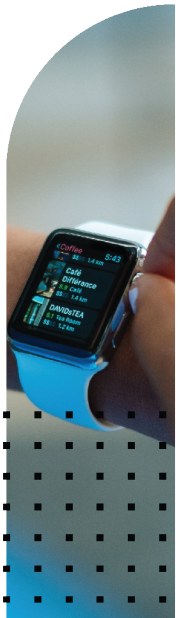
New Features Guide

FortiClient & FortiClient EMS 7.0



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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

September 24, 2021
FortiClient & FortiClient EMS 7.0 New Features Guide
04-700-715077-20210924

TABLE OF CONTENTS

Zero-trust network access

Endpoint: Fabric Agent

Improved TCP forwarding performance - 7.0.1

See ZTNA TCP forwarding access proxy without encryption example.

Endpoint: Remote Access

Dual stack IPv4 and IPv6 for SSL VPN - 7.0.1

FortiClient (Windows) has added SSL VPN dual stack support, where it can send IPv4 and IPv6 traffic over the same tunnel. By default, this feature is disabled. Only FortiOS 7.0 and later versions support this feature.

To enable dual stack for an SSL VPN tunnel in the GUI:

1. In FortiClient, on the *Remote Access* tab, select an existing VPN tunnel or create a new one.
2. Select the *Enable Dual-stack IPv4/IPv6 address* checkbox.

To enable dual stack for an SSL VPN tunnel in the XML:

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <connections>
            <connection>
               <dual_stack>1</dual_stack>
            </connection>
         </connections>
      </sslvpn>
   </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 SSL VPN configuration.

To configure dual stack in FortiOS:

```
config vpn ssl settings
   set dual-stack-mode enable
end
config firewall policy
   edit 14
      set name "ssl-wan1"
      set uuid 26f24a0a-09c4-51eb-daf7-cfb43cea057f
      set srcintf "ssl.root"
      set dstintf "wan1"
      set srcaddr "all"
      set dstaddr "all"
      set srcaddr6 "all"
      set dstaddr6 "myinternalV6"
      set action accept
      set schedule "always"
      set service "ALL"
      set logtraffic all
      set nat enable
      set groups "sslvpn-group" "pki"
      set users "test" "xyan" "dns-split"
   next
end
config firewall policy
   edit 21
```

```
      set uuid 94e3489a-b764-51eb-efad-b7b3762070dd
      set srcintf "ssl.root"
      set dstintf "lan"
      set srcaddr "all"
      set dstaddr "all"
      set srcaddr6 "all"
      set dstaddr6 "myinternalV6"
      set action accept
      set schedule "always"
      set service "ALL"
      set nat enable
      set groups "sslvpn-group"
   next
end
```

The following table summarizes the results:

	FortiOS enabled dual stack	FortiOS disabled dual stack
FortiClient enabled dual stack	FortiClient sends IPv4 and IPv6 traffic over the same tunnel.	The connection fails.
FortiClient disabled dual stack	FortiClient sends IPv4 traffic over an IPv4 tunnel. FortiClient sends IPv6 traffic over an IPv6 tunnel.	FortiClient sends IPv4 traffic over an IPv4 tunnel. FortiClient sends IPv6 traffic over an IPv6 tunnel.

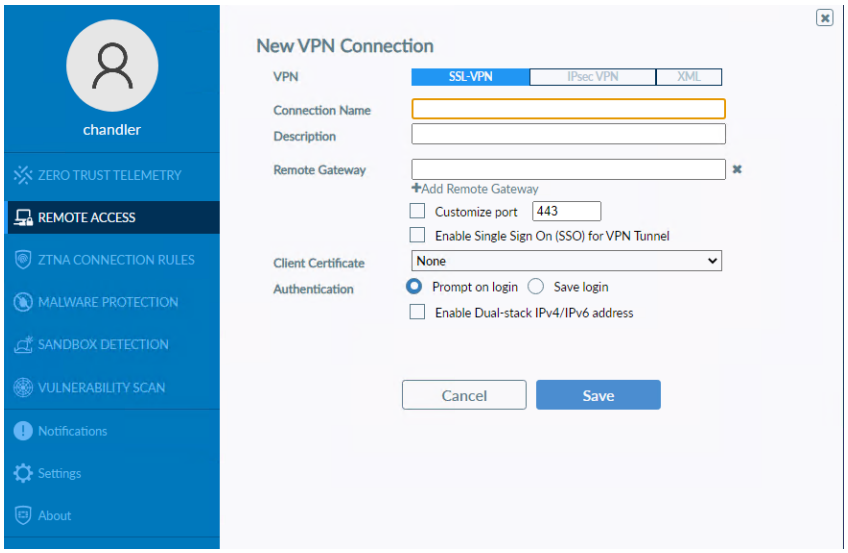
See the *FortiOS Administration Guide*.

SSL VPN security improvements

Default SSL VPN security settings have been improved to help decrease the risk of network attacks. The *Do Not Warn Invalid Server Certificate* option has been removed and is not enabled by default.

After installing FortiClient 7.0 and connecting to EMS, go to Settings. You can see that by default, *Do Not Warn Invalid Server Certificate* is disabled.

When configuring a new SSL VPN tunnel or editing an existing one, the *Do Not Warn Invalid Server Certificate* is not available.



Using a browser as an external user-agent for SAML authentication in an SSL VPN connection - 7.0.1

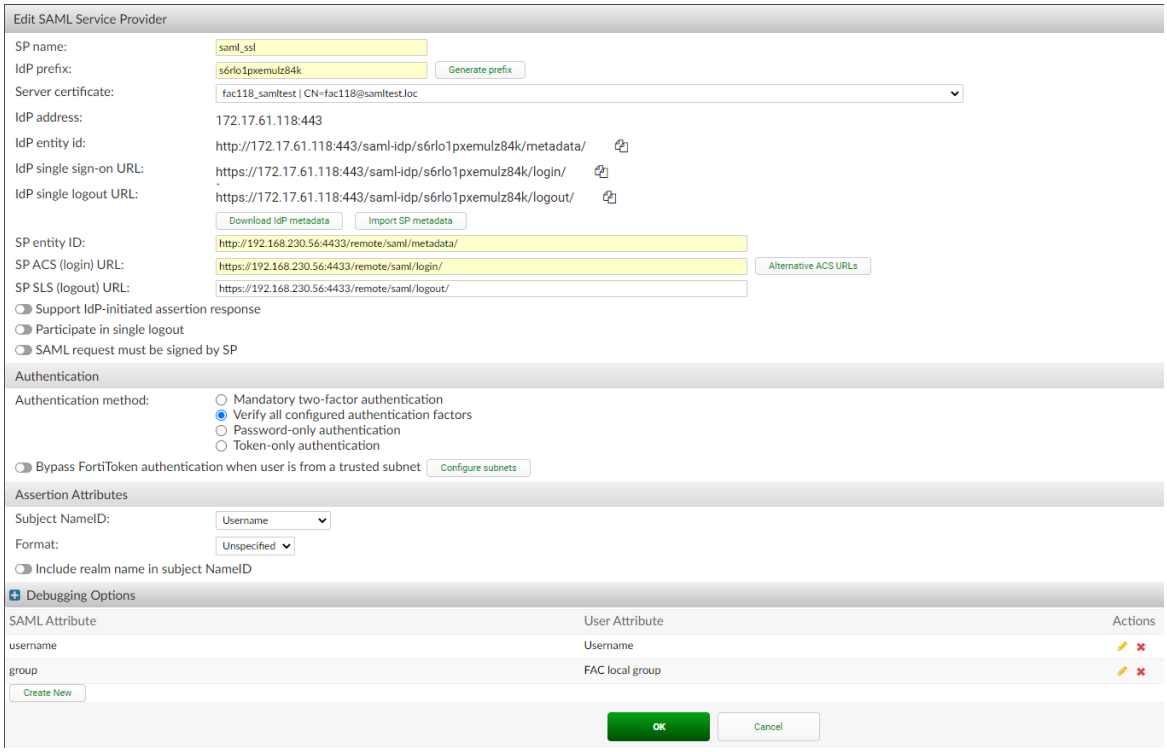
When establishing an SSL VPN tunnel connection, FortiClient can present a SAML authentication request to the end user in a web browser.

FortiClient (Windows) and (macOS) 7.0.1 and EMS 7.0.1 support this feature. FortiClient (Linux) 7.0.1 does not support this feature.

This feature is not supported when SSL VPN realms are configured. When SSL VPN realms are configured and the user provides their SAML authentication credentials in an external browser, FortiClient fails to establish the SSL VPN connection.

To configure FortiAuthenticator as the identity provider (IdP):

1. In FortiAuthenticator, go to *Authentication* > *SAML IdP* > *Service Providers*.
2. Configure a new service provider (SP) for SAML.



3. Go to *Authentication* > *User Management* > *Local Users*.
4. Create a new user.

To configure FortiGate as a SAML SP:

1. In the FortiOS CLI, create a SAML user. Ensure that the SP and IdP details match the details provided by FortiAuthenticator:

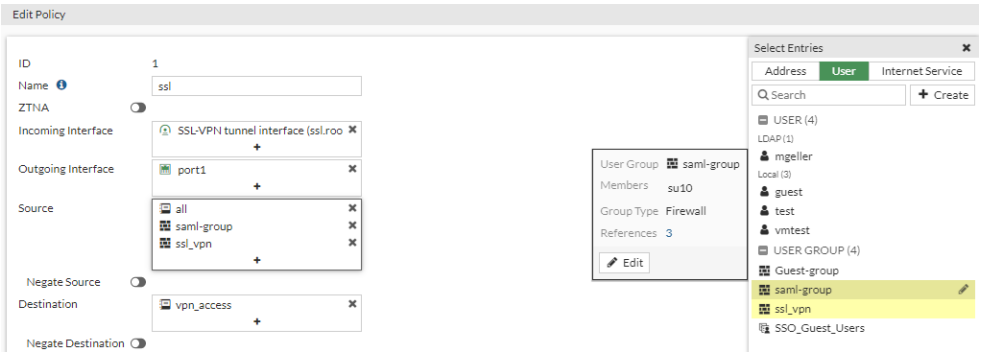
```
config user saml
   edit "su10"
      set cert "Fortinet_Factory"
      set entity-id "http://192.168.230.56:4433/remote/saml/metadata/"
      set single-sign-on-url "https://192.168.230.56:4433/remote/saml/login/"
      set single-logout-url "https://192.168.230.56:4433/remote/saml/logout/"
      set idp-entity-id "http://172.17.61.118:443/saml-idp/s6rlo1pxemulz84k/metadata/"
      set idp-single-sign-on-url "https://172.17.61.118:443/saml-
           idp/s6rlo1pxemulz84k/login/"
      set idp-single-logout-url "https://172.17.61.118:443/saml-
           idp/s6rlo1pxemulz84k/logout/"
      set idp-cert "REMOTE_Cert_1"
      set user-name "username"
      set group-name "group"
      set digest-method sha1
   next
end
```

2. Ensure that the SAML redirect port is set to 8020. SAML external browser authentication uses port 8020 by default. If another service or application is occupying this port, FortiClient displays a message showing that the SAML

redirect port is unavailable.:

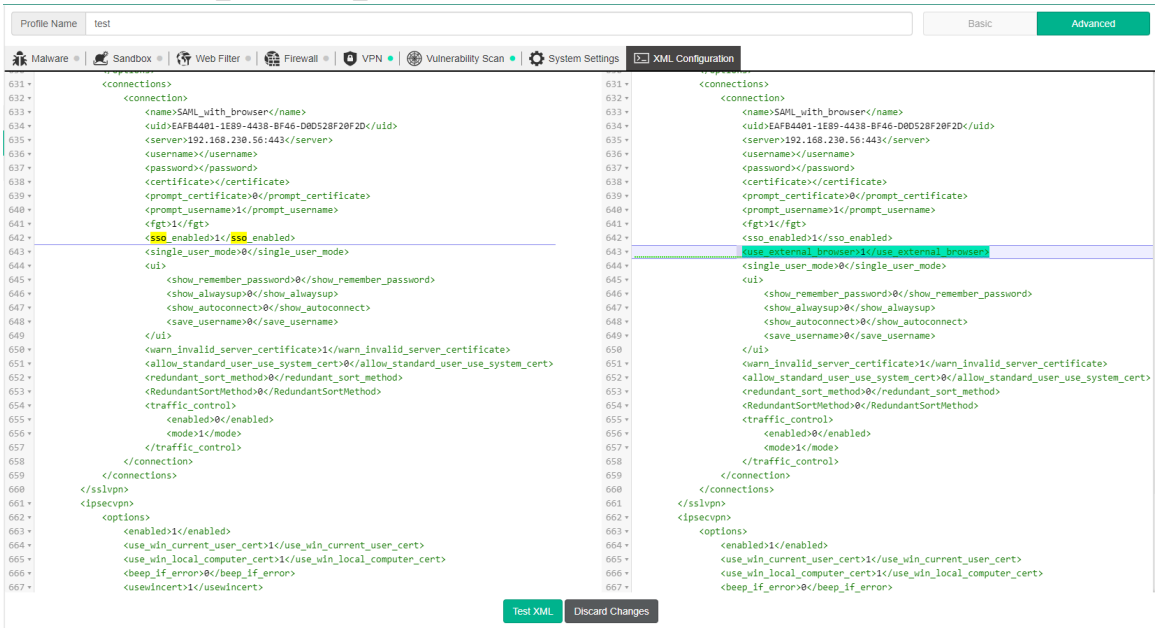
```
config vpn ssl setting
   show full-configuration | grep 8020
      set saml-redirect-port 8020
   next
end
```

3. Create a user group by going to *User & Authentication* > *User Groups* > *Create New*. Provide the required details and add the user that you created in step 1 to this group.
4. Go to *VPN* > *SSL-VPN Settings*. Under *Authentication/Portal Mapping*, create a mapping with the user group that you created in step 3. From the *Portal* dropdown list, select *full-access*. Click *OK*.
5. Go to *Policy & Objects* > *Firewall Policy*. Select the SSL VPN firewall policy. Ensure that the *Source* field includes the SAML user group.



To configure external browser for authentication in EMS:

1. In EMS, go to *Endpoint Profiles* > *Manage Profiles*, and edit the desired profile.
2. On the *VPN* tab, click *Add Tunnel*. Provide the correct gateway information. In *Advanced Settings*, enable *Enable SAML Login*. Configure other fields as desired. Save the tunnel.
3. On the *XML Configuration* tab, under the `<sso_enabled>` element for the tunnel, add `<use_external_browser>1</use_external_browser>`.



4. Click *Test XML*, then save the configuration.

To test the connection in FortiClient:

1. After FortiClient receives the latest configuration update from EMS, go to the *Remote Access* tab.
2. View the tunnel to verify that the *Use external browser as user-agent for saml user authentication field* is enabled.
3. Connect to the tunnel by clicking *SAML Login*. Verify that FortiClient opens your default browser to prompt for authentication. Provide your credentials and click *Login* to establish the connection.

FortiClient EMS

Zero-trust network access

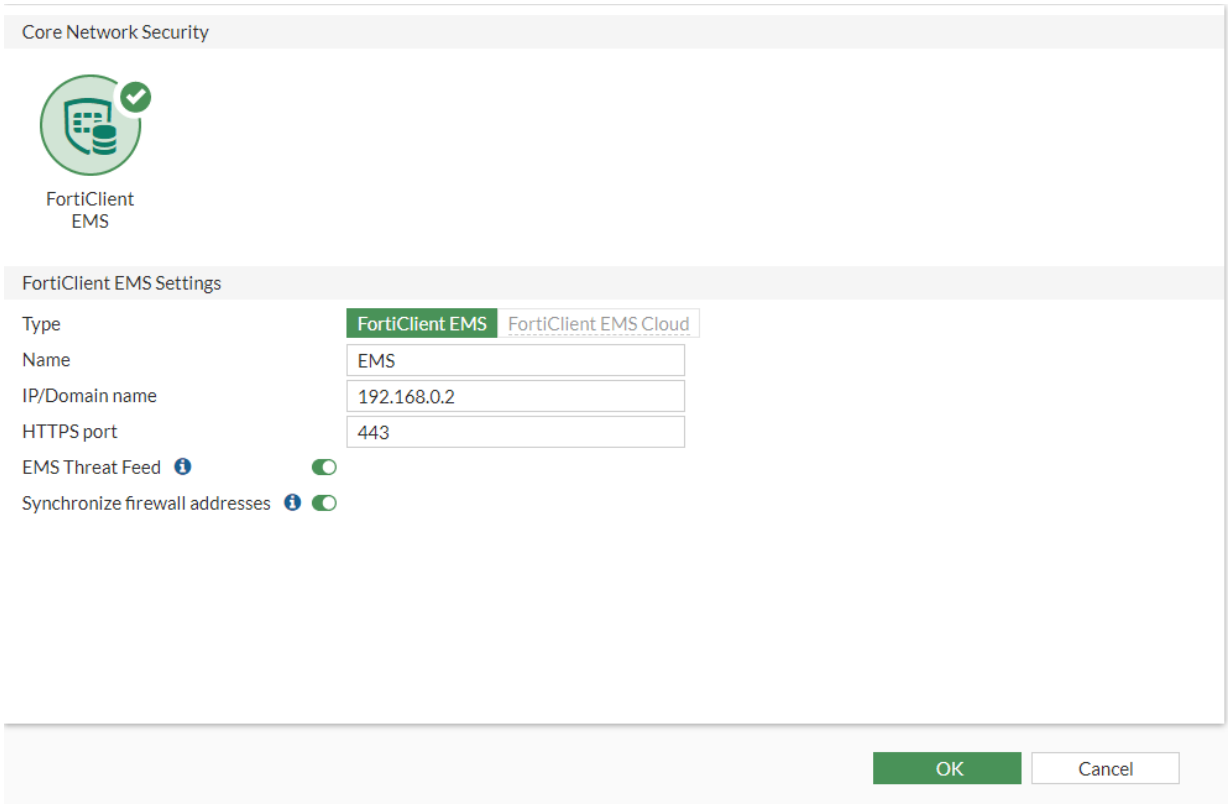
EMS distributes SSL deep inspection CA certificates - 7.0.1

FortiGate can push certificate authority (CA) certificates directly to EMS once it establishes communication with EMS. You no longer have to manually import CA certificates from FortiGate to EMS.

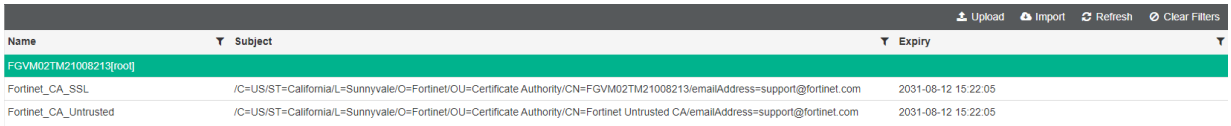
The following instructions assume that FortiGate, EMS, and a FortiClient (Windows) endpoint are already operating as components of a Fortinet Security Fabric. FortiClient is connected to EMS.

To configure EMS to distribute FortiGate CA certificates to FortiClient endpoints:

1. Create an EMS Fabric connector in FortiOS:
   a. In FortiOS, go to *Security Fabric* > *Fabric Connectors*.
   b. Click *Create New*.
   c. Create a new Fabric connector for EMS.

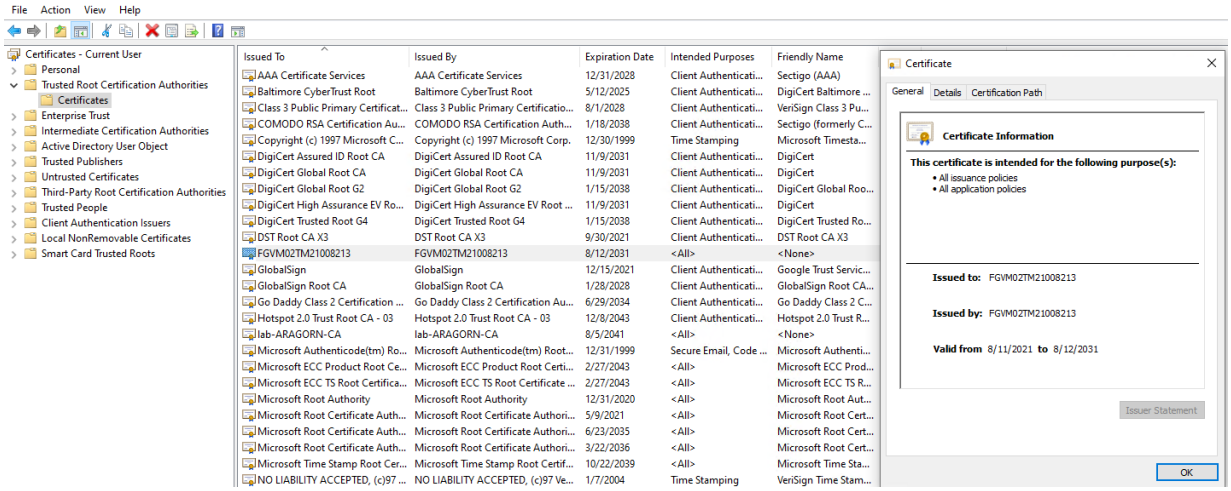


2. Configure EMS to import the certificates:
   a. In EMS, go to *Administration* > *Fabric Devices*.
   b. Authorize the connection request from the FortiGate.
   c. Once the connection succeeds, EMS automatically imports FortiGate CA certificates. To verify this, go to *Endpoint Policy & Components* > *CA Certificates*. This pane lists certificates under the FortiGate serial number.



3. Go to *Endpoint Profiles* > *Manage Profiles*.

4. Select the profile that is applied to the endpoint.
5. On the *System Settings* tab, enable *Install CA Certificate on Client*. Once enabled, the field displays the imported FortiGate certificates. Select the desired certificates to distribute to the endpoints.
6. Click *Save*.
7. After the endpoint receives the profile updates from EMS, open the Manage Computer certificates/Manage User certificates console on the endpoint.
8. Go to *Trusted Root Certification Authorities* > *Certificates*.
9. Confirm that the selected certificates are installed.



Zero Trust tagging rules enhancement - 7.0.1

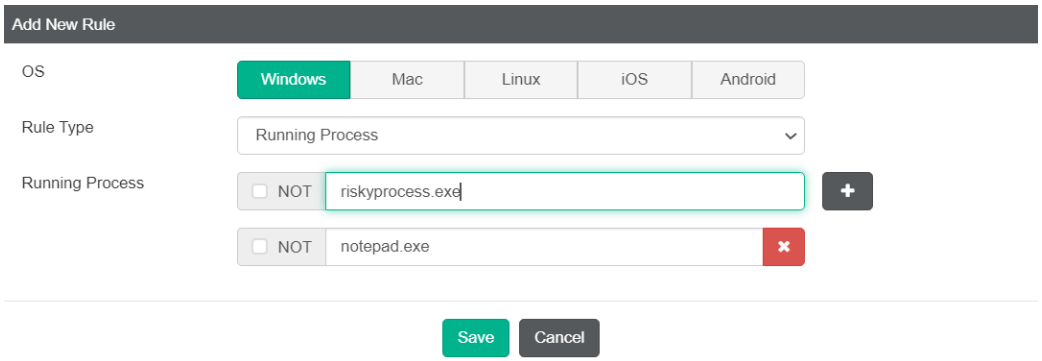
FortiClient EMS adds the following enhancements to Zero Trust tagging rules:

- Logical OR operation support on page 13
- Importing and exporting Zero Trust tagging rules on page 15
- On-Fabric rules on page 16

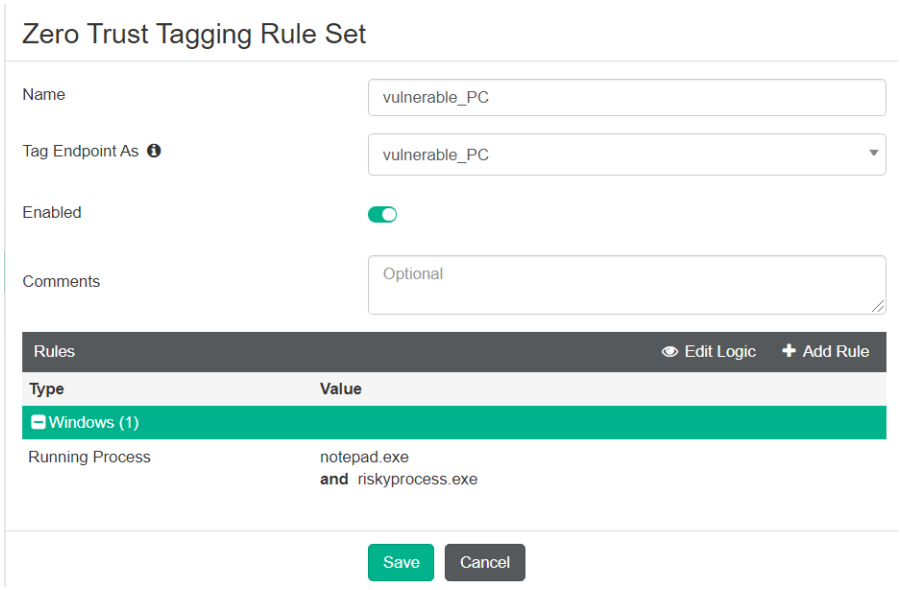
Logical OR operation support

To configure a rule using OR:

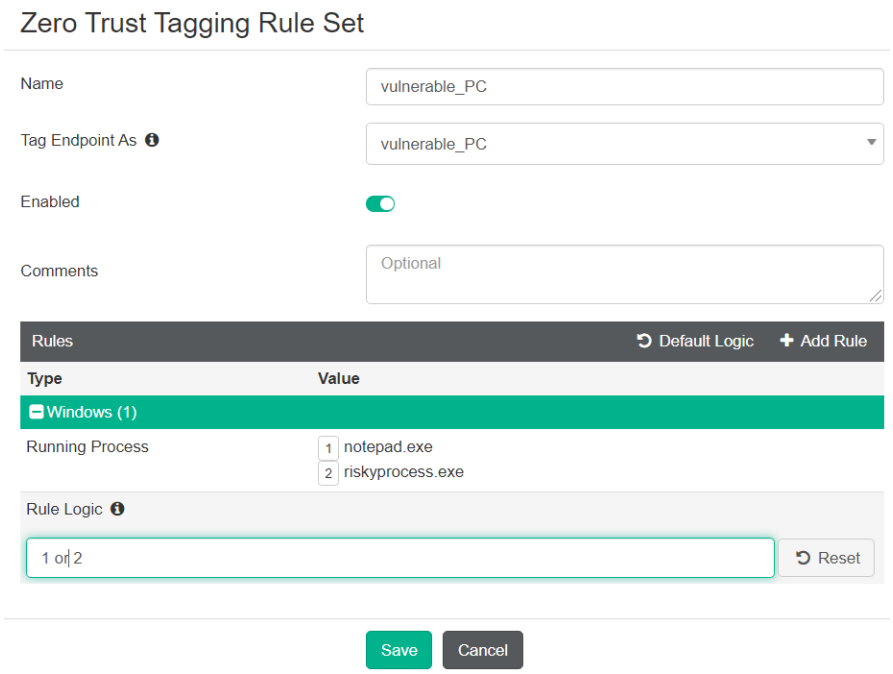
1. Go to *Zero Trust Tags* > *Zero Trust Tagging Rules*.
2. Click *Add*.
3. Click *Add Rule*.
4. Configure a rule as desired. This example configures a Windows running process rule that checks that Notepad and riskyprocess.exe are running on the endpoint.



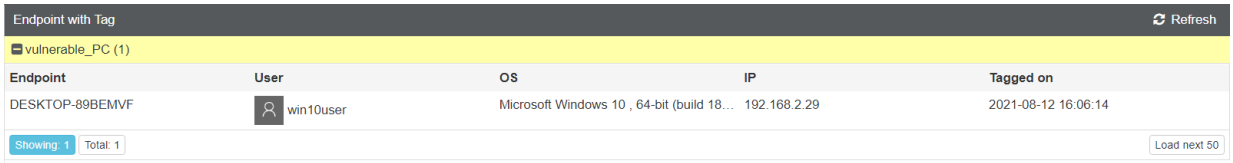
5. Click *Save*. By default, the rule is configured with the logical AND operation. Therefore, in this example, the rule checks that both Notepad and riskyprocess.exe are running on the endpoint.



6. Click *Edit Logic*. Change the logic to OR, then click *Save*.



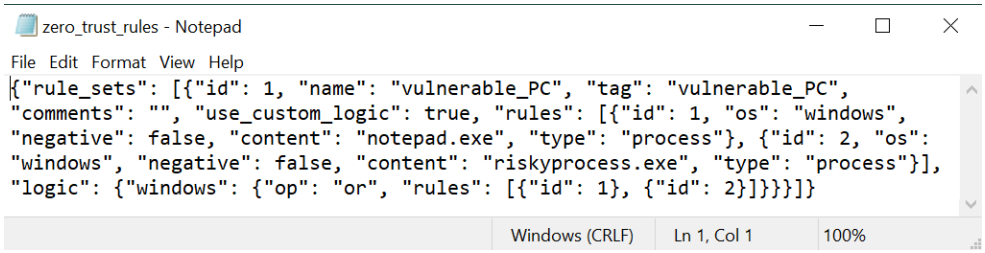
7. To verify the rule, run Notepad on an endpoint that is connected to EMS. Verify that no process named riskyprocess.exe is running on the endpoint.
8. In EMS, go to *Zero Trust Tags* > *Zero Trust Tag Monitor*. Confirm that the endpoint appears under the vulnerable_PC rule.



Importing and exporting Zero Trust tagging rules

To import and export Zero Trust tagging rules:

1. Go to *Zero Trust Tags* > *Zero Trust Tagging Rules*.
2. Click *Export* to export the currently defined rules.
3. Ensure that a JSON file of the rules is downloaded.



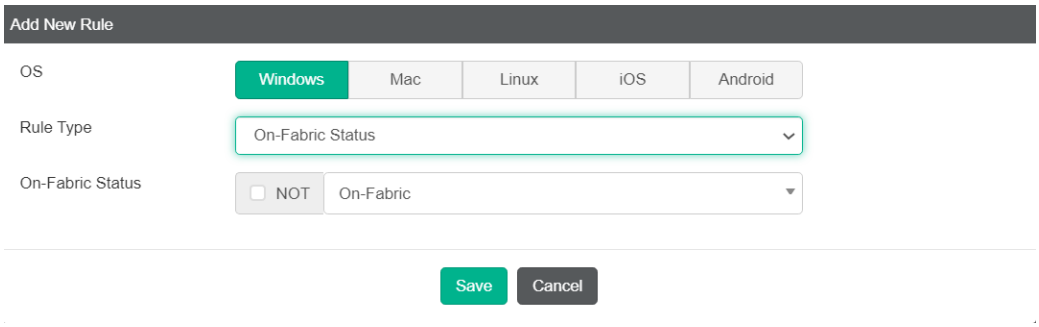
4. You can use import the same rules to another EMS using the JSON files. On another EMS, go to *Zero Trust Tags* > *Zero Trust Tagging Rules* and click *Import*. Browse to and select the desired JSON file. Click *Import*.

On-Fabric rules

EMS supports on-Fabric Zero Trust tagging rules. EMS currently does not support the NOT option for this rule type.

To create an on-Fabric/off-Fabric rule:

1. Go to *Zero Trust Tags* > *Zero Trust Tagging Rules*.
2. Click *Add*.
3. Click *Add Rule*.
4. From the *Rule Type* dropdown list, select *On-Fabric Status*.
5. Click *Save*.



Provisioning ZTNA TCP forwarding rules via EMS - 7.0.1

You can configure ZTNA TCP forwarding rules on the *XML Configuration* tab in an endpoint profile in EMS to push the same rules to multiple endpoints, instead of manually configuring the rules on each endpoint.

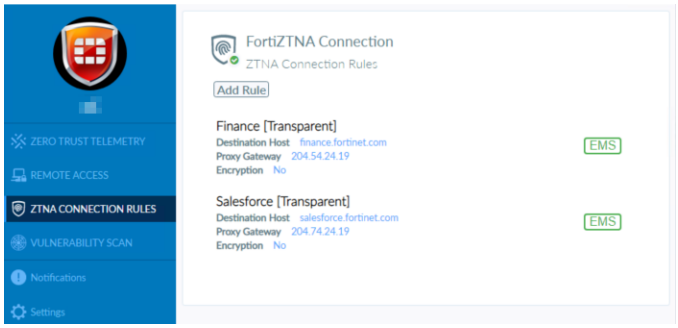
To configure ZTNA TCP forwarding rules via EMS:

1. In EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Select the desired profile.
3. On the *XML Configuration* tab, edit the existing configuration to include the ZTNA rules elements. The following provides an example with two rules:

```
<ztna>
   <enabled>1</enabled>
   <enable_chrome>0</enable_chrome>
   <rules>
      <rule>
         <name>Salesforce</name>
         <destination>salesforce.fortinet.com</destination>
         <gateway>204.74.24.19</gateway>
         <mode>transparent</mode>
         <encryption>0</encryption>
      </rule>
      <rule>
         <name>Finance</name>
         <destination>finance.fortinet.com</destination>
         <gateway>204.54.24.19</gateway>
         <mode>transparent</mode>
         <encryption>0</encryption>
      </rule>
```

```
    </rules>
</ztna>
```

4. Save the profile. After the endpoint receives the profile updates from EMS, you can find the TCP forwarding rules on the FortiClient *ZTNA Connection Rules* tab.



FortiClient does not currently support enabling encryption for a ZTNA rule using XML configuration. If you configure `<encryption>` as `1`, encryption remains disabled for the rule in FortiClient.

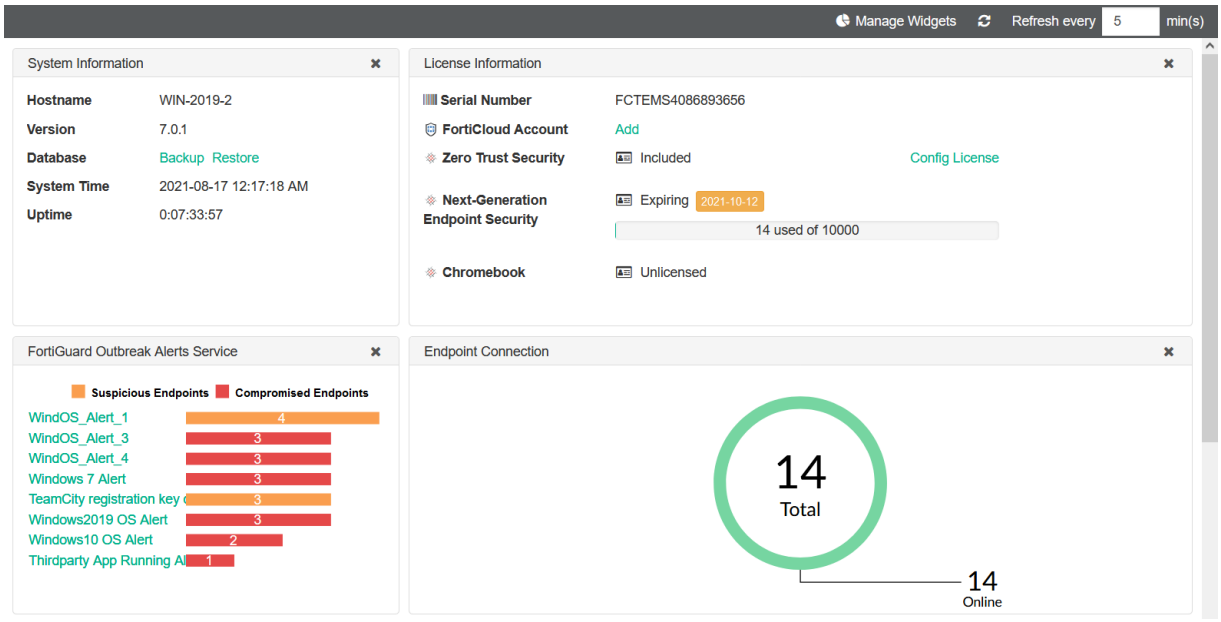
FortiGuard Outbreak Alerts service - 7.0.1

When a new outbreak is discovered in the field, Fortinet releases a new FortiGuard package. This process is as follows:

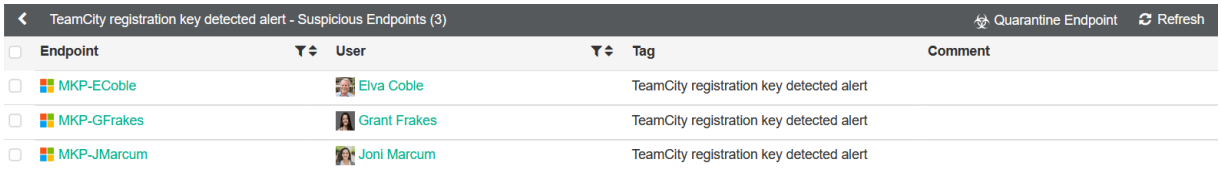
1. Fortinet creates and tests a new FortiGuard outbreak alert rule.
2. Fortinet packages the rule into a FortiGuard object.
3. Fortinet uploads the object to the FortiGuard server.
4. EMS downloads the object from FortiGuard.
5. EMS processes the rule and installs it.
6. If FortiClient detects the outbreak in an endpoint as per the new rule, it tags it accordingly.
7. The EMS administrator can use the outbreak alert tag to quarantine endpoints where FortiClient has detected the outbreak.

A maximum of ten FortiGuard outbreak alert rules can be enabled at the same time.

You can enable the *FortiGuard Outbreak Alerts* Service widget on the dashboard to see outbreak alert details.



You can drill down from this widget to see the list of affected endpoints. You can quarantine endpoints from this pane.



The endpoint summary page also shows any FortiGuard outbreak alert tags applied to the endpoint.

Sending invitation emails

In FortiClient Cloud, administrators can send endpoint users invitation emails to help them connect their FortiClient to FortiClient Cloud. You can now also send invitation emails as an on-premise EMS administrator. This helps non-expert end users to easily connect EMS by copying and pasting their invitation code, scanning a QR code, or clicking the *Register to EMS* link in the invitation email. End users do not need to know the EMS IP address, port number, or site information to connect their endpoint to EMS.

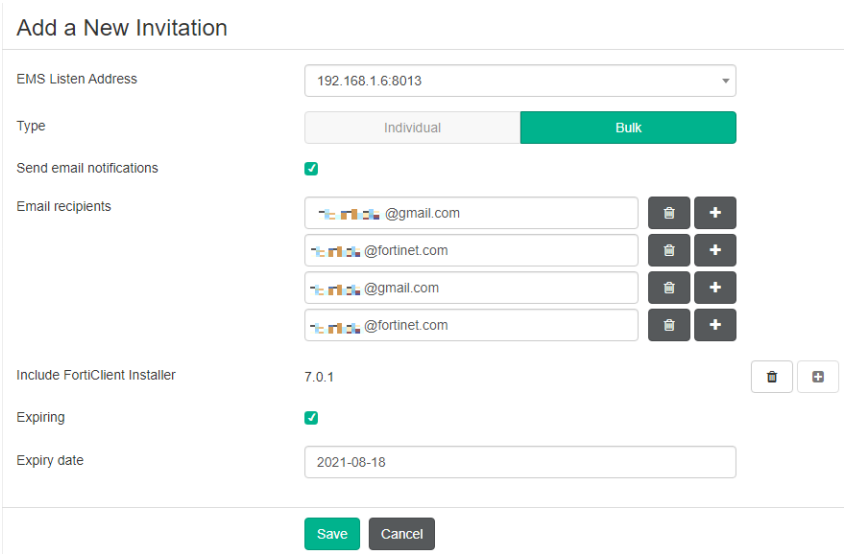
You can enforce that only endpoints that were invited using an invitation email can connect to and be managed by EMS using the *Enforce invitation-only registration for* option in *System Settings* > *EMS Settings*.

To configure an invitation email:

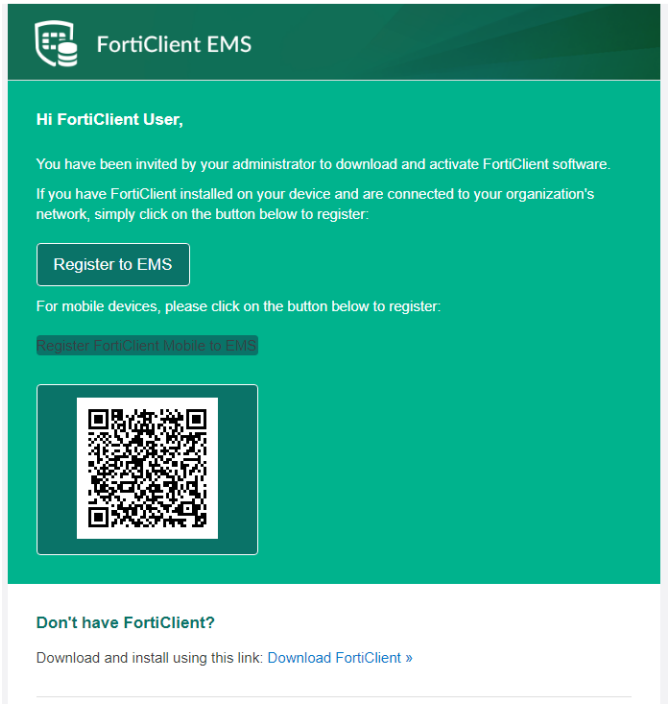
1. Go to *Endpoints* > *Invitations*.
2. Click *Add*.

3. Configure the following fields:

Option	Description
EMS Listen Address	From the dropdown list, select the desired IP address/FQDN to include in the invitation code. FortiClient connects to EMS using this IP address/FQDN.
Type	Select *Individual* to support registering a single endpoint or *Bulk* to support registering multiple endpoints using the same invitation code.
Send email notifications	Enable this option to send the invitation email to an end user. You can only enable this option if you have configured an SMTP server in EMS. See Configuring SMTP Server settings.
Email recipients	Enter one or multiple email addresses to send the invitation code to.
Include FortiClient Installer	Enable this option to include a FortiClient installer in the invitation code. Invitation codes for which this option is enabled must be bulk invitation codes.
Expiring	Enable this option to configure an expiry date for this invitation code.
Expiry date	Configure the desired expiry date for this invitation code. After the invitation code expires, FortiClient cannot register to EMS using this code. By default, the expiry date is five days from the current date.



4. Click *Save*.The endpoint user receives an email that includes an explanation of how to connect to EMS and can use the instructions in the email to connect to EMS.



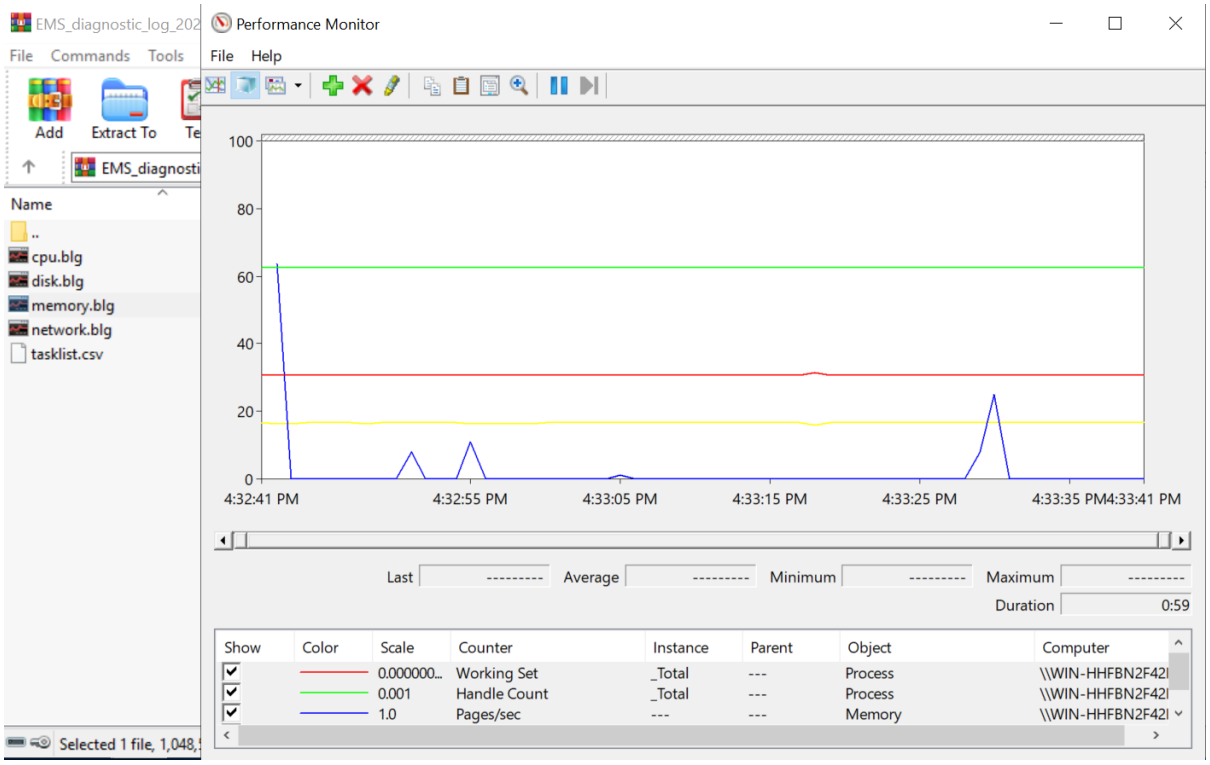
Diagnostic tool - 7.0.1

EMS offers the administrator a convenient means of collecting debug logs available from various backend services into one archive file.

To generate EMS diagnostic logs:

1. Go to *Administration* > *Generate Diagnostic Logs*.
2. If desired, enable *Include Database Backup*.
3. Enter a password to protect the database backup.
4. After entering the password, click *Create*.
5. Wait for a few minutes while EMS records the diagnostic logs. Once EMS creates the log, click *Download* to download it. The diagnostic logs contain diagnostic files that can assist support and development teams to investigate on any issues that pertain to EMS. This mainly comprises of a lightweight database backup, snapshot of CPU and memory usage, EMS logs, and SQL Server files. The following screenshot shows the recording of CPU

and memory usage during EMS diagnosis.



FortiClient Cloud Chromebook support - 7.0.1

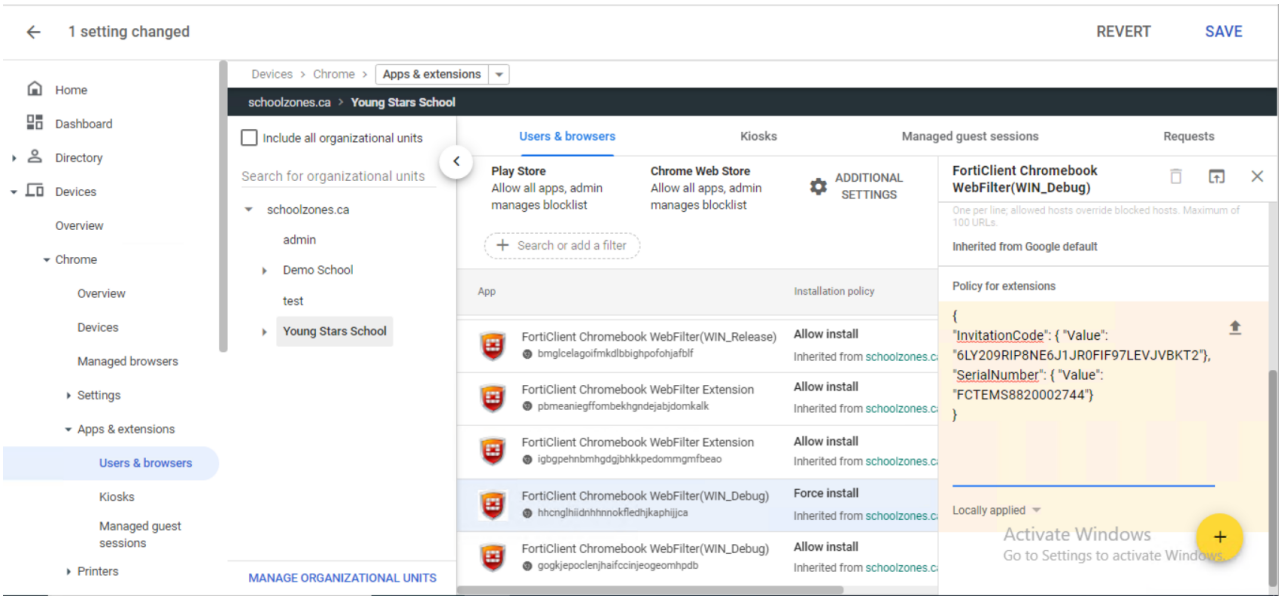
FortiClient Chromebook endpoints can connect to FortiClient Cloud. When using FortiClient Cloud, FortiClient Chromebook endpoints communicate with the FortiClient Cloud proxy and FortiClient Cloud redirects traffic to the correct FortiClient Cloud host.

This change does not affect the end user. The FortiClient Cloud-side configuration is the same as when configuring on-premise EMS for Chromebook management, except the extension policy that you must push out via the Google Admin console to the Chromebooks.

To configure the extension policy for FortiClient Cloud:

1. In the Google Admin console, go to *Devices* > *Chrome* > *Apps & extensions* > *Users & browsers*.
2. Select the extension that you want to push to the Chromebooks.
3. Configure the policy using the invitation code and serial number from your FortiClient Cloud environment. You can find the invitation code by going to *Invitations* in the upper right corner of the FortiClient Cloud GUI. You can find the serial number in the *License Information* widget on the *Dashboard*:

```
{
"InvitationCode": { "Value": "6LY209RIP8NE6J1JR0FIF97LEVJVBKT2"},
"SerialNumber": { "Value": "FCTEMS8820002744"}
}
```



FortiClient license and EMS communication enhancements

The following enhancements have been made to FortiClient license and EMS communication:

- The EMS administrator can prohibit or allow end users to shut down FortiClient.
- FortiClient locally stores its applied license expiry date. Even if FortiClient cannot reach EMS, the features that it is licensed for are still available to the endpoint until the stored license expiry date.

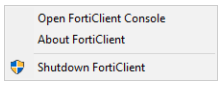
To prohibit end users from shutting down FortiClient:

1. In EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Select the desired profile.
3. On the *System Settings* tab, ensure that *Allow User to Shutdown When Registered to EMS* is disabled.
4. On the *XML Configuration* tab, ensure that the `<system><ui><allow_shutdown_when_registered>` element is configured as `0`.
5. Click *Save*.
6. After an endpoint with the selected profile applied receives the updates from EMS, on the endpoint machine, right-click the FortiTray icon and verify that *Shutdown FortiClient* is grayed out.

To allow end users to shut down FortiClient:

1. In EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Select the desired profile.
3. On the *System Settings* tab, enable *Allow User to Shutdown When Registered to EMS*.
4. On the *XML Configuration* tab, ensure that the `<system><ui><allow_shutdown_when_registered>` element is configured as `1`.
5. Click *Save*.
6. After an endpoint with the selected profile applied receives the updates from EMS, on the endpoint machine, right-click the FortiTray icon and verify that *Shutdown FortiClient* is not grayed out.

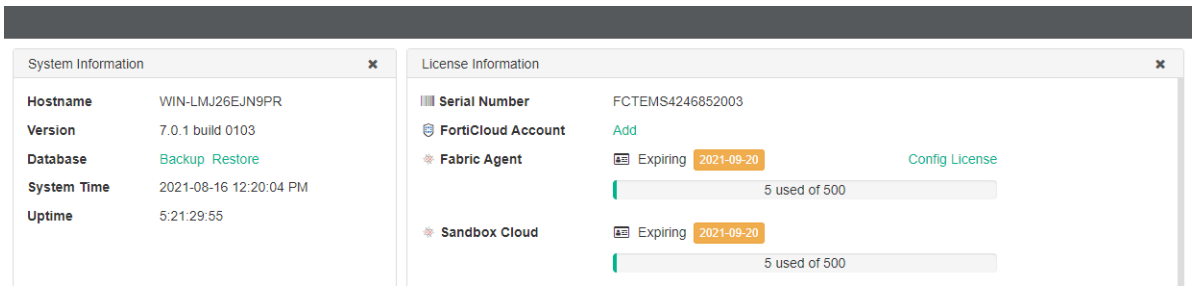
7. Select *Shutdown FortiClient*.



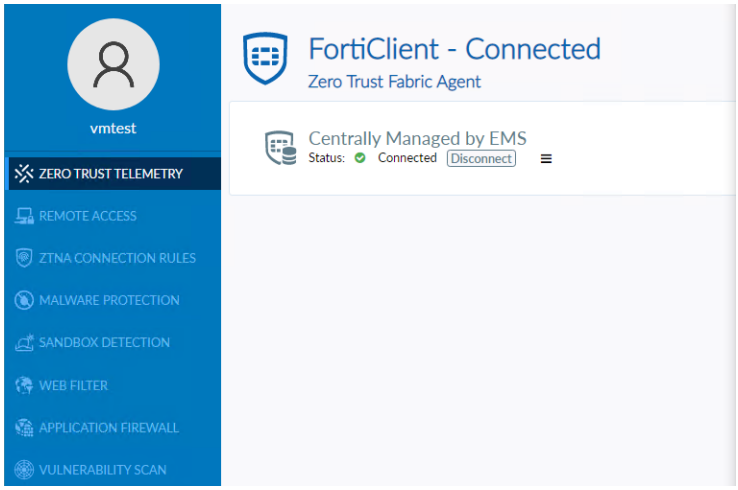
8. In the resulting dialog, click *Yes* to successfully shut down FortiClient. You can restart FortiClient by double-clicking its icon.

To verify that FortiClient stores its license expiry date:

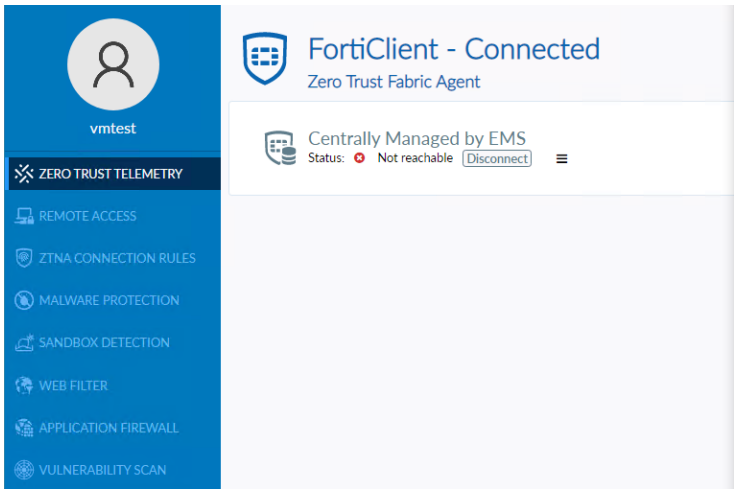
1. Go to the EMS Dashboard. Verify the license expiry date. In this example, the license expires on September 20, 2021.



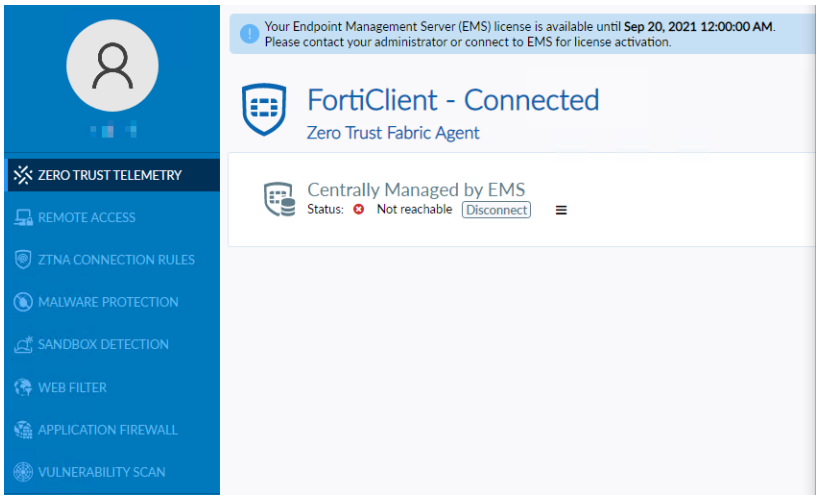
2. Open FortiClient on an endpoint that is connected to EMS. Verify that all licensed features display on the FortiClient GUI.



3. Make the endpoint unreachable to EMS by disabling the network on the endpoint or EMS. Verify that all licensed features still display on the FortiClient GUI.



4. Change the date on the endpoint device to one day before the license expiry (September 19, 2021 in this example). Verify that the FortiClient GUI displays a license expiry warning and that the licensed features still display, since the license has not expired yet.



Change log

Date	Change Description
2021-04-27	Initial release.
2021-08-10	Added for release of 7.0.1: • Improved TCP forwarding performance 7.0.1 on page 4 • EMS distributes SSL deep inspection CA certificates 7.0.1 on page 12
2021-08-11	Added Dual stack IPv4 and IPv6 for SSL VPN 7.0.1 on page 5.
2021-08-16	Added: • SSL VPN security improvements on page 6 • Zero Trust tagging rules enhancement 7.0.1 on page 13 • Sending invitation emails on page 18 • Diagnostic tool 7.0.1 on page 20 Updated EMS distributes SSL deep inspection CA certificates 7.0.1 on page 12.
2021-08-17	Added Provisioning ZTNA TCP forwarding rules via EMS 7.0.1 on page 16, FortiClient license and EMS communication enhancements on page 22, and FortiGuard Outbreak Alerts service 7.0.1 on page 17.
2021-08-26	Added FortiClient Cloud Chromebook support 7.0.1 on page 21.
2021-09-22	Updated Dual stack IPv4 and IPv6 for SSL VPN 7.0.1 on page 5.
2021-09-24	Added Using a browser as an external user-agent for SAML authentication in an SSL VPN connection 7.0.1 on page 7.

www.fortinet.com