connection

Managed by EMS	

Configuration

Policy	all-ep
Profile	all
Off-net Profile	Not Assigned
Installer	Not Assigned
Telemetry Gateway List	Not Assigned
FortiClient Version	6.2.2.0877
FortiClient Serial Number	FCT8003999119882

Status

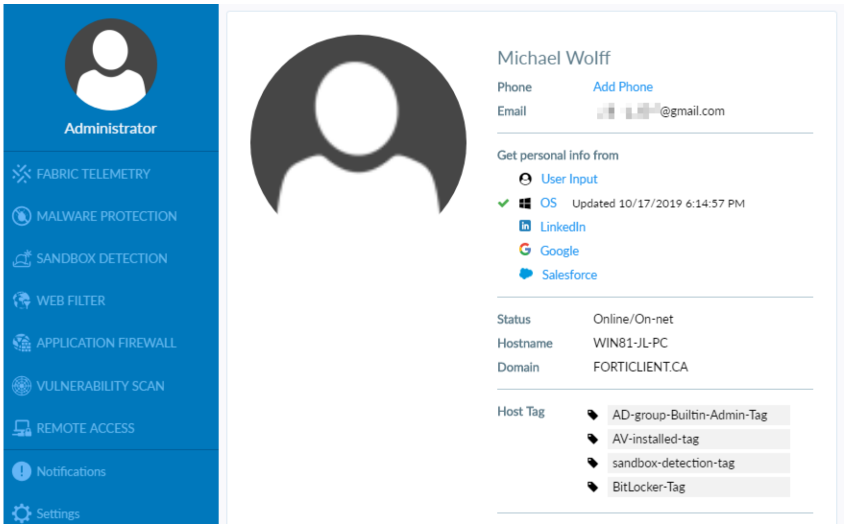
Registered

Features

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

11 of 11 endpoints

If you enabled *Show Host Tags on FortiClient GUI* on the endpoint's applied profile, you can also view the host tags on the FortiClient GUI.



Michael Wolff

Phone	Add Phone
Email	[redacted]@gmail.com

Get personal info from

- User Input
- ✓ OS Updated 10/17/2019 6:14:57 PM
- LinkedIn
- Google
- Salesforce

Status	Online/On-net
Hostname	WIN81-JL-PC
Domain	FORTICLIENT.CA

Host Tag

- AD-group-Builtin-Admin-Tag
- AV-installed-tag
- sandbox-detection-tag
- BitLocker-Tag

Using certificate Fabric authentication

To support FortiOS Fabric authentication moving towards certificate-based authentication, this feature adds support for certificate-based authentication for the Fabric connection between FortiOS and FortiClient Cloud. The FortiClient Cloud administrator can authorize or deny a connection request from a FortiGate. An authorized connection request establishes the Fabric connection between FortiOS and FortiClient Cloud.

To configure FortiOS:

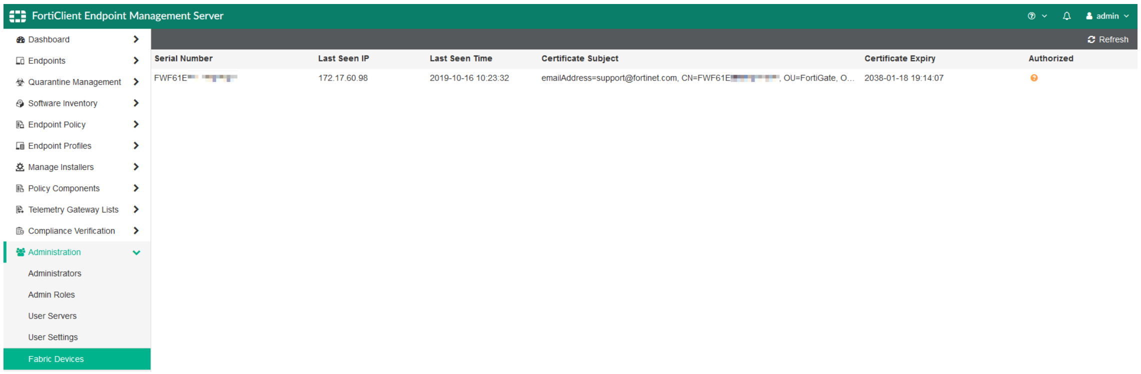
1. Enable FortiHeartbeat:
```
config system interface
   edit "wan1"
      set fortiheartbeat enable
   next
end
```
2. Configure FortiClient Cloud:
```
config endpoint-control fctems
   edit "ems-cloud"
      set serial-number ''
      set fortinetone-cloud-authentication enable
      set source-ip 0.0.0.0
      set call-timeout 5000
   next
end
```

To enable remote HTTPS access in FortiClient Cloud:

1. Go to *System Settings* > *Server.*
2. Under *Shared Settings*, enable *Remote HTTPS access*. Ensure that the *HTTPS port* is defined as 443.

To establish Fabric connection between FortiOS and FortiClient Cloud:

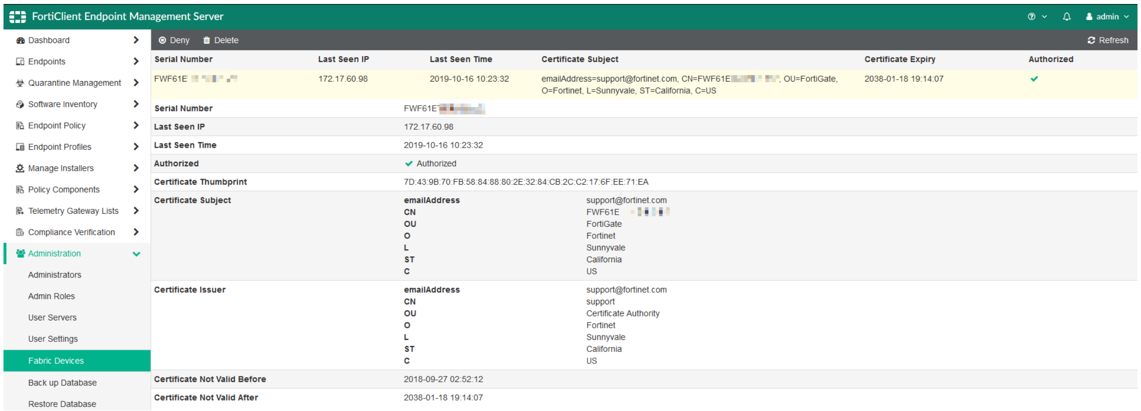
1. Test Fabric device connectivity from FortiOS by entering the `diagnose endpoint fctems-test-connectivity ems95` command. FortiClient Cloud should respond with a `Not authorized` message.
2. Log in to FortiClient Cloud. Do one of the following:
   a. A popup notification prompts you to authorize or deny the Fabric connection for access from that particular FortiGate. The authorization request includes the FortiGate hostname, serial number, and IP address. Click *Authorize*.
   b. If you do not see a popup notification, you can also authorize Fabric devices in *Administration* > *Fabric Devices*. This page shows devices pending authorization with a yellow question mark.



Serial Number	Last Seen IP	Last Seen Time	Certificate Subject	Certificate Expiry	Authorized
FWF61E[redacted]	172.17.60.98	2019-10-16 10:23:32	emailAddress=support@fortinet.com, CN=FWF61E[redacted], OU=FortiGate, O...	2038-01-18 19:14:07	❓

Click the desired device, then click *Authorize*.

3. Go to *Administration* > *Fabric Devices*. Verify that the Fabric connection is established between FortiOS and FortiClient Cloud. The connection's status displays as authorized.

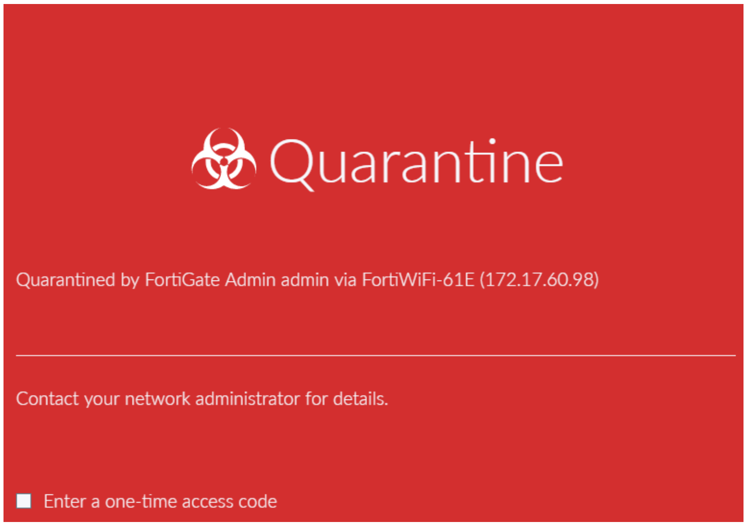


Serial Number	Last Seen IP	Last Seen Time	Certificate Subject	Certificate Expiry	Authorized
FWF61E[redacted]	172.17.60.98	2019-10-16 10:23:32	emailAddress=support@fortinet.com, CN=FWF61E[redacted], OU=FortiGate, O=Fortinet, L=Sunnyvale, ST=California, C=US	2038-01-18 19:14:07	✓

Serial Number	FWF61E[redacted]	
Last Seen IP	172.17.60.98	
Last Seen Time	2019-10-16 10:23:32	
Authorized	✓ Authorized	
Certificate Thumbprint	7D:43:9B:70:FB:58:84:88:80:2E:32:84:CB:2C:C2:17:6F:EE:71:EA	
Certificate Subject	emailAddress CN OU O L ST C	support@fortinet.com FWF61E[redacted] FortiGate Fortinet Sunnyvale California US
Certificate Issuer	emailAddress CN OU O L ST C	support@fortinet.com support Certificate Authority Fortinet Sunnyvale California US
Certificate Not Valid Before	2018-09-27 02:52:12	
Certificate Not Valid After	2038-01-18 19:14:07	

4. Repeat step 1 to test Fabric device connectivity from FortiOS. FortiClient Cloud should respond with a `Connection test passed` message.

5. After FortiClient Cloud authorizes a Fabric device, FortiOS can quarantine an endpoint and remove it from quarantine via FortiClient Cloud. To quarantine an endpoint, run the `diagnose endpoint fctems-queue-complete-calls Q-<endpoint IP address>` command. For example, if the endpoint's IP address is 192.168.10.204, the command would be `diagnose endpoint fctems-queue-complete-calls Q-<192.168.10.204>`. The response should be `SUCCESS! Queued the <call> 'Q-<endpoint IP address>'.<call> stats: total=1, valid=1, queued=1.`



Quarantine

Quarantined by FortiGate Admin admin via FortiWiFi-61E (172.17.60.98)

Contact your network administrator for details.

□ Enter a one-time access code

6. To remove the endpoint from quarantine, run the `diagnose endpoint fctems-queue-complete-calls U-<endpoint IP address>` command.

Fabric connectors

Dynamically group endpoints based on user identity

EMS can now dynamically group endpoints based on their user identity. An end user can provide their user identity in FortiClient for the following social network accounts:

- LinkedIn
- Google
- Salesforce
- User Input

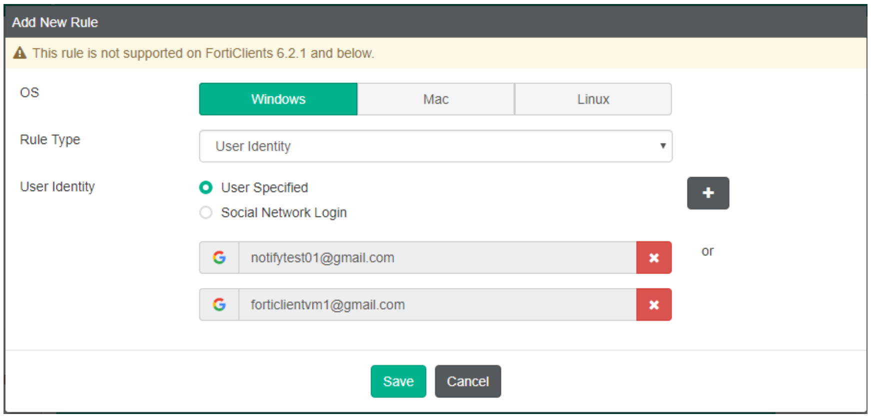
When the end user selects *User Input*, they can specify personal information, including their avatar, name, phone number, and email address. If they select another option, FortiClient reads their avatar, name, phone number, and email address from the corresponding account. FortiClient displays this information and sends it via Telemetry to EMS. EMS uses this information to apply applicable host verification tags on endpoints.

The end user can disconnect FortiClient from the specified account by clicking the *Sign out* button.

In this example, the EMS administrator has configured five compliance verification rules, which apply the following host verification tags to endpoints that fulfill the listed criteria:

Tag name	Endpoint criteria
Specific-Google-Only-Tag	FortiClient is linked to one of the following accounts: • notifytest01@gmail.com (Google account) • forticlientvm1@gmail.com (Google account)
Specified-Google-LinkedIn-Tag	FortiClient is linked to one of the following accounts: • notifytest01@gmail.com (Google account) • forticlientvm1@gmail.com (LinkedIn account)
All-Google-Tag	FortiClient is linked to a Google account.
All-LinkedIn-Tag	FortiClient is linked to a LinkedIn account.
Users-Specified-tag	User selected *User Input* and provided their personal information manually.

The following shows the EMS configuration for the Specific-Google-Only rule, which applies the Specific-Google-Only-Tag to endpoints that satisfy the configured criteria:



Add New Rule

⚠ This rule is not supported on FortiClients 6.2.1 and below.

OS: Windows | Mac | Linux

Rule Type: User Identity

User Identity: ● User Specified ○ Social Network Login

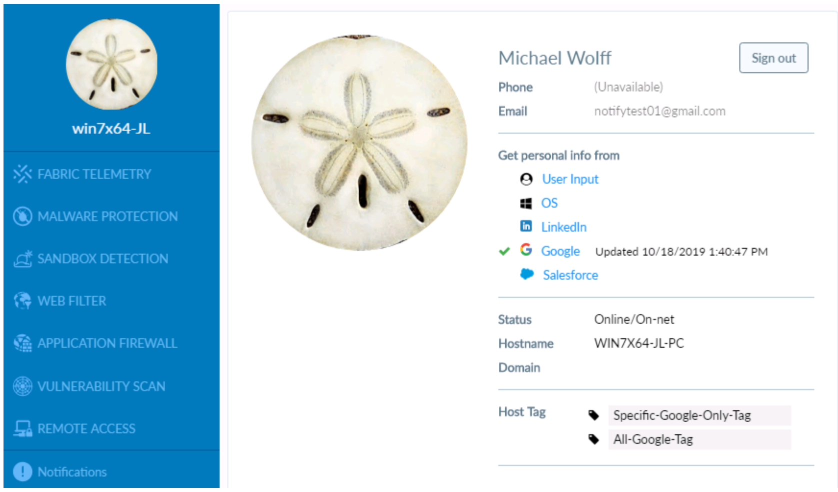
G notifytest01@gmail.com ✖

or

G forticlientvm1@gmail.com ✖

The EMS administrator must enable *Show Host Tags on FortiClient GUI* in the applied endpoint profile for host tags to display in FortiClient.

This user is logged in to their Google account, notifytest01@gmail.com. EMS applies the Specific-Google-Only-Tag tag to the endpoint, since the linked Google account matches one of Specific-Google-Only-Tag's specified Google accounts. EMS also applies the All-Google-Tag to the endpoint, since FortiClient is linked to a Google account:



win7x64-JL

Michael Wolff

Phone (Unavailable)

Email notifytest01@gmail.com

Get personal info from

- User Input
- OS
- LinkedIn
- ✓ Google Updated 10/18/2019 1:40:47 PM
- Salesforce

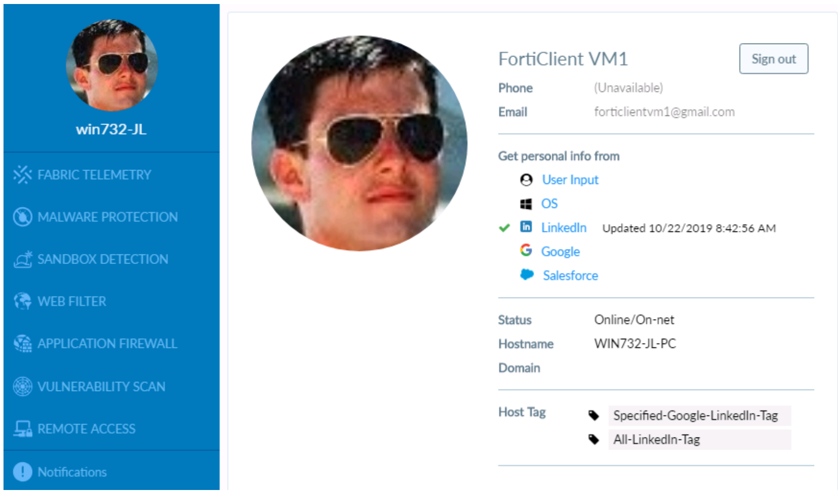
Status Online/On-net

Hostname WIN7X64-JL-PC

Domain

Host Tag Specific-Google-Only-Tag
All-Google-Tag

This user is logged in to their LinkedIn account, forticlientvm1@gmail.com. EMS applies the Specific-Google-LinkedIn-Tag tag to the endpoint, since the linked LinkedIn account matches Specific-Google-LinkedIn-Tag's specified LinkedIn account. EMS also applies the All-LinkedIn-Tag to the endpoint, since FortiClient is linked to a LinkedIn account:



FortiClient VM1

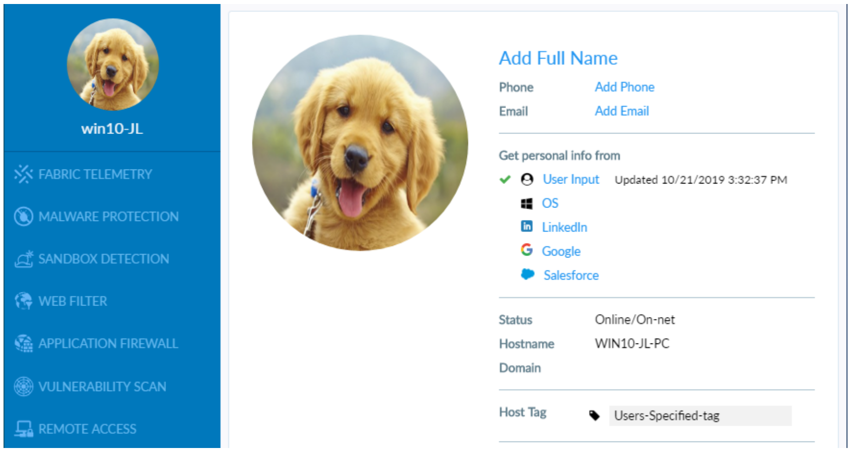
Phone (Unavailable)
Email forticlientvm1@gmail.com

Get personal info from
- User Input
- OS
- ✓ LinkedIn Updated 10/22/2019 8:42:56 AM
- Google
- Salesforce

Status Online/On-net
Hostname WIN732-JL-PC
Domain

Host Tag
- Specified-Google-LinkedIn-Tag
- All-LinkedIn-Tag

This user provided selected *User Input* and provided their personal information manually. EMS applies the User-Specified-tag tag to the endpoint:



Add Full Name

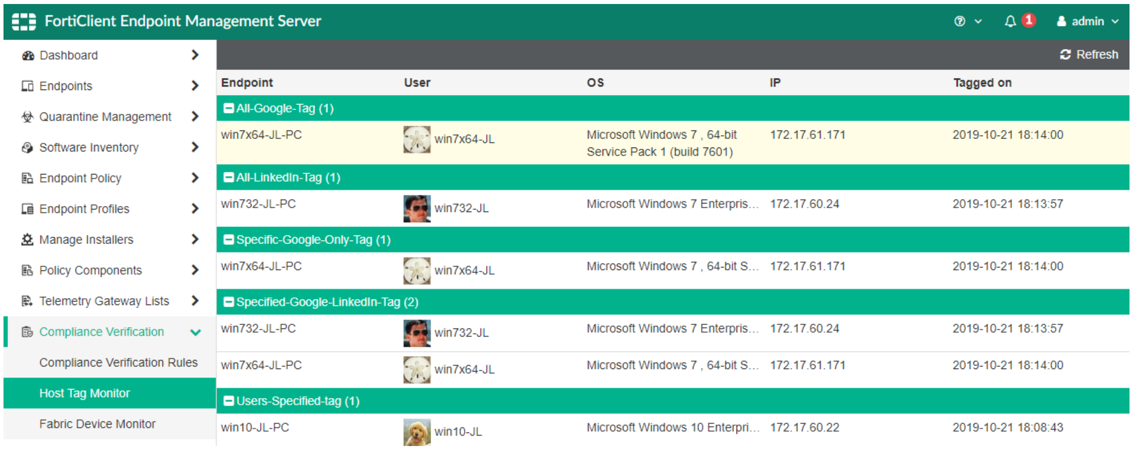
Phone Add Phone
Email Add Email

Get personal info from
- ✓ User Input Updated 10/21/2019 3:32:37 PM
- OS
- LinkedIn
- Google
- Salesforce

Status Online/On-net
Hostname WIN10-JL-PC
Domain

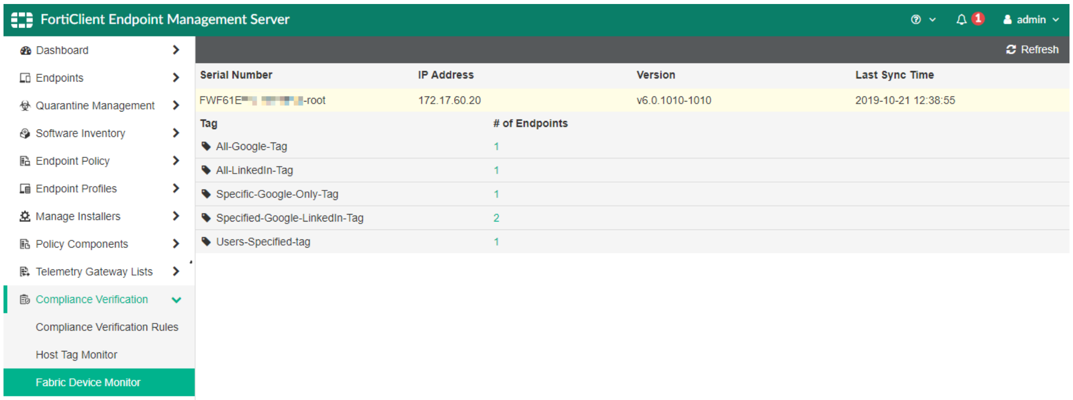
Host Tag
- Users-Specified-tag

The *Host Tag Monitor* page in EMS displays the endpoints that belong to each dynamic group:



Endpoint	User	OS	IP	Tagged on
⊟ All-Google-Tag (1)				
win7x64-JL-PC	win7x64-JL	Microsoft Windows 7 , 64-bit Service Pack 1 (build 7601)	172.17.61.171	2019-10-21 18:14:00
⊟ All-LinkedIn-Tag (1)				
win732-JL-PC	win732-JL	Microsoft Windows 7 Enterpris...	172.17.60.24	2019-10-21 18:13:57
⊟ Specific-Google-Only-Tag (1)				
win7x64-JL-PC	win7x64-JL	Microsoft Windows 7 , 64-bit S...	172.17.61.171	2019-10-21 18:14:00
⊟ Specified-Google-LinkedIn-Tag (2)				
win732-JL-PC	win732-JL	Microsoft Windows 7 Enterpris...	172.17.60.24	2019-10-21 18:13:57
win7x64-JL-PC	win7x64-JL	Microsoft Windows 7 , 64-bit S...	172.17.61.171	2019-10-21 18:14:00
⊟ Users-Specified-tag (1)				
win10-JL-PC	win10-JL	Microsoft Windows 10 Enterpri...	172.17.60.22	2019-10-21 18:08:43

The *Fabric Device Monitor* page in EMS displays the number of endpoints that are applicable for each tag:



Serial Number	IP Address	Version	Last Sync Time
FWF61E[redacted]-root	172.17.60.20	v6.0.1010-1010	2019-10-21 12:38:55

Tag	# of Endpoints
All-Google-Tag	1
All-LinkedIn-Tag	1
Specific-Google-Only-Tag	1
Specified-Google-LinkedIn-Tag	2
Users-Specified-tag	1

EMS supports SAML SSO for login using FortiOS as an IdP

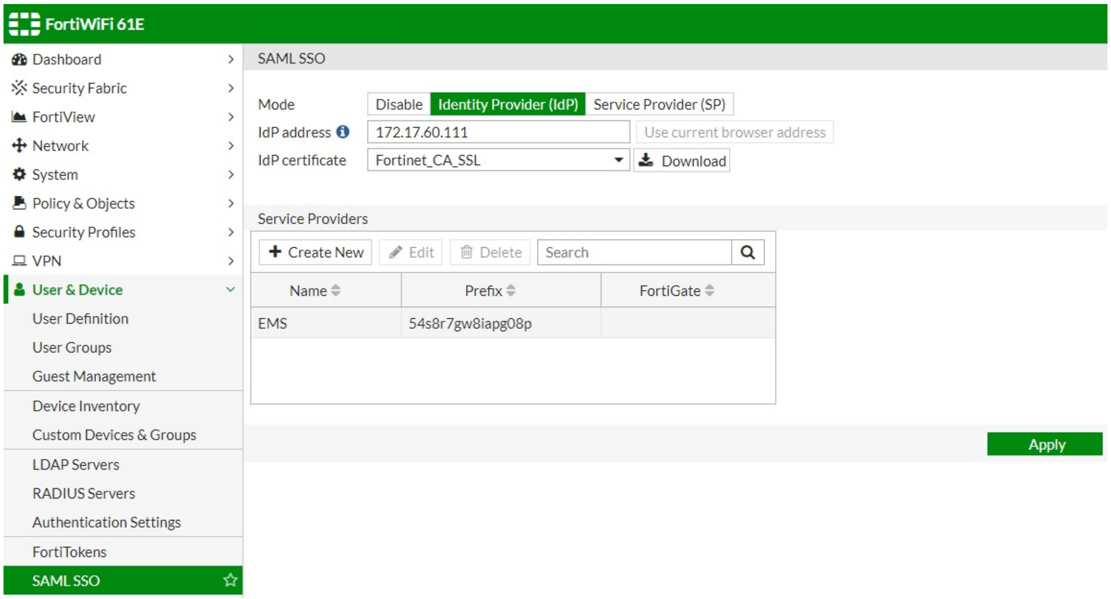
EMS 6.2.2 adds the ability to use SAML single sign on (SSO) using FortiOS as an Identity Provider (IdP).

Currently, EMS supports manually configuring settings for SAML SSO. SAML SSO requires that EMS has HTTPS remote access enabled and a hostname or IP address that FortiOS can access.

> ⚠ You can only use the SAML SSO feature in EMS with a FortiGate as the IdP. EMS does not support using FortiAuthenticator as an IdP or custom IdPs.

To configure SAML SSO in FortiOS:

1. Configure the FortiGate as an IdP:
   a. Go to *User & Device > SAML SSO*.
   b. Set the *Mode* to *Identity Provider (IdP)*.
   c. In the *IdP address* field, enter the FortiOS IP address or FQDN.
   d. From the *IdP certificate* dropdown list, select the SSL IdP certificate.
   e. Click *Download* to download the certificate for use during EMS configuration.
2. Add a Service Provider (SP):
   a. In the *Service Providers* table, click *Create New*.
   b. Enter the SP name, prefix, type, and address. You can use the default autogenerated prefix or click *Generate unique prefix*. Copy the prefix, as you need it when configuring the SP.
   c. In the *SP type* field, select *Fortinet Product*.
   d. (Optional) Configure an SP certificate from EMS.
   e. Click *OK*.



SAML SSO

Mode: Identity Provider (IdP)

IdP address: 172.17.60.111

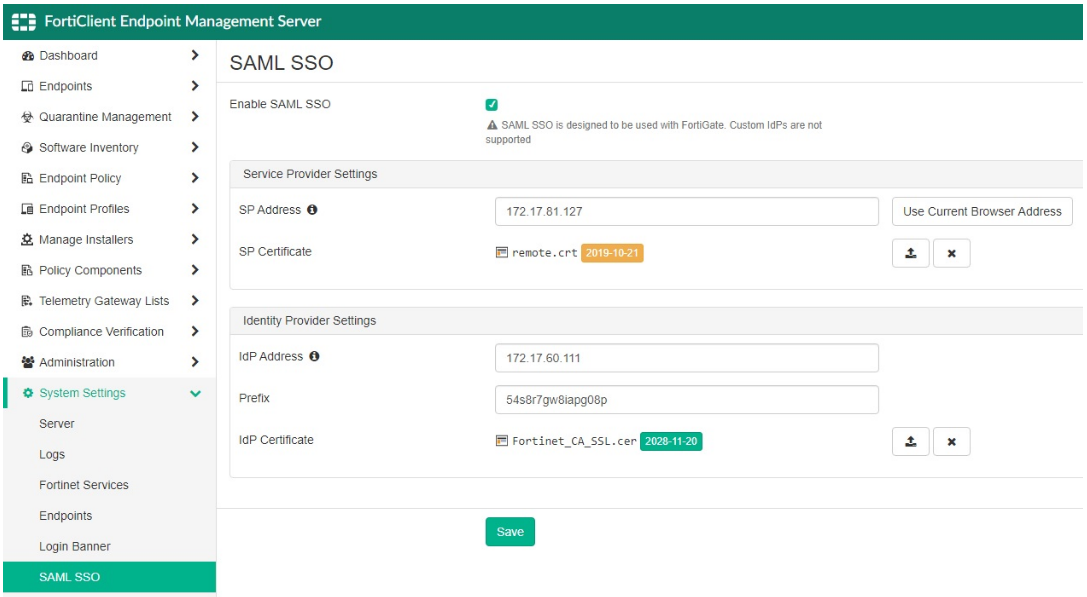
IdP certificate: Fortinet_CA_SSL

Service Providers

Name	Prefix	FortiGate
EMS	54s8r7gw8iapg08p	

To configure SAML SSO in EMS:

1. In EMS, go to *System Settings* > *SAML SSO*.
2. Select *Enable SAML SSO*.
3. Under *Service Provider Settings*, in the *SP Address* field, enter the EMS IP address or FQDN.
4. (Optional) For *SP Certificate*, import the SP certificate.
5. Under *Identity Provider Settings*, in the *IdP Address* field, enter the IP address or FQDN of the FortiGate configured as the IdP.
6. In the *Prefix* field, enter the prefix generated in FortiOS for the SP.
7. In the *IdP Certificate* field, click *Upload new certificate* to upload the IdP certificate. Upload the same certificate that you configured for the IdP (the FortiGate) in FortiOS.



SAML SSO

Enable SAML SSO: ☑

⚠ SAML SSO is designed to be used with FortiGate. Custom IdPs are not supported

Service Provider Settings

SP Address: 172.17.81.127

SP Certificate: remote.crt 2019-10-21

Identity Provider Settings

IdP Address: 172.17.60.111

Prefix: 54s8r7gw8iapg08p

IdP Certificate: Fortinet_CA_SSL.cer 2028-11-20

To log in to EMS using SSO:

1. Double-click the FortiClient Endpoint Management Server icon.
2. Click *Sign in with SSO*.
3. EMS displays the SSO login page. Enter a username and password configured in FortiOS, then click *Login*. This includes local administrators/LDAP and RADIUS users configured in FortiOS for authentication purposes.

When an administrator logs in to EMS with SSO for the first time, they will have restricted permissions. An EMS super administrator can adjust permissions for the new administrator.

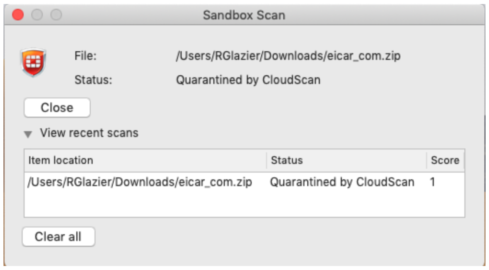
Advanced threats

Cloud-based threat detection

Outbreak protection service provides another layer of protection where FortiClient initiates a real-time cloud lookup of our Global Threat Intelligence database so it can detect and block emerging threats and continue to provide latest protection. FortiClient 6.2.2 adds support for cloud-based threat detection for macOS.

The following describes the process for cloud-based threat detection:

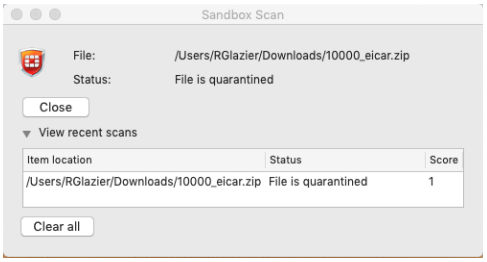
1. A high-risk file, such as an email attachment, network shared resource, webpage, or removable media device is downloaded or executed on the endpoint.
2. FortiClient generates an SHA1 checksum for the file.
3. FortiClient sends the checksum to FortiGuard to determine if it is malicious against the FortiGuard checksum library.
4. One of the following occurs:
   a. If the checksum is found in the library, FortiGuard communicates to FortiClient that the file is deemed malware in the form of a score. A score of 1 is deemed high-risk. By default, FortiClient quarantines the file and terminates any related process.



File: /Users/RGlazier/Downloads/eicar_com.zip
Status: Quarantined by CloudScan

Item location	Status	Score
/Users/RGlazier/Downloads/eicar_com.zip	Quarantined by CloudScan	1

   b. If the checksum is not found in the library, FortiClient submits the file to the configured on-premise FortiSandbox for further analysis. The following shows a file where the checksum does not match any in FortiGuard, but is quarantined by FortiClient using the analysis score from FortiSandbox.



File: /Users/RGlazier/Downloads/10000_eicar.zip
Status: File is quarantined

Item location	Status	Score
/Users/RGlazier/Downloads/10000_eicar.zip	File is quarantined	1

This service only submits high-risk file types. Cloud-based threat detection supports the same default supported file types as FortiSandbox, such as .exe, .doc, .pdf, and .dll.

To access this feature, the endpoint must have the AntiVirus feature installed. When configuring a deployment package for endpoints desired to use cloud-based threat detection, ensure that you enable *AntiVirus* and *Cloud Based Malware Outbreak Detection*.

To configure cloud-based threat detection in the EMS GUI:

1. In EMS, go to *Endpoint Profiles*. Select the desired profile.
2. On the *Malware Protection* tab, enable *Cloud Based Malware Detection*.

To configure cloud-based threat detection by configuring the XML file:

You can configure more advanced options by editing the XML configuration file. You can configure the timeout value, exclusions/exceptions, remediation actions, and events. The following shows a sample XML configuration:

```
<cloudscan>
   <enabled>1</enabled>
   <exceptions>
      <folders>
      </folders>
      <files>
      </files>
      <exclude_files_from_trusted_sources>1</exclude_files_from_trusted_sources>
      <exclude_files_and_folders>0</exclude_files_and_folders>
   </exceptions>
   <response_timeout>5</response_timeout>
   <when>
      <executables_on_removable_media>1</executables_on_removable_media>
      <executables_on_mapped_nw_drives>0</executables_on_mapped_nw_drives>
      <web_downloads>1</web_downloads>
      <email_downloads>1</email_downloads>
   </when>
   <remediation>
      <action>quarantine</action>
      <on_error>allow</on_error>
   </remediation>
</cloudscan>
```

Compliance

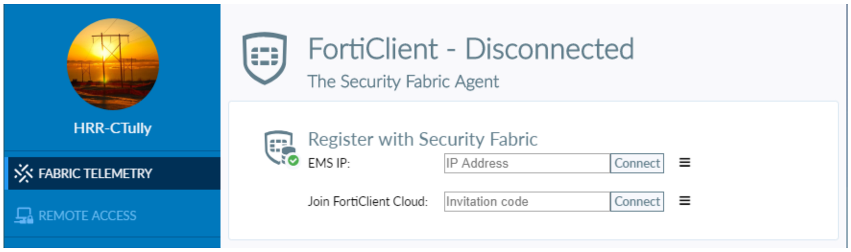
Telemetry connection between FortiClient and FortiOS updates

In 6.2.2, if EMS does not send a Telemetry gateway list to FortiClient, FortiClient does not display options related to FortiGate Telemetry. FortiClient also does not automatically attempt connection to the default gateway when all gateway IP addresses from EMS are not available or reachable.

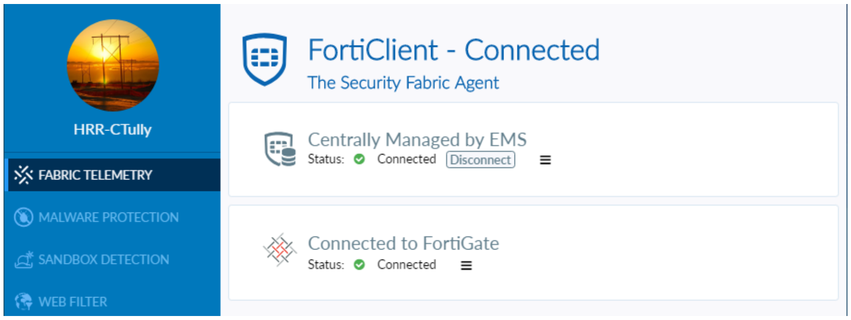
If the administrator configured the FortiClient installer with an on-premise EMS IP address or FortiClient Cloud invitation code, FortiClient automatically connects to either EMS after installation. Otherwise, FortiClient does not automatically connect to any device. The end user must provide an on-premise EMS IP address or FortiClient Cloud invitation code to connect FortiClient to.

The EMS administrator can still create a Telemetry gateway list that includes FortiGate IP addresses. If FortiClient receives the list, it autoconnects to one of the configured FortiGate IP addresses by going through the list, starting with the default gateway, if present. If the EMS administrator removes the Telemetry gateway list, FortiClient disconnects from the FortiGate and remains connected to EMS. If FortiClient is disconnected from EMS, it remains disconnected and does not attempt connection to any device.

The following shows FortiClient when it is first installed and has not connected to EMS. Providing a FortiGate IP address in the *EMS IP* or *Join FortiClient Cloud* field fails to establish a connection.



The following shows FortiClient when it is managed by EMS and connected to a FortiGate. FortiClient has established a connection to the FortiGate using a Telemetry gateway list that EMS has sent to FortiClient via an endpoint policy.



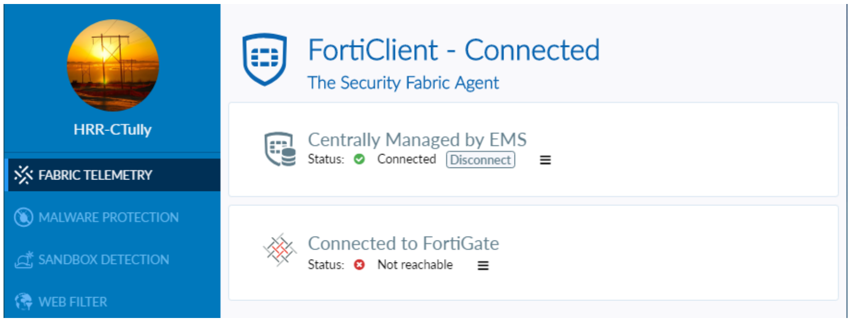
Centrally Managed by EMS

Status: Connected

Connected to FortiGate

Status: Connected

When all FortiGate IP addresses in the received Telemetry gateway list are not reachable or available, FortiClient displays a *Not reachable* status. In this case, FortiClient does not automatically connect to the default gateway.



FortiClient - Connected

The Security Fabric Agent

Centrally Managed by EMS

Status: Connected Disconnect

Connected to FortiGate

Status: Not reachable

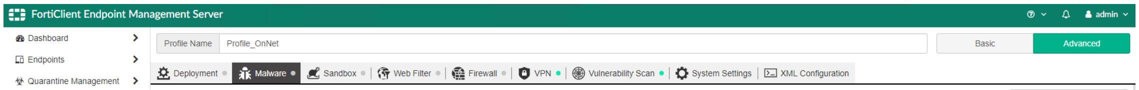
Other

Endpoint profile provisioning based on on-net or off-net status

You can configure an endpoint policy to apply a different profile to the endpoint when it is on-net, compared to when the endpoint is off-net.

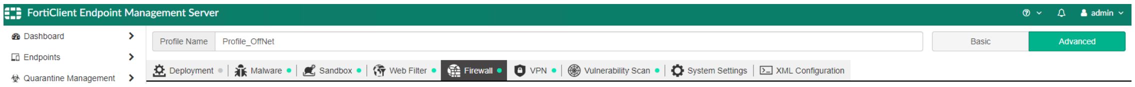
To configure an on-net and off-net profile:

1. Go to *Endpoint Profiles* > *Manage Profiles*. Create a new profile or modify an existing profile to configure the on-net profile. You will configure the policy to apply this profile to endpoints when they are on-net. The example Profile_OnNet profile only has VPN and Vulnerability Scan enabled.



Profile Name: Profile_OnNet

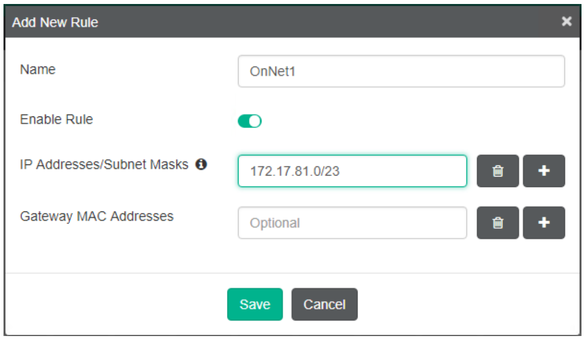
2. Create another profile or modify another existing profile to configure the off-net profile. You will configure the policy to apply this profile to endpoints when they are off-net. The example Profile_OffNet profile has a different feature set enabled than Profile_OnNet: Malware Protection, Sandbox Detection, and Web Filter in addition to VPN and Vulnerability Scan.



Profile Name: Profile_OffNet

To configure an on-net detection rule:

1. Go to *Policy Components* > *On-net Detection Rules*.
2. Click *Add*.
3. In the *Name* field, enter the desired name.
4. Enable the rule by toggling *Enable Rule* on.
5. In the *IP Addresses/Subnet Masks* field, enter the desired values. You can enter multiple values by clicking the + button.
6. (Optional) In the *Gateway MAC Addresses* field, enter the desired values. You can enter multiple values by clicking the + button.
7. Click *Save*. In this example, a policy with this rule set configured will determine an endpoint to be on-net if it is inside the 172.17.81.0/23 subnet.



Name: OnNet1

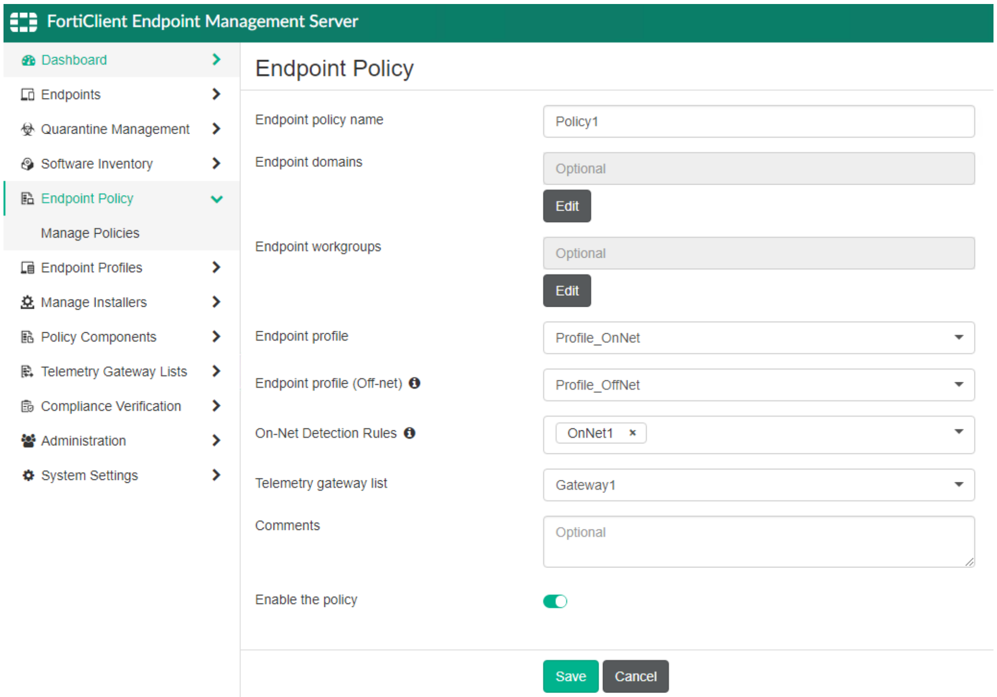
Enable Rule: ●

IP Addresses/Subnet Masks: 172.17.81.0/23

Gateway MAC Addresses: Optional

To configure the endpoint policy:

1. Go to *Endpoint Policy* > *Manage Policies*.
2. Configure the policy:
   1. Click *Add*.
   2. In the *Endpoint Policy Name* field, enter the desired name.
   3. (Optional) In *Endpoint domains*, select the domains to apply the policy to.
   4. (Optional) In *Endpoint workgroups*, select the workgroups of endpoints to apply the policy to.
   5. In *Endpoint Profile*, select an endpoint profile from the dropdown list. This is the on-net profile. In this example, Profile_OnNet is selected.
   6. (Optional) In *Endpoint profile (Off-net)*, select an endpoint profile in the policy to apply to the endpoint when it is off-net according to the on-net detection rules configured in this policy. In this example, Profile_OffNet is selected.
   7. (Optional) In *On-Net Detection Rules*, select the on-net detection rules to include in the policy. In this example, OnNet1 is selected.
   8. (Optional) In *Telemetry gateway list*, select the desired Telemetry gateway list from the dropdown list. You must have already configured a Telemetry gateway list in EMS for this option to be available. See Creating a Telemetry gateway list.
   9. (Optional) In *Comments*, enter any comments.
   10. Enable the policy by toggling *Enable Policy* on.
3. Click *Save*.



Endpoint Policy

Endpoint policy name	Policy1
Endpoint domains	Optional
Endpoint workgroups	Optional
Endpoint profile	Profile_OnNet
Endpoint profile (Off-net)	Profile_OffNet
On-Net Detection Rules	OnNet1 ×
Telemetry gateway list	Gateway1
Comments	Optional
Enable the policy	●

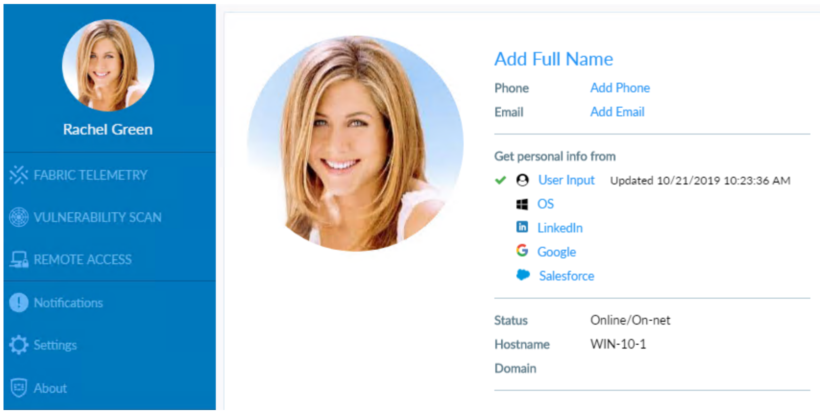
You cannot delete a profile, Telemetry gateway list, or on-net detection rule that is configured as part of a policy. If you attempt to delete such a profile, list, or rule, EMS displays a *Cannot delete an assigned <profile/telemetry gateway list/on-net subnet component>* message.

To delete a profile, list, or rule that is part of a policy, first edit the policy so that it no longer uses that profile, list, or rule, then delete the profile, list, or rule.

To view the results on the endpoint:

The following illustrates the results of configuring an on-net and off-net profile for a policy applied to an endpoint.

In this example, the policy applied to the endpoint does not have on-net detection rules configured. In this case, the endpoint has an online/on-net status and has the feature set enabled in the on-net profile.

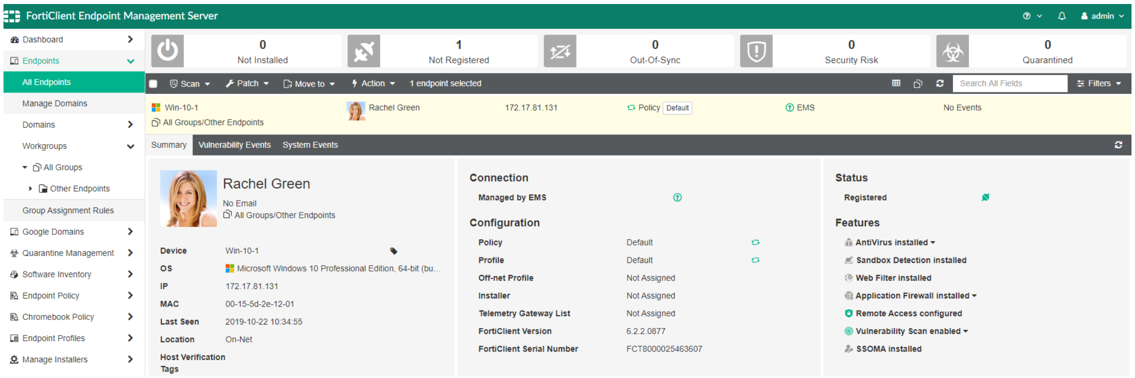


Add Full Name

Phone Add Phone
Email Add Email

Get personal info from
✓ User Input Updated 10/21/2019 10:23:36 AM
OS
LinkedIn
Google
Salesforce

Status Online/On-net
Hostname WIN-10-1
Domain



0 Not Installed | 1 Not Registered | 0 Out-Of-Sync | 0 Security Risk | 0 Quarantined

1 endpoint selected

Win-10-1 | Rachel Green | 172.17.81.131 | Policy Default | EMS | No Events
All Groups/Other Endpoints

Rachel Green
No Email
All Groups/Other Endpoints

Device Win-10-1
OS Microsoft Windows 10 Professional Edition, 64-bit (bu...
IP 172.17.81.131
MAC 00-15-5d-2e-12-01
Last Seen 2019-10-22 10:34:55
Location On-Net
Host Verification Tags

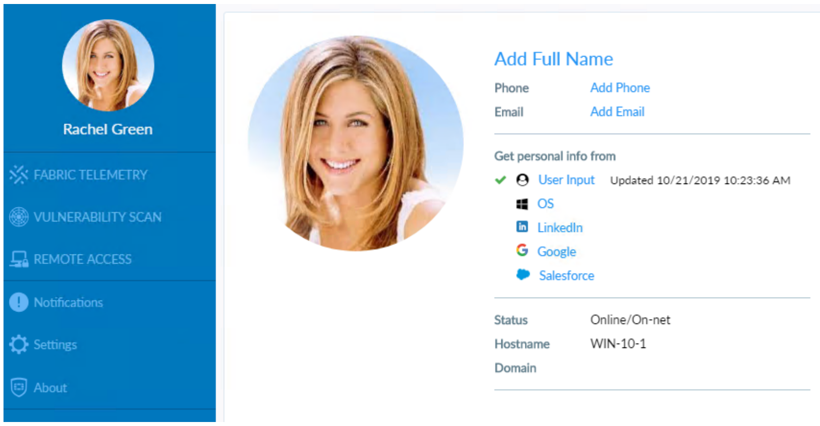
Connection
Managed by EMS

Configuration
Policy Default
Profile Default
Off-net Profile Not Assigned
Installer Not Assigned
Telemetry Gateway List Not Assigned
FortiClient Version 6.2.2.0877
FortiClient Serial Number FCT8000025463607

Status
Registered

Features
AntiVirus installed
Sandbox Detection installed
Web Filter installed
Application Firewall installed
Remote Access configured
Vulnerability Scan enabled
SSOMA installed

In this example, the policy applied to the endpoint has on-net detection rules configured, and on-net and off-net profiles. In this case, the endpoint's IP address is in the configured subnet, so the endpoint has an online/on-net status and the feature set enabled in the on-net profile.

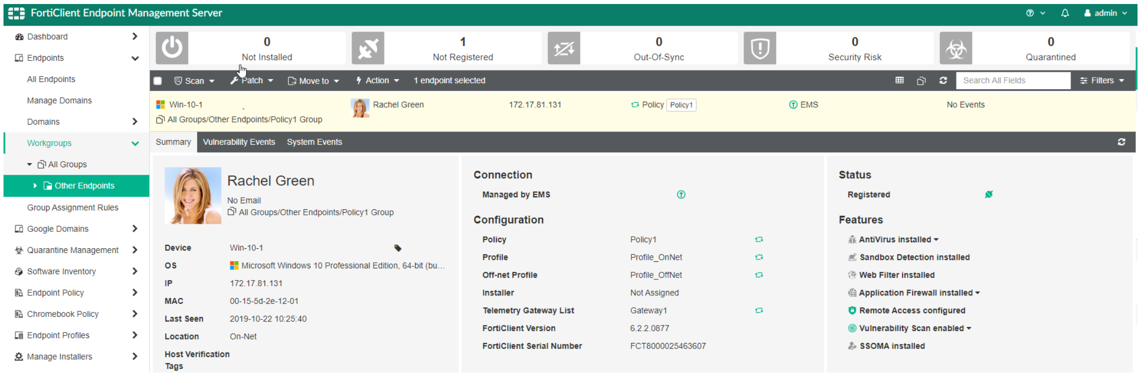


Add Full Name

Phone Add Phone
Email Add Email

Get personal info from
✓ User Input Updated 10/21/2019 10:23:36 AM
OS
LinkedIn
Google
Salesforce

Status Online/On-net
Hostname WIN-10-1
Domain



Win-10-1 · Rachel Green · 172.17.81.131 · Policy Policy1 · EMS · No Events
All Groups/Other Endpoints/Policy1 Group

Rachel Green
No Email
All Groups/Other Endpoints/Policy1 Group

Device	Win-10-1
OS	Microsoft Windows 10 Professional Edition, 64-bit (bu...
IP	172.17.81.131
MAC	00-15-5d-2e-12-01
Last Seen	2019-10-22 10:25:40
Location	On-Net
Host Verification Tags	

Connection

Managed by EMS	

Configuration

Policy	Policy1
Profile	Profile_OnNet
Off-net Profile	Profile_OffNet
Installer	Not Assigned
Telemetry Gateway List	Gateway1
FortiClient Version	6.2.2.0877
FortiClient Serial Number	FCT8000025463607

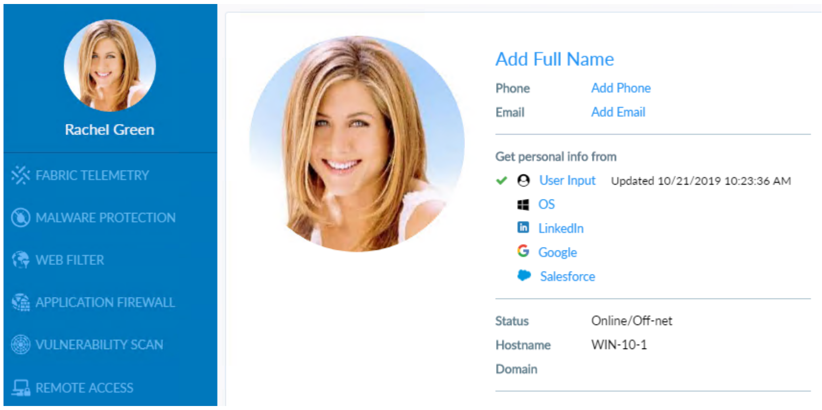
Status

Registered

Features

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

In this case, let's assume that the on-net detection rules have been modified so that endpoints inside the 172.17.93.0/23 subnet are considered-on net, not endpoints inside the 172.17.81.0/23 subnet. The endpoint's IP address, 172.17.81.131, is no longer in the on-net subnet. Therefore, the endpoint has an online/off-net status and the feature set enabled in the off-net profile.

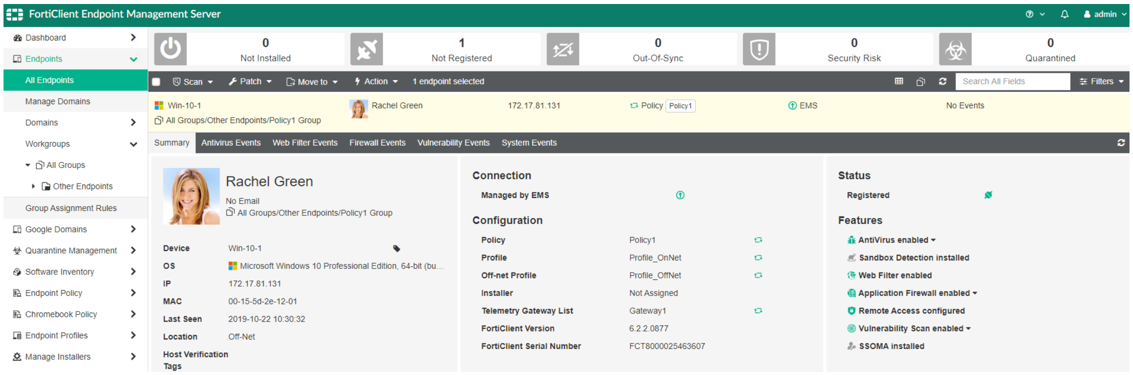


Phone	Add Phone
Email	Add Email

Get personal info from

- ✓ User Input Updated 10/21/2019 10:23:36 AM
- OS
- LinkedIn
- Google
- Salesforce

Status	Online/Off-net
Hostname	WIN-10-1
Domain	



Win-10-1 · Rachel Green · 172.17.81.131 · Policy Policy1 · EMS · No Events
All Groups/Other Endpoints/Policy1 Group

Rachel Green
No Email
All Groups/Other Endpoints/Policy1 Group

Device	Win-10-1
OS	Microsoft Windows 10 Professional Edition, 64-bit (bu...
IP	172.17.81.131
MAC	00-15-5d-2e-12-01
Last Seen	2019-10-22 10:30:32
Location	Off-Net
Host Verification Tags	

Connection

Managed by EMS	

Configuration

Policy	Policy1
Profile	Profile_OnNet
Off-net Profile	Profile_OffNet
Installer	Not Assigned
Telemetry Gateway List	Gateway1
FortiClient Version	6.2.2.0877
FortiClient Serial Number	FCT8000025463607

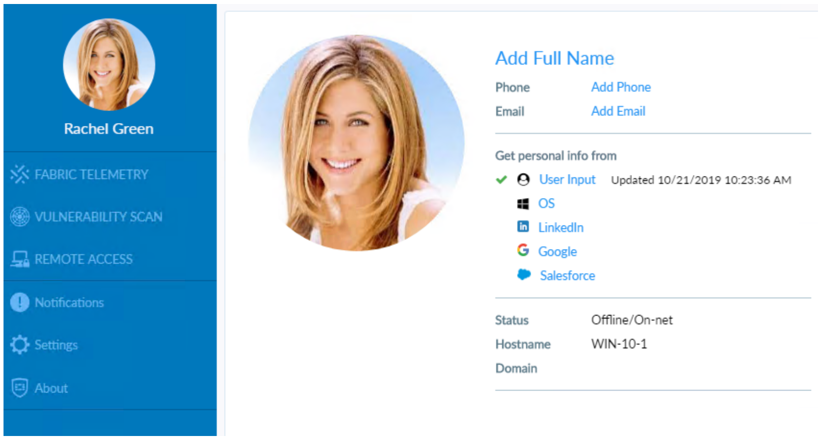
Status

Registered

Features

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

In this case, let's assume that the on-net detection rules have been modified so that endpoints inside the 172.17.81.0/23 subnet are considered on-net. The endpoint's IP address, 172.17.81.131, is in the configured subnet, but the endpoint now cannot connect Telemetry to EMS. The endpoint has an offline/on-net status and EMS displays its location as unavailable.



Add Full Name

Phone Add Phone

Email Add Email

Get personal info from

✓ User Input Updated 10/21/2019 10:23:36 AM

OS

LinkedIn

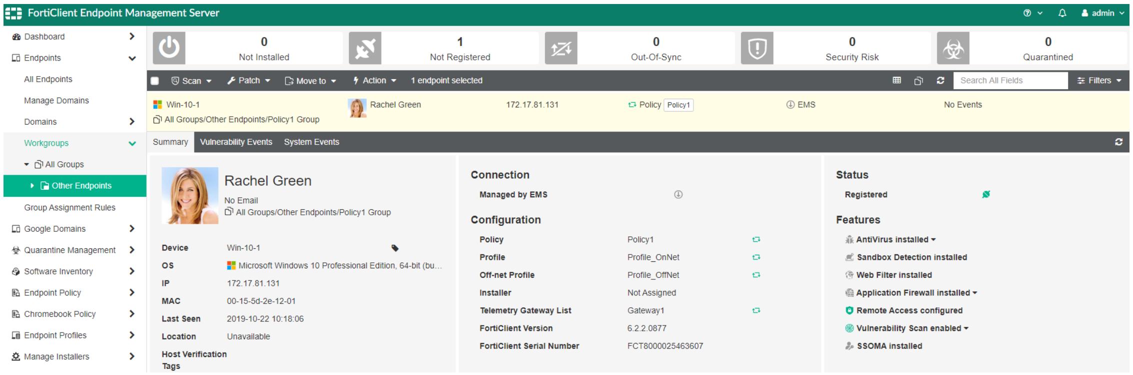
Google

Salesforce

Status Offline/On-net

Hostname WIN-10-1

Domain



0 Not Installed | 1 Not Registered | 0 Out-Of-Sync | 0 Security Risk | 0 Quarantined

1 endpoint selected

Win-10-1 Rachel Green 172.17.81.131 Policy Policy1 EMS No Events

All Groups/Other Endpoints/Policy1 Group

Rachel Green

No Email

All Groups/Other Endpoints/Policy1 Group

Device Win-10-1

OS Microsoft Windows 10 Professional Edition, 64-bit (bu...

IP 172.17.81.131

MAC 00-15-5d-2e-12-01

Last Seen 2019-10-22 10:18:06

Location Unavailable

Host Verification

Tags

Connection

Managed by EMS

Configuration

Policy Policy1

Profile Profile_OnNet

Off-net Profile Profile_OffNet

Installer Not Assigned

Telemetry Gateway List Gateway1

FortiClient Version 6.2.2.0877

FortiClient Serial Number FCT8000025463607

Status

Registered

Features

AntiVirus installed

Sandbox Detection installed

Web Filter installed

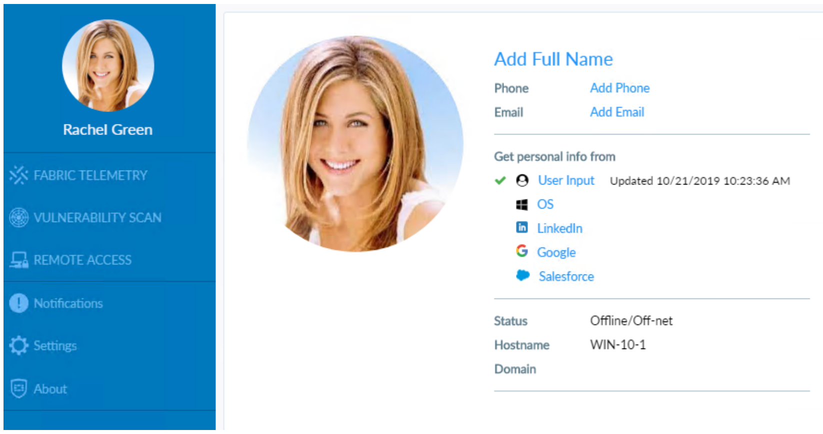
Application Firewall installed

Remote Access configured

Vulnerability Scan enabled

SSOMA installed

Let's modify the on-net detection rules again so that endpoints inside the 172.17.93.0/23 subnet are considered on-net. In this case, the endpoint's IP address, 172.17.81, 131, is not in the configured subnet and the endpoint cannot connect Telemetry to EMS. The endpoint has an offline/off-net status and EMS displays its location as unavailable.



Add Full Name

Phone Add Phone

Email Add Email

Get personal info from

✓ User Input Updated 10/21/2019 10:23:36 AM

OS

LinkedIn

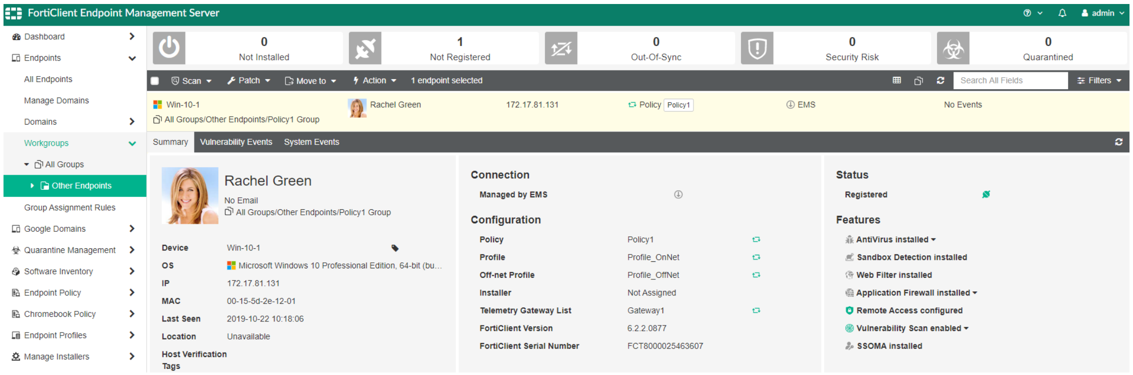
Google

Salesforce

Status Offline/Off-net

Hostname WIN-10-1

Domain



Win-10-1 | Rachel Green | 172.17.81.131 | Policy Policy1 | EMS | No Events
All Groups/Other Endpoints/Policy1 Group

Rachel Green
No Email
All Groups/Other Endpoints/Policy1 Group

Device Win-10-1
OS Microsoft Windows 10 Professional Edition, 64-bit (bu...
IP 172.17.81.131
MAC 00-15-5d-2e-12-01
Last Seen 2019-10-22 10:18:06
Location Unavailable
Host Verification Tags

Connection
Managed by EMS

Configuration
Policy Policy1
Profile Profile_OnNet
Off-net Profile Profile_OffNet
Installer Not Assigned
Telemetry Gateway List Gateway1
FortiClient Version 6.2.2.0877
FortiClient Serial Number FCT8000025463607

Status
Registered

Features
AntiVirus installed
Sandbox Detection installed
Web Filter installed
Application Firewall installed
Remote Access configured
Vulnerability Scan enabled
SSOMA installed

Secured FortiGuard communication

You can now configure FortiGuard Anycast to encrypt communication between FortiClient and a specified FortiGuard Distribution Server (FDS) or your own FortiManager. You can also specify that FortiClient can only receive updates from an FDS located in the specified region: global, U.S, or Europe. You can also configure FortiClient Web Filter to query an Anycast ratings server.

The U.S. and EU Anycast servers are currently unavailable.

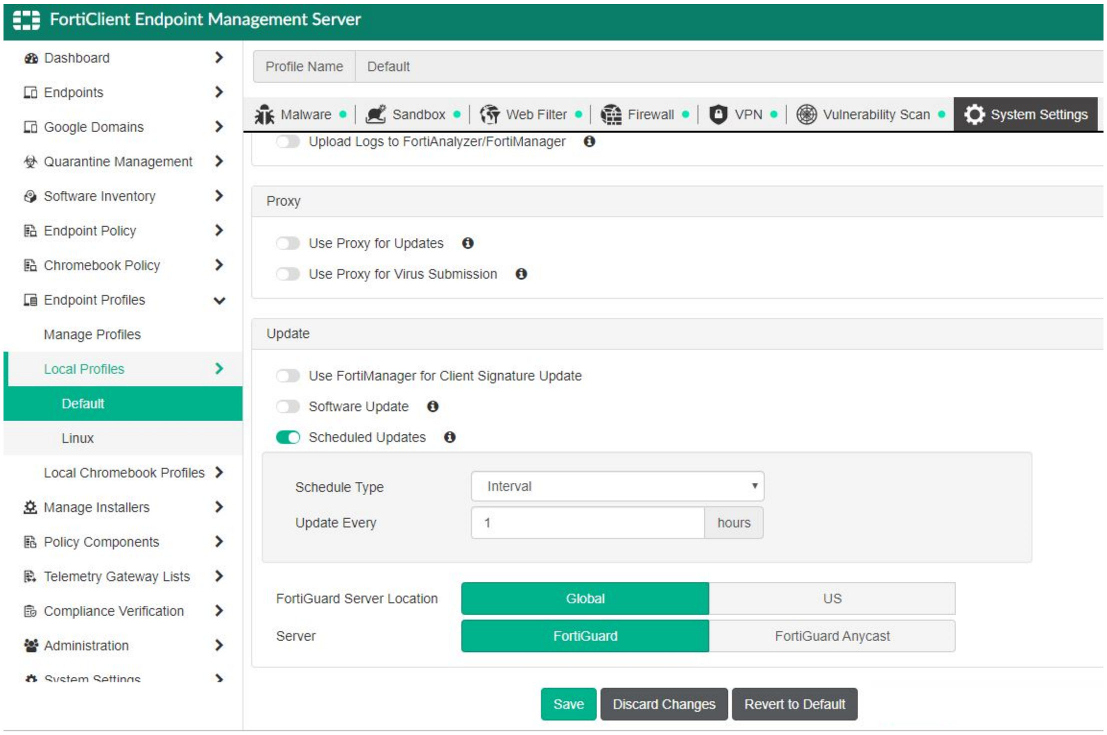
To configure communication to an Anycast FDS server:

You can configure FortiClient to receive engine and signature updates from an Anycast server using HTTPS on port 443.

1. In EMS, go to *Endpoint Profiles*, then select the desired profile.
2. On the *System Settings* tab, under *Update*, select the desired *FortiGuard Server Location*:

Option	Server
Global	fctupdate.fortinet.net
US	fctusupdate.fortinet.net
EU	fcteuupdate.fortinet.net

3. For *Server*, select *FortiGuard Anycast*. Click *Save*.



Profile Name: Default

Upload Logs to FortiAnalyzer/FortiManager

Proxy

Use Proxy for Updates

Use Proxy for Virus Submission

Update

Use FortiManager for Client Signature Update

Software Update

Scheduled Updates

Schedule Type: Interval

Update Every: 1 hours

FortiGuard Server Location: Global | US

Server: FortiGuard | FortiGuard Anycast

After receiving the updated profile from EMS, FortiClient communicates with the configured Anycast server (in this example, the global server at fctupdate.fortinet.net) to receive engine and signature updates using HTTPS on port 443. The end user can trigger a check for updates on the *About* tab in FortiClient. The following shows a sample update log from FortiClient (Linux):

```
20191022 11:08:00.870 [update:INFO] main:219
20191022 11:08:00.870 [update:INFO] main:220 ****************Update starting***************
...
20191022 11:08:00.913 [update:INFO] fcn_upgrade:1515 log_level: 7
20191022 11:08:00.913 [update:INFO] fcn_upgrade:1518 Enable custom fds server :80 failover
     port: 8000 failover to fdg: 1 allow sw update: 0
20191022 11:08:00.913 [update:INFO] main:246 Updating FCTDATA: Update started forced update
20191022 11:08:02.388 [update:INFO] fcn_upgrade:659 Getting current FortiClient Components
     information
20191022 11:08:02.392 [update:INFO] fcn_upgrade:694 current av engine version: 6.2.137
...
20191022 11:08:02.392 [update:INFO] fcn_upgrade:711 current av main sig full version:
     72.1515
...
20191022 11:08:02.392 [update:INFO] fcn_upgrade:728 current av ext sig full version:
     72.1426
...
20191022 11:08:02.401 [update:INFO] fcn_upgrade:756 vcm engine version 2.23
20191022 11:08:03.853 [update:INFO] fcn_upgrade:772 vcm signature version 1.44
20191022 11:08:03.862 [update:INFO] fcn_upgrade:112 firmware: FCT100-FW-6.2.2-297
20191022 11:08:03.862 [update:INFO] fcn_upgrade:128 uid: 0158520161
20191022 11:08:03.862 [update:INFO] fcn_upgrade:141 RegisteredSN: FCTEMS0000099301
20191022 11:08:03.862 [update:INFO] fcn_upgrade:156 sn: FCT8001517749550
20191022 11:08:03.862 [update:INFO] fcn_upgrade:161 uid2: F7D78575DD444792814EDD6B3D3C9201
20191022 11:08:03.862 [update:INFO] fcn_upgrade:175 Name: lo
20191022 11:08:03.862 [update:INFO] fcn_upgrade:175 Name: ens160
```

```
20191022 11:08:03.862 [update:INFO] fcn_upgrade:175 Name: lo
20191022 11:08:03.862 [update:INFO] fcn_upgrade:175 Name: ens160
20191022 11:08:03.862 [update:INFO] fcn_upgrade:188 Found host IP: 172.17.60.133
20191022 11:08:03.879 [update:INFO] fcn_upgrade:205 path: Ubuntu 18.04.1 LTS
20191022 11:08:03.879 [update:INFO] fcn_upgrade:216 os: Linux (Ubuntu 18.04.1 LTS)
20191022 11:08:03.879 [update:INFO] fcn_upgrade:220 language: en
20191022 11:08:03.880 [update:INFO] update_funcs:322 Try to connect to server
      forticlient.fortinet.net:80
20191022 11:08:03.880 [update:DEBG] fr_comm:604 sock_connect_s: host:
      forticlient.fortinet.net, port: 80
20191022 11:08:03.882 [update:DEBG] fcp:886 atributes size: 387, packobj size: 520
...
20191022 11:08:03.884 [update:INFO] fcn_upgrade:786 Start to download FortiClient
      components...
20191022 11:08:03.884 [update:INFO] update_funcs:322 Try to connect to server
      forticlient.fortinet.net:80
20191022 11:08:03.884 [update:DEBG] fr_comm:604 sock_connect_s: host:
      forticlient.fortinet.net, port: 80
20191022 11:08:03.885 [update:DEBG] fcp:886 atributes size: 560, packobj size: 696
...
20191022 11:08:03.886 [update:INFO] fcn_upgrade:832 no new vcm avaliable in FDS.
20191022 11:08:03.886 [update:INFO] fcn_upgrade:849 no new vcm signature avaliable in FDS.
20191022 11:08:03.886 [update:INFO] fcn_upgrade:880 no new av engine avaliable in FDS
20191022 11:08:03.886 [update:INFO] fcn_upgrade:910 no new av main signature avaliable in
      FDS
20191022 11:08:03.886 [update:INFO] fcn_upgrade:972 no new av ext signature avaliable in
      FDS
20191022 11:08:04.383 [update:INFO] fcn_upgrade:1178 Removing temp file
...
20191022 11:08:04.385 [update:INFO] main:257 Updating FCTDATA: Update finished
20191022 11:08:05.473 [update:INFO] main:259 Downloading done ret = 0
20191022 11:09:04.510 [update:INFO] main:219
```

To configure communication to a legacy FDS server:

You can configure FortiClient to receive engine and signature updates from a legacy FDS server using HTTP on port 80. There are currently two legacy FDS servers: global (default) and US.

1. In EMS, go to *Endpoint Profiles*, then select the desired profile.
2. On the *System Settings* tab, under *Update*, select the desired *FortiGuard Server Location*:

Option	Server
Global	forticlient.fortinet.net Default FDS server for FortiClient.
US	usforticlient.fortinet.net

3. For *Server*, select *FortiGuard*. Click *Save*. After receiving the updated profile from EMS, FortiClient communicates with the configured legacy server to receive engine and signature updates using HTTP on port 80. The end user can trigger a check for updates on the *About* tab in FortiClient. The following shows a sample update log from FortiClient (Linux):

```
20191022 11:06:57.515 [update:INFO] main:217
20191022 11:06:57.515 [update:INFO] main:218 ***************Update starting**************
...
20191022 11:06:57.529 [update:INFO] fcn_upgrade:1540 log_level: 7
```

```
20191022 11:06:57.529 [update:INFO] fcn_upgrade:1546 Enable custom fds server :80 failover
     port: 8000 failover to fdg: 1 allow sw update: 0
20191022 11:06:57.529 [update:INFO] main:243 Updating FCTDATA: Update started forced update
20191022 11:06:58.741 [update:INFO] fcn_upgrade:664 Getting current FortiClient Components
     information
20191022 11:06:58.773 [update:INFO] fcn_upgrade:713 current av engine version: 6.2.137
...
20191022 11:06:58.773 [update:INFO] fcn_upgrade:732 current av main sig full version:
     72.1515
...
20191022 11:06:58.773 [update:INFO] fcn_upgrade:751 current av ext sig full version:
     72.1426
...
20191022 11:06:58.773 [update:INFO] fcn_upgrade:776 vcm engine version 2.23
20191022 11:07:00.340 [update:INFO] fcn_upgrade:791 vcm signature version 1.44
20191022 11:07:00.353 [update:INFO] fcn_upgrade:116 firmware: FCT100-FW-6.2.2-297
20191022 11:07:00.353 [update:INFO] fcn_upgrade:130 uid: 0158520161
20191022 11:07:00.353 [update:INFO] fcn_upgrade:144 RegisteredSN: FCTEMS0000099301
20191022 11:07:00.353 [update:INFO] fcn_upgrade:159 sn: FCT8001517749550
20191022 11:07:00.354 [update:INFO] fcn_upgrade:164 uid2: F7D78575DD444792814EDD6B3D3C9201
20191022 11:07:00.354 [update:INFO] fcn_upgrade:178 Name: lo
20191022 11:07:00.354 [update:INFO] fcn_upgrade:178 Name: ens160
20191022 11:07:00.354 [update:INFO] fcn_upgrade:178 Name: lo
20191022 11:07:00.354 [update:INFO] fcn_upgrade:178 Name: ens160
20191022 11:07:00.354 [update:INFO] fcn_upgrade:187 Found host IP: 172.17.60.133
20191022 11:07:00.378 [update:INFO] fcn_upgrade:206 path: Ubuntu 18.04.1 LTS
20191022 11:07:00.378 [update:INFO] fcn_upgrade:217 os: Linux (Ubuntu 18.04.1 LTS)
20191022 11:07:00.378 [update:INFO] fcn_upgrade:221 language: en
20191022 11:07:00.378 [update:INFO] fcn_upgrade:804 Start to download FortiClient
     components...
20191022 11:07:00.378 [update:INFO] update_funcs:307 Try to connect to server
     fctupdate.fortinet.net:443
20191022 11:07:00.430 [update:DEBG] fcp:844 atributes size: 560, packobj size: 696
...
20191022 11:07:00.651 [update:INFO] fcn_upgrade:851 no new vcm avaliable in FDS.
20191022 11:07:00.651 [update:INFO] fcn_upgrade:856 Download vcm successfully.
20191022 11:07:00.651 [update:INFO] fcn_upgrade:861 new vcm signature
     /tmp/.forticlient/update//obj_1_mcDB4W__unpacked.
20191022 11:07:02.135 [update:INFO] fcn_upgrade:864 new vcm signature version is 1.44.
20191022 11:07:02.136 [update:INFO] fcn_upgrade:898 no new av engine avaliable in FDS
20191022 11:07:02.136 [update:INFO] fcn_upgrade:928 no new av main signature avaliable in
     FDS
20191022 11:07:02.136 [update:INFO] fcn_upgrade:989 no new av ext signature avaliable in
     FDS
20191022 11:07:02.741 [update:INFO] fcn_upgrade:1196 Removing temp file
20191022 11:07:02.745 [update:INFO] main:108 sandbox server not configured.
...
20191022 11:07:04.282 [update:INFO] main:257 Downloading done ret = 0
20191022 11:08:00.870 [update:INFO] main:217
```

To configure communication to FortiManager for engine and signature updates:

1. In EMS, go to *Endpoint Profiles*, then select the desired profile.
2. On the *System Settings* tab, under *Update*, enable *Use FortiManager for Client Signature Update*.
3. In the *IP Address/Hostname* field, enter the FortiManager IP address or hostname.
4. In the *Port* field, enter the port number that FortiClient uses to communicate with FortiManager.

5. In the *Failover Port* field, enter the port number that FortiClient uses to communicate with FortiManager in the event of a failover.
6. In the *Timeout* field, enter the timeout interval in seconds.
7. (Optional) Enable *Failover to FDN When FortiManager Is Not Available*. You can configure an Anycast or legacy server as the failover server. Click *Save*. After receiving the updated profile from EMS, FortiClient communicates with the configured FortiManager to receive engine and signature updates using port 80. If FortiClient does not receive any response from FortiManager, it attempts connection to FortiManager using port 8000. If FortiClient still cannot connect to FortiManager, it connects to the configured FDN server. The end user can trigger a check for updates on the *About* tab in FortiClient.

To configure communication to an Anycast ratings server:

You can configure FortiClient Web Filter to query the Anycast ratings server for the categories of requested URLs using HTTPS on port 443.

1. In EMS, go to *Endpoint Profiles*, then select the desired profile.
2. On the *Web Filter* tab, under *Site Categories*, select the desired *FortiGuard Server Location*:

Option	Server
Global	fctguard.fortinet.net
US	fctusguard.fortinet.net
EU	fcteuguard.fortinet.net

3. For *Server*, select *FortiGuard Anycast*. Click *Save*. After receiving the updated profile from EMS, FortiClient queries the configured Anycast ratings server to receive categories of requested URLs using HTTPS on port 443.

To configure communication to a legacy ratings server:

You can configure FortiClient Web Filter to query a legacy ratings server for the categories of requested URLs using UDP on port 8888.

1. In EMS, go to *Endpoint Profiles*, then select the desired profile.
2. On the *Web Filter* tab, under *Site Categories*, select the desired *FortiGuard Server Location*:

Option	Server
Global	fgd1.fortigate.com
US	usfgd1.fortigate.com

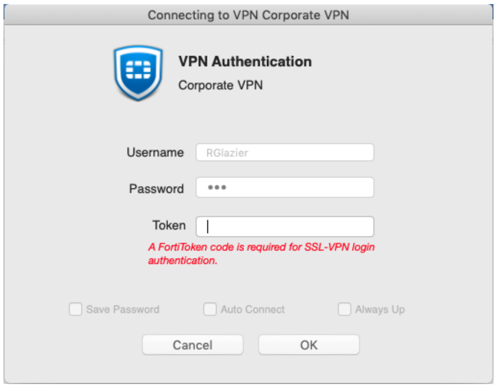
3. For *Server*, select *FortiGuard*. Click *Save*. After receiving the updated profile from EMS, FortiClient queries the configured legacy ratings server to receive categories of requested URLs using UDP on port 8888.

FortiClient (macOS) VPN connection with FortiToken Mobile

Improvements have been made to the FortiClient (macOS) GUI when connecting SSL VPN using FortiToken Mobile (FTM) two-factor authentication (2FA). In the following example, a FortiClient endpoint connects via SSL VPN to a FortiGate with FTM AutoPush enabled.

For an SSL VPN user with FortiToken 2FA enabled, the SSL VPN connection prompt no longer displays an *FTM push* button. You can proceed with the VPN connection in one of the following ways:

- In the *Connecting to VPN* dialog, manually enter the FortiToken. Click *OK*.



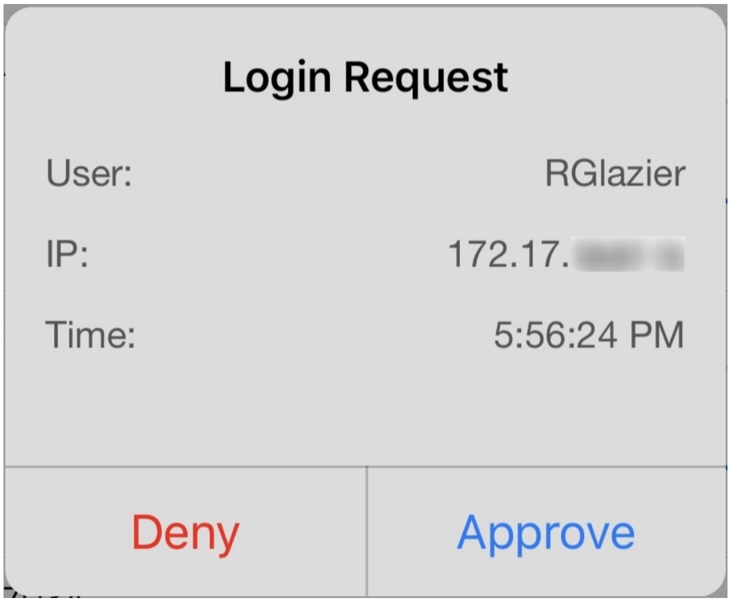
Username: RGlazier

Password: •••

Token:

A FortiToken code is required for SSL-VPN login authentication.

- On your mobile device, select *Approve* on the push notification that you received via your FTM application.



User: RGlazier

IP: 172.17.[redacted]

Time: 5:56:24 PM

FortiClient sends the token to the FortiGate and the VPN connection establishes successfully.

To configure FortiOS:

The WAN interface is the interface connected to ISP. This example shows a configuration for static mode. You can also use DHCP or PPPoE mode. This example establishes the SSL VPN connection over the WAN interface.

1. In the FortiOS GUI, configure the interface and firewall address. The port1 interface connects to the internal network:
   a. Go to *Network > Interfaces* and edit the wan1 interface.
   b. Set *IP/Network Mask* to 172.20.120.123/255.255.255.0.
   c. Edit the port1 interface and set *IP/Network Mask* to 192.168.1.99/255.255.255.0.
   d. Click *OK*.
   e. Go to *Firewall & Objects > Address*. Create an address for the Internet subnet 192.168.1.0.

2. Register the FortiGate for FortiCare Support. To add or download a mobile token on the FortiGate, you must register the FortiGate for FortiCare Support. If your FortiGate is registered, go to step 3.
   1. Go to *Dashboard > Licenses*.
   2. Hover the cursor on *FortiCare Support* to check if the FortiGate is registered for FortiCare. If not, click *FortiCare Support*, then click *Register*.
3. Add FTM to the FortiGate. If your FortiGate has FortiToken installed, go to step 4.
   1. Go to *User & Device > FortiTokens*. Click *Create New*.
   2. Select *Mobile Token*.
   3. In the *Activation Code* field, enter the activation code.
   4. Every FortiGate has two free mobile tokens. Go to *User & Device > FortiTokens* and click *Import Free Trial Tokens*.
4. In the FortiOS CLI, enable FTM push. Ensure that server-ip is reachable from the Internet, then enter the following CLI commands:

```
config system ftm-push
   set server-ip 172.20.120.123
   set status enable
end
```

Change log

Date	Change Description
2019-11-04	Initial release.
2019-11-18	Added Managing endpoints with FortiClient Cloud on page 4, Dynamically group endpoints based on user identity on page 17, and Secured FortiGuard communication on page 32.
2019-11-19	Added Cloud-based threat detection on page 23.
2019-12-19	Added Using certificate Fabric authentication on page 14.
2020-02-26	Added FortiClient (macOS) VPN connection with FortiToken Mobile on page 36.