



FortiClient & FortiClient EMS - New Features Guide

Version 6.4

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



June 05, 2025

FortiClient & FortiClient EMS 6.4 New Features Guide

04-640-630513-20250605

TABLE OF CONTENTS

Overview	4
Security-driven networking	5
SAML support for SSL VPN	5
Zero-trust network access	8
Endpoint: Fabric Agent	8
Identity compliance	8
Endpoint quarantine for Linux	9
Collecting and sending macOS host events to FortiAnalyzer 6.4.1	11
Expanded on-fabric detection rules 6.4.2	11
Compliance verification terminology renamed to Zero Trust 6.4.2	15
Endpoint: Remote Access	16
Selecting closest gateway for VPN connection 6.4.1	16
Application-based split tunnel 6.4.2	18
Backup VPN connection 6.4.3	22
Secure remote access compliance enforcement 6.4.4	23
Endpoint: Endpoint Security	27
FortiSandbox Cloud support for macOS	27
Keyword block support	29
Client handling for HTTPS (browser plugin) for Microsoft Edge browser 6.4.2	30
Malware Protection and Sandbox Detection enhancements 6.4.2	31
Blocking removable devices by class ID 6.4.2	33
FortiClient (Windows) moderate and strict Safe Search levels support 6.4.2	35
FortiClient EMS	38
ZTNA	38
User-based management	38
Customize EMS console UI 6.4.1	39
Enhanced visibility into endpoint 6.4.1	45
Endpoint classification tags 6.4.1	46
Sending upstream connection information for FortiClient (macOS) off-Fabric connections 6.4.2	49
FortiGuard Outbreak Alerts service 6.4.4	50
EMS free trial license endpoint number change	51
Air-gapped network support 6.4.3	51
Index	53
6.4.0	53
6.4.1	53
6.4.2	53
6.4.3	53
6.4.4	54
Change log	55

Overview

This guide provides details of new features introduced in FortiClient & FortiClient EMS 6.4. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable. The guide organizes features into the following sections:

- [Security-driven networking on page 5](#)
- [Zero-trust network access on page 8](#)
 - [Endpoint: Fabric Agent on page 8](#)
 - [Endpoint: Remote Access on page 16](#)
 - [Endpoint: Endpoint Security on page 27](#)
- [FortiClient EMS on page 38](#)
 - [ZTNA on page 38](#)

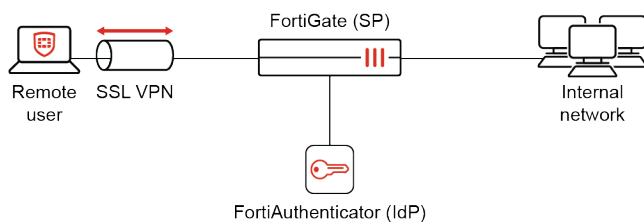
For features introduced in 6.4.1 and later versions, the version number is found at the end of the topic heading. For example, [Expanded on-fabric detection rules 6.4.2 on page 11](#) was introduced in 6.4.2. If a topic heading has no version number at the end, the feature was introduced in 6.4.0.

For a list of all features organized by the version number that they were introduced, see [Index on page 53](#).

Security-driven networking

SAML support for SSL VPN

FortiClient (Windows) 6.4.0 supports SAML authentication for SSL VPN. FortiClient (Windows) can use a SAML identity provider (IdP) to authenticate an SSL VPN connection. You can configure a FortiGate as a service provider (SP) and a FortiAuthenticator or FortiGate as an IdP. The end user uses FortiClient with the SAML single sign on (SSO) option to establish an SSL VPN tunnel to the FortiGate.



This process is as follows:

1. The EMS administrator or end user configures an SSL VPN connection with SAML SSO enabled.
2. FortiClient (Windows) connects to the FortiGate.
3. The FortiGate returns a redirect link to the SAML IdP authorization page.
4. FortiClient (Windows) displays the IdP authorization page in an embedded browser window.
5. The end user enters their credentials in the window to log in.
6. Once the login attempt succeeds, FortiClient (Windows) establishes a tunnel to the FortiGate.

This example configures a FortiGate as the SP and FortiAuthenticator as the IdP.

To configure the FortiGate as the SP:

1. Configure the FortiGate SP to be a SAML user. You must configure the IdP remote certificate from FortiAuthenticator on the FortiGate:

```
config user saml
  edit "saml-user"
    set cert "Fortinet_Factory"
    set entity-id "http://172.17.61.59:11443/remote/saml/metadata/"
    set single-sign-on-url "https://172.17.61.59:11443/remote/saml/login/"
    set single-logout-url "https://172.17.61.59:11443/remote/saml/logout/"
    set idp-entity-id "http://172.17.61.118:443/saml-idp/101087/metadata/"
    set idp-single-sign-on-url "https://172.17.61.118:443/saml-idp/101087/login/"
    set idp-single-logout-url "https://172.17.61.118:443/saml-idp/101087/logout/"
    set idp-cert "REMOTE_Cert_4"
  next
end
```

2. Add the SAML user to the user group:

```
config user group
  edit "saml_grp"
```

```

        set member "saml-user"
    next
end
3. Set the SAML group in SSL VPN settings:
config vpn ssl settings
    config authentication-rule
        edit 1
            set groups "saml-group"
            set portal "full-access"
        next
    next
end

```

To configure FortiAuthenticator as the IdP:

1. In FortiAuthenticator, go to *Authentication > SAML IdP > Service Providers*.
2. Click *Create New*.
3. Configure as desired, then click *OK*.

The screenshot displays the FortiAuthenticator VM web interface. The left sidebar shows the navigation menu with 'SAML IdP' selected. The main area is titled 'Edit SAML Service Provider'. The configuration fields include:

- SP name: saml_vancouver
- IDP prefix: 101087 [Generate unique prefix]
- IDP certificate: fac118.fct.net | C=CA, ST=British Columbia, L=Burnaby, O=Fortinet, CN=fac118.fct.net
- IDP address: 172.17.61.118:443
- IDP entity id: http://172.17.61.118:443/saml-idp/101087/metadata/
- IDP single sign-on URL: https://172.17.61.118:443/saml-idp/101087/login/
- IDP single logout URL: https://172.17.61.118:443/saml-idp/101087/logout/
- SP entity ID: http://172.17.61.59:11443/remote/saml/metadata/
- SP ACS (login) URL: https://172.17.61.59:11443/remote/saml/login/ [Alternative ACS URLs]
- SP SLS (logout) URL: https://172.17.61.59:11443/remote/saml/logout/
- Authentication method: ☒ Enforce two-factor authentication, ☐ Apply two-factor authentication if available (authenticate any user), ☐ Password-only authentication (exclude users without a password), ☐ FortiToken-only authentication (exclude users without a FortiToken)
- Bypass FortiToken authentication when user is from a trusted subnet [Configure subnets]
- Assertion Attributes: Subject NameID: Username, Format: Unspecified
- SAML Attribute: User Attribute, Actions

The 'Create New' button is visible at the bottom left of the form area.

4. To add a local user, go to *Authentication > User Management > Local User*, then click *Create New*. Configure the local user as desired.
5. To import RADIUS users, go to *Authentication > User Management > Remote User > RADIUS Users*. Import the desired RADIUS server.
6. To import LDAP users, go to *Authentication > User Management > Remote User > LDAP Users*. Import the desired LDAP server.

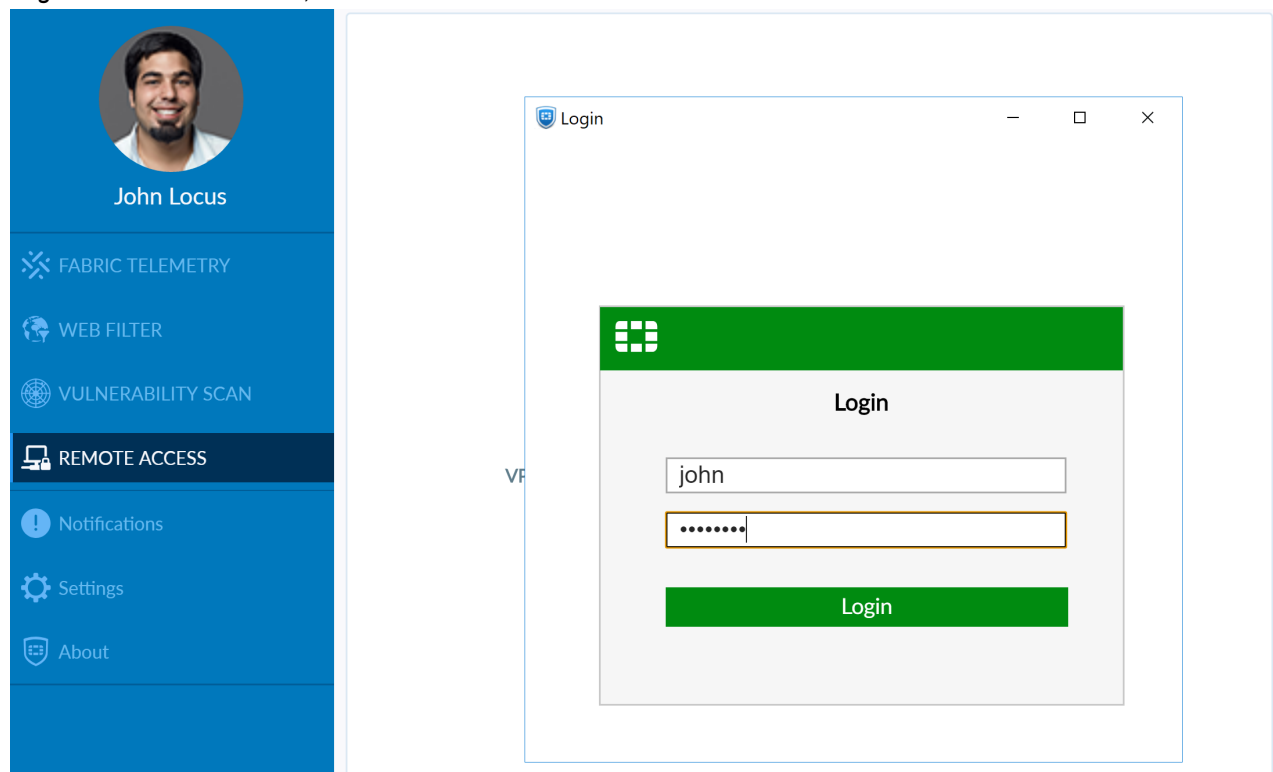
To configure SAML SSO authentication for FortiClient (Windows):

- To configure SAML SSO authentication for a corporate VPN tunnel in EMS, go to *Endpoint Profiles* and select the desired profile. On the *XML Configuration* tab, configure `<sso_enabled>1</sso_enabled>` for the desired tunnel. EMS 6.4.0 does not support GUI implementation for this feature.

- To configure SAML SSO authentication for a personal VPN tunnel in FortiClient (Windows), on the *Remote Access* tab, edit or create a new VPN tunnel. Select the *Enable Single Sign On (SSO) for VPN Tunnel* checkbox.

To connect to a VPN tunnel using SAML authentication:

1. In FortiClient, on the *Remote Access* tab, from the *VPN Name* dropdown list, select the desired VPN tunnel.
2. Click *SAML Login*.
3. FortiClient displays an IdP authorization page in an embedded browser window. Enter your login credentials. Click *Login*. Once authenticated, FortiClient establishes the SSL VPN tunnel.



Zero-trust network access

Endpoint: Fabric Agent

Identity compliance

You can assign different user identification options to different endpoints. These options, visible in FortiClient, include:

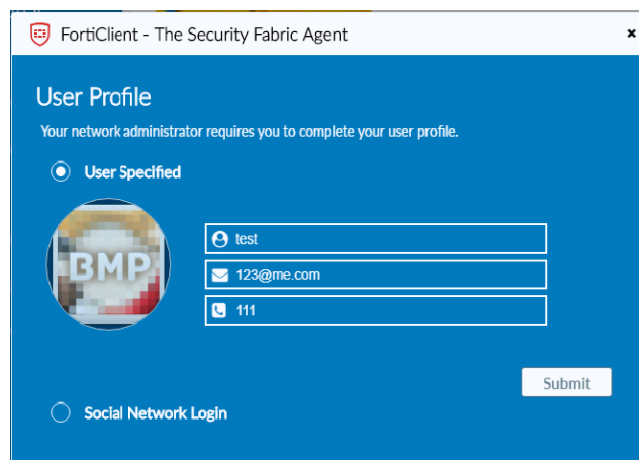
- User Input
- OS
- LinkedIn
- Google
- Salesforce

EMS sends a notification to the endpoint where the user must enter their login information. If the user closes the notification without entering any information, the notification appears again within ten minutes.

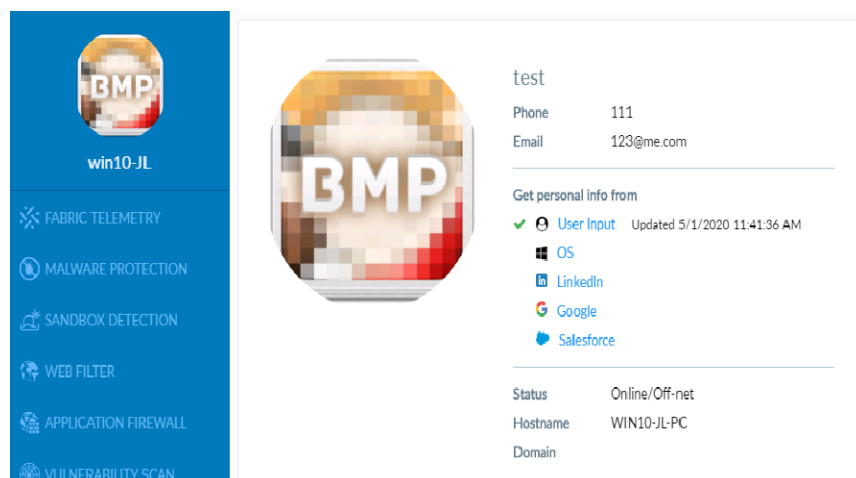
To configure identity compliance:

1. In EMS, go to *Endpoint Profiles*. Select the desired profile, or create a new one.
2. On the *System Settings* tab, under *User Identity Settings*, enable the desired user identification method.
3. If desired, enable *Notify Users to Submit User Identity Information*.
4. Click *Save*.

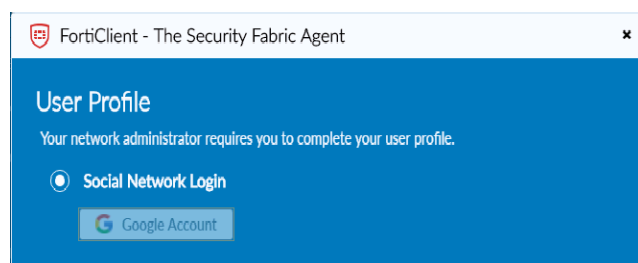
When *Notify Users to Submit User Identity Information* is enabled, the user sees the following notification on the endpoint. If *Manually Enter User Details* is enabled, the user can enter their information manually.



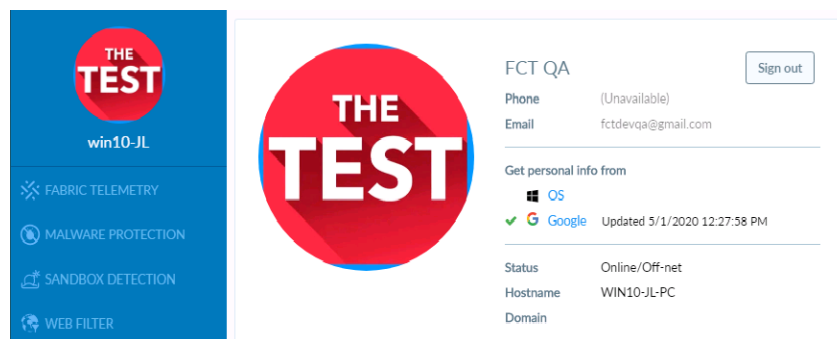
FortiClient displays the entered login information.



If *Google* is enabled, the user can log in to their Google account.



FortiClient displays the Google login information.

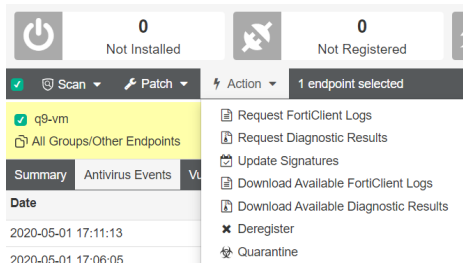


Endpoint quarantine for Linux

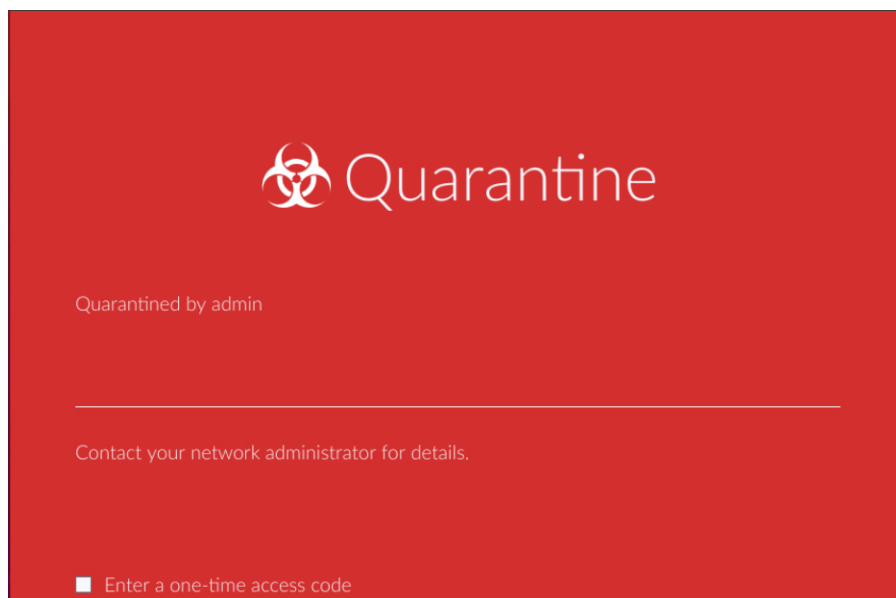
FortiClient & FortiClient EMS 6.4.0 adds quarantine support for FortiClient (Linux). You can quarantine any compromised Linux machine through FortiClient. If a Linux machine is compromised or infected with malicious software, you can isolate the compromised machine by blocking all of the infected machine's network access so that it does not impact other machines or resources on the network.

To quarantine a Linux endpoint:

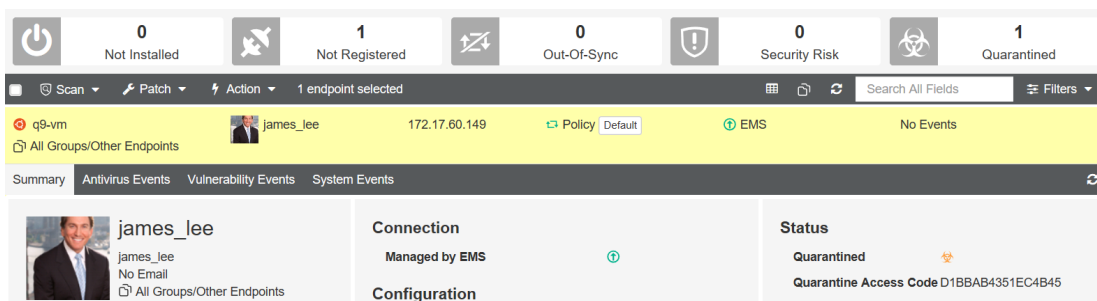
1. In EMS, go to *All Endpoints*, then select the desired endpoint.
2. From the *Action* dropdown list, select *Quarantine*.



After you quarantine the endpoint, FortiClient displays the Quarantine screen and blocks all of the machine's network access. You can also show a customized message on FortiClient when it is quarantined. See [Customizing the endpoint quarantine message](#).



In EMS, the endpoint *Status* on the *Summary* tab changes from *Registered* to *Quarantined*.



After you clear the infected machine of the malicious software or vulnerable application, you can remove the endpoint from quarantine to restore its network connectivity. You can select the endpoint and select *Unquarantine* from the *Actions* dropdown list in EMS, or you can provide the user with the one-time quarantine access code shown on the *Summary* tab in EMS.

Collecting and sending macOS host events to FortiAnalyzer

- 6.4.1

To support lite SIEM functionality for the Fortinet Security Fabric environment, as the Fabric Agent, FortiClient (macOS) collects and sends endpoint host logs (`/var/log/system.log`) to FortiAnalyzer for analysis.

In this configuration, a FortiClient (macOS) endpoint is registered to EMS. FortiAnalyzer has authorized this EMS for log submission. FortiClient (macOS) uploads logs to the FortiAnalyzer as the EMS profile specifies.

To configure this feature in EMS:

1. In EMS, go to *Endpoint Profiles > Manage Profiles*.
2. Select the desired profile.
3. On the *System Settings* tab, enable *Upload Logs to FortiAnalyzer/FortiManager*.
4. Enable *Send OS Events*.
5. In the *IP Address/Hostname* field, enter the FortiAnalyzer IP address.
6. Click *Save*.

The following shows how these logs display in FortiAnalyzer:

The screenshot displays the FortiAnalyzer Log View interface. The top navigation bar shows 'Log View' and 'ADOM: Fabric'. The left sidebar contains a tree view with 'Fabric' expanded, showing 'FortiClient' and 'FortiAnalyzer'. The main content area shows a table of logs with columns: #, Device Name, Serial Number, VDOM, Type, File Name, Size, From, and To. Two logs are visible, both from device 'FCTEMS1187146952'. The first log is 'FCT System Event Elog.log' (4.3k) from 2021-05-07 10:51 to 2021-05-07 10:51. The second log is 'Xlog.log' (12.6k) from 2021-05-07 10:31 to 2021-05-07 10:51.

Below the log table, there is a section for 'SIEM Log of FCTEMS1187146952' with a table showing details for each log entry. The table has columns: #, Date/Time, Registered to Device, UID, Host Name, and FortiClient Source. Five entries are shown, all with a date/time of 11:06:58 and a host name of 'fctqa-mac'. The FortiClient Source is 'MAC' for all entries.

Below the table, there is a 'logDetails' section showing details for the selected log entry. The details include: Date/Time (11:06:58), FortiClient Source (MAC), FortiClientEMS Serial (FCTEMS1187146952), Host Name (fctqa-mac), and Message (May 7 11:06:37 fctqa-mac com.apple.xpc.launchd[1] (com.apple.mdworker.shared.0 6000000-0700-0000-0000-000000000000[51839]): Service exited due to SIGKILL | sent by mds[100]). Other details include Registered to Device (FCTEMS1187146952), Time Stamp (2021-05-07 11:06:58), UID (E9F1B8CC), fct_srctype (sys), and fct_srcver (15.04).

Expanded on-fabric detection rules - 6.4.2

EMS 6.4.2 adds support for eight new on-fabric detection rule types. Earlier EMS versions called on-fabric rules were called on-net detection rules. This enhancement allows you to have greater control over endpoints. You can configure

EMS to apply different profiles to an endpoint depending on its on-/off-fabric status. EMS determines an endpoint's on-/off-fabric status using the following rule types:

- DHCP server
- DNS server
- EMS connection
- Local IP address/subnet
- Default gateway
- Ping server
- Public IP address
- Connection media
- VPN tunnel

The following describes the process for configuring on-fabric detection rules and using them to apply profiles to endpoints:

1. [Configure on-fabric detection rules.](#)
2. Create an on-fabric profile and off-fabric profile.
3. [Create a policy with on-fabric detection rules, an on-fabric profile, and an off-fabric profile.](#)

To configure on-fabric detection rules:

1. Go to *Policy Components > On-fabric Detection Rules*.
2. Click the *Add* button.
3. Configure the *Name*, *Enabled*, and *Comments* fields as desired.
4. Click *Add Rule*.
5. From the *Detection Type* dropdown list, select the desired rule type. Under *Criteria*, AND indicates that the endpoint must meet both criteria for EMS to consider the endpoint as on-fabric. OR indicates that if the endpoint meets any criteria, EMS considers the endpoint as on-fabric. The following describes the rule types:

Rule type	Description
DHCP Server	Configure the IP and/or MAC address or the DHCP code for the desired DHCP server. You can configure just the IP/MAC address, just the DHCP code, or both. If configuring the IP/MAC address, the MAC address is optional.
DNS Server	1. Configure at least one IP address for the desired DNS server. EMS considers the endpoint as satisfying the rule if it is connected to a DNS server that matches the specified configuration. You can configure multiple IP addresses using the + button.
EMS Connection	The only available option for this detection type is that EMS considers the endpoint as satisfying the rule if it is online with EMS.
Local IP/Subnet	Enter an IP address range. Optionally enter the default gateway MAC address. Configuring the MAC address is optional.
Default Gateway	1. Enter the default gateway IP address. Optionally enter the default gateway MAC address.
Ping Server	Enter the server IP address. EMS considers the endpoint as satisfying the rule if it can access the server at the specified IP address. You can configure

Rule type	Description
	multiple addresses using the + button.
Public IP	1. Enter the desired IP address. You can configure multiple addresses using the + button.
Connection Media	1. From the <i>Ethernet</i> and/or <i>Wi-Fi</i> dropdown lists, select <i>Connected</i> or <i>Not Connected</i> .
VPN Tunnel	Enter an SSL or IPsec VPN tunnel name. EMS considers the endpoint as satisfying the rule if it is connected to the VPN tunnel.

6. Click **Save**.

The example shows nine rule sets. If you apply a policy that contains all nine sets to an endpoint, EMS considers the endpoint as on-fabric if it satisfies any set.

On-Fabric Rule Sets				
Name	Enabled			Comments
On-fabric Connection Media	<input checked="" type="checkbox"/>			
On-fabric Default Gateway	<input checked="" type="checkbox"/>			
On-fabric DHCP Server	<input checked="" type="checkbox"/>			
On-fabric DNS Server	<input checked="" type="checkbox"/>			
On-fabric EMS Connection	<input checked="" type="checkbox"/>			
On-fabric Local IP/Subnet	<input checked="" type="checkbox"/>			
On-fabric Ping server	<input checked="" type="checkbox"/>			
On-fabric Public IP	<input checked="" type="checkbox"/>			
On-fabric VPN Tunnel	<input checked="" type="checkbox"/>			

The example shows a rule set that contains two rule types: DHCP server and DNS server. An endpoint must satisfy both rules to satisfy the rule set:

On-Fabric Rule Sets Edit Delete				
Name	Enabled			Comments
On-fabric	<input checked="" type="checkbox"/>			
DHCP Server	<input type="checkbox"/>	IP	192.168.1.1 or 192.168.1.2	
		and		
	<input type="checkbox"/>	MAC	54-b2-03-0a-0b-66	
		or		
	<input type="checkbox"/>	CODE	FCITEMS0117284765	
DNS Server	<input type="checkbox"/>	IP	192.168.1.1	

- The DHCP server rule requires the endpoint to be connected to a DHCP server that has one of the two specified IP addresses (192.168.1.1 or 192.168.1.2) and MAC address (54-b2-03-0a-0b-66), or the specified DHCP code (FCITEMS0117284765).
- The DNS server rule requires the endpoint to be connected to a DNS server that has the specified IP address (192.168.1.1).

The following shows the XML configuration for the same rule set:

```
<forticlient_configuration>
  <version>6.4.1</version>
  <partial_configuration>1</partial_configuration>
  <endpoint_control>
    <onnet_addresses/>
    <onnet_mac_addresses/>
    <onnet_rules>
      <rule_set>
```

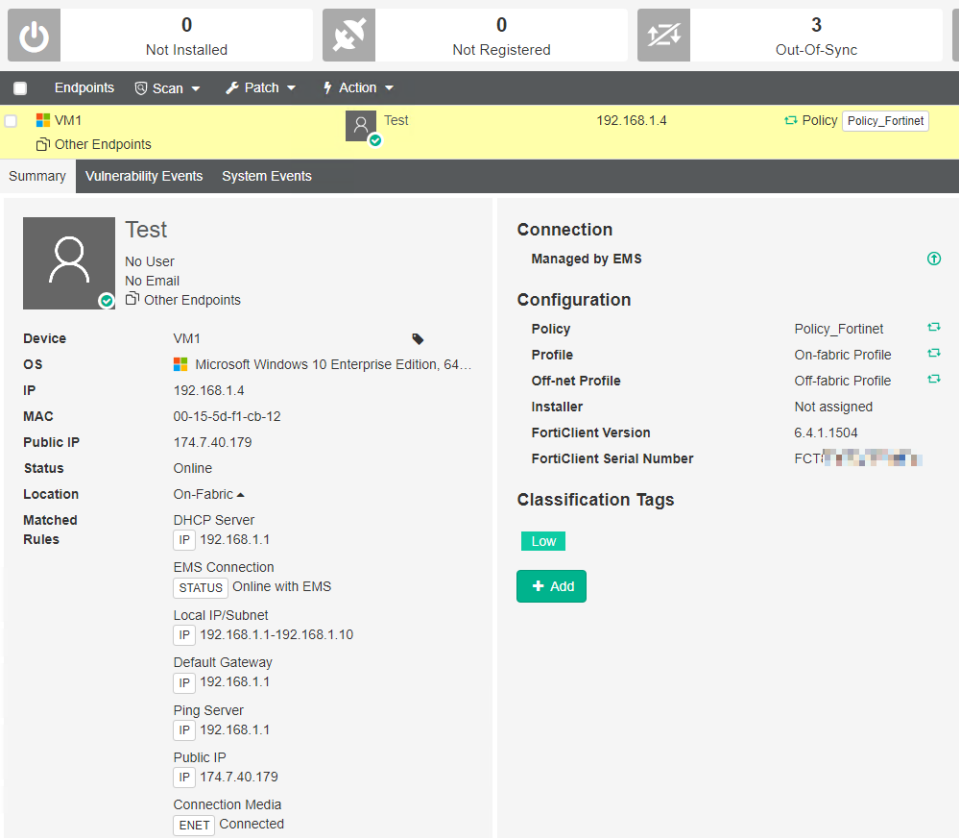
```
<dhcp_server>
  <dhcp_code>
    <criteria id="0">FCTEMS0117284765</criteria>
  </dhcp_code>
  <ip_address>
    <criteria id="1">192.168.1.1</criteria>
    <criteria id="2">192.168.1.2</criteria>
  </ip_address>
  <mac_address>
    <criteria id="3">54-b2-03-0a-0b-66</criteria>
  </mac_address>
</dhcp_server>
<dns_server>
  <ip_address>
    <criteria id="4">192.168.1.1</criteria>
  </ip_address>
</dns_server>
</rule_set>
</onnet_rules>
</endpoint_control>
</forticlient_configuration>
```

To configure a policy with on-fabric detection rules, an on-fabric profile, and an off-fabric profile:

The following steps assume that you have already configured two endpoint profiles.

1. Go to *Endpoint Policy > Manage Policies*.
2. Create a new policy or edit an existing policy.
3. From the *Profile* dropdown list, select the profile to apply to endpoints that are on-fabric.
4. From the *Profile (Off-Fabric)* dropdown list, select the profile to apply to endpoints that are off-fabric.
5. In the *On-Fabric Detection Rules* field, select the desired rules to include in the policy.
6. Click **Save**.

Registered FortiClient endpoints that you have applied this policy to receive both the on-Fabric and off-Fabric profiles. The on-Fabric or off-Fabric profile is applied to the endpoint depending on its on- or off-Fabric status. If you do not define an off-Fabric profile in the applied policy, the on-Fabric profile is applied. The EMS endpoint summary displays all matched rules for an on-Fabric endpoint.

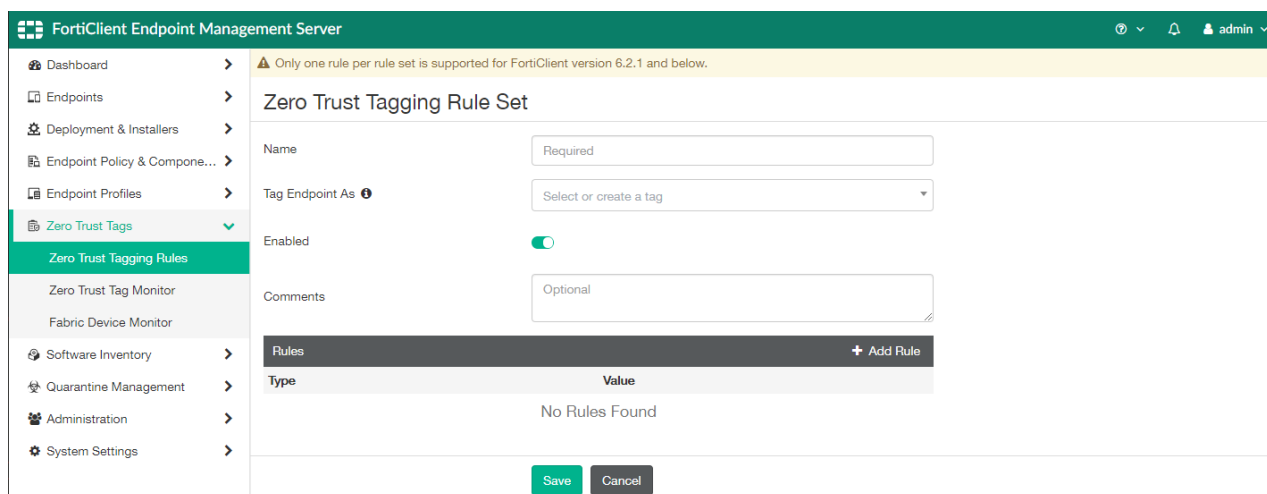
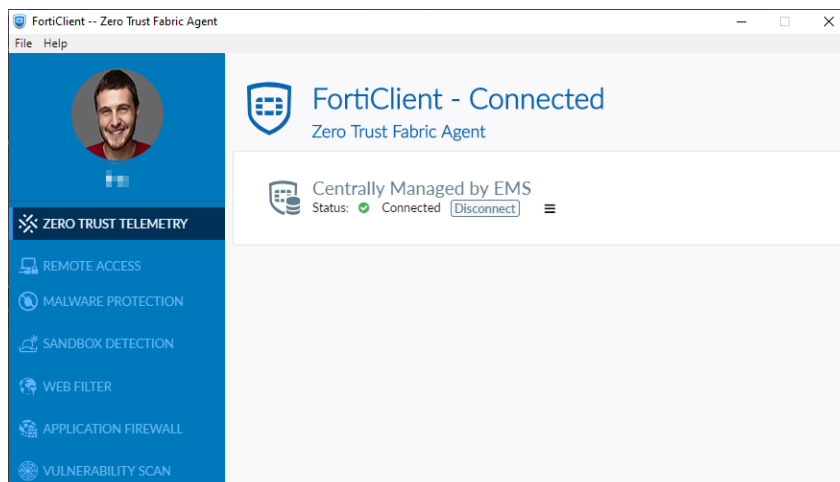


Compliance verification terminology renamed to Zero Trust - 6.4.2

Several features in FortiClient and FortiClient EMS have been renamed. The functionality of these features remains the same:

Old name	New name
Fabric Telemetry	Zero Trust Telemetry
Security Fabric Agent	Zero Trust Fabric Agent
Compliance verification rules	Zero Trust tagging rules
Compliance verification/host tags	Zero Trust tags

Both product GUIs reflect these name changes. In FortiClient, the *Remote Access* tab has also been moved and is now the second tab, under the *Zero Trust Telemetry* tab.



Endpoint: Remote Access

Selecting closest gateway for VPN connection - 6.4.1

FortiClient (Windows) uses one of the following methods to choose the closest remote gateway for VPN connection:

- Based on ping response time duration
- Based on TCP round trip time (TCP three-way handshake (SYN, SYN-ACK, ACK))

To configure this option in EMS:

1. Go to *Endpoint Profiles > Manage Profiles*.
2. Select the desired profile.
3. On the *VPN* tab, click *Add Tunnel*.

4. In *Basic Settings*, add multiple remote gateways, then click *Add Tunnel*.

Creating VPN Tunnel

Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Name

sslvpn-resilience-ping-based

Cannot contain the characters: *%&<>.

Type

SSL VPN IPsec VPN

Remote Gateway

172.17.61.68:4433

172.17.61.39:10439

Port

443

☐ Require Certificate

☒ Prompt for Username

Add Tunnel Cancel

5. On the *XML Configuration* tab, find the tunnel, and modify the `<RedundantSortMethod>` value as desired. This value controls which method FortiClient selects the remote gateway when connecting to this VPN tunnel:

Value	Description
0	Priority-based. FortiClient tries remote gateways in the order defined in the server list to connect to VPN.
1	FortiClient connects to the gateway that has a shorter ping response time.
2	FortiClient connects to the gateway that has a shorter TCP round trip time (TCP three-way handshake (SYN, SYN-ACK, ACK))

6. Save the profile.

To verify the configuration:

- In FortiClient, attempt to connect to the newly configured VPN tunnel.
- Do one of the following:
 - If you selected the ping response method, manually ping the remote gateways in Command Prompt. Confirm that FortiClient connected using the gateway with the shorter ping response time. You can also capture packets with Wireshark during VPN connection and observe that pings to both remote gateways are present.

```

C:\Users\qa>ping fgt68.com

Pinging fgt68.com [172.17.61.68] with 32 bytes of data:
Reply from 172.17.61.68: bytes=32 time=1ms TTL=254
Reply from 172.17.61.68: bytes=32 time<1ms TTL=254
Reply from 172.17.61.68: bytes=32 time<1ms TTL=254
Reply from 172.17.61.68: bytes=32 time<1ms TTL=254

Ping statistics for 172.17.61.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

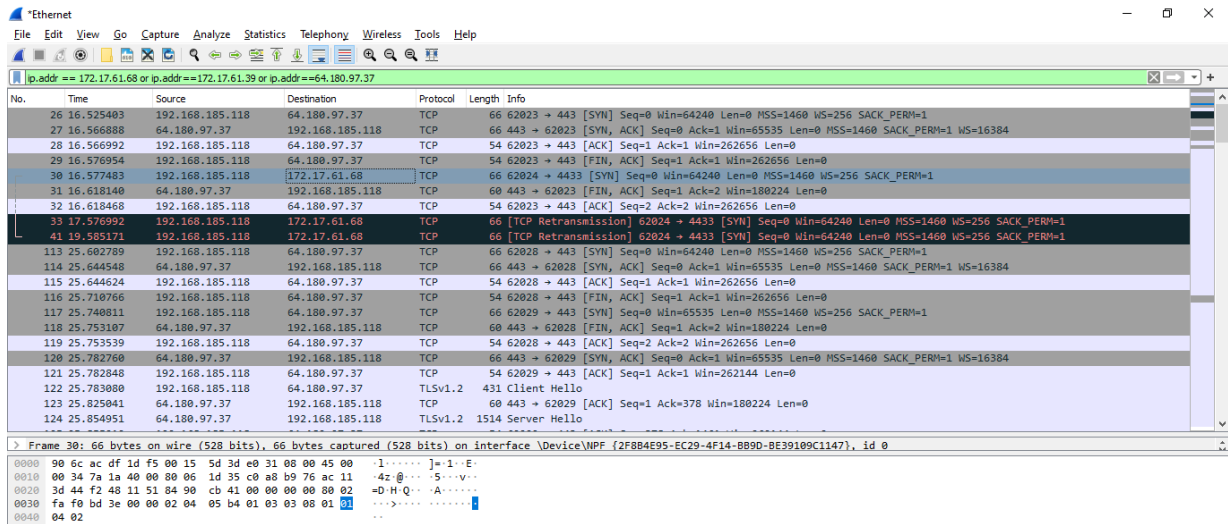
C:\Users\qa>ping ssldemo.fortinet.com

Pinging ssldemo.fortinet.com [64.180.97.37] with 32 bytes of data:
Reply from 64.180.97.37: bytes=32 time=41ms TTL=246
Reply from 64.180.97.37: bytes=32 time=41ms TTL=246
Reply from 64.180.97.37: bytes=32 time=40ms TTL=246
Reply from 64.180.97.37: bytes=32 time=41ms TTL=246

Ping statistics for 64.180.97.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 41ms, Average = 40ms

```

- b. If you selected the TCP round trip time method, use Wireshark to capture packets. Observe that SYN, SYN-ACK, ACK traffic to both remote gateways are present. Confirm that FortiClient connected using the remote gateway with the shorter TCP round trip time.



Application-based split tunnel - 6.4.2

FortiClient (Windows) supports source application-based split tunnel, where you can specify which application traffic to exclude from the VPN tunnel. You can exclude high bandwidth-consuming applications. For example, you can exclude applications like the following from the VPN tunnel:

- Microsoft Office 365
- Microsoft Teams
- Skype
- GoToMeeting
- Zoom
- WebEx
- YouTube

You must configure these settings in the endpoint profile in EMS. The scope for the setting is for all VPN tunnels for that profile. The following instructions assume that you have already configured a remote SSL or IPsec VPN server in FortiOS. See the [FortiOS documentation](#).

This feature does not support explicitly including traffic in the VPN tunnel.



Currently FortiClient (macOS) and FortiClient (Linux) do not support source application-based split tunnel.

To configure application-based split tunnel using the GUI:

1. In EMS, go to *Endpoint Profiles*, and select the desired profile.
2. On the *VPN* tab, select an existing tunnel or create a new tunnel.
3. Under *Split Tunnel > Application Based*, configure the following fields:

Configuration	Description
Application Based	<p>Enable application-based split tunnel. FortiClient (Windows) supports source application-based split tunnel, where you can specify which application traffic to exclude from the VPN tunnel. You can exclude high bandwidth-consuming applications for improved performance. For example, you can exclude applications like the following from the VPN tunnel:</p> <ul style="list-style-type: none"> • Microsoft Office 365 • Microsoft Teams • Skype • GoToMeeting • Zoom • WebEx • YouTube <p>Once the VPN tunnel is up, FortiClient binds the specified excluded applications to the physical interface.</p>
Type	Select <i>Exclude</i> to configure whether to exclude certain application traffic from the VPN tunnel.
Local Applications	<p>You can only exclude local applications from the VPN tunnel. Click <i>Add</i>. In the <i>Add Application(s)</i> field, specify which application traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface. You can specify an application using its process name, full path, or the directory where it is installed. When entering the directory, you must end the value with \. You can enter file and directory paths using environment variables, such as %LOCALAPPDATA%, %programfiles%, and %appdata%. Do not use spaces in the tail or head, or add double quotes to full paths with spaces. You can add multiple entries by separating them with a semicolon.</p> <p>For example, to exclude Microsoft Teams and Firefox from the VPN tunnel, you can enter any of the following combinations:</p> <ul style="list-style-type: none"> • Application Name: teams.exe;firefox.exe • Full Path: C:\Users\<username>appData\Local\Microsoft\Teams\current\Teams.exe;C:\Pr

Configuration	Description
	<p>ogram Files\Mozilla Firefox\firefox.exe</p> <ul style="list-style-type: none"> Directory: C:\Users\<username>appData\Local\Microsoft\Teams\current\;C:\Program Files\Mozilla Firefox\ <p>To find a running application's full path, on the <i>Details</i> tab in Task Manager, add the <i>Image path name</i> column.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>
Cloud Applications	<p>You can exclude cloud applications. Click <i>Add</i>. In the list, select the desired applications, then click <i>Add</i>.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>
Domain	<p>You can exclude domains. After you exclude a domain, any associated traffic will not go through the VPN tunnel when accessed through a popular browser such as Chrome, Edge, or Firefox. Click <i>Add</i>. In the <i>Add Domain(s)</i> field, enter the desired domains, using ; to configure multiple entries.</p> <p>For example, if you configure the VPN tunnel to exclude youtube.com, youtube.com and *.youtube.com are excluded from the tunnel.</p> <p>Select the application checkbox, then click <i>Remove</i> to remove it from the list.</p>

This example shows excluding the Microsoft Teams using the application name, full path, and directory. It also excludes Teams and other web conferencing cloud applications, such as Zoom and Cisco WebEx:

Editing VPN Tunnel - Add Application/Domain ✕

Add Application(s)

Application can be specified by its name, full path or the directory where it is installed. Environment variables (e.g. %programfiles%, %appdata%) can be used in file and directory path. Multiple entries can be separated by ; (e.g. chrome.exe;explore.exe)

For example:
 Application Name: chrome.exe
 Full Path: C:\Program Files\Internet Explorer\explore.exe
 Directory: C:\windows\ (must end with "\")

Add
Cancel

Creating VPN Tunnel

Changes to this VPN tunnel will not be saved until the profile is saved.

Basic Settings

Split Tunnel

Application Based

Advanced Settings

On Connect Script

On Disconnect Script

Application Based

Type: Include Exclude

Local Applications

Name
<input type="checkbox"/> teams.exe
<input type="checkbox"/> C:\Users\<username>\appData\Local\Microsoft\Teams\current\Teams.exe
<input type="checkbox"/> C:\Users\<username>\appData\Local\Microsoft\Teams\current
<input type="button" value="Remove"/>
<input type="button" value="+ Add"/>

Cloud Applications

Name
<input type="checkbox"/> Microsoft-Skype_Teams
<input type="checkbox"/> Cisco-Webex
<input type="checkbox"/> Cisco-Webex.FedRAMP
<input type="checkbox"/> Zoom.us-Zoom.Meeting
<input type="button" value="Remove"/>
<input type="button" value="+ Add"/>

Domain

Domain
No Content Found
<input type="button" value="Remove"/>
<input type="button" value="+ Add"/>

Add Tunnel Cancel

Editing VPN Tunnel - Add Application/Domain

Add Cloud Application(s)

Application Search

<input type="checkbox"/>	Google-Basic.Service
<input type="checkbox"/>	Google-Google.Cloud
<input type="checkbox"/>	Google-Google.Bot
<input type="checkbox"/>	Google-Gmail
<input type="checkbox"/>	Facebook-Basic.Service
<input type="checkbox"/>	Facebook-Whatsapp
<input type="checkbox"/>	Facebook-Instagram
<input type="checkbox"/>	Apple-Basic.Service
<input type="checkbox"/>	Apple-App.Store
<input type="checkbox"/>	Apple-APNs
<input type="checkbox"/>	Yahoo-Basic.Service
<input type="checkbox"/>	Microsoft-Basic.Service
<input checked="" type="checkbox"/>	Microsoft-Skype_Teams
<input type="checkbox"/>	Microsoft-Office365
<input type="checkbox"/>	Microsoft-Azure
<input type="checkbox"/>	Microsoft-Bing.Bot

Add Cancel

- Assign the profile to the desired endpoints. When VPN is up on those endpoints, the application traffic specified in the profile will be excluded from the VPN tunnel as configured.

Backup VPN connection - 6.4.3

You can configure FortiClient to connect to a preconfigured SSL VPN tunnel instead when connection to a configured IPsec VPN tunnel fails. This feature is convenient for connecting to VPN when the IPsec VPN tunnel is blocked or if a public router or gateway performs IPsec VPN NAT incorrectly.

This guide assumes that the EMS administrator has already configured an SSL VPN tunnel and IPsec VPN tunnel on the desired endpoint profile. For details on creating VPN tunnels in EMS, see [VPN](#).

To configure a backup VPN connection:

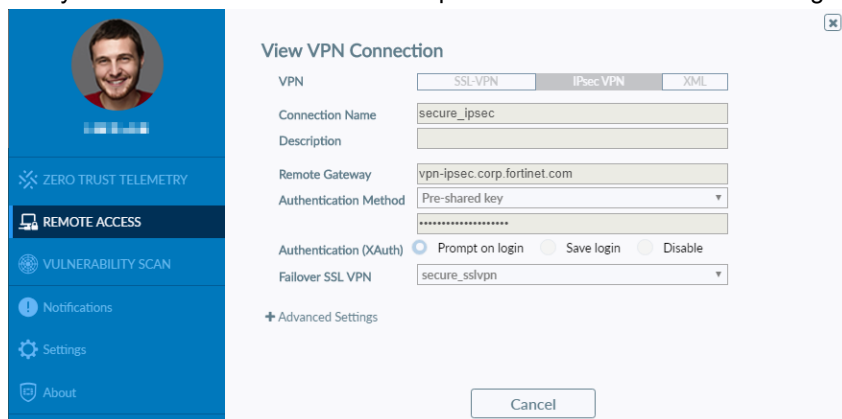
1. In EMS, go to *Endpoint Profiles > Manage Profiles*.
2. Edit the desired profile, then do one of the following:
 - a. Configure this feature from the GUI. You can configure this feature from the GUI in EMS 6.4.4 and later versions. Do the following:
 - i. Edit the desired IPsec VPN tunnel.
 - ii. In *Advanced Settings*, from the *Failover SSL VPN Connection* dropdown list, select the desired SSL VPN connection.
 - iii. Click *Save*.
 - b. Configure this feature using XML. In EMS 6.4.3, you can only configure this feature using XML. On the *XML Configuration* tab, configure the following for the desired IPsec VPN tunnel. The following configures the `secure_sslvpn` tunnel as the backup tunnel:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
      <connections>
        <connection>
          <ike_settings>
            <failover_sslvpn_connection>SSLVPN HQ</failover_sslvpn_connection>
          <ike_settings>
        </connection>
      </connections>
    </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

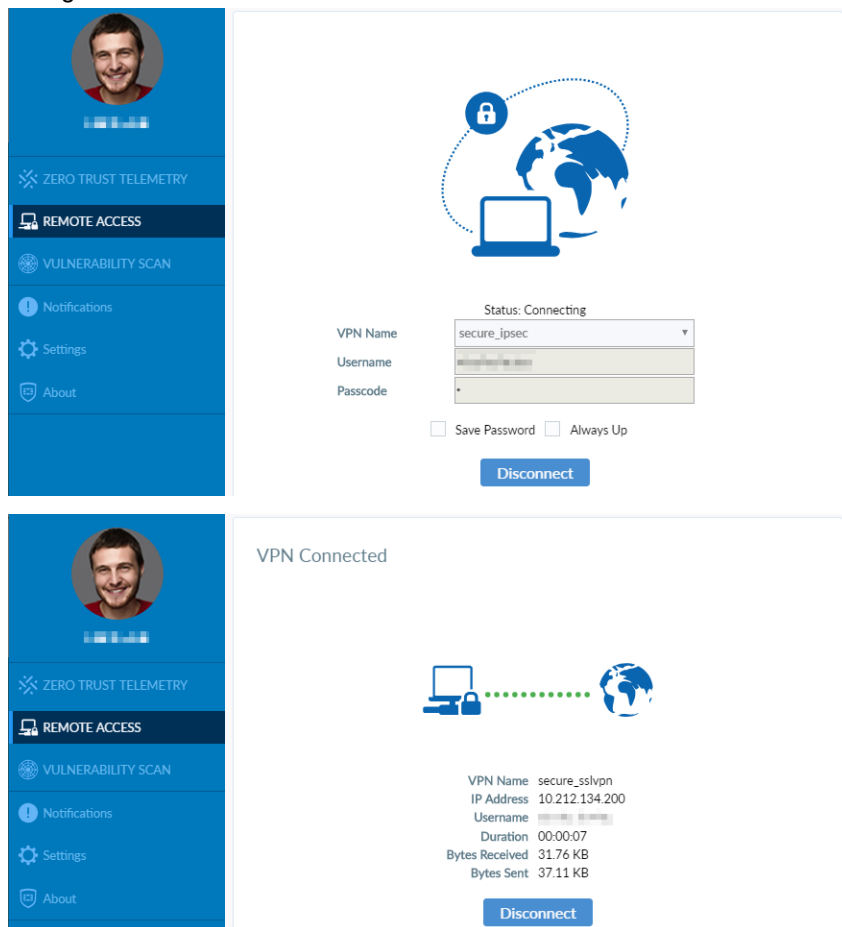
This is a balanced but incomplete XML configuration fragment. It includes all closing tags but omits some important elements to complete the IPsec VPN configuration.

3. After FortiClient receives the next update from EMS, on the *Remote Access* tab, from the *VPN Name* dropdown list, select the IPsec VPN tunnel.
4. Select *View the selected connection*.

5. Verify that the *Failover SSL VPN* field specifies the SSL VPN tunnel configured in step 2.



6. Attempt connection to the IPsec VPN tunnel when you know that it will fail. FortiClient automatically connects to the configured SSL VPN tunnel instead.



Secure remote access compliance enforcement - 6.4.4

You can restrict devices from accessing an SSL VPN tunnel based on the Zero Trust tags applied on the endpoint. This helps to safeguard the internal network from threats that end user devices have. For example, consider that your

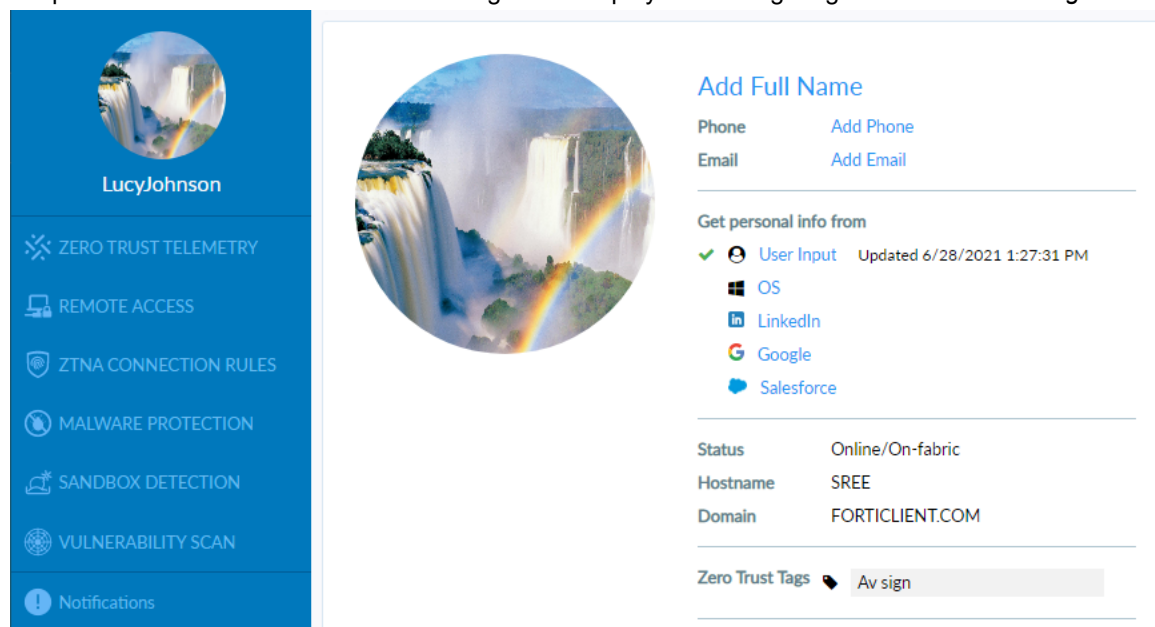
organization allows employees and customers to bring their own devices and connect them to a corporate VPN tunnel to access the internal organization network. If these devices have vulnerabilities or do not have the latest antivirus (AV) signatures, they may affect the internal network. You can use this feature to block such endpoints from connecting to the corporate VPN tunnel.

To block endpoints that do not have the latest AV signatures from connecting to the VPN tunnel:

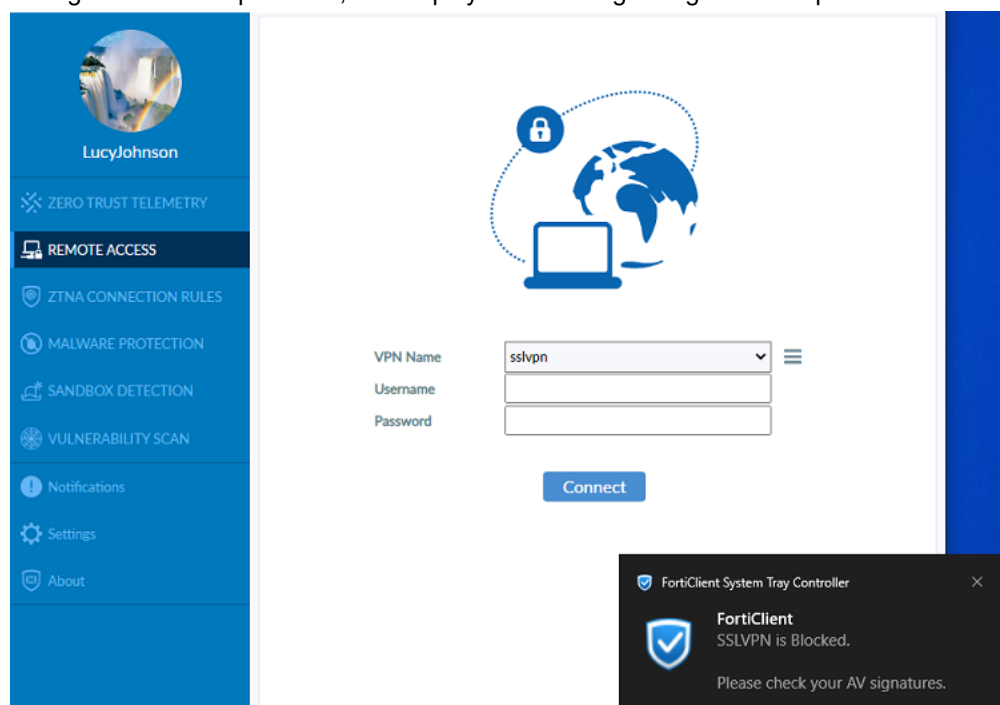
1. Create a Zero Trust tagging rule set that tags endpoints that do not have the latest AV signatures as "Av sign":
 - a. Go to *Zero Trust Tags > Zero Trust Tagging Rules*.
 - b. Click *Add*.
 - c. In the *Tag Endpoint As* field, create a new "Av sign" tag.
 - d. Toggle *Enabled* to on.
 - e. Click *Add Rule*.
 - f. For Windows devices, from the *Rule Type* dropdown list, select *AntiVirus Software*.
 - g. From the dropdown list, select *AV Signature is up-to-date*.
 - h. Select the *NOT* checkbox.
 - i. Click *Save*.
 - j. Click *Save* again.
2. Configure the options on the endpoint profile:
 - a. Go to *Endpoint Profiles > Manage Profiles*.
 - b. Edit the desired profile, or create a new one.
 - c. On the *VPN* tab, enable *Enable Secure Remote Access*.
 - d. Select an existing VPN tunnel, or create a new one by clicking *Add Tunnel*.
 - e. In *Advanced Settings*, for *Host Tag*, select *Prohibit*.
 - f. From the *Select a Tag* dropdown list, select *Av sign*.
 - g. Enable *Customize Host Check Fail Warning*.
 - h. Enter a message to display to users when their connection to the VPN tunnel is prohibited due to critical vulnerabilities on their device.

- i. Configure other fields as desired.

- j. On the *System Settings* tab, enable *Show Host Tag on FortiClient GUI*.
- k. Save the configuration.
3. After FortiClient receives the latest configuration from EMS, click the user avatar to view the About page. An endpoint that does not have the latest AV signature displays the Av sign tag under *Zero Trust Tags*.



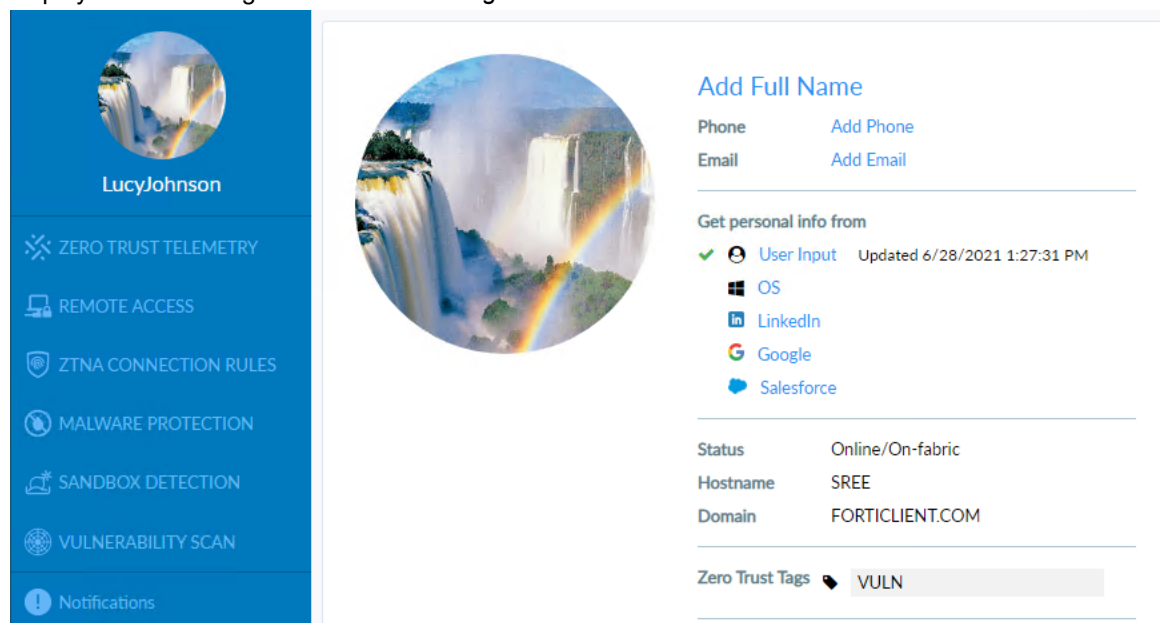
4. On the *Remote Access* tab, attempt to connect to the SSL VPN tunnel. FortiClient blocks the connection since the AV signature is not up-to-date, and displays the warning configured in step 2.



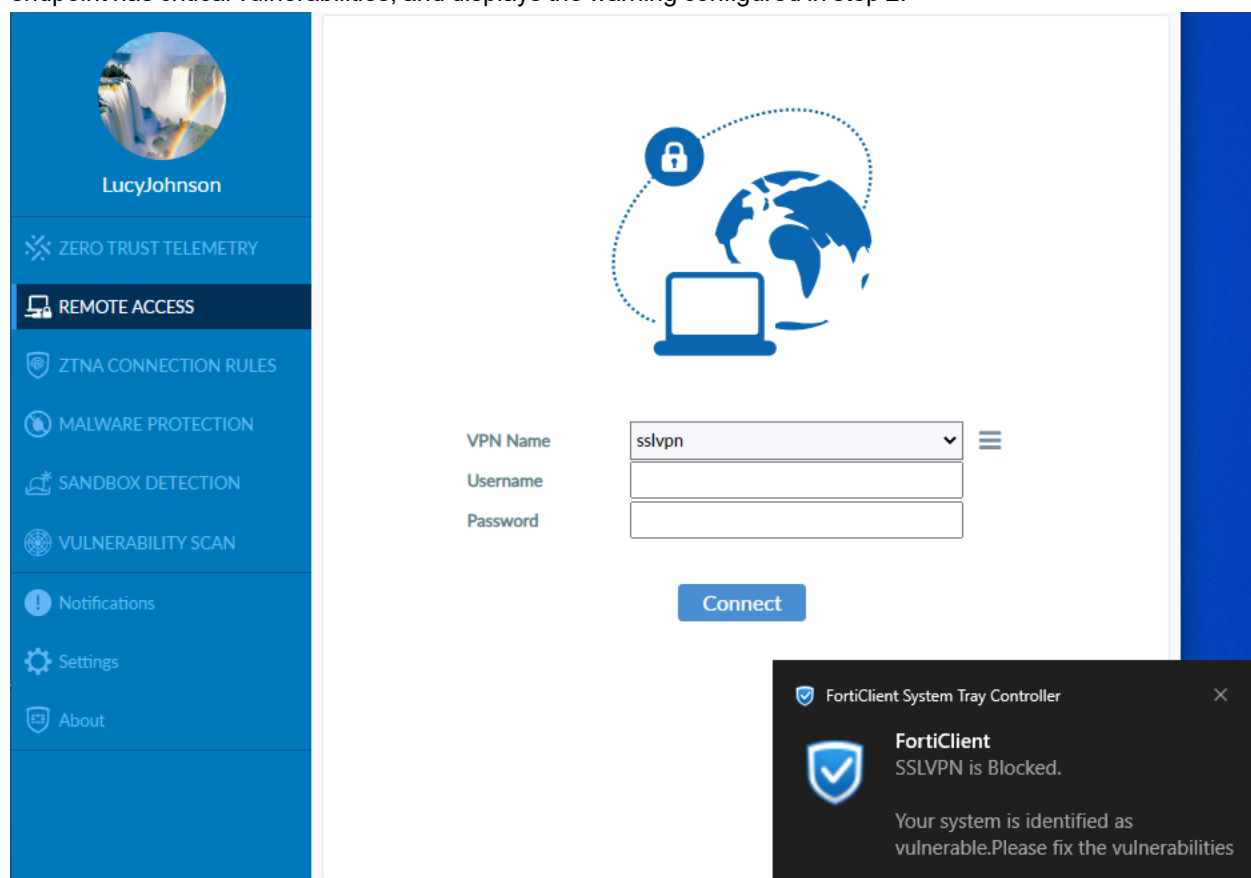
5. Update AV signatures and retry connection to the SSL VPN tunnel. Connection will be successful.

To block endpoints that do not have critical vulnerabilities from connecting to the VPN tunnel:

1. Create a Zero Trust tagging rule set that tags endpoints with critical vulnerabilities with the "VULN" tag:
 - a. Go to *Zero Trust Tags > Zero Trust Tagging Rules*.
 - b. Click *Add*.
 - c. In the *Tag Endpoint As* field, create a new "VULN" tag.
 - d. Toggle *Enabled* to on.
 - e. Click *Add Rule*.
 - f. For Windows devices, from the *Rule Type* dropdown list, select *VULN*.
 - g. From the *Severity Level* dropdown list, select *Critical*.
 - h. Click *Save*.
 - i. Click *Save* again.
2. Configure the options on the endpoint profile:
 - a. Go to *Endpoint Profiles > Manage Profiles*.
 - b. Edit the desired profile, or create a new one.
 - c. On the *VPN* tab, enable *Enable Secure Remote Access*.
 - d. Select an existing VPN tunnel, or create a new one by clicking *Add Tunnel*.
 - e. In *Advanced Settings*, for *Host Tag*, select *Prohibit*.
 - f. From the *Select a Tag* dropdown list, select *VULN*.
 - g. Enable *Customize Host Check Fail Warning*.
 - h. Enter a message to display to users when their connection to the VPN tunnel is prohibited due to critical vulnerabilities on their device.
 - i. Configure other fields as desired.
 - j. On the *System Settings* tab, enable *Show Host Tag on FortiClient GUI*.
 - k. Save the configuration.
3. After FortiClient receives the latest configuration from EMS, on the *Vulnerability Scan* tab, click *Scan Now* to detect vulnerabilities on the system.
4. After the scan completes, click the user avatar to view the About page. An endpoint that has critical vulnerabilities displays the VULN tag under *Zero Trust Tags*.



- On the *Remote Access* tab, attempt to connect to the SSL VPN tunnel. FortiClient blocks the connection since the endpoint has critical vulnerabilities, and displays the warning configured in step 2.



- Patch the critical vulnerabilities and retry connection to the SSL VPN tunnel. Connection will be successful.

Endpoint: Endpoint Security

FortiSandbox Cloud support for macOS

FortiClient (macOS) now supports FortiSandbox Cloud. FortiClient (macOS) can send files to FortiSandbox Cloud for analysis. Based on the result, FortiClient allows the user to access the file, or flags the file as malicious and blocks access to it.

The endpoint must be licensed using a license that includes the FortiSandbox feature.

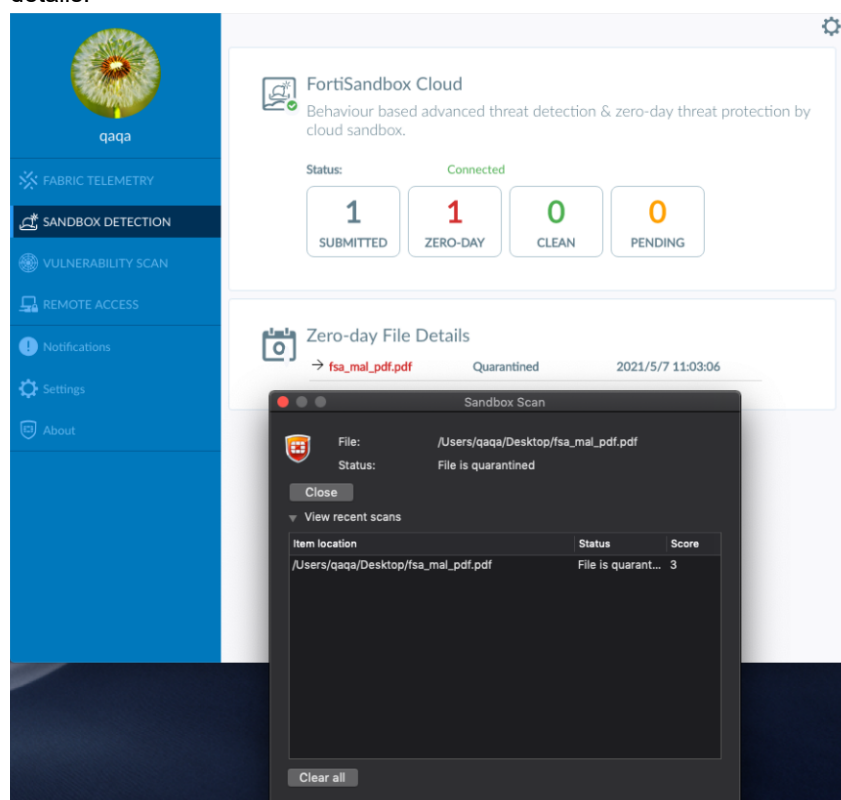
To configure FortiSandbox Cloud in EMS:

- In EMS, go to *Endpoint Profiles > Manage Profiles*.
- Select the desired profile.
- On the *Sandbox* tab, enable *Sandbox Detection*.
- For *FortiSandbox*, select *Cloud*.

5. For *Inspection Mode*, select *High-Risk Files*.
6. Click **Save**.

To verify this feature in FortiClient (macOS):

1. Open the FortiClient console on a macOS endpoint that you have assigned the selected profile to. After the endpoint receives the latest profile from EMS, go to the *Sandbox Detection* tab to view the FortiSandbox Cloud status and detections.
2. Click the *Settings* icon in the top-right corner. You can view the Sandbox settings.
3. FortiSandbox Cloud detection occurs based on the EMS configuration. The following shows that a file was downloaded from the Internet and FortiClient submitted it to FortiSandbox Cloud for inspection and analysis. FortiClient also records the detection result and other details. As FortiSandbox Cloud identified this file as malicious, it performed the configured action for malicious files, which is quarantine. The *Sandbox Scan* notification also displays details such as file location, status, and FortiSandbox score. You can click *View recent scans* to view details.



The *Sandbox Detection* tab also displays the following information:

Submitted	Number of files that FortiClient submitted to FortiSandbox.
Zero-Day	Number of zero-day files that FortiSandbox detected.
Clean	Number of clean files that FortiSandbox detected.
Pending	Number of files pending FortiSandbox detection results.
Zero-day File Details	Zero-day file details such as file name, configured action upon detection, and the detection time.

Keyword block support

You can configure keyword scanning on search engines for Chromebook endpoints. EMS has a content safeguard service-provided file with a list of words in various languages for different categories. The *Keyword Scanning on Search Engine* feature supports monitoring and blocking searches for banned words that users perform in popular search engines.

To enable keyword scanning on search engines:

1. In EMS, go to *Endpoint Profiles*. Select the desired Chromebook profile, or create a new one.
2. Enable *Keyword Scanning on Search Engine*.
3. Configure the following features:

Banned Word Search

Enable to configure actions (block or monitor) to take when the user searches for terms that belong to the following categories:

- Violence/Terrorism
- Extremist
- Pornography
- Cyber Bullying
- Self Harm

Custom Banned Words

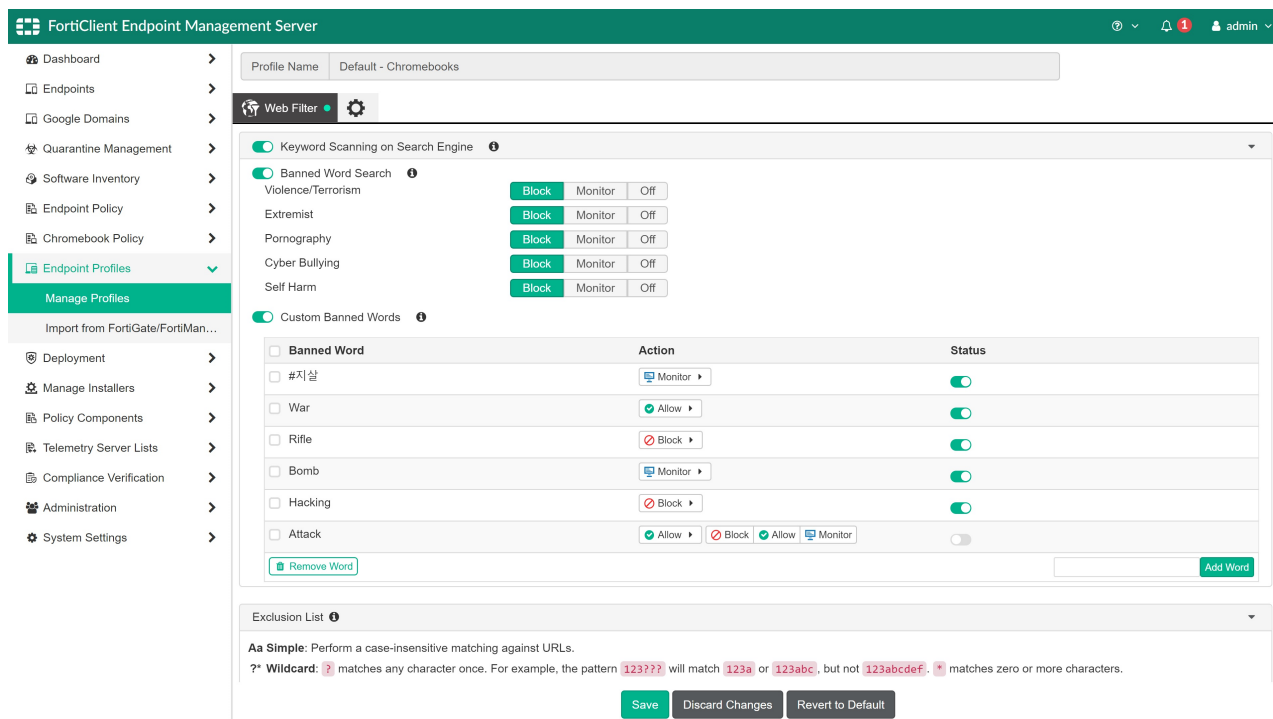
Configure actions for individual terms. Enable *Custom Banned Words*, type the desired term in the *Add Word* field, then click *Add Word*. Configure the action for the term (*Block*, *Monitor*, or *Allow*), then toggle the *Status* to *On*.

You can remove a term from the *Custom Banned Word* list by selecting the checkbox beside the term, then clicking the *Remove Word* button.

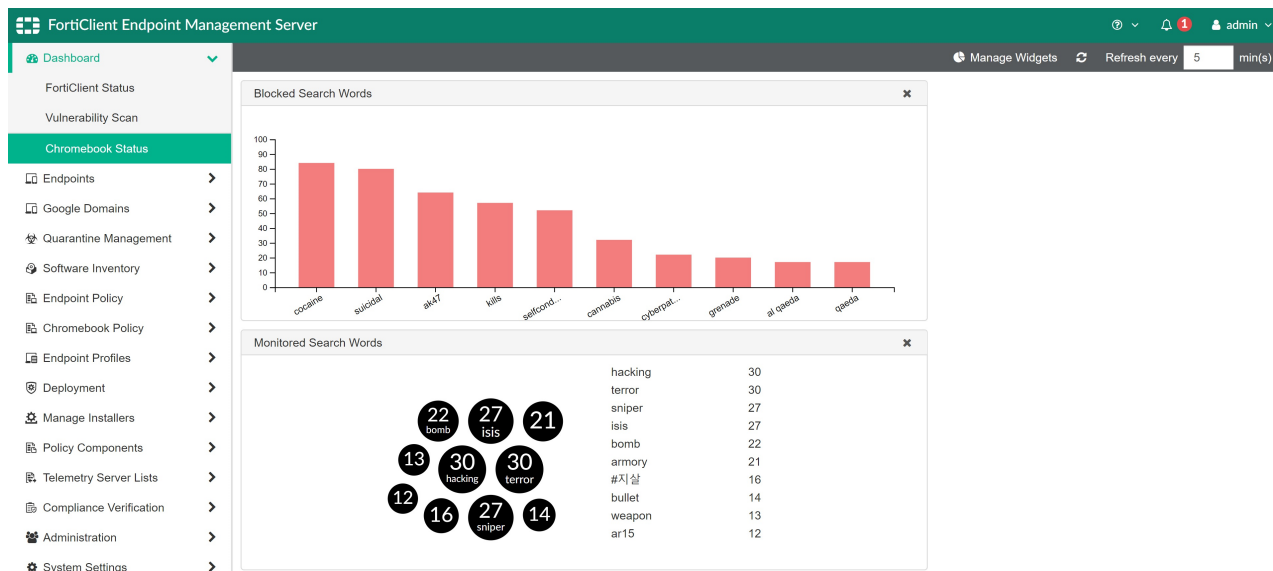
The custom term may belong to a category under *Banned Word Search*. If the action configured for the category under *Banned Word Search* and the action configured for the term under *Custom Banned Words* differ, EMS applies the action configured under *Custom Banned Words*.

Blocking a term prevents the user from accessing the site. The browser displays a blocked page that you can customize from EMS. See [Customizing Web Filter messages](#).

Monitoring a term logs whenever the user searches for this term and presents this information in the related dashboard widgets and EMS logs. If configured, EMS also sends this information to FortiAnalyzer.



Two new widgets in *Dashboard > Chromebook Status*, *Most Searched Monitored Words* and *Most Searched Allowed Words*, represent the user statistics.



Client handling for HTTPS (browser plugin) for Microsoft Edge browser - 6.4.2

The FortiClient Web Filter plugin that improves detection and enforcement of Web Filter rules on HTTPS sites is now available for Microsoft Edge on Windows endpoints. For details, see *Enable Web Browser Plugin for HTTPS Web Filtering* in the [FortiClient EMS Administration Guide](#).

Malware Protection and Sandbox Detection enhancements - 6.4.2

FortiClient and FortiClient EMS 6.4.2 add the following enhancements to Malware Protection and Sandbox Detection:

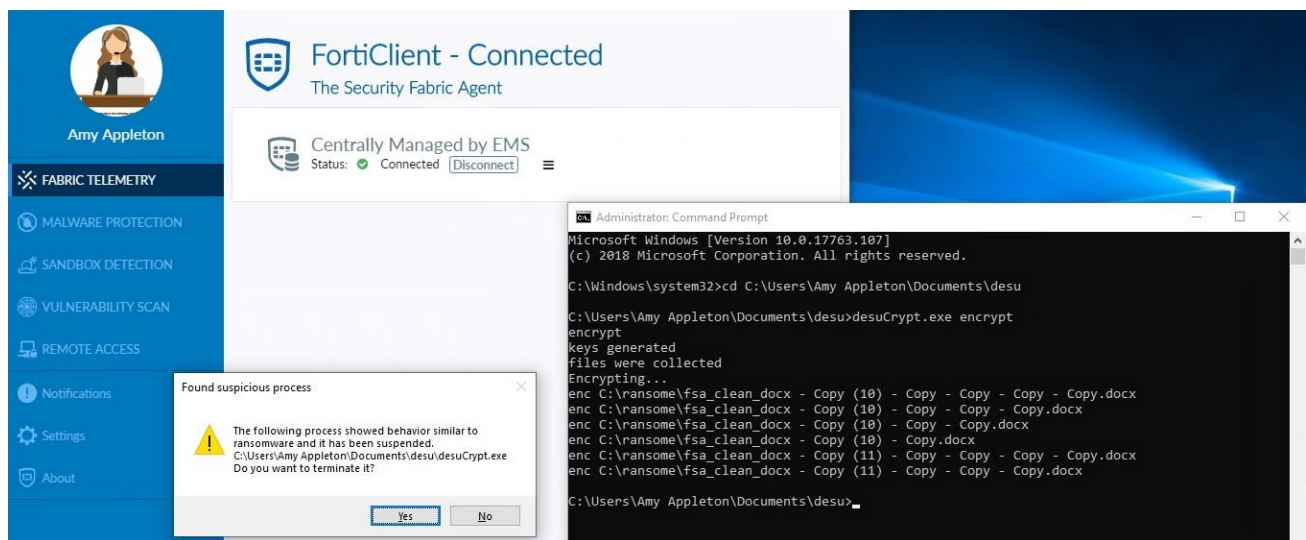
- **Anti-ransomware:** new feature that helps detect any suspicious ransomware activity.
- **Antiexploit:** enhancement that shields applications from attacks and improves security.
- **Sandbox Detection:** enhancement to send files that exhibit unknown behavior from removable devices such as CDs to FortiSandbox.

Anti-ransomware

To configure antiransomware:

1. In EMS, go to *Endpoint Profiles > Manage Profiles*.
2. On the *Malware* tab, enable *Anti-Ransomware*.
3. Under *Protected Folders*, click *Add Folder* and include the desired folders in anti-ransomware protection.
4. In the *Protected File Types* field, enter the desired file types to include in anti-ransomware protection.
5. From the *Action* dropdown list, select the desired action.
6. In the *Action Timeout* field, enter the desired timeout value in seconds.
7. Click *Save*.

In this example, after the EMS administrator configures antiransomware protection and the configuration is synced to the FortiClient endpoint, the Desuencrypt tool is used to simulate the encryption of files in a folder. After Desuencrypt starts the encryption process, FortiClient shows a popup that it detected ransomware activity.



If you select **Yes**, FortiClient terminates the encryption process.

If you do not select an option in the popup, FortiClient waits for the default action timeout and proceeds with whichever of the following actions is configured:

- Block access and warn the user if suspicious activity is detected
- Warn the user and resume after the timeout

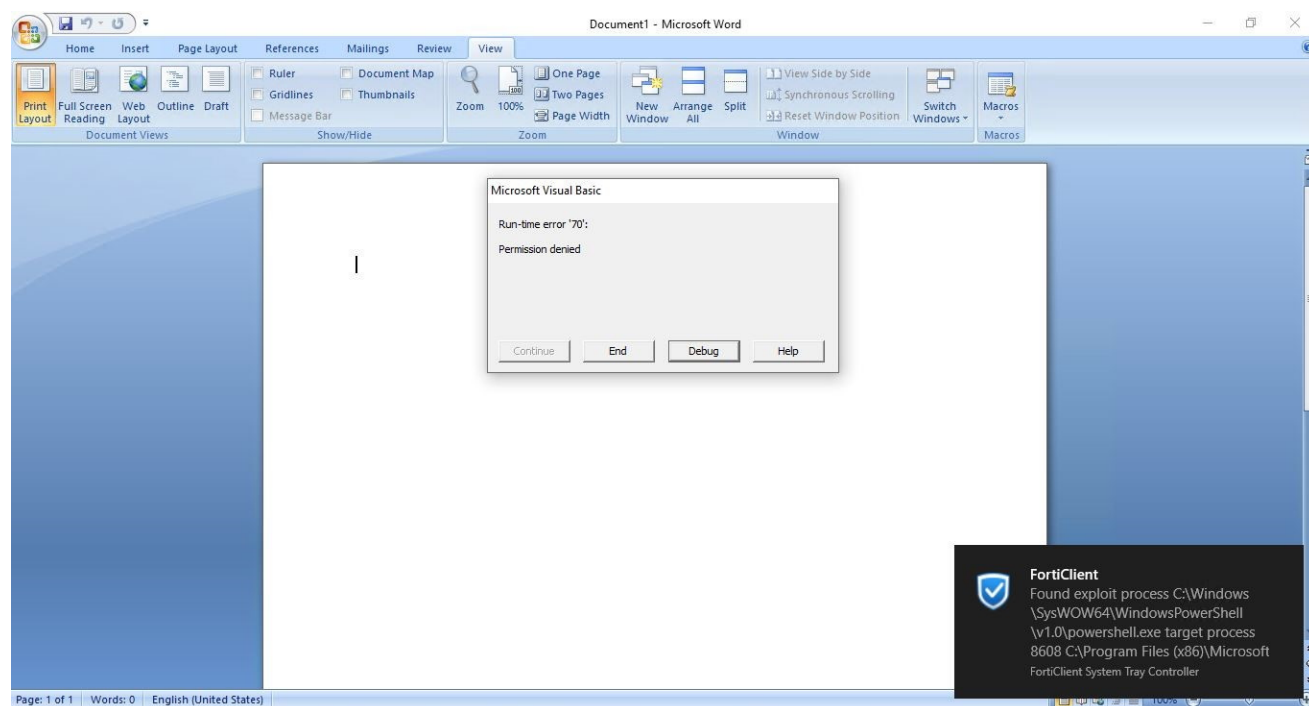
Antiexploit

The antiexploit feature monitors commonly used applications for attempts to exploit unknown vulnerabilities.

To configure antiexploit:

1. In EMS, go to *Endpoint Profiles > Manage Profiles*.
2. On the *Malware* tab, enable *Real-Time Protection* and *Anti-Exploit*. You must enable *Real-Time Protection* for the Anti-Exploit feature to function.
3. Click *Save*.

In this example, after the EMS administrator configures antiexploit and the configuration is synced to the FortiClient endpoint, Microsoft Word 2007 macros are used to simulate an exploit. Once the macro is executed, FortiClient detects the exploit with a popup and terminates it.



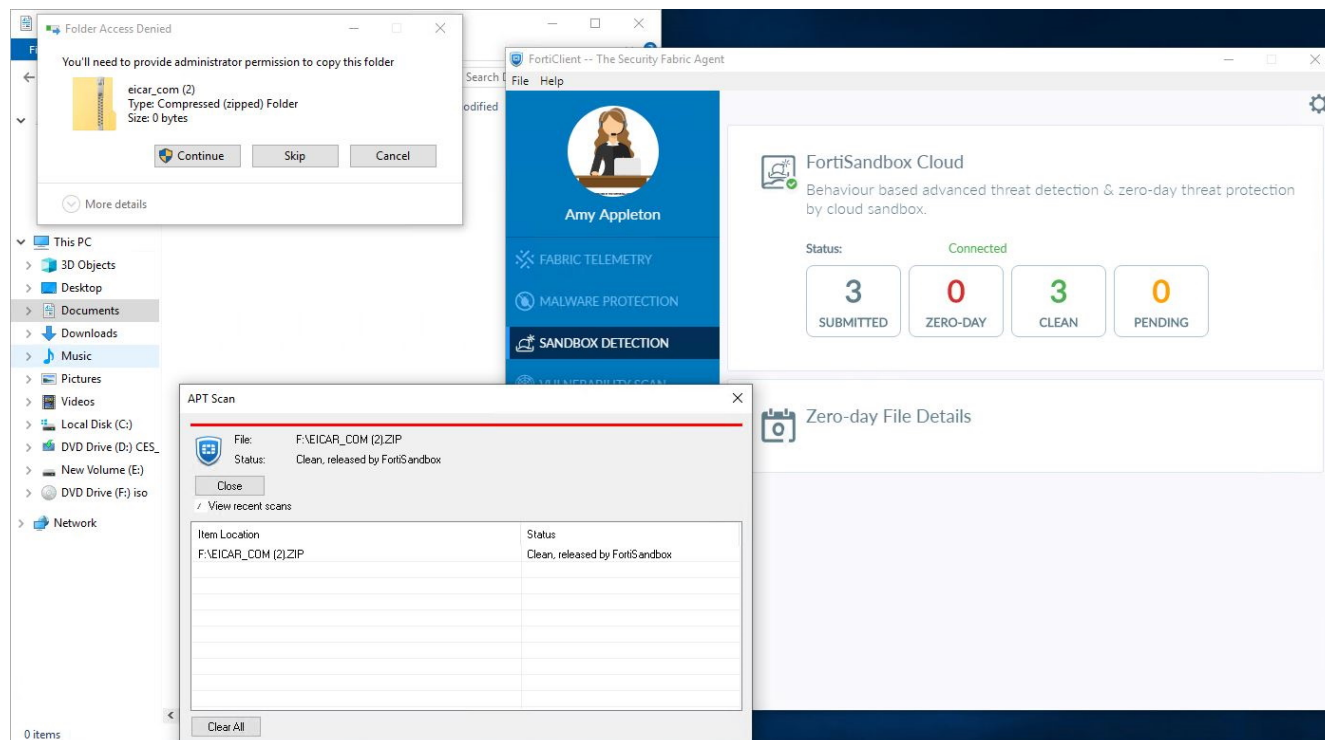
Sandbox Detection

Sandbox Detection allows file submission options from removable devices.

To configure Sandbox Detection submission options from removable devices:

1. In EMS, go to *Endpoint Profiles > Manage Profiles*.
2. On the *Sandbox* tab, under *Server*, configure connection to Sandbox Cloud or a Sandbox appliance.
3. Under *File Submission Options*, enable *All Files Executed from Removable Media*.
4. Click *Save*.

In this example, after the EMS administrator configures this feature and the configuration is synced to the FortiClient endpoint, a removable CD-ROM with malicious folders is connected to the endpoint. The user attempts to copy the folders from the CD-ROM to a local folder. FortiClient displays a popup and submits the folder to Sandbox Cloud.



Blocking removable devices by class ID - 6.4.2

You can define multiple rules to block, monitor, or allow removable devices, such as the following:

- Human interface devices
- Windows portable devices
- Bluetooth devices
- CD-ROM drive
- Smart card reader
- USB device
- Camera device

You can configure rules using device properties including the class, manufacturer, vendor ID, product ID, and revision. You can enter regular expressions in PERL or simple format (exact match). One profile supports multiple rules. FortiClient EMS ignores empty fields. If FortiClient detects an existing removable device's properties matches a rule, it applies the configured action (block, allow, or monitor).

You can find the hardware properties of a removable device using Hardware Manager or USBDeView.

To configure Removable Media Access:

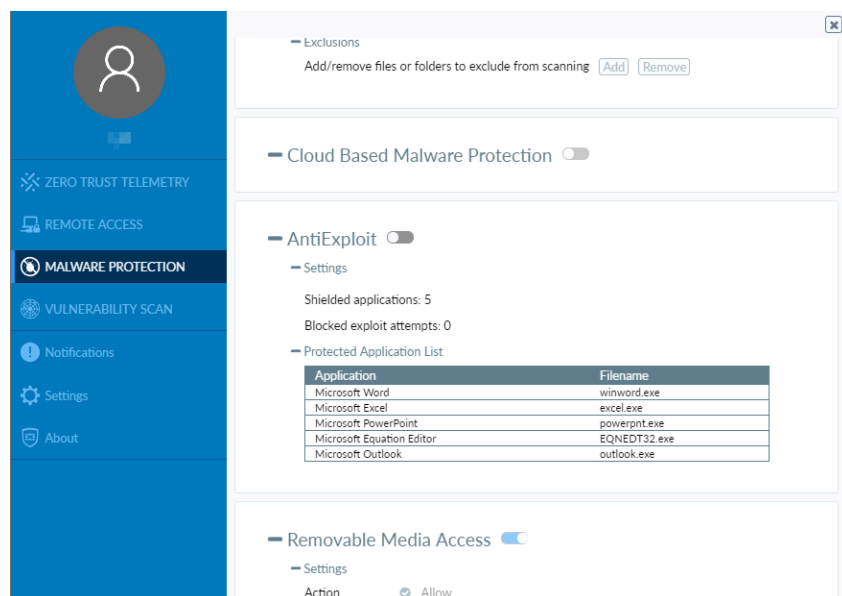
1. In EMS, go to Endpoint Profiles > Manage Profiles.
2. On the Malware tab, enable Removable Media Access.

3. Configure the following:

Options	Description
Show bubble notifications	Display a bubble notification when FortiClient takes action with a removable media device.
Action	<p>Configure the action to take with removable media devices connected to the endpoint that match this rule. Available options are:</p> <ul style="list-style-type: none"> • <i>Allow</i>: Allow access to removable media devices connected to the endpoint that match this rule. • <i>Block</i>: Block access to removable media devices connected to the endpoint that match this rule. • <i>Monitor</i>: Log removable media device connections to the endpoint that match this rule.
Description	Enter the desired rule description.
Type	<p>Select <i>Simple</i> or <i>Regular Expression</i> for the rule type.</p> <p>When <i>Simple</i> is selected, FortiClient performs case-insensitive matching against classes, manufacturers, vendor IDs, product IDs, and revisions.</p> <p>When <i>Regular Expression</i> is selected, FortiClient uses Perl Compatible Regular Expressions (PCRE) to perform matching against classes, manufacturers, vendor IDs, product IDs, and revisions.</p>
Class	Enter the device class.
Manufacturer	Enter the device manufacturer.
Vendor ID	Enter the device vendor ID.
Product ID	Enter the device product ID.
Revision	Enter the device revision number.
Remove this rule	Remove this rule from the profile.
Add a new rule	Add a new removable media access rule.
Move this rule up/down	Move this rule up or down. If a connected device is eligible for multiple rules, FortiClient applies the highest rule to the device.
Default removable media access	<p>Configure the action to take with removable media devices that do not match any configured rules. Available options are:</p> <ul style="list-style-type: none"> • <i>Allow</i>: Allow access to removable media devices connected to the endpoint that do not match any configured rules. • <i>Block</i>: Block access to removable media devices connected to the endpoint that do not match any configured rules. • <i>Monitor</i>: Log removable media device connections to the endpoint that do not match any configured rules.

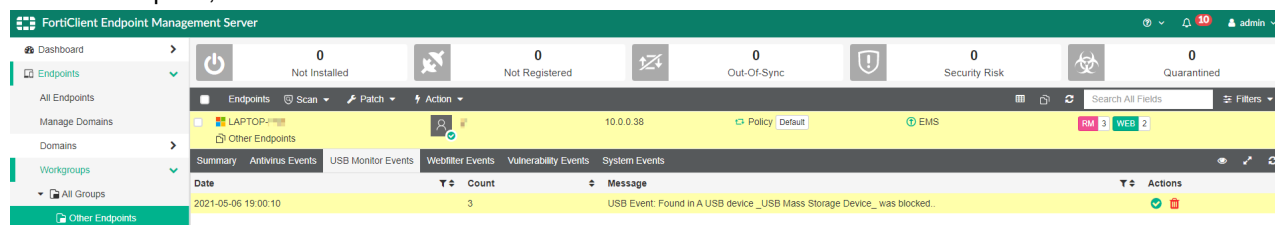
4. Click **Save**.

The FortiClient GUI currently does not display all defined removable media rules. It only displays the default action, which is applied if the removable device does not match all defined rules.



To view endpoint removable media events:

1. In EMS, go to *Endpoints* and go to the desired endpoint.
2. Click the endpoint, then select the *USB Monitor Events* tab.



FortiClient (Windows) moderate and strict Safe Search levels support - 6.4.2

Like the Chromebook extension, FortiClient (Windows) now supports the Moderate and Strict levels for the Safe Search feature.

To configure Safe Search for FortiClient (Windows) endpoints:

1. In EMS, go to *Endpoint Profiles*.
2. On the *Web Filter* tab, select *Enable Safe Search*.
3. For *Restriction Level*, select *Moderate* or *Strict*. This setting affects the content that endpoint users can access via YouTube and search engine, including Google and Bing.
4. Click *Save*.

When the restriction level is moderate, YouTube content restriction is set to Moderate. Users can view videos labeled "moderate".

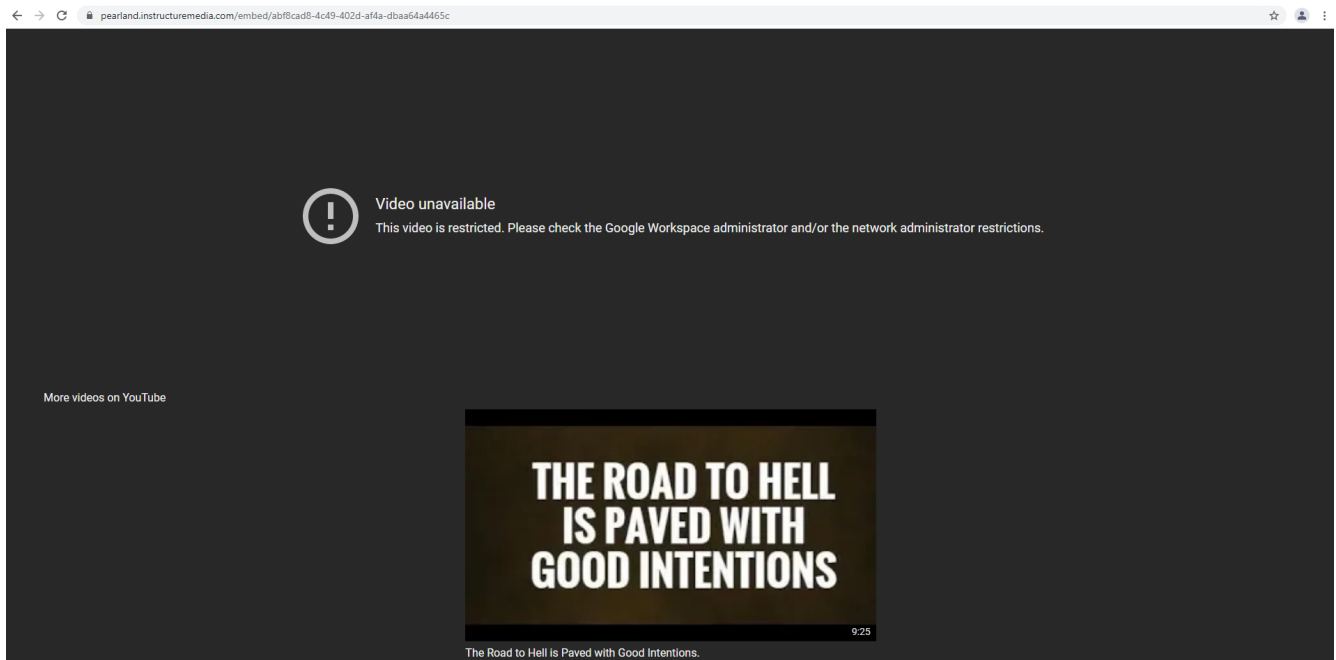
The top screenshot shows the YouTube 'Check content restrictions' page. It features a table with DNS and HTTP header restrictions for various domains. The bottom screenshot shows a video player for 'Alexis de Tocqueville & the shocking concepts we use to teach in school'. The video frame displays the text 'THE STORY of LIBERTY' over an image of the American flag.

	DNS restrictions	HTTP header restrictions
www.youtube.com	Moderate	-
m.youtube.com	Moderate	-
www.youtube-nocookie.com	Moderate	-
youtube.googleapis.com	Moderate	-
ytubei.googleapis.com	Moderate	-

When the restriction level is strict, YouTube content restriction is set to Strict. Users cannot view videos labeled "moderate".

This screenshot shows the same YouTube 'Check content restrictions' page, but with the restriction level set to 'Strict' for all domains.

	DNS restrictions	HTTP header restrictions
www.youtube.com	Moderate	-
m.youtube.com	Strict	-
www.youtube-nocookie.com	Strict	-
youtube.googleapis.com	Strict	-
ytubei.googleapis.com	Strict	-



FortiClient EMS

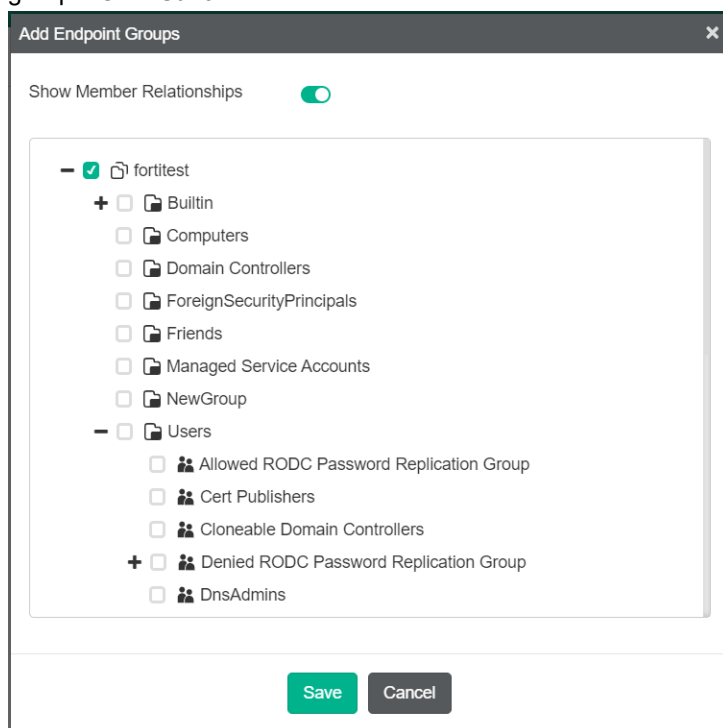
ZTNA

User-based management

You can assign FortiClient policies based on endpoint devices in organizational units.

To assign device groups, user groups, and users to a policy:

1. Go to *Endpoint Policy*. Create a new policy or select an existing one.
2. In the *Endpoint Groups* field, click *Edit*. In the *Add Endpoint Groups* dialog, select the desired device and/or user groups. Click *Save*.



3. In the *Users* field, select the desired users.
4. Click *Save*.

When FortiClient connects to EMS, the following occurs:

1. If a policy is assigned to the FortiClient user, EMS assigns that policy to the endpoint.
2. If there are policies for the FortiClient group container and/or user groups, EMS assigns the policy with the highest global priority.

- If there are inherited policies for group containers and/or user groups, EMS assigns the inherited policy with the highest global priority.

In *Endpoint Policy > Manage Policies*, you can click *Edit Columns* to select which columns to display.

Manage Policies displays a progress line that indicates each policy's FortiClient synchronization status. The *Endpoint Count* column shows the number of FortiClient endpoints with the policy assigned and the number of endpoints that have not been seen for the past 30 days.

Edit Delete		+ Add Change Priority Refresh Clear Filters Edit Columns			
Name	Assigned Groups	Profile	Policy Components	Endpoint Count	Enabled
Policy_1	All Groups	<div> <div>PROFILE Profile_1</div> <div>OFF-NET Default</div> </div> <div>100% ✓</div>		<div>1</div> <div>4 endpoints not seen for last 30 days</div>	✓
Policy_2	fortitest pbufay rgreen	<div> <div>PROFILE Profile_2</div> <div>OFF-NET Default</div> </div> <div>100% ✓</div>		<div>2</div>	✓
Default		<div> <div>PROFILE Default</div> </div>		<div>0</div>	✓

Click the endpoint count to see the endpoint list.

Endpoints (4) Refresh						
Hostname	User	Policy	Profile	Off-Net Profile	Connection	Last Seen
DESKTOP-6DQIEPJ	J	Policy_1	Profile_1	Default	Not Managed	2020-05-01 13:07:15
MKP-DRichey	Dexter Richey	Policy_1	Profile_1	Default	Not Managed	2020-05-01 13:07:33
MKP-GFrakes	Grant Frakes	Policy_1	Profile_1	Default	Not Managed	2020-05-01 13:07:33
MKP-RHock	Rachelle Hock	Policy_1	Profile_1	Default	Not Managed	2020-05-01 13:07:34

To deploy FortiClient to endpoints with user-based management:

- (Optional) Create a custom installer.
- Go to *System Settings > Feature Select*. Select the features to globally show and hide. In 6.4.0, you no longer select available features for each deployment package.
- Create a deployment package.
- Create a deployment configuration.

For details on this deployment process, see [Deployment](#).

In *Deployment > Management Deployment*, the *Deployment Package* column displays a progress line indicating each deployment package's deployment state.

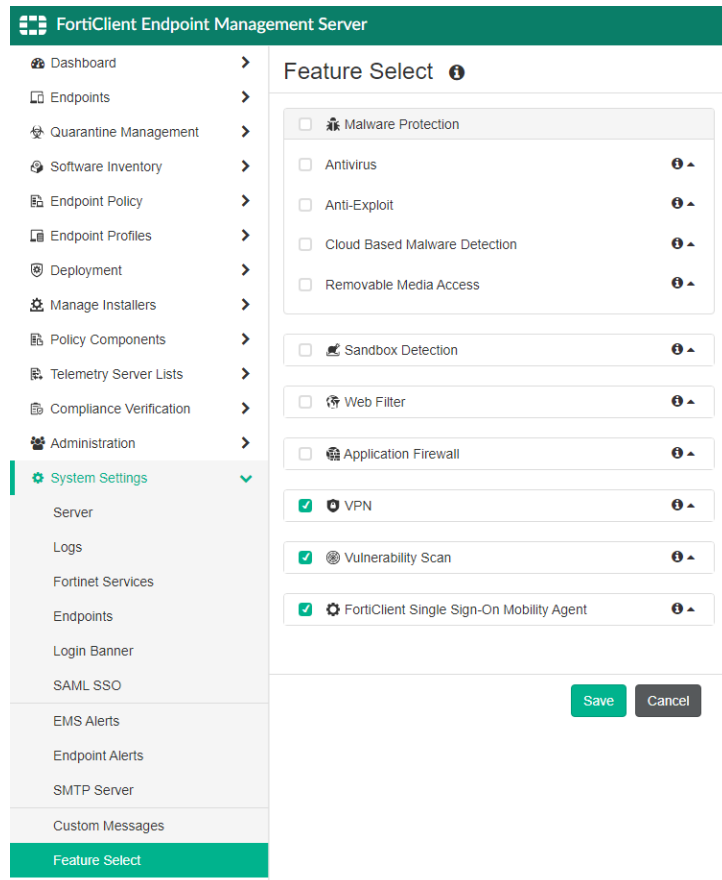
+ Add Change Priority Refresh					
Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled
Deployment_Group1	All Groups/Other Endpoints	<div> <div>Deployment_6.4</div> </div>		1	✓
Deployment_Group2	fortitest/ForeignSecurityPrincipals fortitest/Managed Service Accounts	<div> <div>Deployment_6.2.6</div> </div>		2	□

Customize EMS console UI - 6.4.1

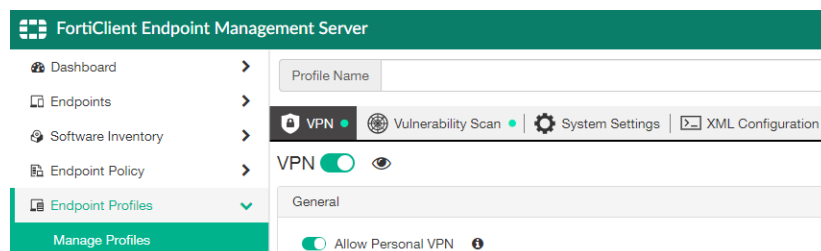
You can use Feature Select to enable and disable different features in EMS. Only features enabled in Feature Select display in other EMS configuration areas. This allows you to have more control to customize your EMS.

Example 1

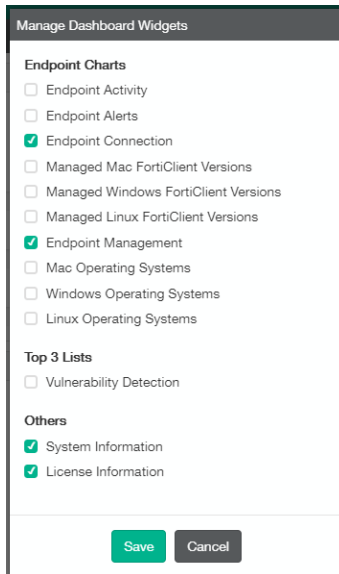
This example enables VPN, Vulnerability Scan, and FortiClient Single Sign-On Mobility Agent and disables Malware Protection, Sandbox Detection, Web Filter, and Application Firewall in Feature Select.



Only enabled features appear in other EMS configuration areas. In an endpoint profile, the Malware Protection, Sandbox Detection, Web Filter, and Application Firewall tabs are not available for configuration.



The *Manage Dashboards Widgets* dialog does not list the Antivirus Detection, Sandbox Detection, or Web Filter Detection widgets.



Manage Dashboard Widgets

Endpoint Charts

- ☐ Endpoint Activity
- ☐ Endpoint Alerts
- ☒ Endpoint Connection
- ☐ Managed Mac FortiClient Versions
- ☐ Managed Windows FortiClient Versions
- ☐ Managed Linux FortiClient Versions
- ☒ Endpoint Management
- ☐ Mac Operating Systems
- ☐ Windows Operating Systems
- ☐ Linux Operating Systems

Top 3 Lists

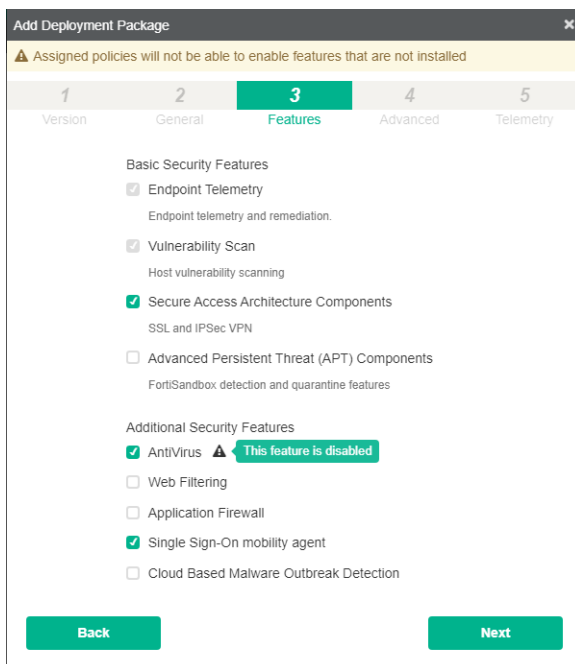
- ☐ Vulnerability Detection

Others

- ☒ System Information
- ☒ License Information

Save **Cancel**

All feature options still display when creating a deployment package. A warning appears beside features disabled in Feature Select. If in this example you enable AntiVirus in a deployment package, the deployment package installs AntiVirus on the endpoint. However, the AntiVirus feature is disabled on the endpoint and does not appear in the FortiClient GUI.



Add Deployment Package

⚠ Assigned policies will not be able to enable features that are not installed

1 2 **3** 4 5
Version General **Features** Advanced Telemetry

Basic Security Features

- ☒ Endpoint Telemetry
Endpoint telemetry and remediation.
- ☒ Vulnerability Scan
Host vulnerability scanning
- ☒ Secure Access Architecture Components
SSL and IPSec VPN
- ☐ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features

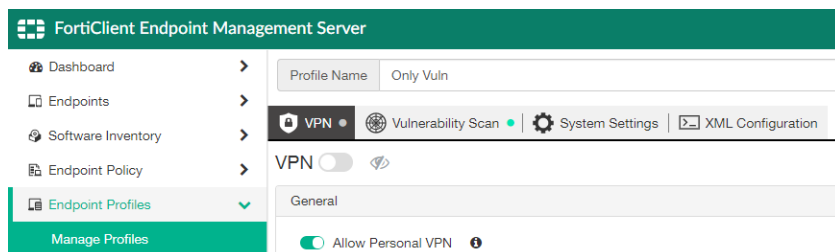
Additional Security Features

- ☒ AntiVirus ⚠ This feature is disabled
- ☐ Web Filtering
- ☐ Application Firewall
- ☒ Single Sign-On mobility agent
- ☐ Cloud Based Malware Outbreak Detection

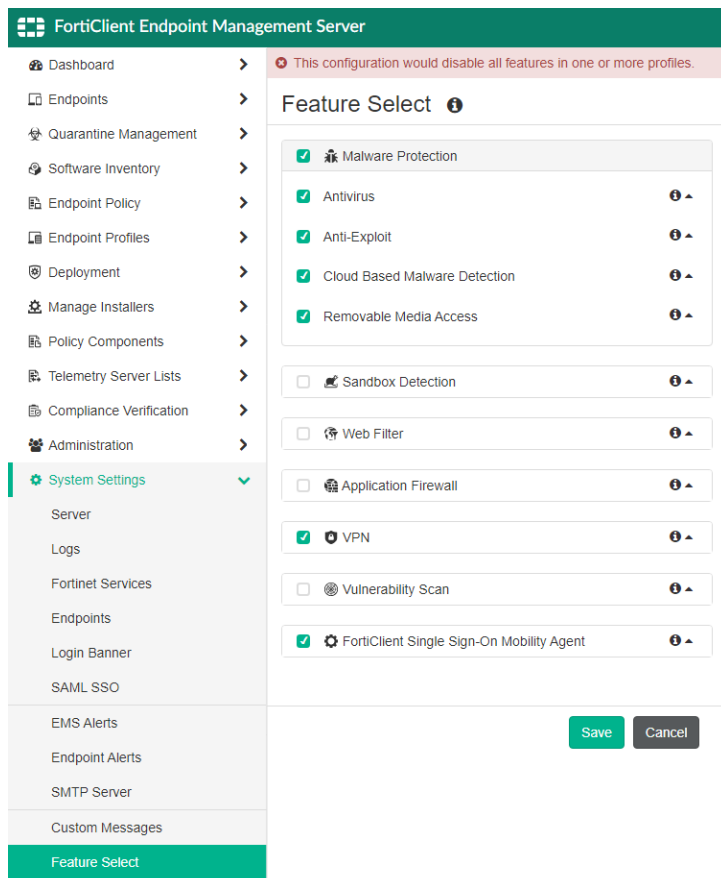
Back **Next**

Example 2

This example creates a profile with only Vulnerability Scan enabled.



Since this profile only has Vulnerability Scan enabled, EMS does not allow you to disable Vulnerability Scan in *Feature Select* and displays a warning at the top of the GUI.



Example 3

This example enables all features and creates a profile where VPN is enabled.

FortiClient Endpoint Management Server

- Dashboard
- Endpoints
- Quarantine Management
- Software Inventory
- Endpoint Policy
- Endpoint Profiles
- Deployment
- Manage Installers
- Policy Components
- Telemetry Server Lists
- Compliance Verification
- Administration
- System Settings**
 - Server
 - Logs
 - Fortinet Services
 - Endpoints
 - Login Banner
 - SAML SSO
 - EMS Alerts
 - Endpoint Alerts
 - SMTP Server
 - Custom Messages
 - Feature Select**

Feature Select

- ☒ Malware Protection
 - ☒ Antivirus
 - ☒ Anti-Exploit
 - ☒ Cloud Based Malware Detection
 - ☒ Removable Media Access
- ☒ Sandbox Detection
- ☒ Web Filter
- ☒ Application Firewall
- ☒ VPN
- ☒ Vulnerability Scan
- ☒ FortiClient Single Sign-On Mobility Agent

Save **Cancel**

FortiClient Endpoint Management Server

Profile Name: HQ

Malware | Sandbox | Web Filter | Firewall | **VPN** | Vulnerability Scan | System Settings

VPN

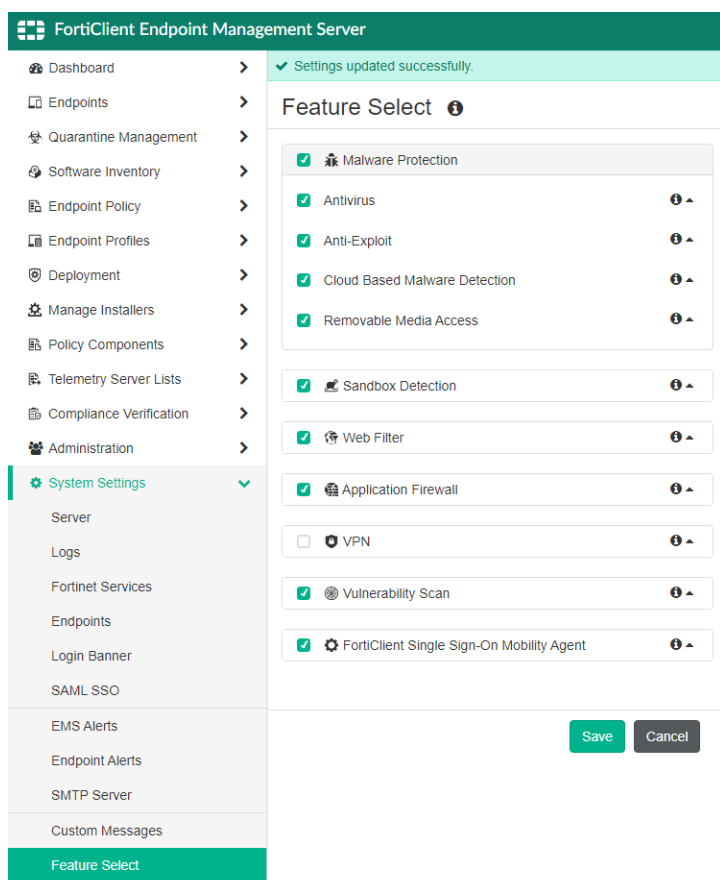
General

- ☒ Allow Personal VPN
- ☐ Disable Connect/Disconnect
- ☐ Show VPN before Logon

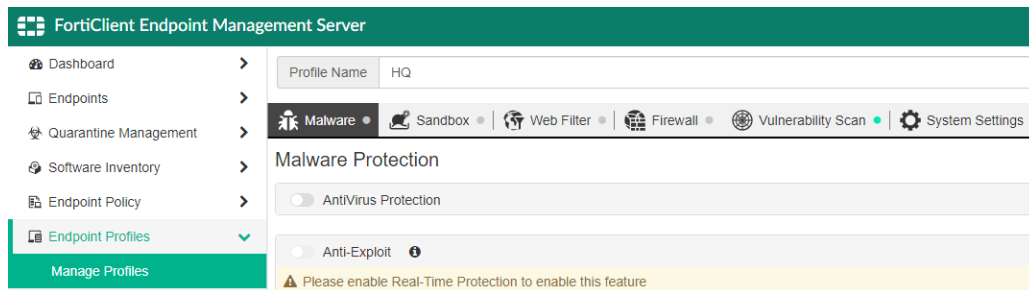
When an endpoint receives that profile, the Remote Access tab is enabled in FortiClient.



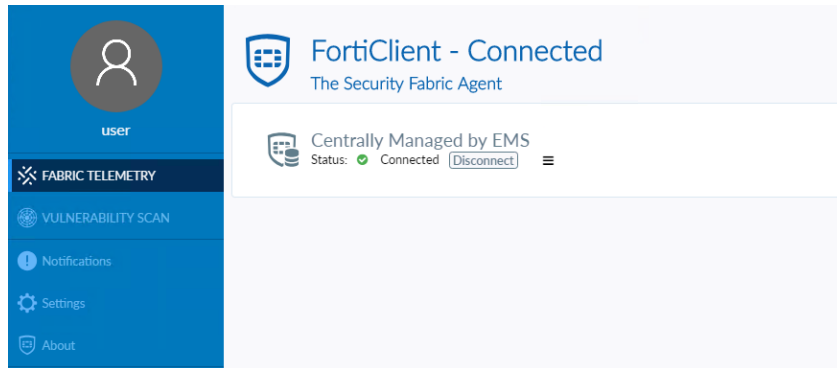
Then, disable VPN in Feature Select.



The VPN tab is no longer available for configuration in endpoint profiles.



After the endpoint syncs with EMS, the Remote Access tab does not appear in FortiClient.



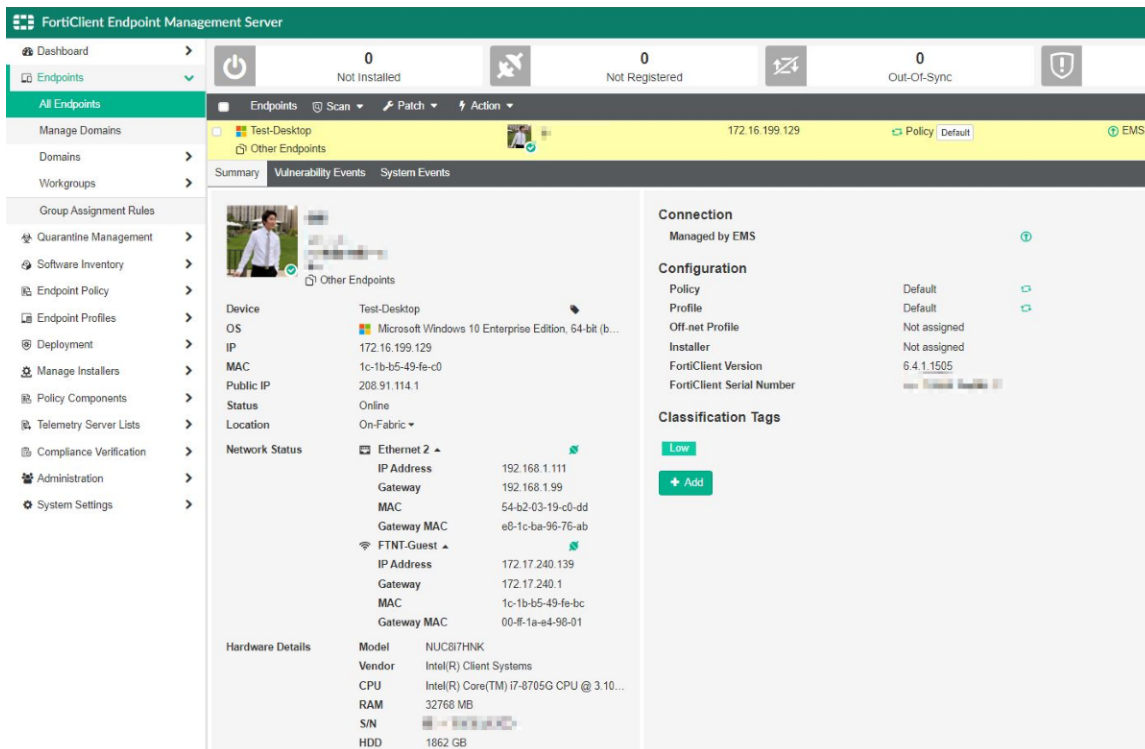
Enhanced visibility into endpoint - 6.4.1

In 6.4.1, FortiClient captures more endpoint details that are visible in the EMS GUI. You can use these details to hunt down rogue AP connections or hacking into unauthorized Ethernet ports. The additional endpoint information visible in EMS helps with further analysis.

Newly visible endpoint details include:

- Network:
 - Connection type (Ethernet or WiFi)
 - IP address
 - Gateway IP address
 - MAC address
 - Gateway MAC address
 - WiFi SSID
- Hardware:
 - Model
 - Vendor
 - CPU
 - RAM
 - Serial number
 - Hard disk drive

The following shows an endpoint's network status and hardware details information displayed in the EMS GUI:



Endpoint classification tags - 6.4.1

EMS 6.4.1 introduces tags for grouping and classifying endpoints that can help with assessing incident impact and prioritizing incidents by SOC analysts or SOAR playbooks.

You can assign a classification tag to an endpoint. Classification tags include the following:

- Default importance level tags (low, medium, high, or critical) to specify an endpoint's importance in the organization. You can tag critical endpoints accordingly and monitor them for security incidents.
- Custom tags. Configuring a maximum of eight custom tags is recommended. Configuring more than eight custom tags may result in performance or management issues. You can assign multiple custom tags to an endpoint or group of endpoints.

FortiAnalyzer Fabric View shows tags for each endpoint. FortiAnalyzer FortiSoC playbook pulls endpoint information from EMS using an EMS connector.

The following describes the process for configuring a classification tag and viewing the data in FortiAnalyzer:

1. [Configure and apply classification tags to endpoints in EMS.](#)
2. Configure FortiAnalyzer to receive the tags:
 - a. [Configure the EMS-FortiAnalyzer Fabric connection.](#)
 - b. [Run the FortiSoC playbook to retrieve endpoint information from EMS.](#)

To configure and apply classification tags to endpoints in EMS:

By default, EMS tags all newly registered endpoints with the Low default importance tag.

1. In EMS, go to *Endpoints*.
2. To apply tags to a single endpoint, go to the desired endpoint. Under *Classification Tags*, to create a new custom tag, click the *Add* button, enter the desired tag, then click the *+* button. You can also assign a new importance tag to the endpoint.

3. To apply tags to multiple endpoints, select all desired endpoints, then select *Action* > *Set Importance* or *Set Custom Tags*.

To configure the EMS-FortiAnalyzer Fabric connection:

1. In FortiAnalyzer, go to *Fabric View*.
2. Click the *Fabric Connectors* tab, then click *Create New*.
3. Click the *FortiClient EMS* tile. The *Create New Fabric Connector* dialog opens.

4. In the *Configuration* tab, configure the connector settings, enter the EMS IP address and administrator credentials.

Create New Fabric Connector

FortiClient EMS

Configuration | Actions

Name: EMS Connector

Description: Connector to execute remote EMS operations

IP/FQDN: 172.17.81.170

Username: admin

Password: ••••••••

Status: ☒ ON

< Back OK Cancel

5. On the *Actions* tab, leave the default settings.
6. Click **OK**.

To run the FortiSoC playbook to retrieve endpoint information from EMS:

1. In FortiAnalyzer, in the Fabric ADOM, go to *FortiSoC > Automation > Playbook*.
2. Click *Create New*, then *New Playbook created from scratch*.
3. Add an on-demand playbook with two tasks:


```
* FabricView--FortiSoC--Playbook
-- EMS_GET_ENDPOINTS (no parameters)
-- LOCALHOST_UPDATE_ASSET_AND_IDENTITY (use parameter ems_endpoints = previous_task_id.ems_endpoints)
```
4. Click **Save**.
5. Click **Run**. Accept the *Manually Run Playbook* prompt.
6. Go to *Automation > Playbook Monitor*. You can view the running playbook status.
7. Once the corresponding playbook job finishes running, go to *Fabric View > Assets*. The endpoint and its tags display.

Endpoint	Tags	User	MAC Address	IP Address	FortiClient UUID	Hardware	Vulnerabilities
DESKTOP-RIK3OAS	all_registered_clients, Medium, Department A	Robert Clavier	00:15:5d:90:f2:00	192.168.137.243	D05A4CF2856240D4856C243AEF1E6A1D	WIN64	

Sending upstream connection information for FortiClient (macOS) off-Fabric connections - 6.4.2

Endpoints sometimes need to form legitimate off-Fabric connections to EMS. For example, if an employee has brought their mobile device to an off-net environment, they must connect to EMS off-Fabric. In this scenario, the additional information that this enhancement provides allows you deeper visibility into the endpoint's connection information. You can also use this information for other scenarios, such as hunting down rogue AP connections or hacking into unauthorized Ethernet ports.

FortiClient (macOS) 6.4.2 and later versions sends the following upstream network connection information for Ethernet and Wi-Fi connections to EMS 6.4.2 and later versions:

- IP address
- MAC address
- Gateway IP address
- Gateway MAC address

For Wi-Fi connections, FortiClient (macOS) also sends the SSID. For VPN connections, FortiClient (macOS) sends the IP address information.

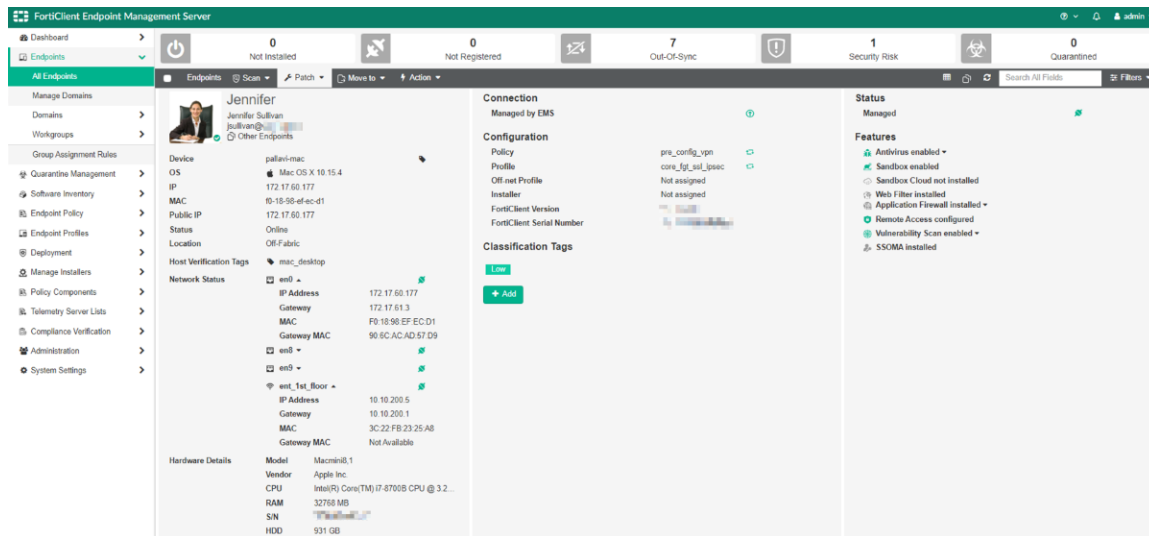
EMS displays this information in *All Endpoints > Summary > Network Status / Hardware Details*.

The following shows how EMS displays the macOS endpoint's active VPN and Ethernet interface details:

The screenshot displays the FortiClient Endpoint Management Server interface. The top navigation bar includes a dashboard with various status indicators: 0 Not Installed, 0 Not Registered, 6 Out of Sync, 1 Security Risk, and 0 Quarantined. The left sidebar shows a tree view with categories like Manage Domains, Domains, Workgroups, Group Assignment Rules, Quarantine Management, Software Inventory, Endpoint Policy, Endpoint Profiles, Deployment, Manage Installers, Policy Components, Telemetry Server Lists, Compliance Verification, Administration, and System Settings. The main content area is divided into three panels for the selected endpoint 'Jennifer Sullivan' (j.sullivan@v...).

- Device Information:**
 - Device: test's_Mac
 - OS: Mac OS X 10.15.4
 - IP: 10.212.134.200
 - MAC: 00:80:29:7B:8B:A7
 - Public IP: 209.121.79.107
 - Status: Online
 - Location: Off-Fabric
 - Host Verification Tags: mac_desktop
- Network Status:**
 - Network: utun2
 - IP Address: 10.212.134.200
 - Gateway: Not Available
 - MAC: Not Available
 - en0:
 - IP Address: 10.100.93.101
 - Gateway: 10.100.93.1
 - MAC: 00:0C:29:7B:8B:A7
 - Gateway MAC: 00:0C:29:6F:90:2E
 - en2:
- Hardware Details:**
 - Model: VMware7.1
 - Vendor: Apple Inc.
 - CPU: Intel(R) Core(TM) i7-6700B CPU @ 3.20...
 - RAM: 4096 MB
 - S/N: [Redacted]
 - HDD: 39 GB
- Connection:** Managed by EMS
- Configuration:**
 - Policy: pvc_config_vpn
 - Off-net Profile: conr_fip_vul_ipsec
 - Off-net Profile: Not assigned
 - Installer: Not assigned
 - FortiClient Version: [Redacted]
 - FortiClient Serial Number: [Redacted]
- Classification Tags:** Low
- Status:** Managed
- Features:**
 - Antivirus enabled
 - Sandbox enabled
 - Sandbox Cloud not installed
 - Web Filter installed
 - Application Firewall installed
 - Remote Access configured
 - Vulnerability Scan enabled
 - SSOMA installed

The following shows how EMS displays the macOS endpoint's active Wi-Fi and Ethernet interface details:

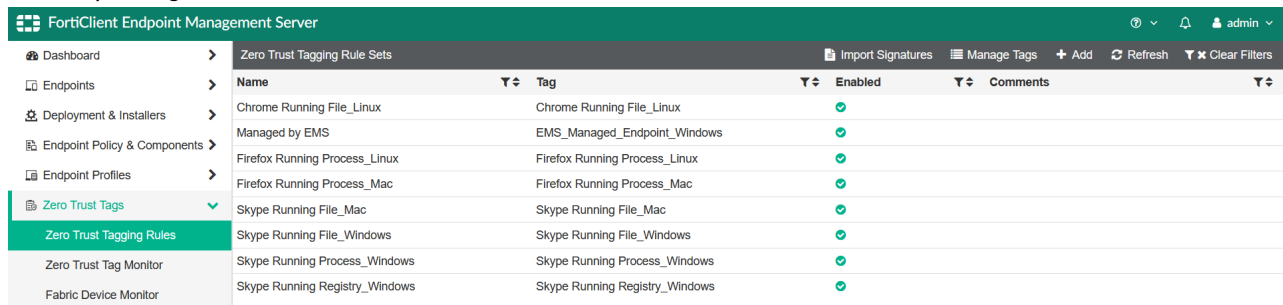


FortiGuard Outbreak Alerts service - 6.4.4

You can use a Zero Trust tagging rule as a predefined rule for FortiGuard outbreak alerts by uploading rule signatures.

To configure a Zero Trust tagging rule as a predefined rule for outbreak alerts by uploading rule signatures:

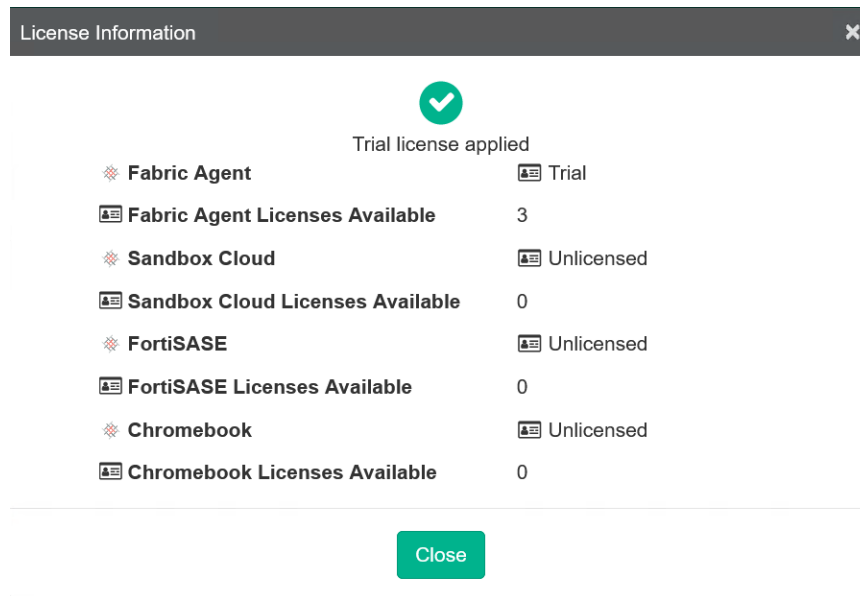
1. In EMS, go to *Zero Trust Tags > Zero Trust Tagging Rules*.
2. Click *Import Signatures*.



3. In the *Import FortiGuard Outbreak Alert Signatures* dialog, upload a JSON file. The JSON file should contain an array of alert objects, each with a tag name and array of signatures. Each signature should have the following properties: `os` (windows, mac, linux, ios, android), `type` (file, registry, process), and `content`. If the import succeeds, EMS displays a *FortiGuard outbreak alert signatures imported successfully* message. If the file is formatted incorrectly, EMS shows an *Invalid JSON* error.
4. View tagged endpoints in *Zero Trust Tags > Zero Trust Tag Monitor*.

EMS free trial license endpoint number change

The EMS free trial license now allows provisioning and management of three Windows, macOS, Linux, iOS, and Android endpoints, as opposed to ten. This change applies to EMS 6.2 and 6.4.



Air-gapped network support - 6.4.3

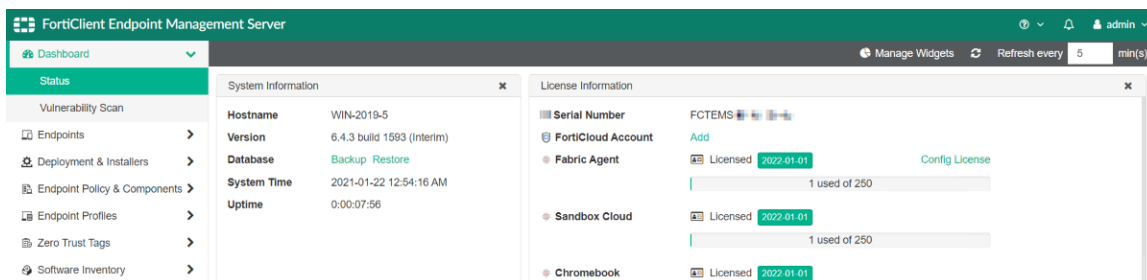
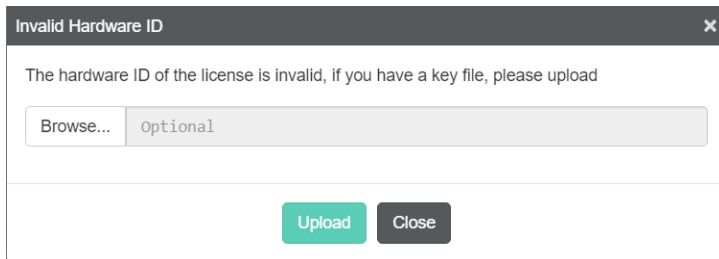
If you are deploying EMS in an air-gapped or isolated network where EMS cannot access the Internet, you can configure EMS to receive updates from FortiManager to deploy to FortiClient. In offline mode, FortiManager allows export and import of FortiGuard packages from FortiManager for provisioning as a FortiGuard distribution server. You can export FortiGuard packages from an online FortiManager to import to an offline FortiManager that will provide signature, engine, and FortiClient installer updates to EMS. EMS receives AntiVirus, Web Filter, Application Firewall, Vulnerability Scan, and Sandbox signatures and engines updates and FortiClient installers from FortiManager and deploys updates to FortiClient while in an air-gapped or isolated network.

This feature is also useful if you have experienced hardware failure and need to install EMS on another server. Fortinet customer support can provide a key file to allow you to apply your original license to EMS on the new server.

To configure EMS for an air-gapped network:

1. Contact [Fortinet Customer Service & Support](#). Provide them with your original EMS license file and the IP address of the new machine where you will install EMS. They provide you with a key file.
2. Install EMS. See [Installing FortiClient EMS](#).
3. Go to *System Settings > EMS settings*. Ensure that the value in the *Listen on IP* field matches the IP address that you gave to Customer Service & Support in step 1. Otherwise, EMS will not be able to validate the key file.
4. In EMS, on the *License Information* widget, select *Config License*.
5. For *License Source*, select *File Upload*.

6. In *License File*, browse to and upload your original license file.
7. EMS detects that the hardware ID associated with the license has changed and prompts you to upload the key file. Browse to and upload the key file that Customer Service & Support provided to you. If the key file matches the license file, the EMS license is activated.



8. Enable EMS to use FortiManager for signature updates:
 - a. Go to *System Settings > FortiGuard Servings*.
 - b. Enable *Use FortiManager for client software/signature updates*.
 - c. Configure the fields for the desired FortiManager.
 - d. Click *Save*.
9. Enable endpoint profiles to use FortiManager for signature updates:
 - a. Go to *Endpoint Profiles > Manage Profiles*.
 - b. Select the desired profile.
 - c. On the *System Settings* tab, under *Update*, enable *Use FortiManager for Client Signature Update*.
 - d. Configure the fields for the same FortiManager as you configured in step 8.
 - e. Configure the update schedule as desired.
 - f. Click *Save*.

Index

The following index provides a list of all new features added to FortiClient and EMS 6.4. The index allows you to quickly identify the version where the feature first became available in FortiClient and EMS.

6.4.0

- SAML support for SSL VPN on page 5
- Identity compliance on page 8
- Endpoint quarantine for Linux on page 9
- FortiSandbox Cloud support for macOS on page 27
- Keyword block support on page 29

6.4.1

- Collecting and sending macOS host events to FortiAnalyzer 6.4.1 on page 11
-

6.4.2

- Expanded on-fabric detection rules 6.4.2 on page 11
- Compliance verification terminology renamed to Zero Trust 6.4.2 on page 15

6.4.3

- Backup VPN connection 6.4.3 on page 22
- Air-gapped network support 6.4.3 on page 51

6.4.4

- [Secure remote access compliance enforcement 6.4.4 on page 23](#)
- [FortiGuard Outbreak Alerts service 6.4.4 on page 50](#)

Change log

Date	Change description
2020-05-12	Initial release.
2020-06-01	Added SAML support for SSL VPN on page 5.
2020-06-18	Added EMS free trial license endpoint number change on page 51.
2020-08-24	Initial release of FortiClient & FortiClient EMS 6.4.1.
2020-12-17	Initial release of FortiClient & FortiClient EMS 6.4.2.
2021-01-26	Added Sending upstream connection information for FortiClient (macOS) off-Fabric connections 6.4.2 on page 49.
2021-02-09	Initial release of FortiClient & FortiClient EMS 6.4.3.
2021-03-09	Added .
2021-05-10	Added Selecting closest gateway for VPN connection 6.4.1 on page 16.
2021-05-17	Added: <ul style="list-style-type: none">• Compliance verification terminology renamed to Zero Trust 6.4.2 on page 15• Collecting and sending macOS host events to FortiAnalyzer 6.4.1 on page 11• FortiSandbox Cloud support for macOS on page 27• Blocking removable devices by class ID 6.4.2 on page 33• FortiClient (Windows) moderate and strict Safe Search levels support 6.4.2 on page 35
2021-05-18	Updated Application-based split tunnel 6.4.2 on page 18.
2021-06-02	Initial release of FortiClient & FortiClient EMS 6.4.4.
2021-07-14	Added Backup VPN connection 6.4.3 on page 22 and Secure remote access compliance enforcement 6.4.4 on page 23.
2022-09-19	Updated Application-based split tunnel 6.4.2 on page 18.
2025-06-05	Updated Endpoint classification tags 6.4.1 on page 46.



FORTINET®



Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.