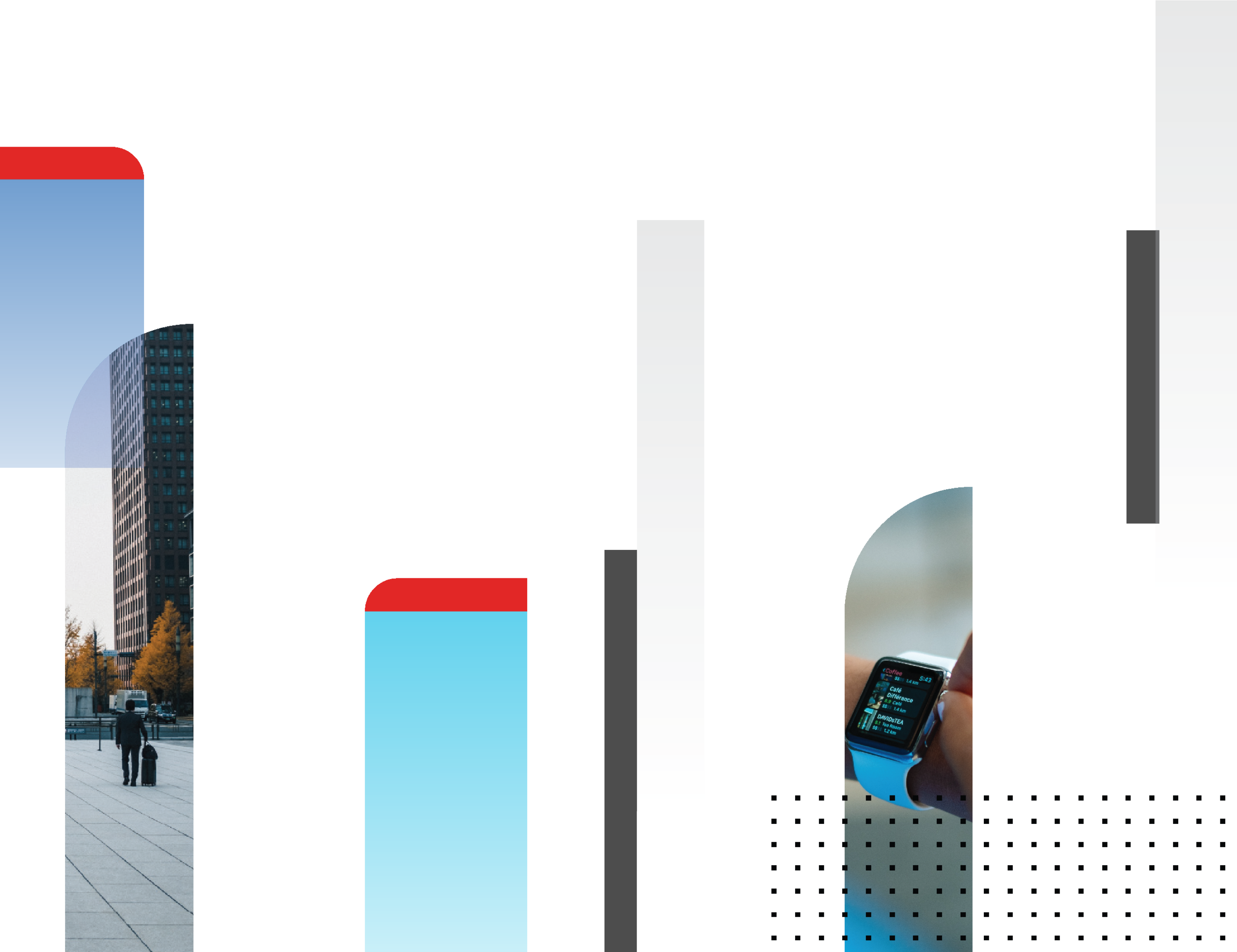
New Features Guide

FortiClient & FortiClient EMS 7.0



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

March 28, 2023
FortiClient & FortiClient EMS 7.0 New Features Guide
04-700-715077-20230328

TABLE OF CONTENTS

Overview

This guide provides details of new features introduced in FortiClient & FortiClient EMS 7.0. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable. The guide organizes features into the following sections:

- ZTNA on page 6
    - Endpoint: Fabric Agent on page 6
    - Endpoint: Remote Access on page 21
- FortiClient EMS on page 30
    - Zero-trust network access on page 30

For features introduced in 7.0.1 and later versions, the version number is found at the end of the topic heading. For example, EMS distributes SSL deep inspection CA certificates 7.0.1 on page 31 was introduced in 7.0.1. If a topic heading has no version number at the end, the feature was introduced in 7.0.0.

For a list of all features organized by the version number that they were introduced, see Index on page 72.

ZTNA

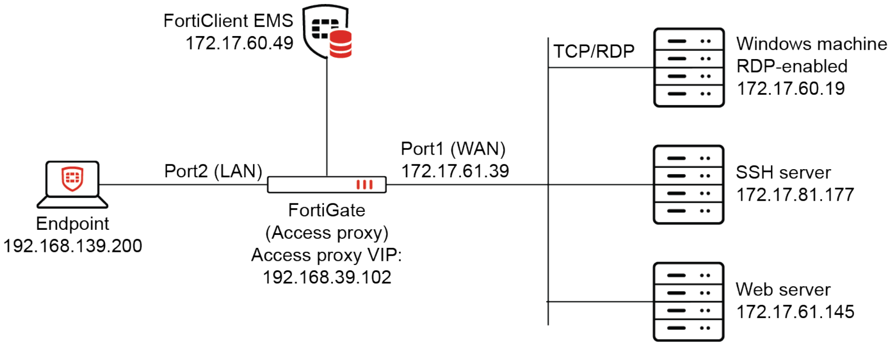
Endpoint: Fabric Agent

Improved TCP forwarding performance - 7.0.1

In 7.0.1, FortiClient supports encryption and non-encryption modes for zero trust network access (ZTNA) via a toggle switch. You can manually add ZTNA rules in the FortiClient GUI or receive rules from EMS. This feature requires the following prerequisites:

- You must configure a Fortinet Security Fabric connector between FortiOS and EMS.
- You must properly configure FortiOS ZTNA-related settings. See ZTNA TCP forwarding access proxy example.
- FortiClient must be registered to EMS.
- You must add ZTNA rules in EMS or FortiClient.

The following shows the topology for the example configuration. In this topology, RDP access is configured to one server, and SSH access to another.



To configure ZTNA rules in EMS:

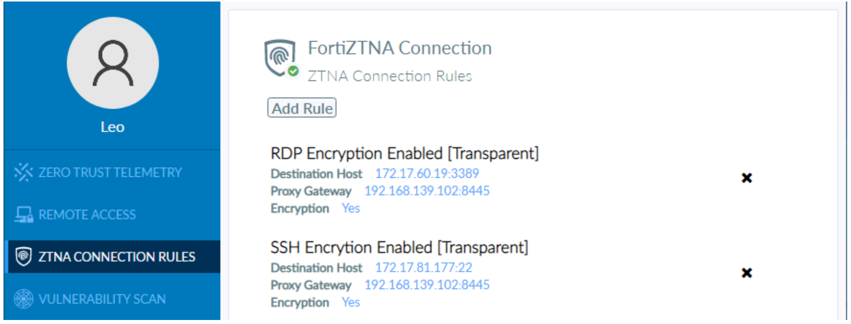
1. In EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Edit the desired profile.
3. On the *XML Configuration* tab, add the following configuration:

```
<ztna>
   <enabled>1</enabled>
   <rules>
      <rule>
         <name>RDP Forwarding</name>
         <destination>172.17.60.19:3389</destination>
         <gateway>192.168.139.102:8445</gateway>
         <encryption>1</encryption>
         <mode>transparent</mode>
      </rule>
      <rule>
         <name>SSH Forwarding</name>
         <destination>172.17.81.177:22</destination>
         <gateway>192.168.139.102:8445</gateway>
         <encryption>1</encryption>
         <mode>transparent</mode>
      </rule>
   </rules>
</ztna>
```

4. Save the configuration.

To configure ZTNA rules in FortiClient:

1. In FortiClient, go to the *ZTNA Connection Rules* tab.
2. Create the RDP forwarding rule:
   a. Click *Add Rule*.
   b. In the *Rule Name* field, enter RDP Encryption Enabled.
   c. In the *Destination Host* field, enter 172.17.60.19:3389.
   d. In the *Proxy Gateway* field, enter 192.168.139.102:8445.
   e. For *Mode*, select *Transparent*.
   f. Select the *Encryption* checkbox.
   g. Click *Create*.
3. Create the SSH forwarding rule:
   a. Click *Add Rule*.
   b. In the *Rule Name* field, enter SSH Encryption Enabled.
   c. In the *Destination Host* field, enter 172.17.81.177:22.
   d. In the *Proxy Gateway* field, enter 192.168.139.102:8445.
   e. For *Mode*, select *Transparent*.
   f. Select the *Encryption* checkbox.
   g. Click *Create*.



RDP Encryption Enabled [Transparent]
Destination Host 172.17.60.19:3389
Proxy Gateway 192.168.139.102:8445
Encryption Yes

SSH Encrytion Enabled [Transparent]
Destination Host 172.17.81.177:22
Proxy Gateway 192.168.139.102:8445
Encryption Yes

To verify the configuration:

1. Start an SSH connection to 172.17.81.177 via ZTNA.
2. Run debug commands in FortiOS:
   ```
   diagnose wad debug enable category all
   diagnose wad debug enable level verbose
   diagnose debug enable
   ```
3. Check the debug logs to verify whether encryption is enabled. When encryption is enabled, the debug logs contain the line `GET tcpaddress=172.17.81.177&port=22&tls=1 HTTP1.1`. When encryption is disabled, the debug logs contain the line `GET tcpaddress=172.17.81.177&port=22&tls=0 HTTP1.1`.

Antiransomware file backup and restoration - 7.0.2

After detecting ransomware behavior on the endpoint FortiClient restores files that the detected ransomware encrypted.

You can configure this feature using the following XML elements:

```
<forticlient_configuration>
   <rs_protection>
      <backup_interval>1</backup_interval>
      <backup_file_size_limit>1</backup_file_size_limit>
      <backup_disk_quota>10</backup_disk_quota>
   </rs_protection>
</forticlient_configuration>
```

XML tag	Description
`<backup_interval>`	Enter the desired backup interval value in hours. After the configured interval, FortiClient backs up files that the detected ransomware encrypted.
`<backup_file_size_limit>`	Enter the desired size limit in MB for ransomware-encrypted files for FortiClient to back up.
`<backup_disk_quota>`	Enter the desired backup disk quota value as a percentage.

See Antiransomware for the complete list of antiransomware XML elements.

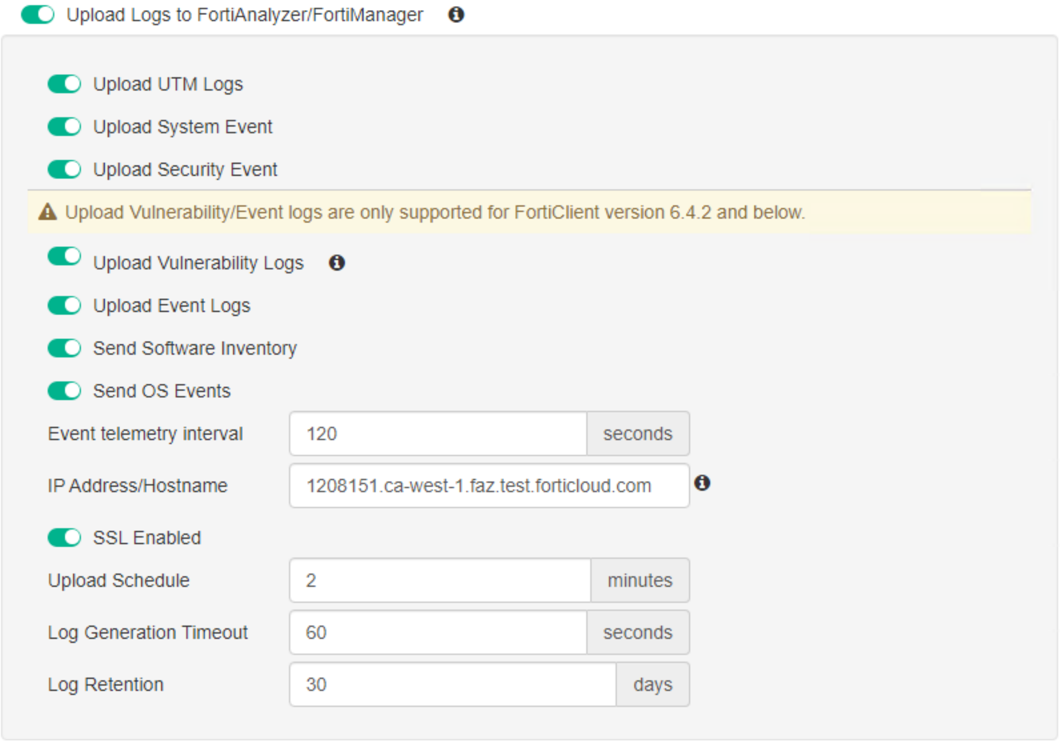
Logging to FortiAnalyzer Cloud - 7.0.3

This guide provides information on configuring and integrating FortiAnalyzer Cloud for logging support. To use this feature, you must have configured the appropriate license with FortiAnalyzer Cloud entitlement. The functionality is similar to on-premise FortiAnalyzer support for logging.

To configure logging to FortiAnalyzer Cloud:

1. In EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Edit the desired profile.
3. On the *Settings* tab, enable *Upload Logs to FortiAnalyzer/FortiManager*.

4. In the *IP Address/Hostname* field, enter the FortiAnalyzer Cloud instance fully qualified domain name.



- Upload Logs to FortiAnalyzer/FortiManager: on
- Upload UTM Logs: on
- Upload System Event: on
- Upload Security Event: on

⚠ Upload Vulnerability/Event logs are only supported for FortiClient version 6.4.2 and below.

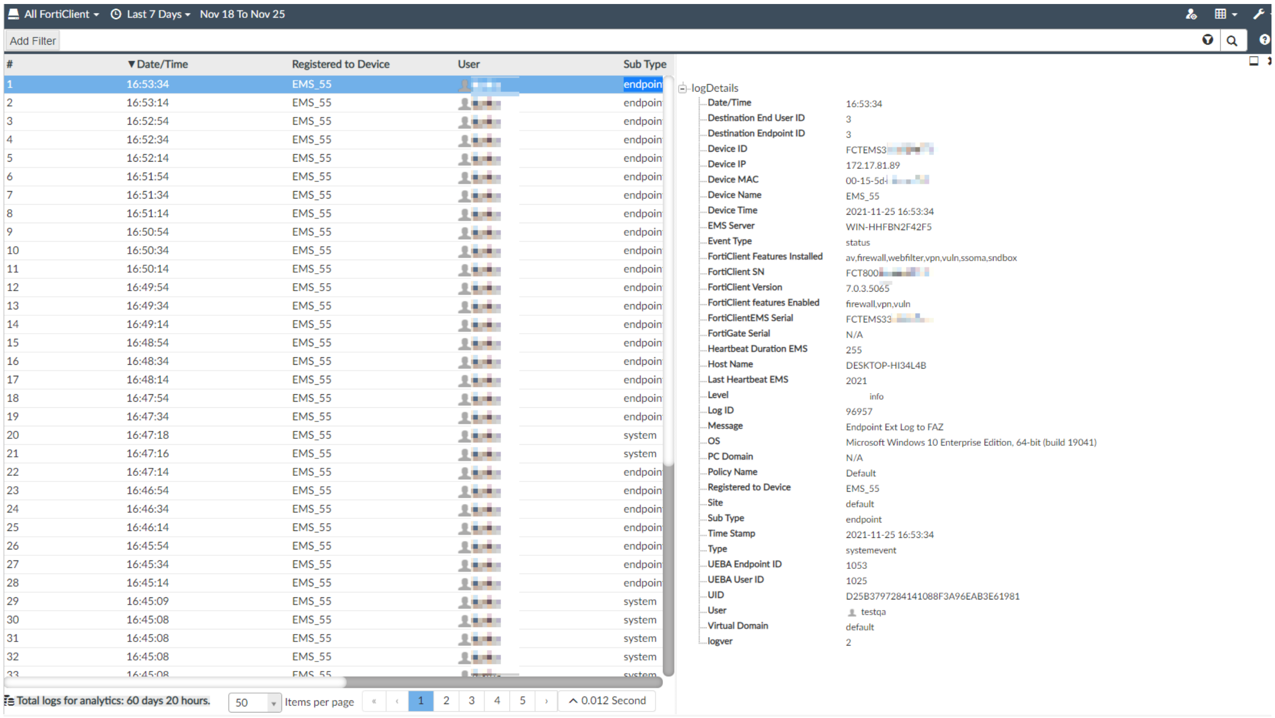
- Upload Vulnerability Logs: on
- Upload Event Logs: on
- Send Software Inventory: on
- Send OS Events: on

Event telemetry interval	120	seconds
IP Address/Hostname	1208151.ca-west-1.faz.test.forticloud.com	

- SSL Enabled: on

Upload Schedule	2	minutes
Log Generation Timeout	60	seconds
Log Retention	30	days

5. Configure other fields as desired and save the profile.
6. In FortiAnalyzer Cloud, go to *Device Manager*.
7. Authorize and add EMS.
8. Once FortiClient can reach FortiAnalyzer Cloud, it uploads logs to FortiAnalyzer Cloud as per the defined upload schedule. Go to *Log View* to see the log details.



#	▼Date/Time	Registered to Device	User	Sub Type
1	16:53:34	EMS_55	[redacted]	endpoin
2	16:53:14	EMS_55	[redacted]	endpoin
3	16:52:54	EMS_55	[redacted]	endpoin
4	16:52:34	EMS_55	[redacted]	endpoin
5	16:52:14	EMS_55	[redacted]	endpoin
6	16:51:54	EMS_55	[redacted]	endpoin
7	16:51:34	EMS_55	[redacted]	endpoin
8	16:51:14	EMS_55	[redacted]	endpoin
9	16:50:54	EMS_55	[redacted]	endpoin
10	16:50:34	EMS_55	[redacted]	endpoin
11	16:50:14	EMS_55	[redacted]	endpoin
12	16:49:54	EMS_55	[redacted]	endpoin
13	16:49:34	EMS_55	[redacted]	endpoin
14	16:49:14	EMS_55	[redacted]	endpoin
15	16:48:54	EMS_55	[redacted]	endpoin
16	16:48:34	EMS_55	[redacted]	endpoin
17	16:48:14	EMS_55	[redacted]	endpoin
18	16:47:54	EMS_55	[redacted]	endpoin
19	16:47:34	EMS_55	[redacted]	endpoin
20	16:47:18	EMS_55	[redacted]	system
21	16:47:16	EMS_55	[redacted]	system
22	16:47:14	EMS_55	[redacted]	endpoin
23	16:46:54	EMS_55	[redacted]	endpoin
24	16:46:34	EMS_55	[redacted]	endpoin
25	16:46:14	EMS_55	[redacted]	endpoin
26	16:45:54	EMS_55	[redacted]	endpoin
27	16:45:34	EMS_55	[redacted]	endpoin
28	16:45:14	EMS_55	[redacted]	endpoin
29	16:45:09	EMS_55	[redacted]	system
30	16:45:08	EMS_55	[redacted]	system
31	16:45:08	EMS_55	[redacted]	system
32	16:45:08	EMS_55	[redacted]	system
33	16:45:08	EMS_55	[redacted]	system

Total logs for analytics: 60 days 20 hours. 50 Items per page « ‹ 1 2 3 4 5 › ^ 0.012 Second

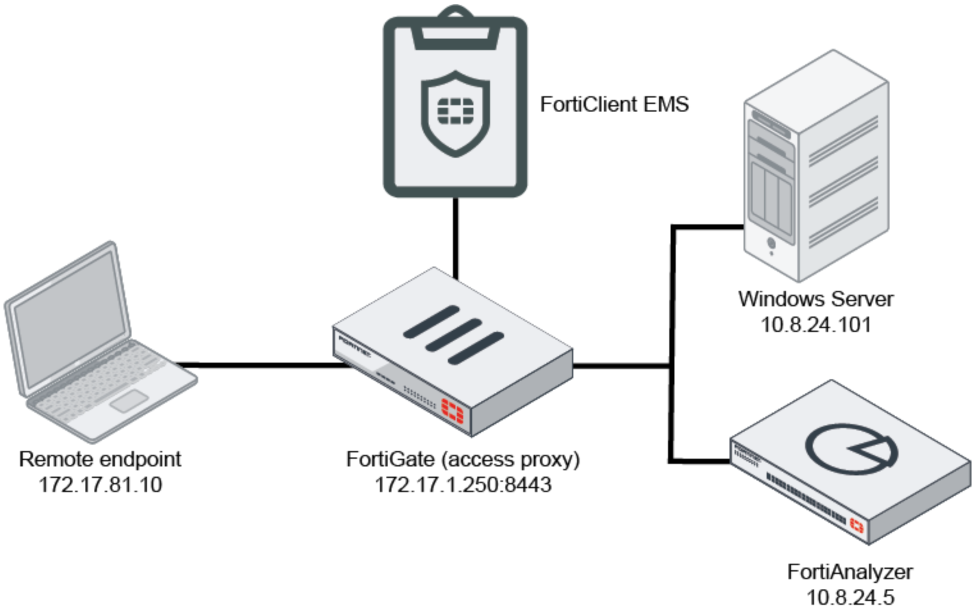
logDetails

Date/Time	16:53:34
Destination End User ID	3
Destination Endpoint ID	3
Device ID	FCTEMS3[redacted]
Device IP	172.17.81.89
Device MAC	00-15-5d-[redacted]
Device Name	EMS_55
Device Time	2021-11-25 16:53:34
EMS Server	WIN-HHFBN2F42F5
Event Type	status
FortiClient Features Installed	av,firewall,webfilter,vpn,vuln,ssoma,sndbox
FortiClient SN	FCT800[redacted]
FortiClient Version	7.0.3.5065
FortiClient features Enabled	firewall,vpn,vuln
FortiClientEMS Serial	FCTEMS33[redacted]
FortiGate Serial	N/A
Heartbeat Duration EMS	255
Host Name	DESKTOP-HI34L4B
Last Heartbeat EMS	2021
Level	info
Log ID	96957
Message	Endpoint Ext Log to FAZ
OS	Microsoft Windows 10 Enterprise Edition, 64-bit (build 19041)
PC Domain	N/A
Policy Name	Default
Registered to Device	EMS_55
Site	default
Sub Type	endpoint
Time Stamp	2021-11-25 16:53:34
Type	systemevent
UEBA Endpoint ID	1053
UEBA User ID	1025
UID	D25B3797284141088F3A96EAB3E61981
User	testqa
Virtual Domain	default
logver	2

FQDN-based ZTNA TCP forwarding services - 7.0.3

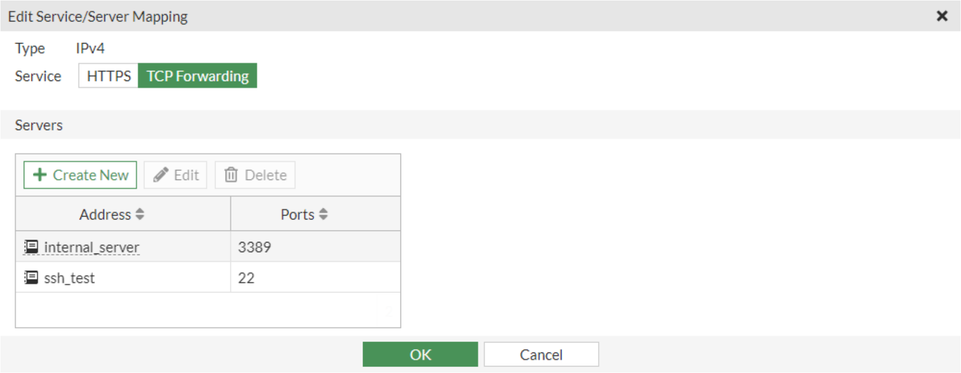
FortiClient 7.0.3 adds support for using fully qualified domain names (FQDN) as destination hosts in zero trust network access (ZTNA) TCP forwarding rules. This allows you to avoid exposing private/internal IP addresses to end users by using FQDNs instead.

The following shows the topology for this example. This example uses two FQDNs, rdp.win.test and ssh.win.test, in place of the Windows server IP address, 10.8.24.100. This hides the internal IP address, 10.8.24.100, from end users.



To configure FortiOS:

1. In FortiOS, go to *Policy & Objects* > *ZTNA* > *ZTNA Servers*.
2. Click *Create New*.
3. For *Type*, select *IPv4*.
4. For *Service*, select *TCP Forwarding*.
5. Under *Servers*, configure RDP and SSH services.



Type IPv4

Service TCP Forwarding

Address	Ports
internal_server	3389
ssh_test	22

6. Click *OK*.

7. In the CLI, add the rdp.win.test FQDN to RDP and SSH services as the domain:

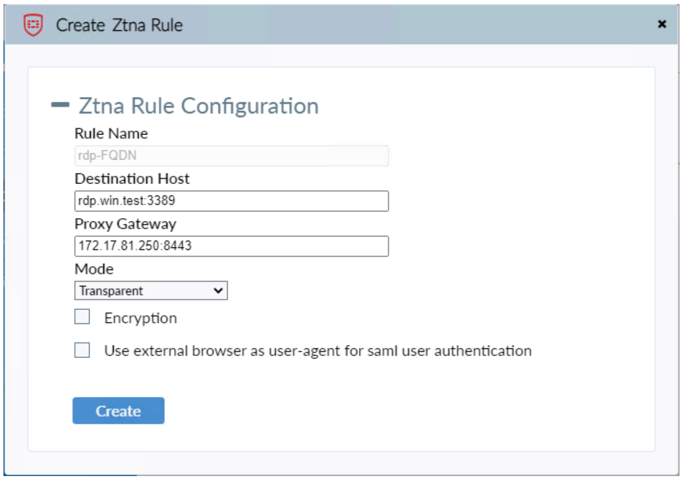
```
config firewall access-proxy
    edit "ZTNA-test"
        set vip "ZTNA-test"
        set client-cert enable
        config api-gateway
            edit 2
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 1
                        set address "internal_server"
                        set domain "rdp.win.test"
                        set mappedport 3389
                    next
                    edit 2
                        set address "ssh_test"
                        set domain "ssh.win.test"
                        set mappedport 22
                    next
                end
            next
        end
    next
end
```

8. Ensure that you configured the ZTNA policy rule and firewall policy as desired.

To configure ZTNA rules:

1. You can configure ZTNA rules from FortiClient or EMS. If using FortiClient, connect to the EMS that is connected to the FortiGate acting as the TCP forwarding server.
2. Do one of the following:
   a. If using FortiClient, go to *ZTNA Connection Rules*.
   b. If using EMS, go to *Endpoint Profiles > ZTNA Connection Rules*.
3. Create the RDP server rule:
   a. Click *Add Rule*.
   b. In the Rule Name field, enter the desired name.
   c. In the *Destination Host* field, enter rdp.win.test:<port number>.
   d. In the *Proxy Gateway* field, enter the FortiGate IP address and port number. In this example, it is 172.17.81.250:8443.

e. Click *Create*.



Ztna Rule Configuration

Rule Name: rdp-FQDN

Destination Host: rdp.win.test:3389

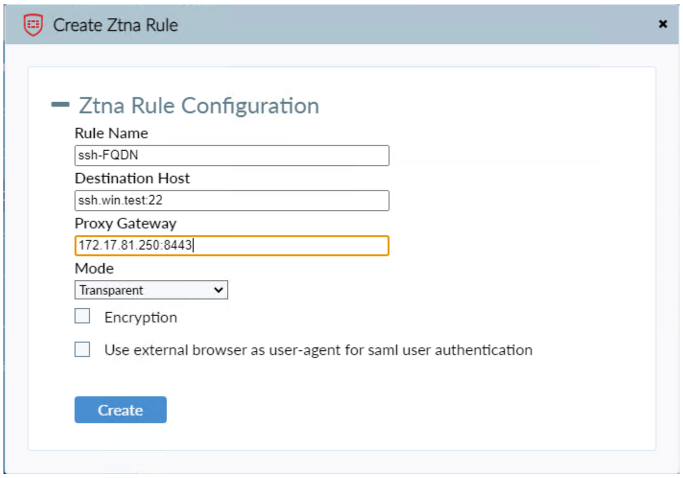
Proxy Gateway: 172.17.81.250:8443

Mode: Transparent

□ Encryption

□ Use external browser as user-agent for saml user authentication

4. Create the SSH server rule:
   a. Click *Add Rule*.
   b. In the *Rule Name* field, enter the desired name.
   c. In the *Destination Host* field, enter ssh.win.test:<port number>.
   d. In the *Proxy Gateway* field, enter the FortiGate IP address and port number. In this example, it is 172.17.81.250:8443.
   e. Click *Create*.



Ztna Rule Configuration

Rule Name: ssh-FQDN

Destination Host: ssh.win.test:22

Proxy Gateway: 172.17.81.250:8443

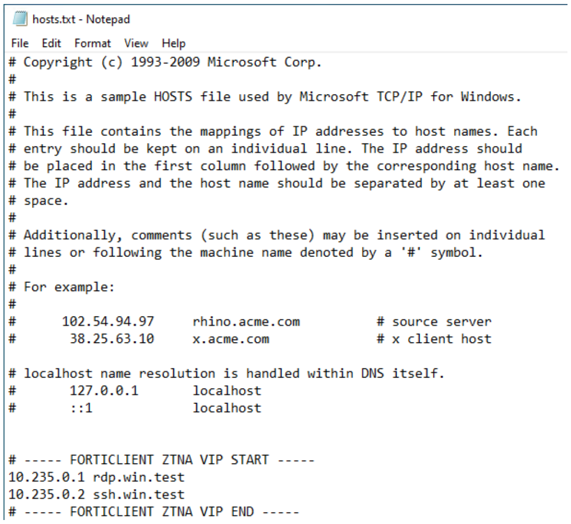
Mode: Transparent

□ Encryption

□ Use external browser as user-agent for saml user authentication

To verify the configuration:

1. Go to C:/Windows/System32/drivers/etc.
2. Open the hosts file with a text editor.
3. Confirm that FortiClient automatically edited the hosts file. If FortiClient sees traffic to these IP addresses, it forwards the traffic to the ZTNA access proxy with the destination set as the corresponding FQDN. You can verify this by pinging these two domain names in Command Prompt.



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

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


# ----- FORTICLIENT ZTNA VIP START -----
10.235.0.1 rdp.win.test
10.235.0.2 ssh.win.test
# ----- FORTICLIENT ZTNA VIP END -----
```

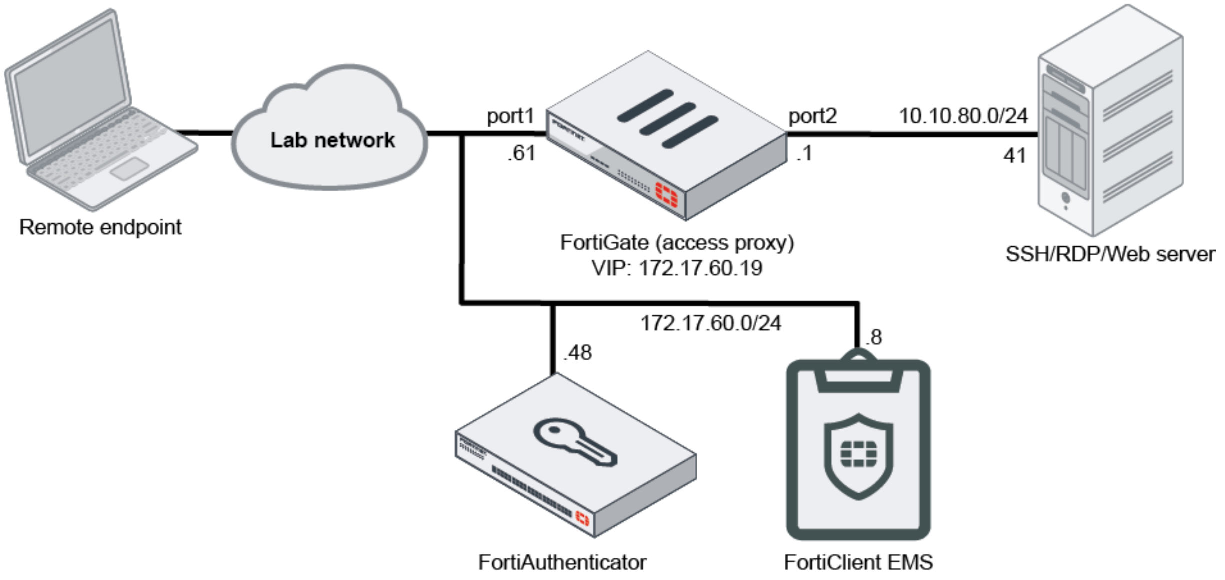
4. Start an SSH session in Command Prompt using `ssh admin@ssh.win.test`.
5. FortiClient displays an authentication prompt. Enter the credentials in the popup.
6. You can see that the session started. Command Prompt requests the password.
7. Start a remote session with Remote Desktop Connection.
8. Enter your credentials in the popup. A remote access session starts.

Browser as external user agent for ZTNA user authentication - 7.0.3

Using a browser as an external user agent for zero trust network access (ZTNA) user authentication requires the following:

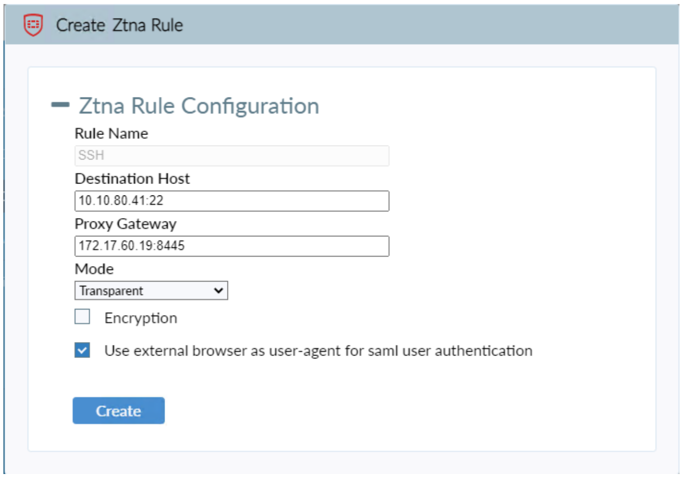
- The FortiGate and EMS must be connected as part of a Fortinet Security Fabric.
- You must have properly configured ZTNA settings in FortiOS.
- FortiClient must be registered to EMS.
- You must have configured ZTNA rules in EMS or FortiClient.

The following shows the topology for this example:



To add a ZTNA rule in FortiClient:

1. Go to *ZTNA Connection Rules*.
2. Click *Add Rule*.
3. Configure a rule as desired. Enable *Use external browser as user-agent for saml user authentication*. This example configures an SSH server.
4. Click *Create*.



Create Ztna Rule

Ztna Rule Configuration

Rule Name: SSH

Destination Host: 10.10.80.41:22

Proxy Gateway: 172.17.60.19:8445

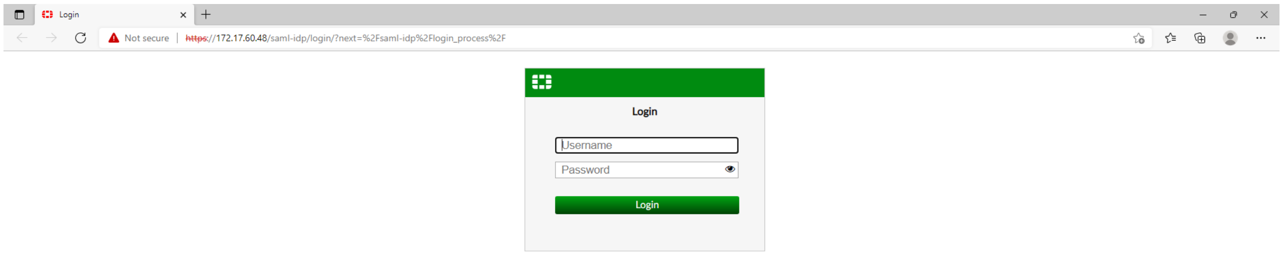
Mode: Transparent

☐ Encryption

☑ Use external browser as user-agent for saml user authentication

To verify the configuration:

1. Attempt to connect to the configured SSH server.
2. The browser may display a prompt to select a certificate for authentication. If so, install the desired certificate as directed. The browser displays a FortiAuthenticator authentication web portal.


Login
Not secure
~~https~~://172.17.60.48/saml-idp/login/?next=%2Fsaml-idp%2Flogin_process%2F
Login
Username
Password
Login

3. Log in via the browser. The endpoint can now access the SSH server.

FDS update support for antiransomware behavior rules - 7.0.3

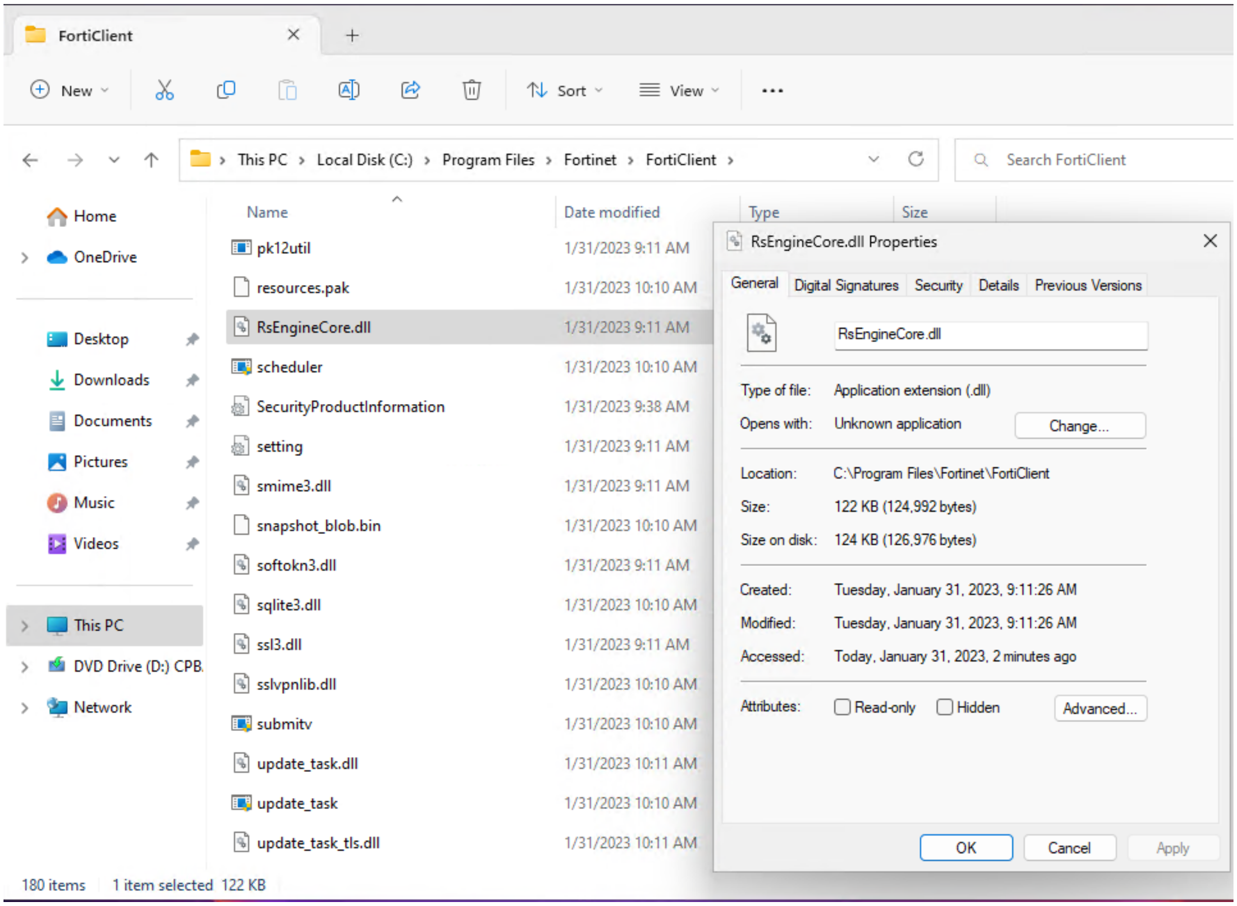
FortiClient adds FortiGuard Distribution Server (FDS) support for updates to the antiransomware engine and rules update, as is already the case for antivirus. FortiClient has supported ransomware detection since 6.4.2. Prior to this enhancement, updates in technique or detection rules were not applied until the next FortiClient patch release, which could take months.

This enhancement keeps all users' antiransomware engines/signatures updated without a new patch update using FDS. Consider that all users are connected to the corporate FDS. When Fortinet creates a new antiransomware engine/signature and uploads it to FDS, all users receive the updated antiransomware engine/signature.

Updated antiransomware engine/signature versions depend on the FortiClient firmware version. FortiClient implements different engine updates for different versions.

To check engine/signature version on the endpoint:

1. After a fresh install of FortiClient, go to C:\Program Files\Fortinet\FortiClient.
2. Right-click the RsEngineCore.dll file, then select *Properties*.



Name	Date modified
pk12util	1/31/2023 9:11 AM
resources.pak	1/31/2023 10:10 AM
RsEngineCore.dll	1/31/2023 9:11 AM
scheduler	1/31/2023 10:10 AM
SecurityProductInformation	1/31/2023 9:38 AM
setting	1/31/2023 9:11 AM
smime3.dll	1/31/2023 9:11 AM
snapshot_blob.bin	1/31/2023 10:10 AM
softokn3.dll	1/31/2023 9:11 AM
sqlite3.dll	1/31/2023 10:10 AM
ssl3.dll	1/31/2023 9:11 AM
sslvpnlib.dll	1/31/2023 10:10 AM
submitv	1/31/2023 10:10 AM
update_task.dll	1/31/2023 10:11 AM
update_task	1/31/2023 10:10 AM
update_task_tls.dll	1/31/2023 10:11 AM

180 items 1 item selected 122 KB

RsEngineCore.dll

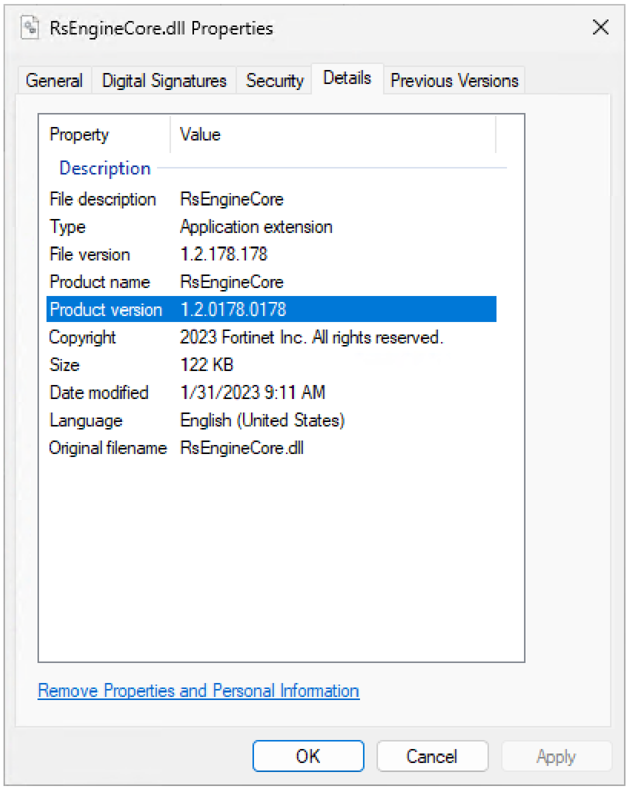
Type of file: Application extension (.dll)
Opens with: Unknown application

Location: C:\Program Files\Fortinet\FortiClient
Size: 122 KB (124,992 bytes)
Size on disk: 124 KB (126,976 bytes)

Created: Tuesday, January 31, 2023, 9:11:26 AM
Modified: Tuesday, January 31, 2023, 9:11:26 AM
Accessed: Today, January 31, 2023, 2 minutes ago

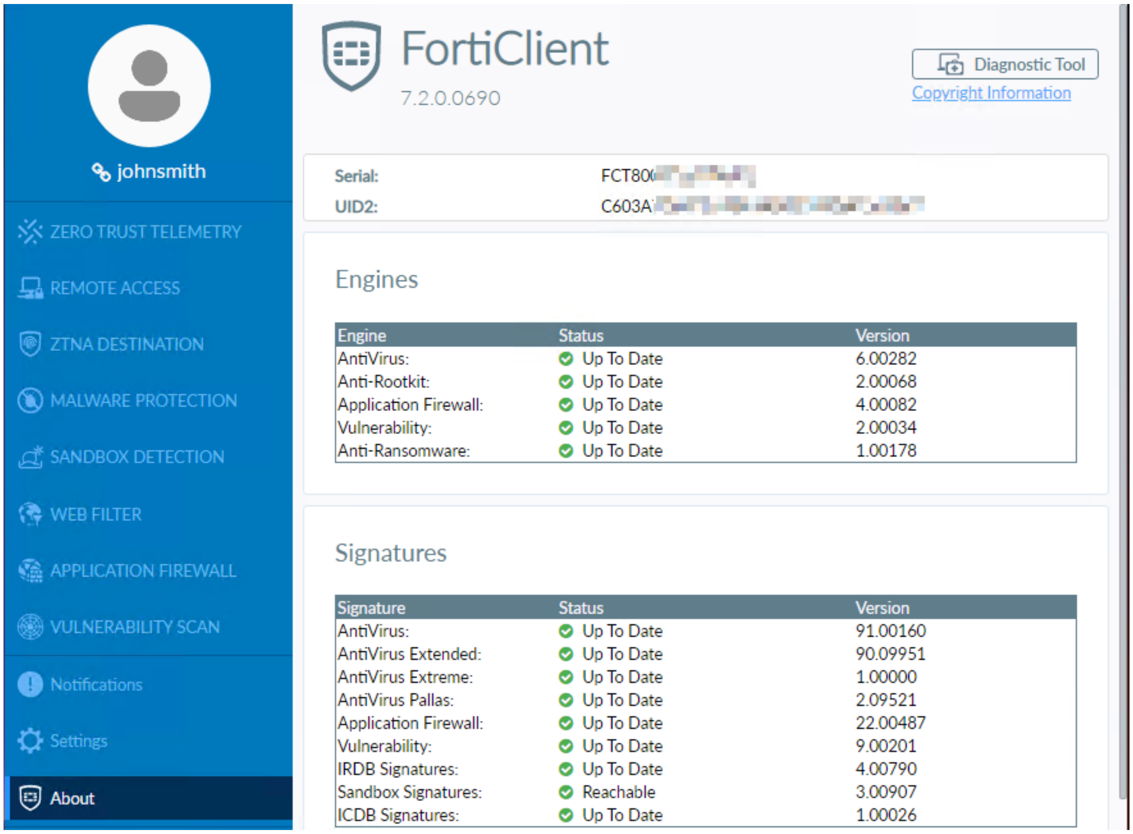
Attributes: ☐ Read-only ☐ Hidden

3. On the *Details* tab, confirm the *Product version*. This is the antiransomware engine version, which should be the same as the installed version of FortiClient.



Property	Value
Description	
File description	RsEngineCore
Type	Application extension
File version	1.2.178.178
Product name	RsEngineCore
Product version	1.2.0178.0178
Copyright	2023 Fortinet Inc. All rights reserved.
Size	122 KB
Date modified	1/31/2023 9:11 AM
Language	English (United States)
Original filename	RsEngineCore.dll

4. Register FortiClient to EMS.
5. On the *About* page, confirm the antiransomware engine version. This should be the same as the version from step 3.



Serial: FCT80[redacted]

UID2: C603A[redacted]

Engines

Engine	Status	Version
AntiVirus:	Up To Date	6.00282
Anti-Rootkit:	Up To Date	2.00068
Application Firewall:	Up To Date	4.00082
Vulnerability:	Up To Date	2.00034
Anti-Ransomware:	Up To Date	1.00178

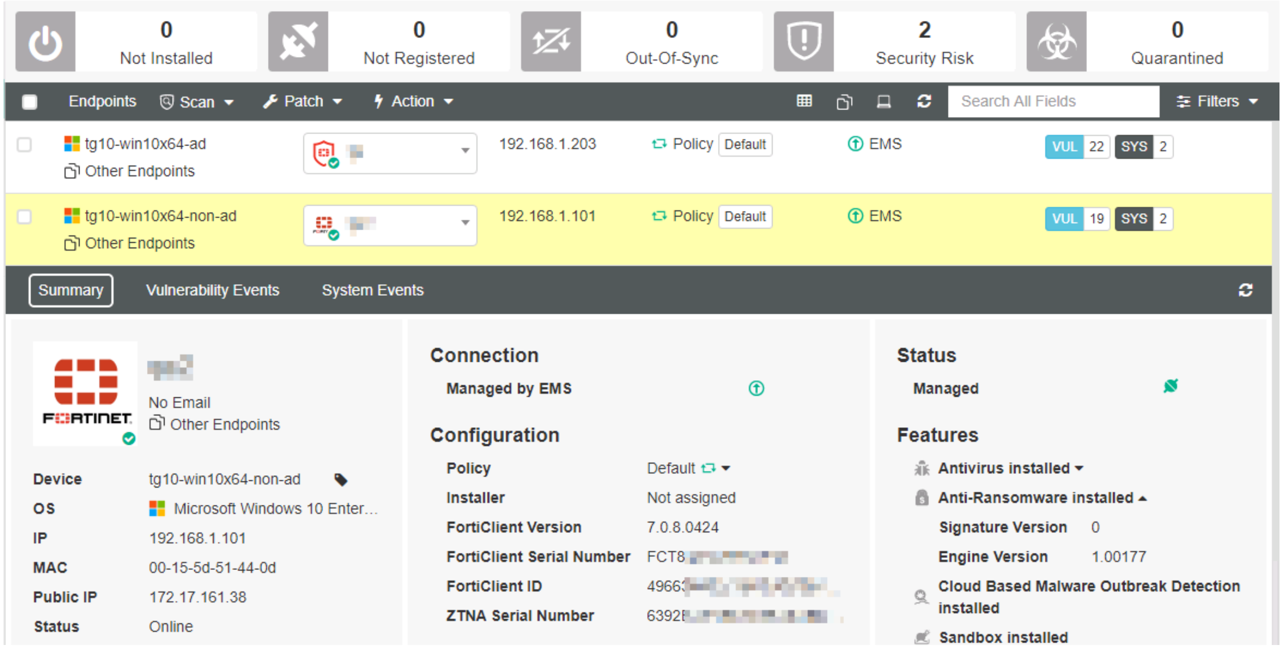
Signatures

Signature	Status	Version
AntiVirus:	Up To Date	91.00160
AntiVirus Extended:	Up To Date	90.09951
AntiVirus Extreme:	Up To Date	1.00000
AntiVirus Pallas:	Up To Date	2.09521
Application Firewall:	Up To Date	22.00487
Vulnerability:	Up To Date	9.00201
IRDB Signatures:	Up To Date	4.00790
Sandbox Signatures:	Reachable	3.00907
ICDB Signatures:	Up To Date	1.00026

6. After Fortinet uploads a new engine/signature to FDS, you can verify that FortiClient received the update by repeating the previous steps to check the versions in the RsEngineCore.dll file and on the FortiClient *About* page.

To check engine/signature version on EMS:

1. In EMS, go to *Endpoints* > *All Endpoints*.
2. Select the desired endpoint to view its details. Under *Features*, EMS displays the endpoint's antiransomware engine version.



tg10-win10x64-ad Other Endpoints	[redacted]	192.168.1.203	Policy Default	EMS	VUL 22 SYS 2
tg10-win10x64-non-ad Other Endpoints	[redacted]	192.168.1.101	Policy Default	EMS	VUL 19 SYS 2

[redacted]
No Email
Other Endpoints

Device	tg10-win10x64-non-ad
OS	Microsoft Windows 10 Enter…
IP	192.168.1.101
MAC	00-15-5d-51-44-0d
Public IP	172.17.161.38
Status	Online

Connection

Managed by EMS	

Configuration

Policy	Default
Installer	Not assigned
FortiClient Version	7.0.8.0424
FortiClient Serial Number	FCT8[redacted]
FortiClient ID	4966[redacted]
ZTNA Serial Number	6392[redacted]

Status

Managed

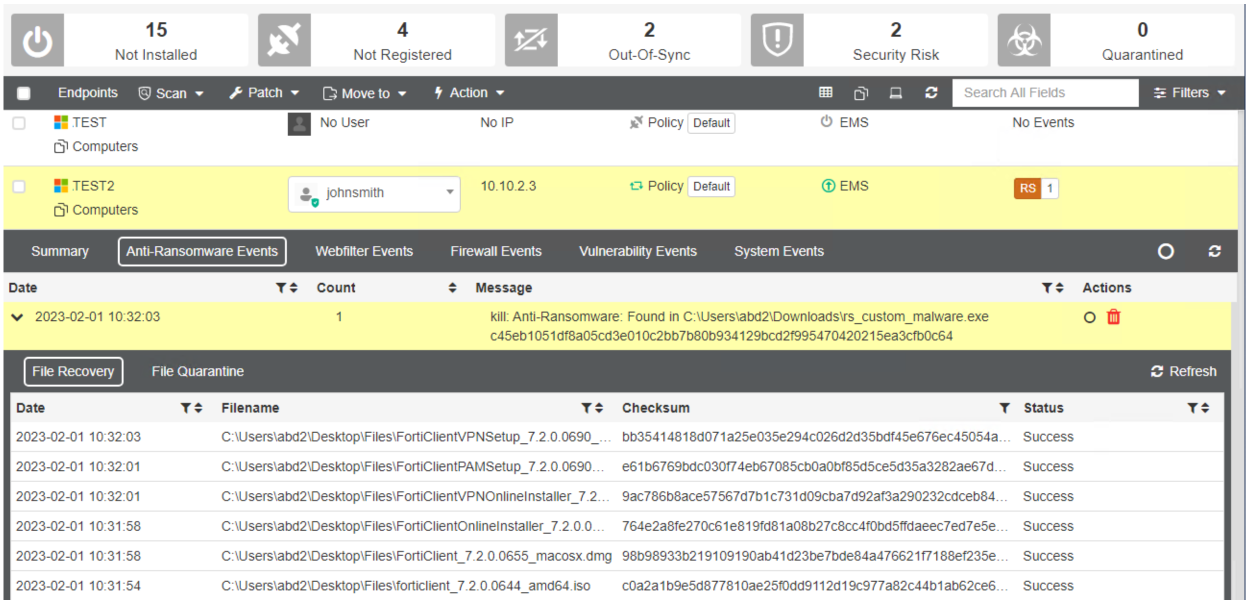
Features

- Antivirus installed
- Anti-Ransomware installed
  - Signature Version 0
  - Engine Version 1.00177
- Cloud Based Malware Outbreak Detection installed
- Sandbox installed

3. Go to *System Settings* > *FortiGuard Services* > *View Signature List* to verify the antiransomware engine and signature version.

To view antiransomware events on the EMS:

1. The antiransomware feature stops and quarantines detected ransomware and restores the encrypted files to the backup folder at C:\Program Files\Fortinet\FortiClient\backup. These events are logged locally on the FortiClient. FortiClient sends the events to EMS. On EMS, go to *Endpoints* > *All Endpoints*.
2. Select the desired endpoint.
3. Go to the *Anti-Ransomware Events* tab. All detected ransomware events display.
4. Go to the *File Recovery* and *File Quarantine* tabs to view recovered and quarantined files, respectively.



TEST Computers	No User	No IP	Policy Default	EMS	No Events
TEST2 Computers	johnsmith	10.10.2.3	Policy Default	EMS	RS 1

Date	Count	Message	Actions
2023-02-01 10:32:03	1	kill: Anti-Ransomware: Found in C:\Users\abd2\Downloads\rs_custom_malware.exe c45eb1051df8a05cd3e010c2bb7b80b934129bcd2f995470420215ea3cfb0c64	

Date	Filename	Checksum	Status
2023-02-01 10:32:03	C:\Users\abd2\Desktop\Files\FortiClientVPNSetup_7.2.0.0690_…	bb35414818d071a25e035e294c026d2d35bdf45e676ec45054a…	Success
2023-02-01 10:32:01	C:\Users\abd2\Desktop\Files\FortiClientPAMSetup_7.2.0.0690…	e61b6769bdc030f74eb67085cb0a0bf85d5ce5d35a3282ae67d…	Success
2023-02-01 10:32:01	C:\Users\abd2\Desktop\Files\FortiClientVPNOnlineInstaller_7.2…	9ac786b8ace57567d7b1c731d09cba7d92af3a290232cdceb84…	Success
2023-02-01 10:31:58	C:\Users\abd2\Desktop\Files\FortiClientOnlineInstaller_7.2.0.0…	764e2a8fe270c61e819fd81a08b27c8cc4f0bd5ffdaeec7ed7e5e…	Success
2023-02-01 10:31:58	C:\Users\abd2\Desktop\Files\FortiClient_7.2.0.0655_macosx.dmg	98b98933b219109190ab41d23be7bde84a476621f7188ef235e…	Success
2023-02-01 10:31:54	C:\Users\abd2\Desktop\Files\forticlient_7.2.0.0644_amd64.iso	c0a2a1b9e5d877810ae25f0dd9112d19c977a82c44b1ab62ce6…	Success

ZTNA certificate serial number mismatch - 7.0.7

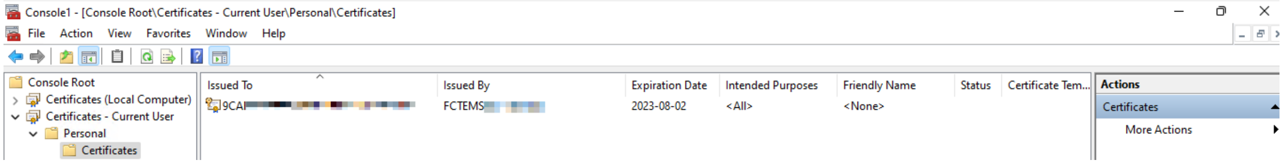
Each time that FortiClient registers to EMS, EMS provisions a new zero trust network access (ZTNA) device certificate to the endpoint. The new certificate may assign a new serial number (SN) to the endpoint. In this scenario, a browser-initiated ZTNA session may continue to use the cached ZTNA certificate key with the old SN.The SN of the FortiClient certificate on the endpoint was incorrect and differed from the ZTNA SN that EMS displayed. This resulted in ZTNA client certificate authentication failing due to the certificate mismatch, as FortiOS received the record from EMS.

To resolve this issue, EMS resends the old SN to FortiClient. FortiClient checks if the SN matches with its SN. If the SNs match, FortiClient does not send a new certificate request. If the SNs do not match, FortiClient sends a new certificate request to resolve the mismatch.

FortiClient and EMS retain the same ZTNA certificate as long as FortiClient is connecting and reconnecting to the same EMS server. The described mismatch occurs if FortiClient deregisters, then registers to a new EMS.

The following describes this scenario:

1. The user registers FortiClient to EMS. The Windows certificate store receives the ZTNA certificate. In the Microsoft Management Console (MMC), go to *Certificates - Current User* > *Personal* > *Certificates*. Confirm that the ZTNA certificate displays.



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
9CA[redacted]	FCTEMS[redacted]	2023-08-02	<All>	<None>		

2. The user connects to a browser with ZTNA using a web proxy. MMC continues to display the ZTNA certificate.
3. The user deregisters FortiClient from EMS. MMC continues to display the ZTNA certificate. In this scenario, the user did not close the browser. The browser still has the session ticket that the FortiOS access proxy sent cached.
4. The user reregisters to EMS. EMS resends the SN to FortiClient. FortiClient attempts to match this SN with the saved SN. As these SNs match, FortiClient does not send a new certificate request. Browser sessions continue to work.
5. The user deregisters FortiClient from EMS and reregisters to another EMS server. The new EMS server sends its SN to FortiClient. FortiClient attempts to match this SN with the saved SN. As these SNs do not match, FortiClient sends a new certificate request.
6. The user uninstalls FortiClient from the endpoint. The uninstall removes the SN from logs and the certificate from the certificate store.

Logs have been updated for this feature to include the SN:

- In endpoint logs, the ZTNA certificate SN functionality has been added to FortiEsnac logs in `FCKARPLY` and `FCREGRPLY` in C:\Program Files\Fortinet\FortiClient\logs\trace:

```
[FortiESNAC 928 debug] REPLY=FCKARPLY: CONT|1|EMSSN|FCTEMS8822090184:WIN-
      H0CJAOMVVTR|UPLD_PRT|8013|KA_INTERVAL|20|LIC_FEATS|6224895|LIC_
      ED|1680159600|AUTH_PRD|0|SNAPTIME|0|QUAR|0|AVTR|1|AV_
      SIG|90.04285|SERIAL|<serial number>|EMS_ONNET|0|RUN_SRV_CMD|4096|WF_PAGE_
      URL|eddyfct.ems.com:10443/wfcustompages/default/webfilter_custom_pages.enc|WF_
      CHKSM|65bc4c8aef2d9219ff5743d91a754a0e36ac0dd2c9501cb1e30eae22225|TAGS|0000000
      0000
```

```
[FortiESNAC 636 debug] REPLY=FCREGRPLY: REG|0-FCTEMS8822090184:45:WIN-
      H0CJAOMVVTR:default:20:43230:1:8:227|AV_SIG|90.04285|AUTH_PRD|0|LIC_
      FEATS|6224895|LIC_ED|1680159600|SOFT_CRC|2|TOKEN|D9D8D261-2177-4539-B755-
```

```
4351FE29F28C|SERIAL|<serial number>|EMS_
ONNET|0|ZFGTIP|eJydkcFOwzAMhu88RdQ7TQOCTcjLXmCcxr0KiRtFSp0pcQd7e7JVE0h0HLjZv
3...
```

- In EMS logs, the ZTNA certificate SN functionality has been added to FCMDaemon log in `FCKARPLY` and `FCREGRPLY` in C:\Program Files (x86)\Fortinet\FortiClientEMS\logs:

```
result: CC3F3949FC6E4D91BD2399207988680A - FCREGRPLY: REG|0-
     FCTEMS8822090184:45:WIN-H0CJAOMVVTR:default:20:43230:1:8:227|AV_
     SIG|90.04285|AUTH_PRD|0|LIC_FEATS|6224895|LIC_ED|1680159600|SOFT_
     CRC|2|TOKEN|DD2AA1F4-5CE8-437A-953D-A133B4C28C19|SERIAL|<serial number>|EMS_
     ONNET|0|ZFGTIP|eJydkcFOwzAMhu88RdQ7TQOCTcjLXmCcxr0KiRtFSp0pcQd7e7JVE...
```

```
result: CC3F3949FC6E4D91BD2399207988680A - FCKARPLY:
     CONT|1|EMSSN|FCTEMS8822090184:WIN-H0CJAOMVVTR|UPLD_PRT|8013|KA_INTERVAL|20|LIC_
     FEATS|6224895|LIC_ED|1680159600|AUTH_PRD|0|SNAPTIME|0|QUAR|0|AVTR|1|AV_
     SIG|90.04285|SERIAL|<serial number>|EMS_ONNET|0|RUN_SRV_CMD|4096|WF_PAGE_
     URL|eddyfct.ems.com:10443/wfcustompages/default/webfilter_custom_pages.enc|WF_
     CHKSM|65bc4c8aef2d9219ff5743d91a754a0e36ac0dd2c9501cb1e30eae22225|TAGS|0000000
     0000|
```

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, FortiClient disables this feature. 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.

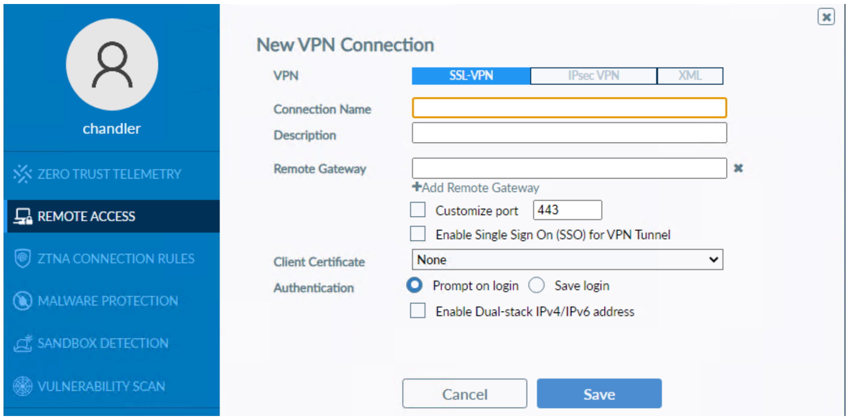
See the Dual stack IPv4 and IPv6 support for SSL VPN.

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 disabled by default.

After installing FortiClient 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, *Do Not Warn Invalid Server Certificate* is unavailable.



New VPN Connection

VPN: SSL-VPN

Connection Name

Description

Remote Gateway

□ Customize port 443

□ Enable Single Sign On (SSO) for VPN Tunnel

Client Certificate: None

Authentication: ● Prompt on login ○ Save login

□ Enable Dual-stack IPv4/IPv6 address

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

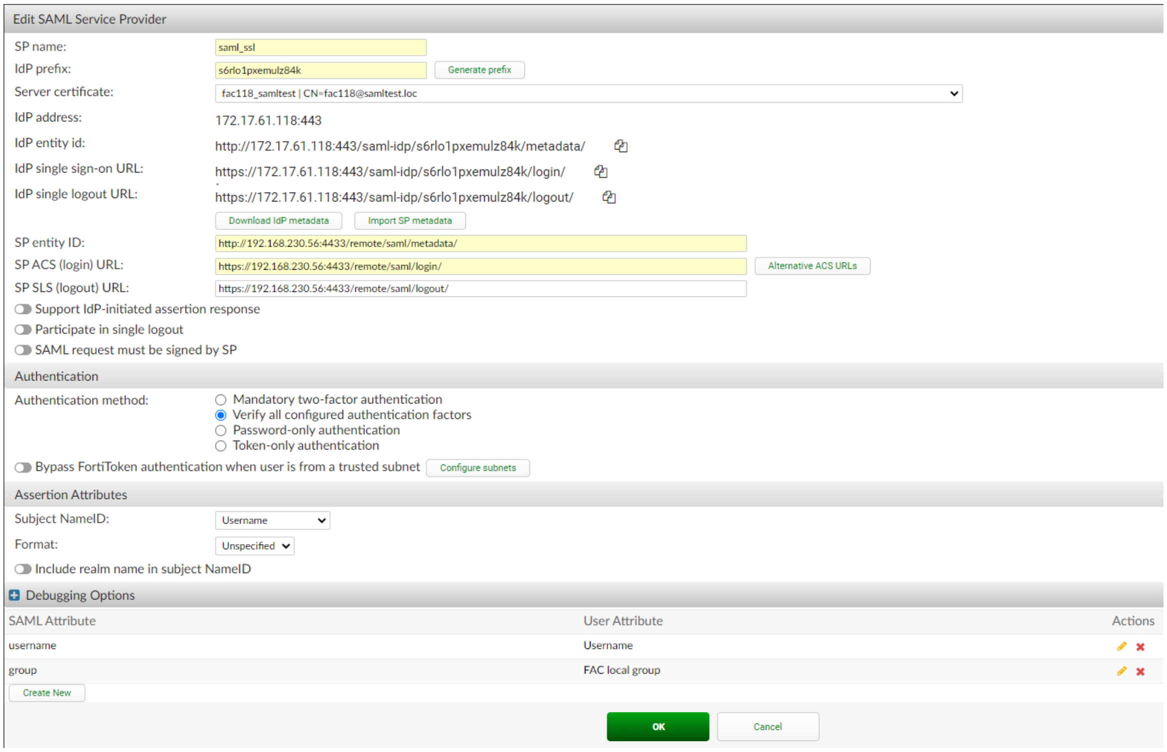
When establishing an SSL VPN tunnel connection, FortiClient can present a SAML authentication request to the end user in a web browser.

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.

FortiClient and EMS do not support this feature 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.



Edit SAML Service Provider

SP name: saml_ssl
IdP prefix: s6rlo1pxemulz84k
Server certificate: fac118_samltest | CN=fac118@samltest.loc
IdP address: 172.17.61.118:443
IdP entity id: http://172.17.61.118:443/saml-idp/s6rlo1pxemulz84k/metadata/
IdP single sign-on URL: https://172.17.61.118:443/saml-idp/s6rlo1pxemulz84k/login/
IdP single logout URL: https://172.17.61.118:443/saml-idp/s6rlo1pxemulz84k/logout/
SP entity ID: http://192.168.230.56:4433/remote/saml/metadata/
SP ACS (login) URL: https://192.168.230.56:4433/remote/saml/login/
SP SLS (logout) URL: https://192.168.230.56:4433/remote/saml/logout/
Support IdP-initiated assertion response
Participate in single logout
SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory two-factor authentication
● Verify all configured authentication factors
○ Password-only authentication
○ Token-only authentication
Bypass FortiToken authentication when user is from a trusted subnet

Assertion Attributes

Subject NameID: Username
Format: Unspecified
Include realm name in subject NameID

Debugging Options

SAML Attribute	User Attribute	Actions
username	Username	✎ ✖
group	FAC local group	✎ ✖

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 that FortiAuthenticator provided:

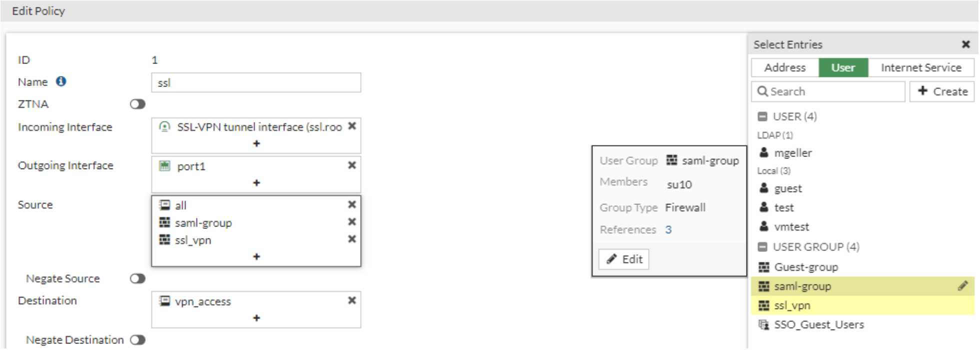
```
config user saml
   edit "su10"
      set cert "Fortinet_Factory"
      set entity-id "http://192.168.230.56:4433/remote/saml/metadata/"
      set single-sign-on-url "https://192.168.230.56:4433/remote/saml/login/"
```

```
    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 occupies 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.



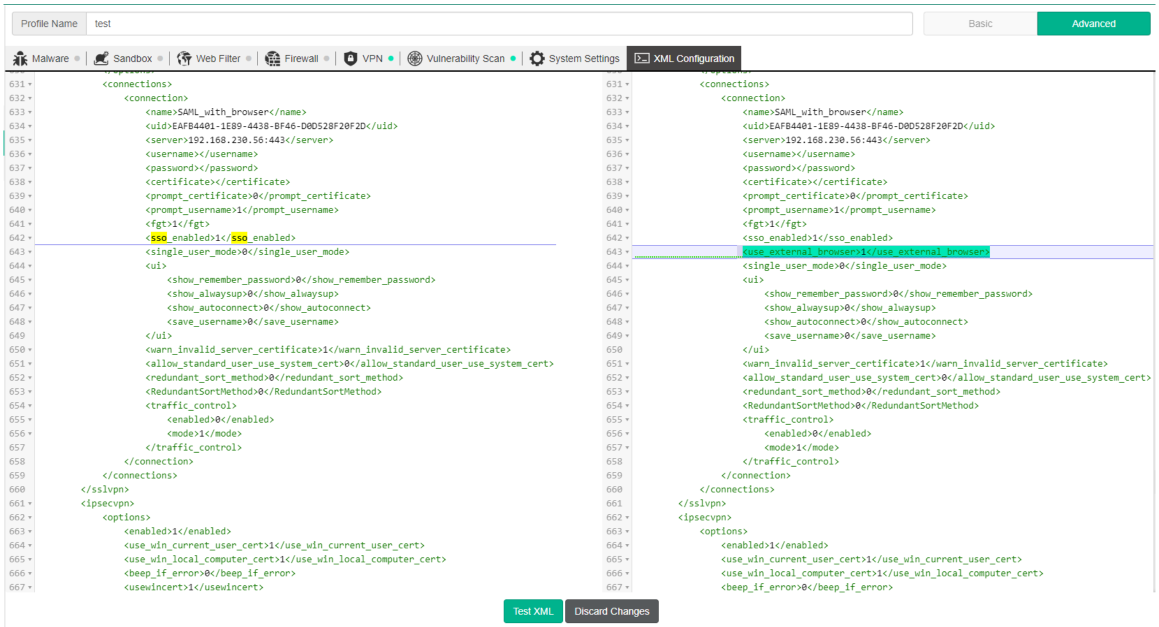
Edit Policy

ID 1
Name ssl
ZTNA
Incoming Interface SSL-VPN tunnel interface (ssl.roo
Outgoing Interface port1
Source all, saml-group, ssl_vpn
Negate Source
Destination vpn_access
Negate Destination

User Group saml-group
Members su10
Group Type Firewall
References 3

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>`.



```
        <connections>
            <connection>
                <name>SAML_with_browser</name>
                <uid>EAFB4401-1E89-4438-BF46-D0D528F20F2D</uid>
                <server>192.168.230.56:443</server>
                <username></username>
                <password></password>
                <certificate></certificate>
                <prompt_certificate>0</prompt_certificate>
                <prompt_username>1</prompt_username>
                <fgt>1</fgt>
                <sso_enabled>1</sso_enabled>
                <single_user_mode>0</single_user_mode>
                <ui>
                    <show_remember_password>0</show_remember_password>
                    <show_alwaysup>0</show_alwaysup>
                    <show_autoconnect>0</show_autoconnect>
                    <save_username>0</save_username>
                </ui>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <allow_standard_user_use_system_cert>0</allow_standard_user_use_system_cert>
                <redundant_sort_method>0</redundant_sort_method>
                <RedundantSortMethod>0</RedundantSortMethod>
                <traffic_control>
                    <enabled>0</enabled>
                    <mode>1</mode>
                </traffic_control>
            </connection>
        </connections>
    </sslvpn>
    <ipsecvpn>
        <options>
            <enabled>1</enabled>
            <use_win_current_user_cert>1</use_win_current_user_cert>
            <use_win_local_computer_cert>1</use_win_local_computer_cert>
            <beep_if_error>0</beep_if_error>
            <usewincert>1</usewincert>
```

```
        <connections>
            <connection>
                <name>SAML_with_browser</name>
                <uid>EAFB4401-1E89-4438-BF46-D0D528F20F2D</uid>
                <server>192.168.230.56:443</server>
                <username></username>
                <password></password>
                <certificate></certificate>
                <prompt_certificate>0</prompt_certificate>
                <prompt_username>1</prompt_username>
                <fgt>1</fgt>
                <sso_enabled>1</sso_enabled>
                <use_external_browser>1</use_external_browser>
                <single_user_mode>0</single_user_mode>
                <ui>
                    <show_remember_password>0</show_remember_password>
                    <show_alwaysup>0</show_alwaysup>
                    <show_autoconnect>0</show_autoconnect>
                    <save_username>0</save_username>
                </ui>
                <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                <allow_standard_user_use_system_cert>0</allow_standard_user_use_system_cert>
                <redundant_sort_method>0</redundant_sort_method>
                <RedundantSortMethod>0</RedundantSortMethod>
                <traffic_control>
                    <enabled>0</enabled>
                    <mode>1</mode>
                </traffic_control>
            </connection>
        </connections>
    </sslvpn>
    <ipsecvpn>
        <options>
            <enabled>1</enabled>
            <use_win_current_user_cert>1</use_win_current_user_cert>
            <use_win_local_computer_cert>1</use_win_local_computer_cert>
            <beep_if_error>0</beep_if_error>
```

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

To test the connection in FortiClient:

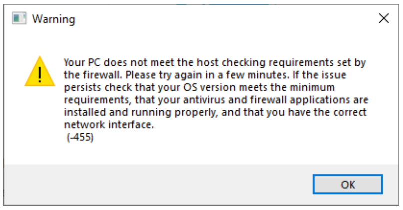
1. After FortiClient receives the latest configuration update from EMS, go to the *Remote Access* tab.
2. View the tunnel to verify that the *Use external browser as user-agent for saml user authentication field* is enabled.
3. Connect to the tunnel by clicking *SAML Login*. Verify that FortiClient opens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

FortiGate-powered host check for free VPN client - 7.0.3

FortiGate-powered host check supports the following for the FortiClient free VPN client:

- Operating system (OS) check
- Antivirus (AV)-only
- Firewall-only
- AV and firewall
- Custom software host check:
  - File
  - Running process
  - Registry

During VPN connection, if the free VPN client detects that the currently running system environment does not meet a setting that FortiGate-powered host check requires, it displays a warning.



Your PC does not meet the host checking requirements set by the firewall. Please try again in a few minutes. If the issue persists check that your OS version meets the minimum requirements, that your antivirus and firewall applications are installed and running properly, and that you have the correct network interface.
(-455)

To enable OS check on FortiOS:

The following configures a check that the endpoint runs Windows 10.

```
config vpn ssl web portal
   edit "full-access"
      set os-check enable
      config os-check-list "windows-10"
         set action deny
      end
   end
end
```

To enable AV-only check on FortiOS:

The following configures a check that requires that AV is enabled on the endpoint:

```
config vpn ssl web portal
   edit "full-access"
      set host-check av
end
```

To enable firewall-only check on FortiOS:

The following configures a check that requires that firewall is enabled on the endpoint:

```
config vpn ssl web portal
   edit "full-access"
      set host-check fw
end
```

To enable AV and firewall check on FortiOS:

The following configures a check that requires that AV and firewall are enabled on the endpoint:

```
config vpn ssl web portal
   edit "full-access"
      set host-check av-fw
end
```

To enable custom file check on FortiOS:

The following configures a check that requires that c:\temp\mytest.txt and %ProgramFiles%\Fortinet\FortiClient\FortiClient.exe exist in the defined directories:

```
config vpn ssl web host-check-software
    edit "file_exist"
        config check-item-list
```

```
            edit 1
                set target "c:\\temp\\mytest.txt"
            next
            edit 2
                set target "%ProgramFiles%\\Fortinet\\FortiClient\\FortiClient.exe"
            next
        end
    next
end
config vpn ssl web portal
    edit "full-access"
        set host-check custom
        set host-check-policy "file_exist"
    next
end
```

To enable custom running process check on FortiOS:

The following configures a check that requires that a designated process, in this case FortiClient.exe, runs on the endpoint:

```
config vpn ssl web host-check-software
    edit "Running-Process"
        config check-item-list
            edit 1
                set type process
                set target "FortiClient.exe"
            next
        end
    next
end
config vpn ssl web portal
    edit "full-access"
        set host-check custom
        set host-check-policy "Running-Process"
    next
end
```

To enable custom registry check on FortiOS:

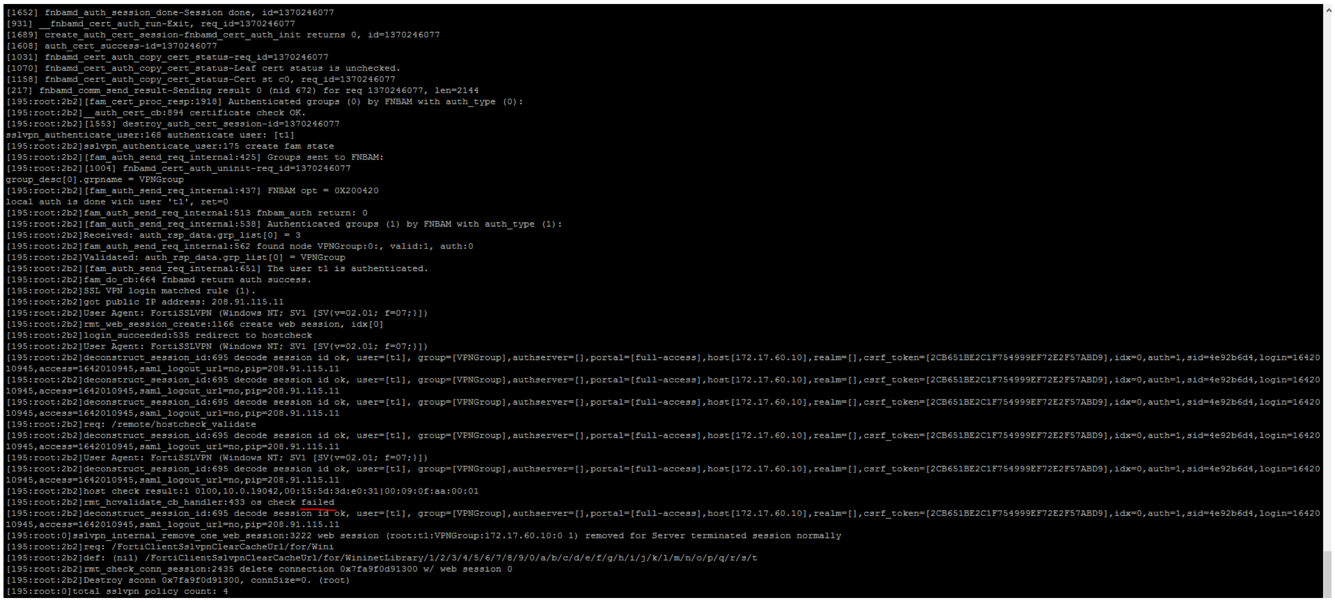
The following configures a check that requires that a designated string or dword value in a registry key exist. In this example, the designated value is `FA_IKE:enabled==1`:

```
config vpn ssl web host-check-software
    edit "hostcheck-condition-registry"
        config check-item-list
            edit 1
                set type registry
                set target "HKLM\\SOFTWARE\\Fortinet\\FortiClient\\FA_IKE:enabled==1"
            next
        end
    next
end
config vpn ssl web portal
    edit "full-access"
        set host-check custom
        set host-check-policy "hostcheck-condition-registry"
    next
end
```

To perform debugging on FortiOS:

```
diagnose debug reset
diagnose debug application sslvpn -1
diagnose debug application samld -1
diagnose debug application fnbamd -1
diagnose debug enable
```

The following shows an example of debugging output when host check fails:



```
[1652] fnbamd_auth_session_done-Session done, id=1370246077
[931] __fnbamd_cert_auth_run-Exit, req_id=1370246077
[1689] create_auth_cert_session-fnbamd_cert_auth_init returns 0, id=1370246077
[1608] auth_cert_success-id=1370246077
[1031] fnbamd_cert_auth_copy_cert_status-req_id=1370246077
[1070] fnbamd_cert_auth_copy_cert_status-Leaf cert status is unchecked.
[1158] fnbamd_cert_auth_copy_cert_status-Cert st c0, req_id=1370246077
[217] fnbamd_comm_send_result-Sending result 0 (nid 672) for req 1370246077, len=2144
[195:root:2b2][fam_cert_proc_resp:1918] Authenticated groups (0) by FNBAM with auth_type (0):
[195:root:2b2]__auth_cert_cb:894 certificate check OK.
[195:root:2b2][1553] destroy_auth_cert_session-id=1370246077
sslvpn_authenticate_user:168 authenticate user: [t1]
[195:root:2b2]sslvpn_authenticate_user:175 create fam state
[195:root:2b2][fam_auth_send_req_internal:425] Groups sent to FNBAM:
[195:root:2b2][1004] fnbamd_cert_auth_uninit-req_id=1370246077
group_desc[0].grpname = VPNGroup
[195:root:2b2][fam_auth_send_req_internal:437] FNBAM opt = 0X200420
local auth is done with user 't1', ret=0
[195:root:2b2]fam_auth_send_req_internal:513 fnbam_auth return: 0
[195:root:2b2][fam_auth_send_req_internal:538] Authenticated groups (1) by FNBAM with auth_type (1):
[195:root:2b2]Received: auth_rsp_data.grp_list[0] = 3
[195:root:2b2]fam_auth_send_req_internal:562 found node VPNGroup:0:, valid:1, auth:0
[195:root:2b2]Validated: auth_rsp_data.grp_list[0] = VPNGroup
[195:root:2b2][fam_auth_send_req_internal:651] The user t1 is authenticated.
[195:root:2b2]fam_do_cb:664 fnbamd return auth success.
[195:root:2b2]SSL VPN login matched rule (1).
[195:root:2b2]got public IP address: 208.91.115.11
[195:root:2b2]User Agent: FortiSSLVPN (Windows NT; SV1 [SV{v=02.01; f=07;}])
[195:root:2b2]rmt_web_session_create:1166 create web session, idx[0]
[195:root:2b2]login_succeeded:535 redirect to hostcheck
[195:root:2b2]User Agent: FortiSSLVPN (Windows NT; SV1 [SV{v=02.01; f=07;}])
[195:root:2b2]deconstruct_session_id:695 decode session id ok, user=[t1], group=[VPNGroup],authserver=[],portal=[full-access],host[172.17.60.10],realm=[],csrf_token=[2CB651BE2C1F754999EF72E2F57ABD9],idx=0,auth=1,sid=4e92b6d4,login=16420
10945,access=1642010945,saml_logout_url=no,pip=208.91.115.11
[195:root:2b2]deconstruct_session_id:695 decode session id ok, user=[t1], group=[VPNGroup],authserver=[],portal=[full-access],host[172.17.60.10],realm=[],csrf_token=[2CB651BE2C1F754999EF72E2F57ABD9],idx=0,auth=1,sid=4e92b6d4,login=16420
10945,access=1642010945,saml_logout_url=no,pip=208.91.115.11
[195:root:2b2]deconstruct_session_id:695 decode session id ok, user=[t1], group=[VPNGroup],authserver=[],portal=[full-access],host[172.17.60.10],realm=[],csrf_token=[2CB651BE2C1F754999EF72E2F57ABD9],idx=0,auth=1,sid=4e92b6d4,login=16420
10945,access=1642010945,saml_logout_url=no,pip=208.91.115.11
[195:root:2b2]req: /remote/hostcheck_validate
[195:root:2b2]deconstruct_session_id:695 decode session id ok, user=[t1], group=[VPNGroup],authserver=[],portal=[full-access],host[172.17.60.10],realm=[],csrf_token=[2CB651BE2C1F754999EF72E2F57ABD9],idx=0,auth=1,sid=4e92b6d4,login=16420
10945,access=1642010945,saml_logout_url=no,pip=208.91.115.11
[195:root:2b2]User Agent: FortiSSLVPN (Windows NT; SV1 [SV{v=02.01; f=07;}])
[195:root:2b2]deconstruct_session_id:695 decode session id ok, user=[t1], group=[VPNGroup],authserver=[],portal=[full-access],host[172.17.60.10],realm=[],csrf_token=[2CB651BE2C1F754999EF72E2F57ABD9],idx=0,auth=1,sid=4e92b6d4,login=16420
10945,access=1642010945,saml_logout_url=no,pip=208.91.115.11
[195:root:2b2]host check result:1 0100,10.0.19042,00:15:5d:3d:e0:31|00:09:0f:aa:00:01
[195:root:2b2]rmt_hcvalidate_cb_handler:433 os check failed
[195:root:2b2]deconstruct_session_id:695 decode session id ok, user=[t1], group=[VPNGroup],authserver=[],portal=[full-access],host[172.17.60.10],realm=[],csrf_token=[2CB651BE2C1F754999EF72E2F57ABD9],idx=0,auth=1,sid=4e92b6d4,login=16420
10945,access=1642010945,saml_logout_url=no,pip=208.91.115.11
[195:root:0]sslvpn_internal_remove_one_web_session:3222 web session (root:t1:VPNGroup:172.17.60.10:0 1) removed for Server terminated session normally
[195:root:2b2]req: /FortiClientSslvpnClearCacheUrl/for/Wini
[195:root:2b2]def: (nil) /FortiClientSslvpnClearCacheUrl/for/WininetLibrary/1/2/3/4/5/6/7/8/9/0/a/b/c/d/e/f/g/h/i/j/k/l/m/n/o/p/q/r/s/t
[195:root:2b2]rmt_check_conn_session:2435 delete connection 0x7fa9f0d91300 w/ web session 0
[195:root:2b2]Destroy sconn 0x7fa9f0d91300, connSize=0. (root)
[195:root:0]total sslvpn policy count: 4
```

Autoconnect on login as an Azure AD user - 7.0.7

You can configure FortiClient to automatically connect to a specified VPN tunnel immediately using Azure Active Directory (AD) credentials after it installs and receives its configuration from EMS. Whenever the user logs in to Windows using their Azure AD credentials, FortiClient silently and automatically connects to the specified VPN tunnel without the user needing to reenter their credentials or open the FortiClient console.

This feature requires FortiOS 7.2.1 or later.

To enable this feature, the following configuration steps are required:

1. Create and configure application registration in Azure.
2. Configure FortiOS with the `auth-url` setting within the SAML server entry configuration.
3. Configure the corresponding Remote Access profile in EMS using XML configuration to support Azure autologin and autoconnect on install.

For details on this configuration, see Autoconnect on logging in as an Azure AD user.

FortiClient EMS

Zero-trust network access

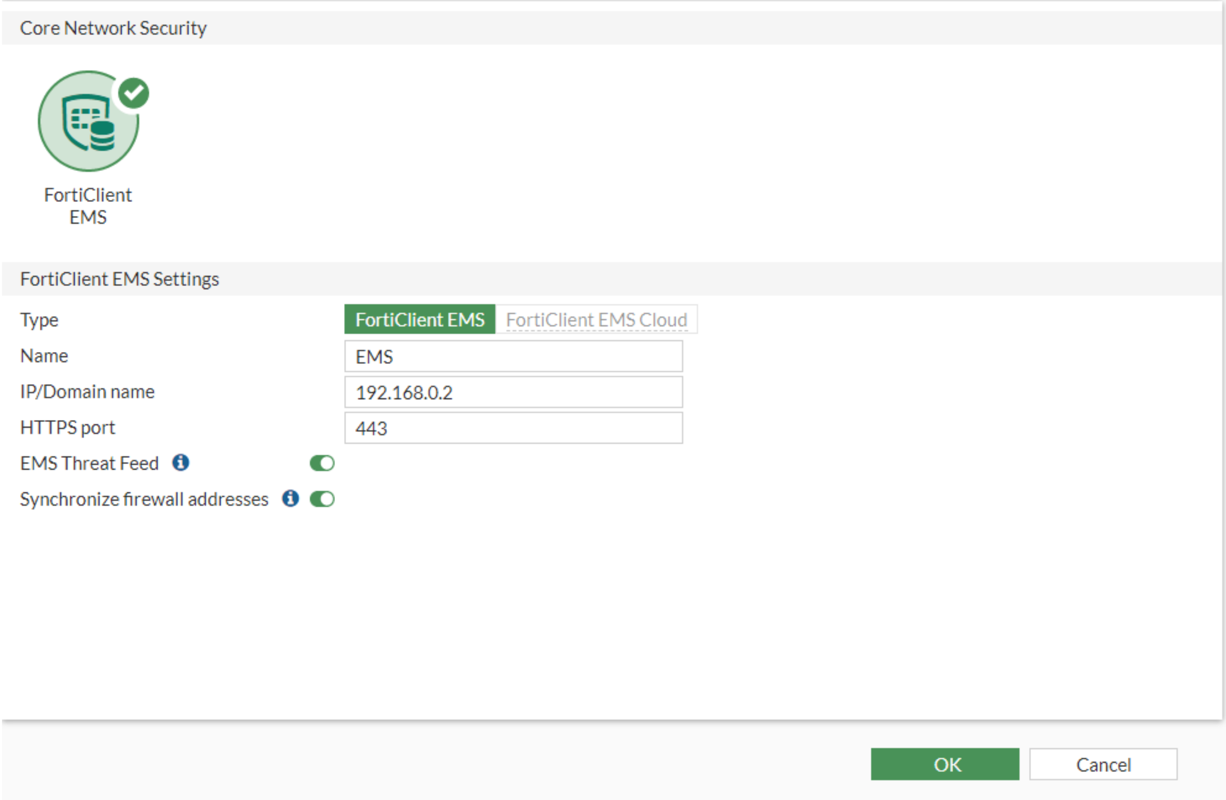
EMS distributes SSL deep inspection CA certificates - 7.0.1

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.

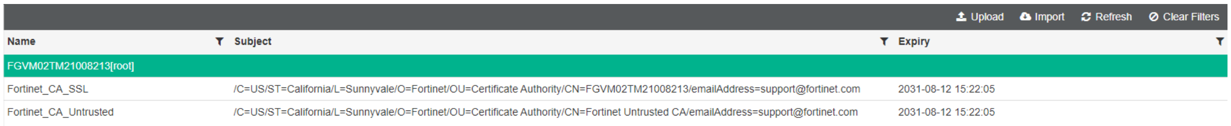


Core Network Security

FortiClient EMS Settings

Type	FortiClient EMS / FortiClient EMS Cloud
Name	EMS
IP/Domain name	192.168.0.2
HTTPS port	443
EMS Threat Feed	●
Synchronize firewall addresses	●

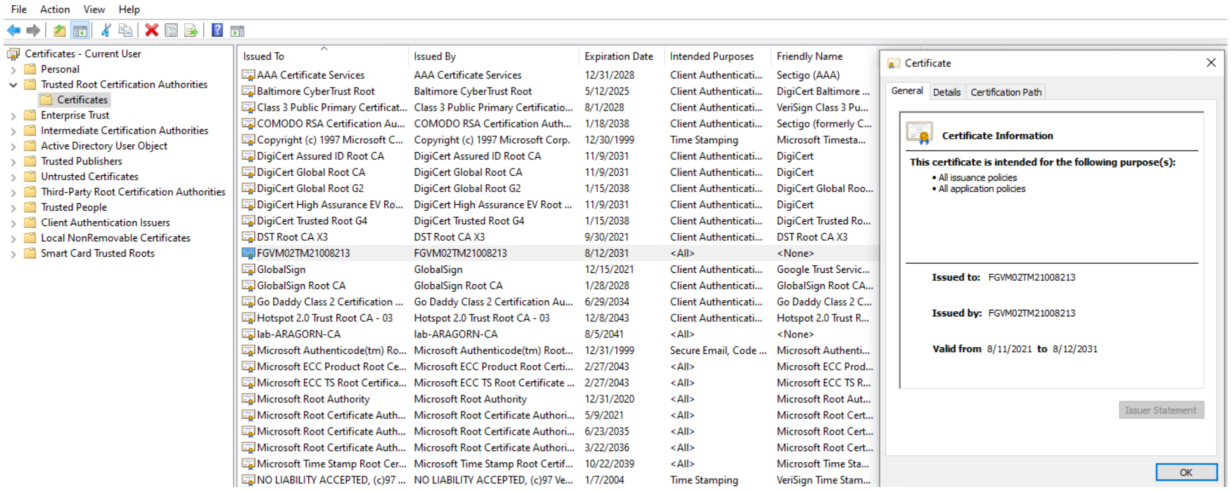
2. Configure EMS to import the certificates:
   a. In EMS, go to *Administration > Fabric Devices*.
   b. Authorize the connection request from the FortiGate.
   c. Once the connection succeeds, EMS automatically imports FortiGate CA certificates. To verify this, go to *Endpoint Policy & Components >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



Name	Subject	Expiry
FGVM02TM21008213[root]		
Fortinet_CA_SSL	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=FGVM02TM21008213/emailAddress=support@fortinet.com	2031-08-12 15:22:05
Fortinet_CA_Untrusted	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=Fortinet Untrusted CA/emailAddress=support@fortinet.com	2031-08-12 15:22:05

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.


File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Local NonRemovable Certificates
Smart Card Trusted Roots
Certificate
General
Details
Certification Path
Issuer Statement
OK

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati...	Sectigo (AAA)
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati...	DigiCert Baltimore ...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Client Authenticati...	VeriSign Class 3 Pu...
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	1/18/2038	Client Authenticati...	Sectigo (formerly C...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Global Roo...
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Client Authenticati...	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati...	DigiCert Trusted Ro...
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...	DST Root CA X3
FGVM02TM21008213	FGVM02TM21008213	8/12/2031	<All>	<None>
GlobalSign	GlobalSign	12/15/2021	Client Authenticati...	Google Trust Servic...
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticati...	GlobalSign Root CA...
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	Client Authenticati...	Go Daddy Class 2 C...
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Client Authenticati...	Hotspot 2.0 Trust R...
lab-ARAGORN-CA	lab-ARAGORN-CA	8/5/2041	<All>	<None>
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043	<All>	Microsoft ECC Prod...
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS R...
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	10/22/2039	<All>	Microsoft Time Sta...
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	1/7/2004	Time Stamping	VeriSign Time Stam...

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: FGVM02TM21008213

Issued by: FGVM02TM21008213

Valid from 8/11/2021 **to** 8/12/2031

Zero Trust tagging rules enhancement - 7.0.1

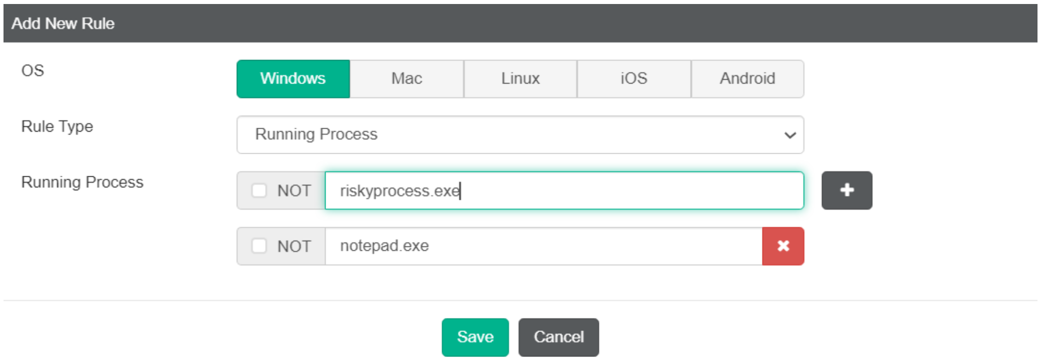
FortiClient EMS adds the following enhancements to Zero Trust tagging rules:

- Logical OR operation support on page 32
- Importing and exporting Zero Trust tagging rules on page 34
- On-Fabric rules on page 35

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.



Add New Rule

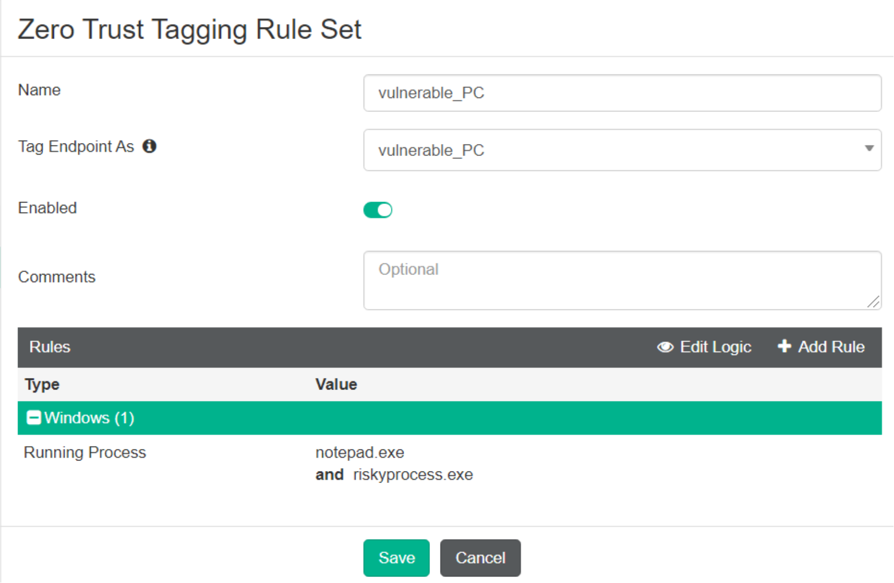
OS: Windows | Mac | Linux | iOS | Android

Rule Type: Running Process

Running Process: □ NOT riskyprocess.exe

□ NOT notepad.exe

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.



Zero Trust Tagging Rule Set

Name: vulnerable_PC

Tag Endpoint As: vulnerable_PC

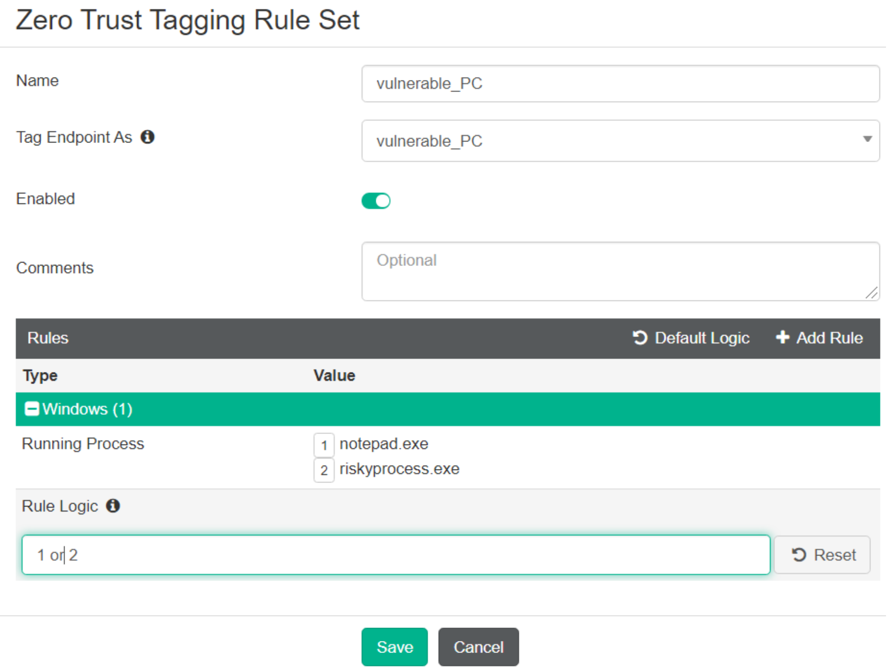
Enabled: ●

Comments: Optional

Rules

Type	Value
Windows (1)	
Running Process	notepad.exe **and** riskyprocess.exe

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



Zero Trust Tagging Rule Set

Name	vulnerable_PC
Tag Endpoint As	vulnerable_PC
Enabled	●
Comments	Optional

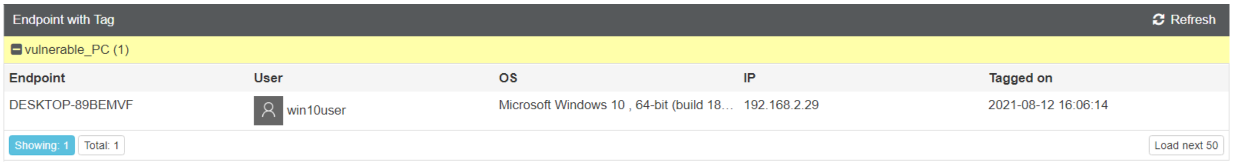
Type	Value
Windows (1)	
Running Process	1 notepad.exe 2 riskyprocess.exe

Rule Logic

1 or 2

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.



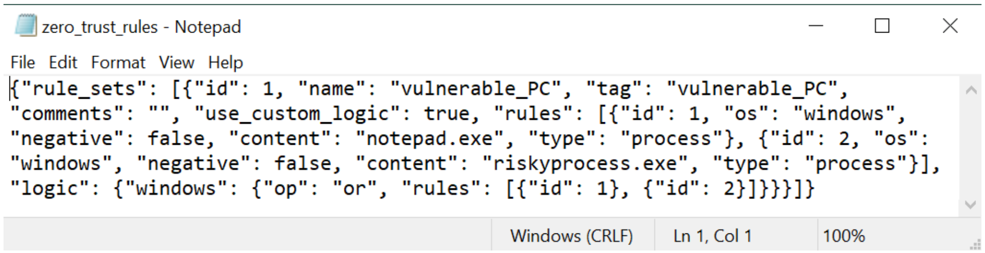
vulnerable_PC (1)

Endpoint	User	OS	IP	Tagged on
DESKTOP-89BEMVF	win10user	Microsoft Windows 10 , 64-bit (build 18...	192.168.2.29	2021-08-12 16:06:14

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.



```
{"rule_sets": [{"id": 1, "name": "vulnerable_PC", "tag": "vulnerable_PC",
"comments": "", "use_custom_logic": true, "rules": [{"id": 1, "os": "windows",
"negative": false, "content": "notepad.exe", "type": "process"}, {"id": 2, "os":
"windows", "negative": false, "content": "riskyprocess.exe", "type": "process"}],
"logic": {"windows": {"op": "or", "rules": [{"id": 1}, {"id": 2}]}}}]}
```

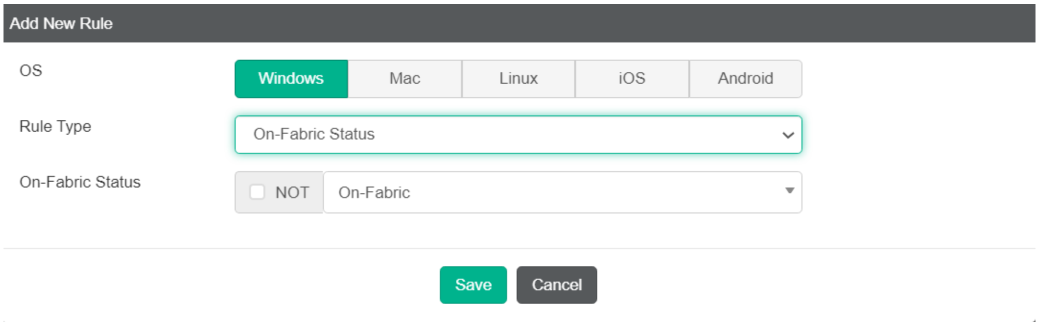
4. You can use import the same rules to another EMS using the JSON files. On another EMS, go to *Zero Trust Tags* > *Zero Trust Tagging Rules* and click *Import*. Browse to and select the desired JSON file. Click *Import*.

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*.



Add New Rule

OS: Windows | Mac | Linux | iOS | Android

Rule Type: On-Fabric Status

On-Fabric Status: □ NOT | On-Fabric

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.

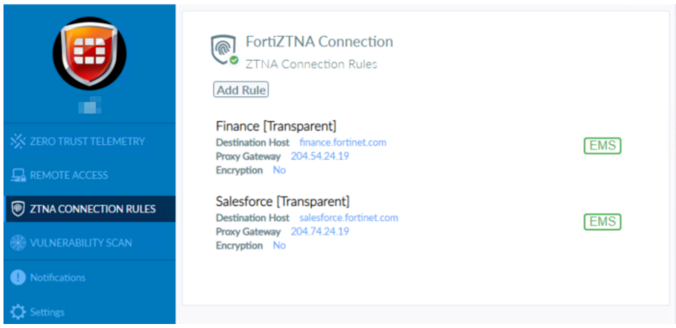
To configure ZTNA TCP forwarding rules via EMS:

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.



Finance [Transparent]
Destination Host finance.fortinet.com
Proxy Gateway 204.54.24.19
Encryption No

Salesforce [Transparent]
Destination Host salesforce.fortinet.com
Proxy Gateway 204.74.24.19
Encryption No

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.

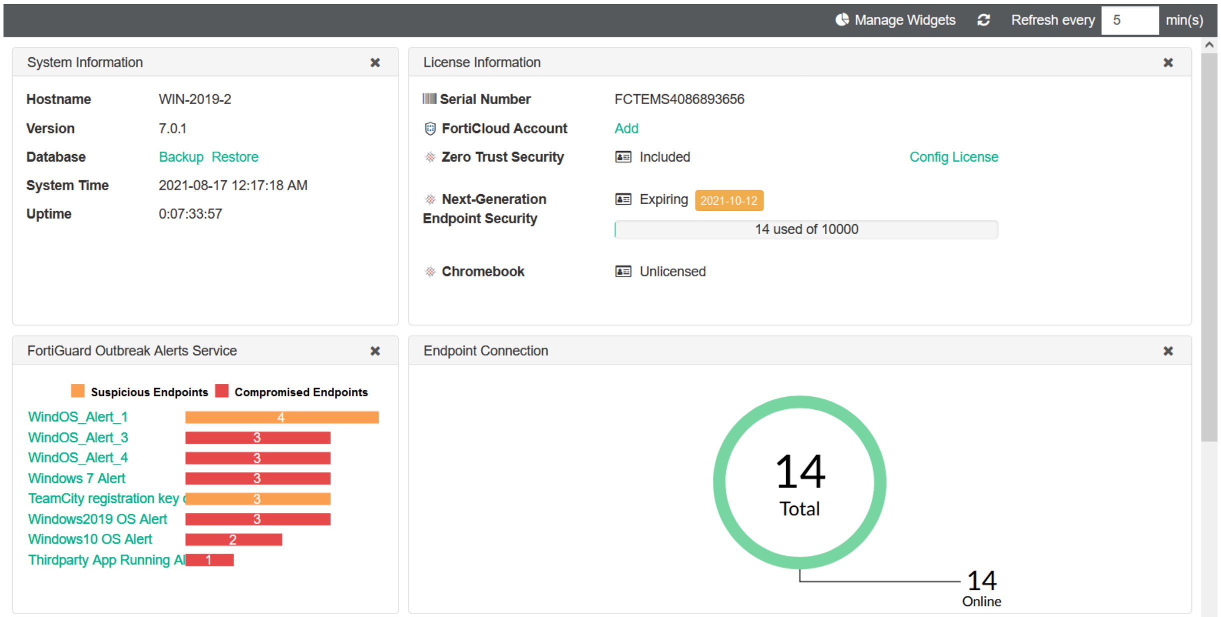
FortiGuard Outbreak Alerts service - 7.0.1

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.



System Information

Hostname	WIN-2019-2
Version	7.0.1
Database	Backup Restore
System Time	2021-08-17 12:17:18 AM
Uptime	0:07:33:57

License Information

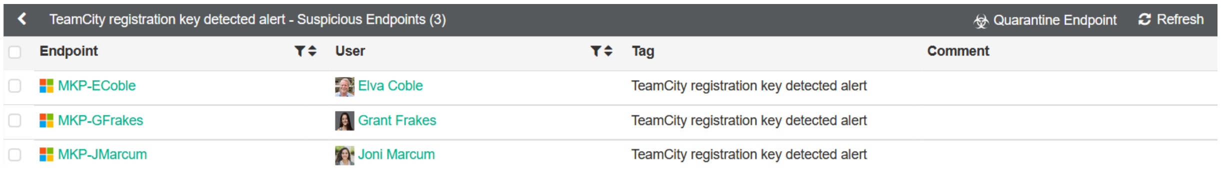
Serial Number	FCTEMS4086893656	
FortiCloud Account	Add	
Zero Trust Security	Included	Config License
Next-Generation Endpoint Security	Expiring 2021-10-12 14 used of 10000	
Chromebook	Unlicensed	

FortiGuard Outbreak Alerts Service

	🟧 Suspicious Endpoints	🟥 Compromised Endpoints
WindOS_Alert_1	4	
WindOS_Alert_3		3
WindOS_Alert_4		3
Windows 7 Alert		3
TeamCity registration key d	3	
Windows2019 OS Alert		3
Windows10 OS Alert		2
Thirdparty App Running Al		1

Endpoint Connection

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

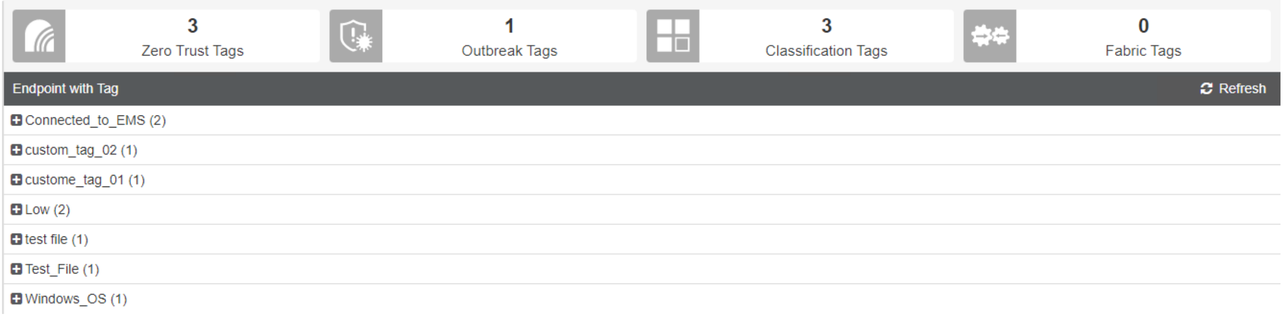

TeamCity registration key detected alert - Suspicious Endpoints (3)

Endpoint	User	Tag	Comment
MKP-ECoble	Elva Coble	TeamCity registration key detected alert	
MKP-GFrakes	Grant Frakes	TeamCity registration key detected alert	
MKP-JMarcum	Joni Marcum	TeamCity registration key detected alert	

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

Tag management and visibility improvement - 7.0.3

You can now clearly identify all tag types and their marked endpoints on the *Zero Trust Tag Monitor* page.


3	1	3	0
Zero Trust Tags	Outbreak Tags	Classification Tags	Fabric Tags

Endpoint with Tag

- Connected_to_EMS (2)
- custom_tag_02 (1)
- custome_tag_01 (1)
- Low (2)
- test file (1)
- Test_File (1)
- Windows_OS (1)

The page displays a tab for each tag category. You can click each tab to see endpoints tagged with that tag type.

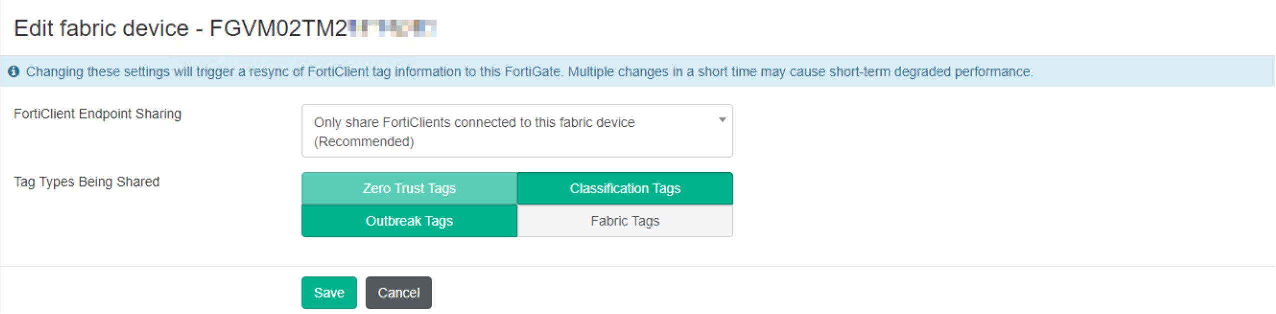
You also have the option to choose which tags to share with a Fabric device for access control. You can choose from outbreak tags, classification tags, and Fabric tags. The following instructions assume that EMS is already connected to a FortiGate as part of a Fortinet Security Fabric.

To configure FortiClient endpoint tag sharing:

1. Go to *Administration > Fabric Devices*.
2. Select the desired FortiGate to edit.
3. From the *FortiClient Endpoint Sharing* dropdown list, select one of the following:

Option	Description
Share all FortiClients	EMS shares tag information of endpoints connected to all authorized Fabric devices with this FortiGate.
Only share FortiClients connected to this fabric device (Recommended)	EMS only shares tag information of endpoints connected to this Fabric device. This is the default and recommended option.
Share FortiClients connected to selected fabric devices	You can select up to four authorized Fabric devices. EMS shares the tag information of endpoints connected to these Fabric devices with the FortiGate.

4. In the *Tag Types Being Shared* field, select the desired tag types to share with the Fabric device. Zero Trust Tags is selected by default. You cannot deselect Zero Trust tags. You can select any or none of the other tag types to share with this Fabric device.
5. Click *Save*.



Edit fabric device - FGVM02TM2[redacted]

Changing these settings will trigger a resync of FortiClient tag information to this FortiGate. Multiple changes in a short time may cause short-term degraded performance.

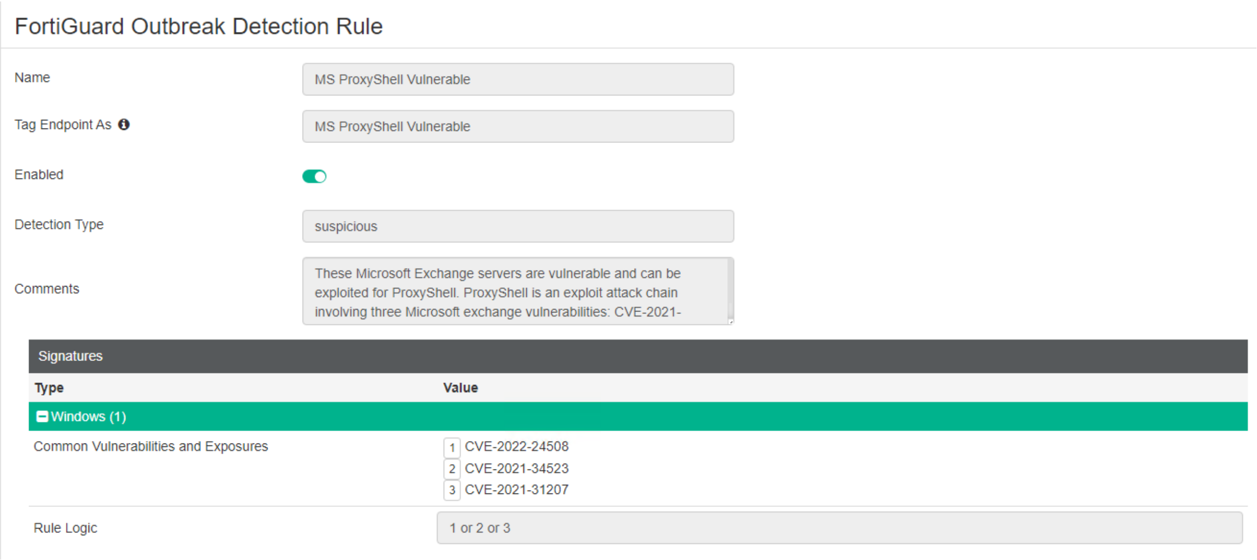
FortiClient Endpoint Sharing: Only share FortiClients connected to this fabric device (Recommended)

Tag Types Being Shared: Zero Trust Tags, Classification Tags, Outbreak Tags, Fabric Tags

FortiGuard Outbreak Alerts support for tagging endpoints for specific vulnerabilities - 7.0.4

The FortiGuard Outbreak Alerts service has added support for rules that include common vulnerabilities and exposures (CVE) IDs. You can now also configure Common Vulnerabilities and Exposures Zero Trust tagging rules. This makes it more convenient for you to check and patch an endpoint that has the critical known vulnerabilities.

The following shows a FortiGuard Outbreak rule that EMS has downloaded from FortiGuard. You can view the configured CVE IDs when viewing the rule details in EMS. You can also read more details about these vulnerabilities in the information that the *Comments* field provides. In this example, the rule is applicable to an endpoint where CVE-2022-24508, CVE-2021-34523, or CVE-2021-31207 is present.



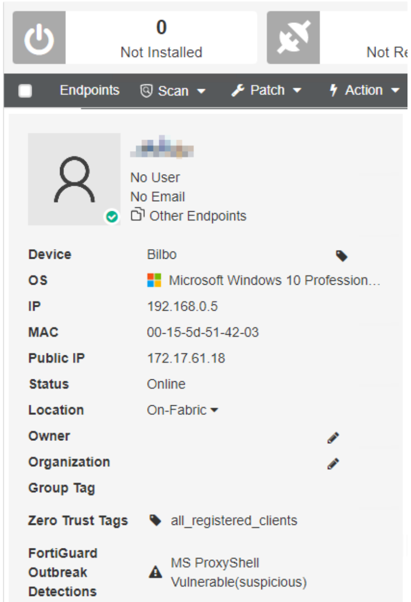
FortiGuard Outbreak Detection Rule

Name	MS ProxyShell Vulnerable
Tag Endpoint As	MS ProxyShell Vulnerable
Enabled	●
Detection Type	suspicious
Comments	These Microsoft Exchange servers are vulnerable and can be exploited for ProxyShell. ProxyShell is an exploit attack chain involving three Microsoft exchange vulnerabilities: CVE-2021-

Signatures

Type	Value
Windows (1)	
Common Vulnerabilities and Exposures	1 CVE-2022-24508 2 CVE-2021-34523 3 CVE-2021-31207
Rule Logic	1 or 2 or 3

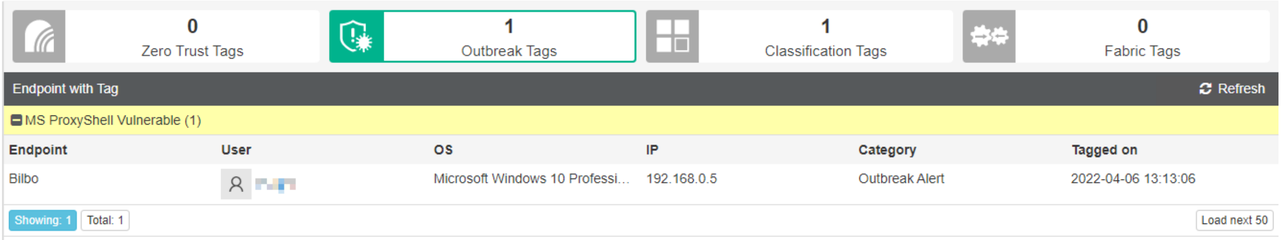
When FortiClient detects one of the configured CVEs on an endpoint, the endpoint summary in EMS shows that EMS has tagged the endpoint with the appropriate FortiGuard outbreak tag.



[redacted]
No User
No Email
Other Endpoints

Device	Bilbo
OS	Microsoft Windows 10 Profession...
IP	192.168.0.5
MAC	00-15-5d-51-42-03
Public IP	172.17.61.18
Status	Online
Location	On-Fabric
Owner	
Organization	
Group Tag	
Zero Trust Tags	all_registered_clients
FortiGuard Outbreak Detections	MS ProxyShell Vulnerable(suspicious)

You can also go to *Zero Trust Tags > Zero Trust Tag Monitor* and filter by *Outbreak Tags* to view the endpoint.



MS ProxyShell Vulnerable (1)

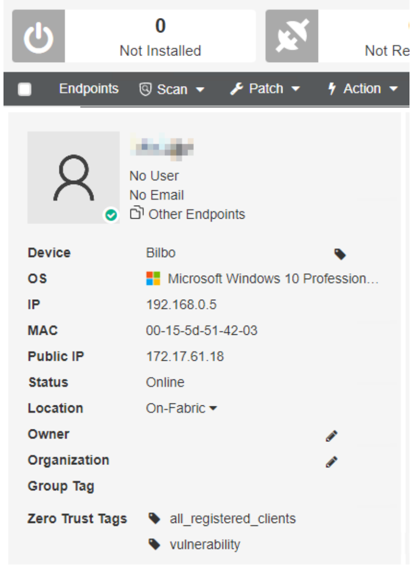
Endpoint	User	OS	IP	Category	Tagged on
Bilbo	[redacted]	Microsoft Windows 10 Professi...	192.168.0.5	Outbreak Alert	2022-04-06 13:13:06

Showing: 1 Total: 1 Load next 50

To configure a CVE Zero Trust tagging 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 *Common Vulnerabilities and Exposures*.
5. In the *CVEs* field, enter the desired CVE ID in the format CVE-xxxx-xxxxx. If desired, click the + button to configure multiple CVE IDs.
6. Click *Save*.
7. Configure other fields as desired, then save the rule.

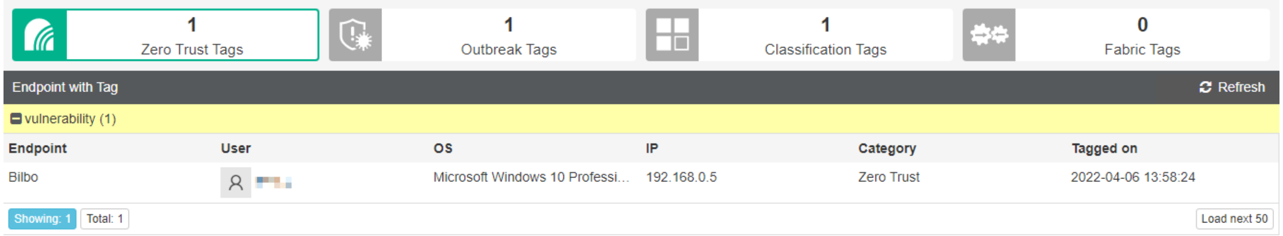
When FortiClient detects one of the configured CVEs on an endpoint, the endpoint summary in EMS shows that EMS has tagged the endpoint with the appropriate Zero Trust tag.



[redacted]
No User
No Email
Other Endpoints

Device	Bilbo
OS	Microsoft Windows 10 Profession...
IP	192.168.0.5
MAC	00-15-5d-51-42-03
Public IP	172.17.61.18
Status	Online
Location	On-Fabric
Owner	
Organization	
Group Tag	
Zero Trust Tags	all_registered_clients vulnerability

You can also go to *Zero Trust Tags* > *Zero Trust Tag Monitor* and filter by *Zero Trust Tags* to view the endpoint.



Endpoint	User	OS	IP	Category	Tagged on
Bilbo	[redacted]	Microsoft Windows 10 Professi...	192.168.0.5	Zero Trust	2022-04-06 13:58:24

Individual onboarding process - 7.0.6

EMS 7.0.6 introduces a new registration method: onboarding users. With this new individual onboarding process, you have the option to verify user identity during the registration process. You can enforce user verification during the onboarding process to secure the connection between EMS and endpoints, and block unknown users and endpoints from registering to EMS.

The following includes two examples:

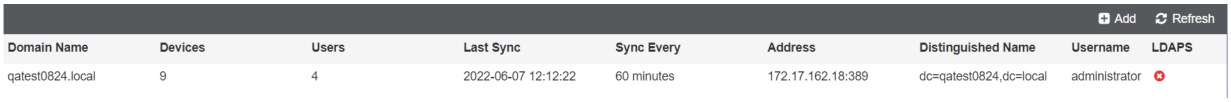
- Individual onboarding process with SAML authentication using an LDAP domain user account
- Enforcing reauthentication for an onboarding user

While the first example uses SAML authentication as the verification type for the invitation, you can also configure local or LDAP verification.

Individual onboarding process with SAML authentication using an LDAP domain user account

To configure individual onboarding with SAML authentication using an LDAP domain user account:

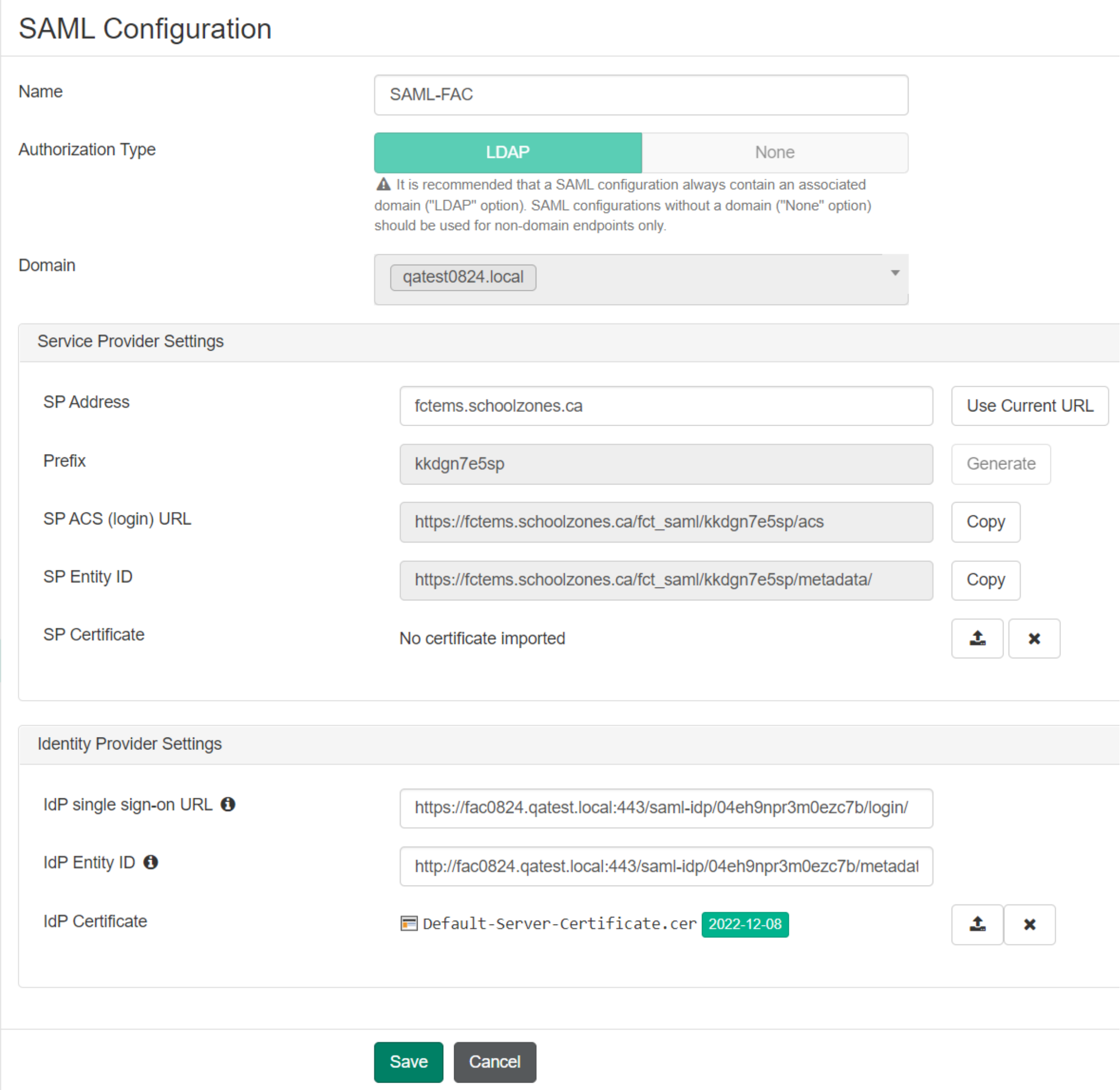
1. Configure EMS:
   a. In EMS, go to *Endpoints* > *Manage Domains*.
   b. Import the desired Active Directory domain. During the onboarding process, EMS authenticates user identities based on this domain. In this example, the domain is qatest0824.local.



Domain Name	Devices	Users	Last Sync	Sync Every	Address	Distinguished Name	Username	LDAPS
qatest0824.local	9	4	2022-06-07 12:12:22	60 minutes	172.17.162.18:389	dc=qatest0824,dc=local	administrator	✗

   c. Go to *User Management* > *SAML Configuration*.
   d. Add a SAML configuration with the imported domain. For *Authorization Type*, select *LDAP*. From the *Domain* dropdown list, select the newly imported domain. In this configuration, EMS is the service provider (SP), and FortiAuthenticator is the identity provider (IdP). Under *Identity Provider Settings*, enter your FortiAuthenticator

details. Click *Save*.



SAML Configuration

Name	SAML-FAC	
Authorization Type	LDAP / None	
	⚠ It is recommended that a SAML configuration always contain an associated domain ("LDAP" option). SAML configurations without a domain ("None" option) should be used for non-domain endpoints only.	
Domain	qatest0824.local	

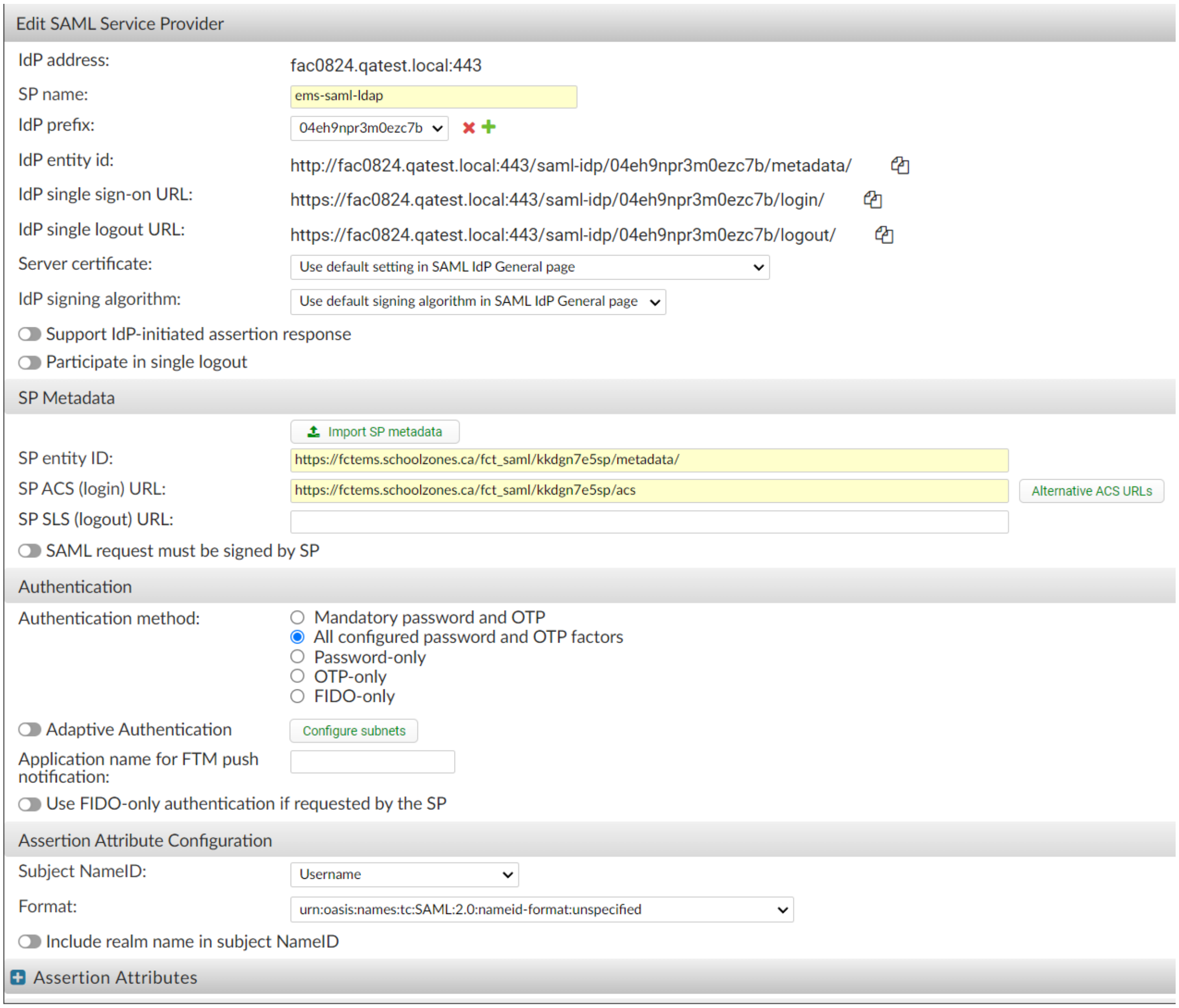
Service Provider Settings

SP Address	fctems.schoolzones.ca	Use Current URL
Prefix	kkdgn7e5sp	Generate
SP ACS (login) URL	https://fctems.schoolzones.ca/fct_saml/kkdgn7e5sp/acs	Copy
SP Entity ID	https://fctems.schoolzones.ca/fct_saml/kkdgn7e5sp/metadata/	Copy
SP Certificate	No certificate imported	

Identity Provider Settings

IdP single sign-on URL	https://fac0824.qatest.local:443/saml-idp/04eh9npr3m0ezc7b/login/	
IdP Entity ID	http://fac0824.qatest.local:443/saml-idp/04eh9npr3m0ezc7b/metadat	
IdP Certificate	Default-Server-Certificate.cer 2022-12-08	

e. In FortiAuthenticator, configure EMS as an SP.



Edit SAML Service Provider

IdP address:	fac0824.qatest.local:443
SP name:	ems-saml-ldap
IdP prefix:	04eh9npr3m0ezc7b
IdP entity id:	http://fac0824.qatest.local:443/saml-idp/04eh9npr3m0ezc7b/metadata/
IdP single sign-on URL:	https://fac0824.qatest.local:443/saml-idp/04eh9npr3m0ezc7b/login/
IdP single logout URL:	https://fac0824.qatest.local:443/saml-idp/04eh9npr3m0ezc7b/logout/
Server certificate:	Use default setting in SAML IdP General page
IdP signing algorithm:	Use default signing algorithm in SAML IdP General page

○ Support IdP-initiated assertion response

○ Participate in single logout

SP Metadata

SP entity ID:	https://fctems.schoolzones.ca/fct_saml/kkdgn7e5sp/metadata/
SP ACS (login) URL:	https://fctems.schoolzones.ca/fct_saml/kkdgn7e5sp/acs
SP SLS (logout) URL:	

○ SAML request must be signed by SP

Authentication

Authentication method:

○ Mandatory password and OTP
● All configured password and OTP factors
○ Password-only
○ OTP-only
○ FIDO-only

○ Adaptive Authentication

Application name for FTM push notification:

○ Use FIDO-only authentication if requested by the SP

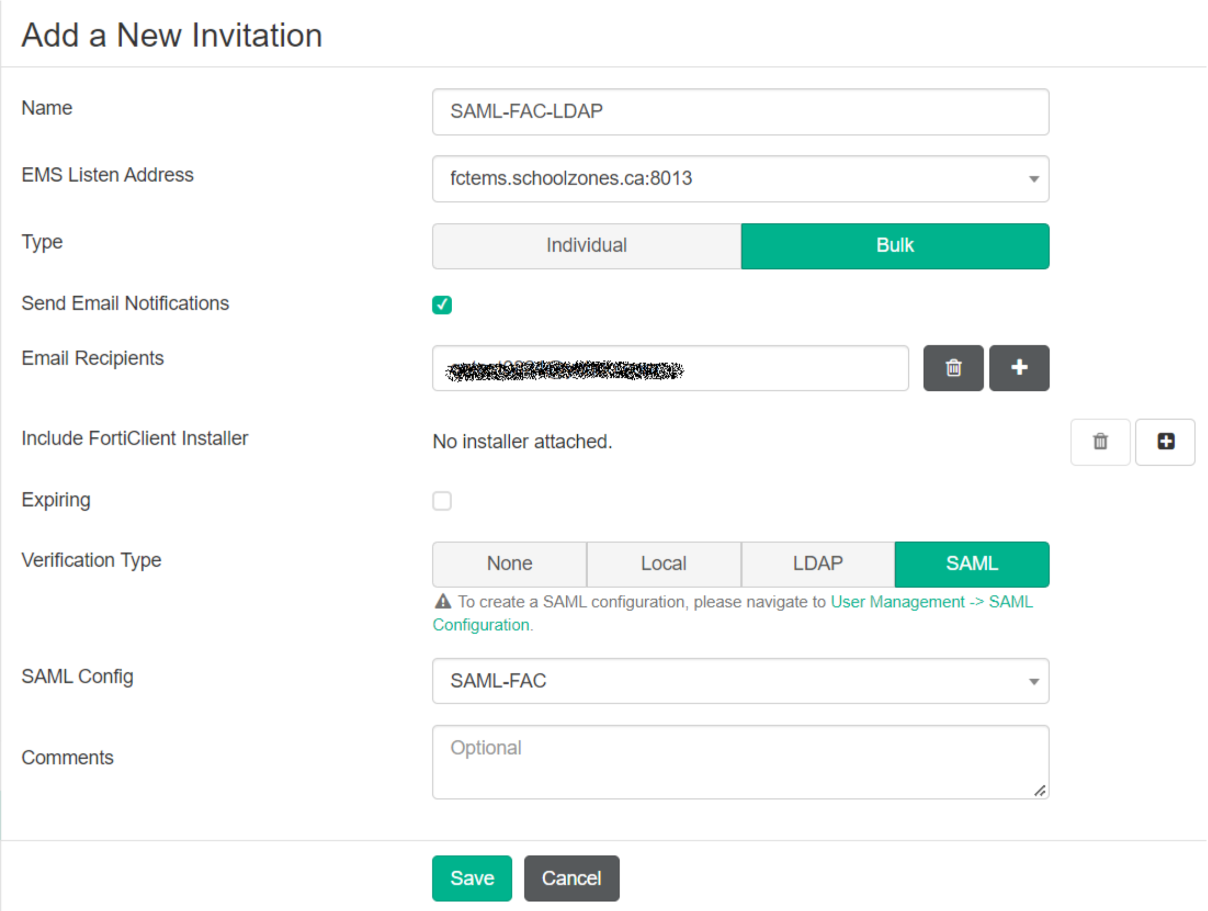
Assertion Attribute Configuration

Subject NameID:	Username
Format:	urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified

○ Include realm name in subject NameID

Assertion Attributes

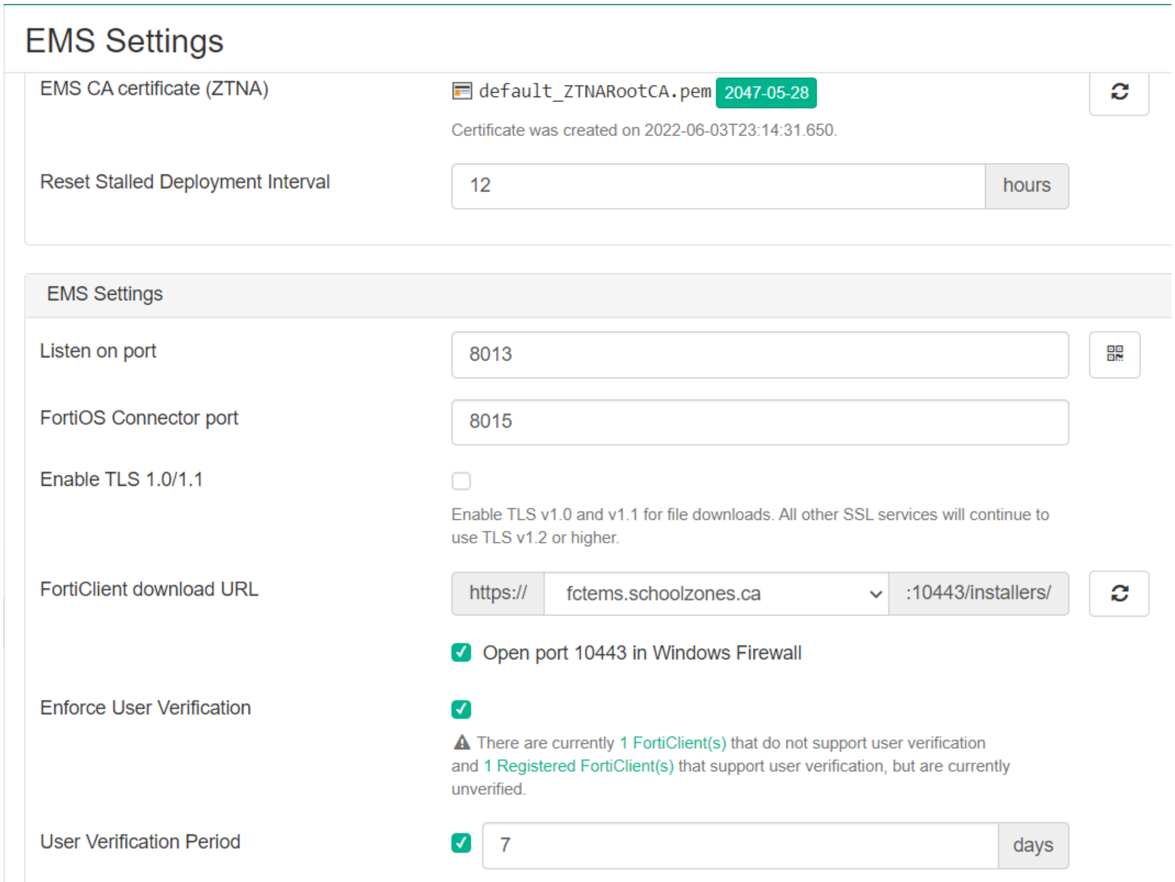
f. In EMS, go to *User Management* > *Invitations*. Configure the desired recipients to receive their invitation codes over email. For *Verification Type*, select *SAML*. From the *SAML Config* dropdown list, select the SAML configuration that you created. Click *Save*.



Add a New Invitation

Name	SAML-FAC-LDAP
EMS Listen Address	fctems.schoolzones.ca:8013
Type	Individual / [✓ Bulk]
Send Email Notifications	☑
Email Recipients	[redacted]
Include FortiClient Installer	No installer attached.
Expiring	□
Verification Type	None / Local / LDAP / [✓ SAML] ⚠ To create a SAML configuration, please navigate to User Management -> SAML Configuration.
SAML Config	SAML-FAC
Comments	Optional

g. Go to *System Settings* > *EMS Settings*. Enable *Enforce User Verification*. This forces FortiClient to register to EMS using user onboarding.



EMS Settings

EMS CA certificate (ZTNA): default_ZTNARootCA.pem 2047-05-28
Certificate was created on 2022-06-03T23:14:31.650.

Reset Stalled Deployment Interval: 12 hours

EMS Settings

Listen on port: 8013

FortiOS Connector port: 8015

Enable TLS 1.0/1.1: □
Enable TLS v1.0 and v1.1 for file downloads. All other SSL services will continue to use TLS v1.2 or higher.

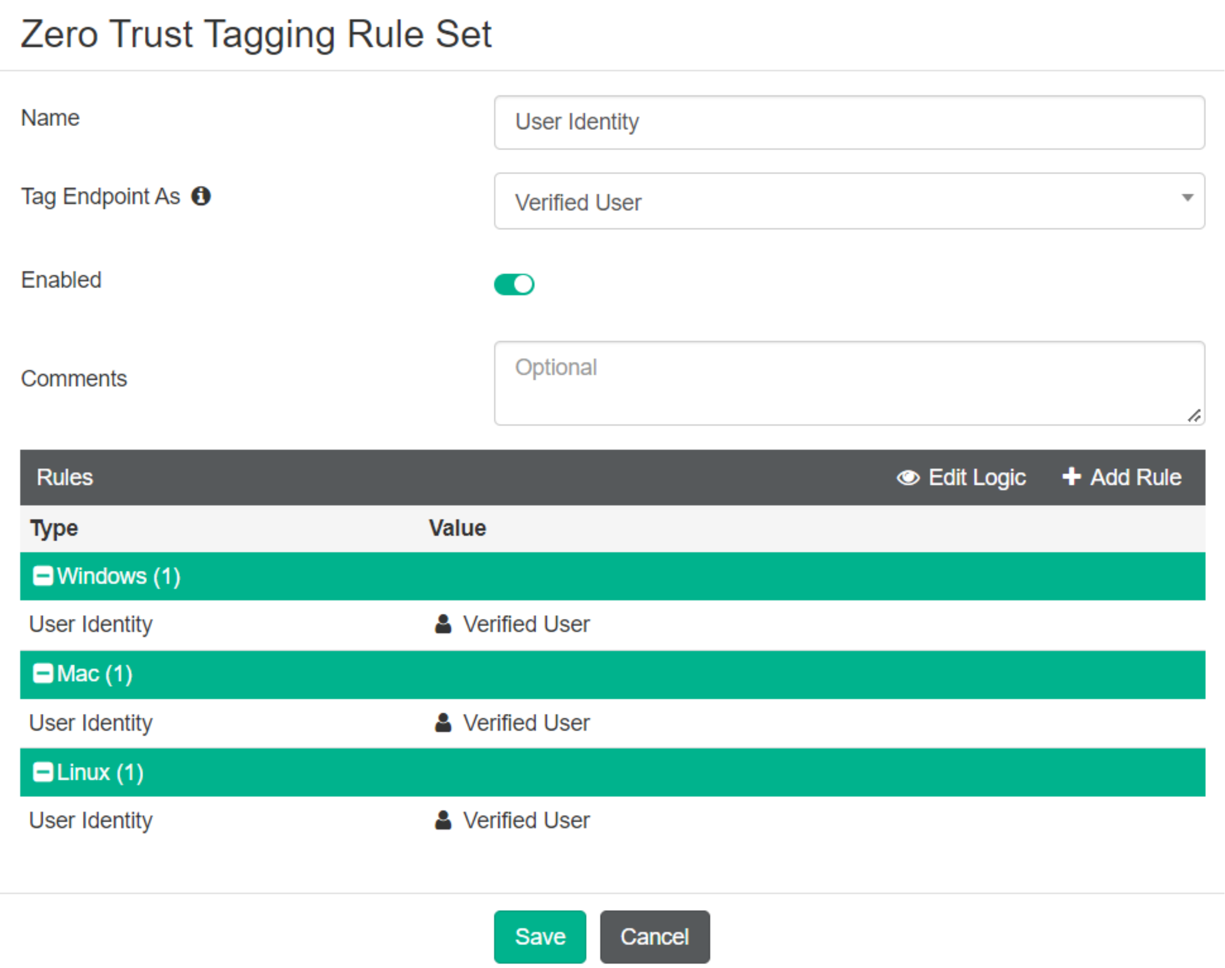
FortiClient download URL: https:// fctems.schoolzones.ca :10443/installers/

☑ Open port 10443 in Windows Firewall

Enforce User Verification: ☑
⚠ There are currently 1 FortiClient(s) that do not support user verification and 1 Registered FortiClient(s) that support user verification, but are currently unverified.

User Verification Period: ☑ 7 days

h. Go to *Zero Trust Tags* > *Zero Trust Tagging Rules*. Add a Zero Trust tagging rule to tag registered endpoints with verified users.



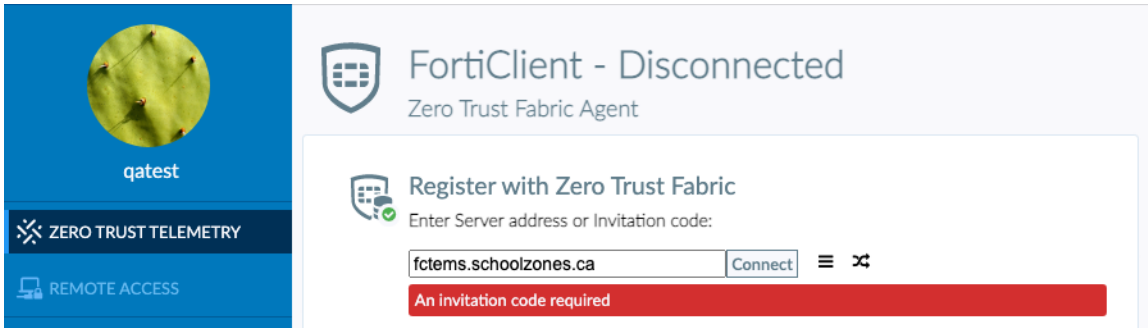
Zero Trust Tagging Rule Set

Name	User Identity
Tag Endpoint As	Verified User
Enabled	●
Comments	Optional

Rules

Type	Value
Windows (1)	
User Identity	Verified User
Mac (1)	
User Identity	Verified User
Linux (1)	
User Identity	Verified User

2. In FortiClient on an unregistered endpoint, attempt to register to EMS using the EMS fully qualified domain name. EMS rejects the connection attempt. FortiClient displays an error that EMS require an invitation code.



FortiClient - Disconnected

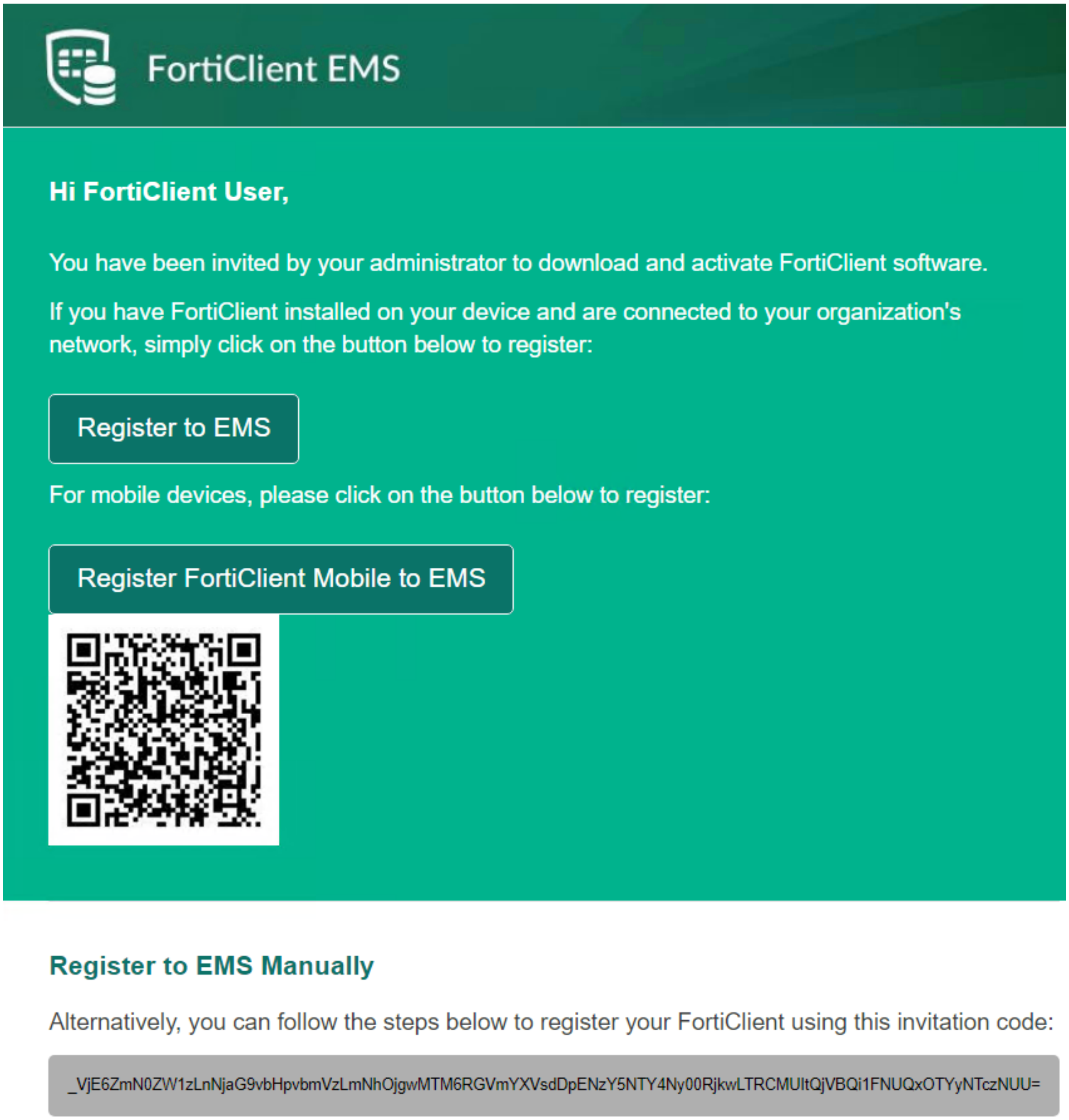
Zero Trust Fabric Agent

Register with Zero Trust Fabric

Enter Server address or Invitation code: fctems.schoolzones.ca

An invitation code required

3. Register FortiClient to EMS:
   a. Do one of the following to start the process of registering FortiClient to EMS:
      i. Open the invitation email. and click *Register to EMS*. Follow the instructions to register to EMS.



Hi FortiClient User,

You have been invited by your administrator to download and activate FortiClient software.

If you have FortiClient installed on your device and are connected to your organization's network, simply click on the button below to register:

For mobile devices, please click on the button below to register:

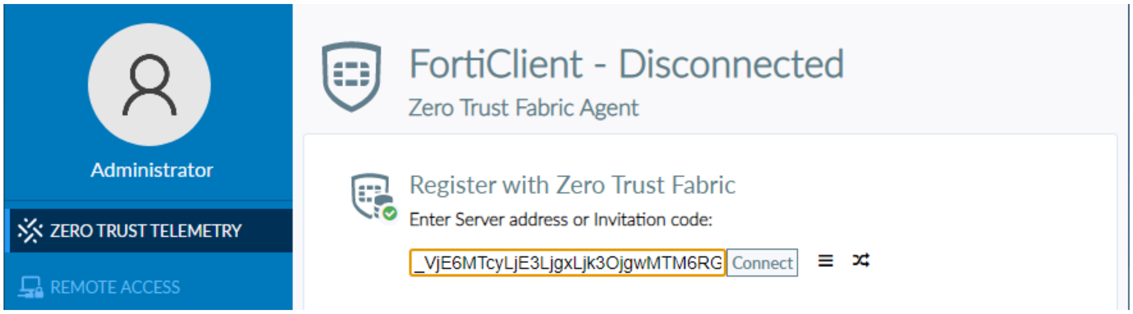
Register to EMS Manually

Alternatively, you can follow the steps below to register your FortiClient using this invitation code:

```
_VjE6ZmN0ZW1zLnNjaG9vbHpvbmVzLmNhOjgwMTM6RGVmYXVsdDpENzY5NTY4Ny00RjkwLTRCMUItQjVBQi1FNUQxOTYyNTczNUU=
```

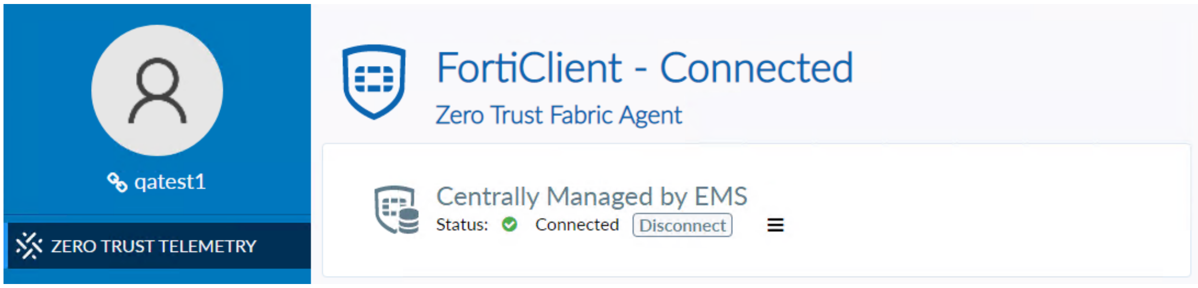
      ii. Open the invitation email, and copy the invitation code. Enter the invitation code on the *Zero Trust*

Telemetry tab, and click *Connect*.



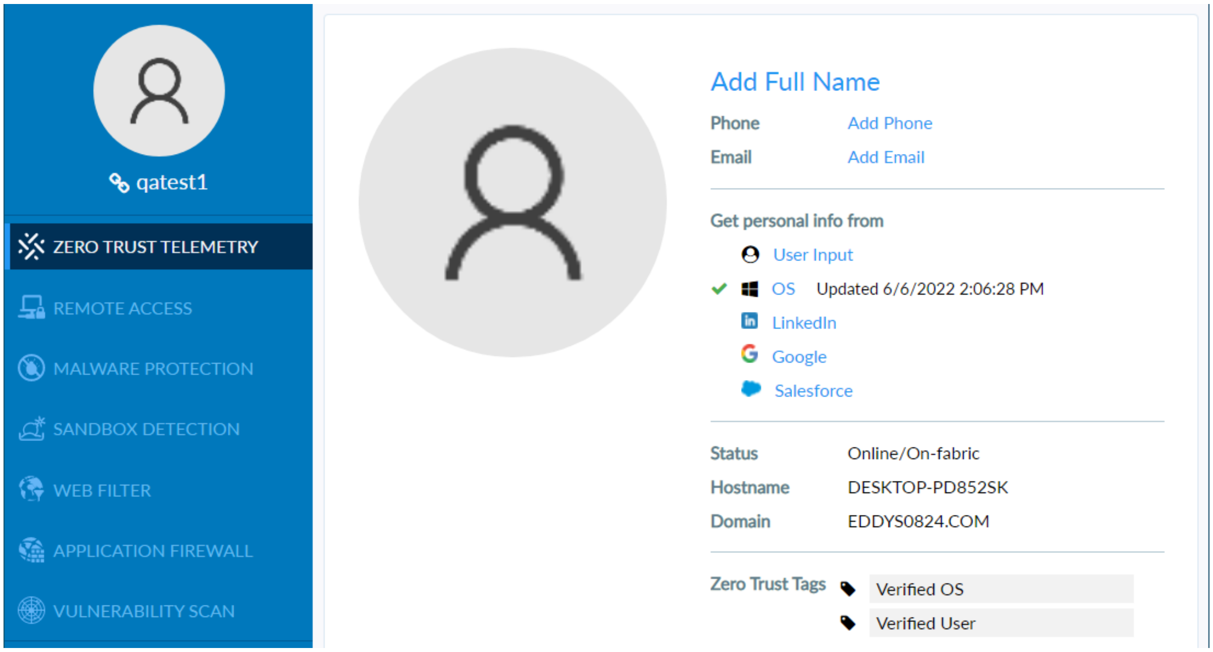
Enter Server address or Invitation code: _VjE6MTcyLjE3LjgxLjk3OjgwMTM6RG

b. In the popup, provide your LDAP user credentials, then click *Login*. FortiClient proceeds with the registration process after authentication succeeds. After FortiClient successfully registers to EMS, the username in FortiClient changes to the verified user account, and a chain icon appears beside the username to indicate that FortiClient is registered with a verified user.



Status: Connected

4. Go to the About page to confirm that the Verified User tag displays.



Phone Add Phone

Email Add Email

✓ OS Updated 6/6/2022 2:06:28 PM

Status Online/On-fabric

Hostname DESKTOP-PD852SK

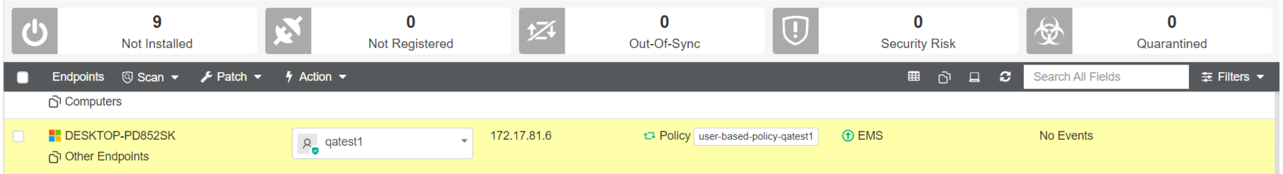
Domain EDDYS0824.COM

Zero Trust Tags Verified OS

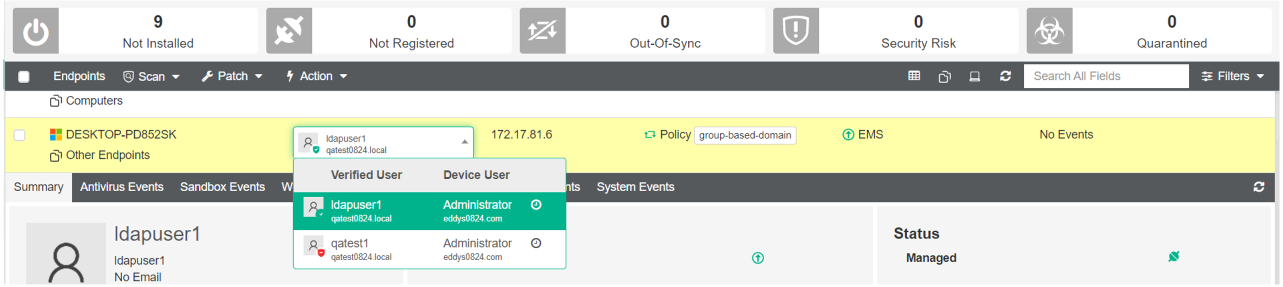
Verified User

5. In EMS, go to *Endpoint Policy & Components* > *Managed Policies*. Create a policy to apply to the selected user. In the *Users* field, select the desired user. This policy takes priority over group-based policies that the endpoint may also be eligible for.

6. Go to *Endpoints* > *All Endpoints*. Select the endpoint. Confirm that EMS applied the user-specific policy that you created to the endpoint.



7. On the same endpoint, register FortiClient with a new user. the endpoint summary displays a new active user. As the endpoint is no longer eligible for the user-specific policy, EMS applies a group-based policy to the endpoint instead. You can view all registered users for that endpoint.



Enforcing reauthentication for an onboarding user

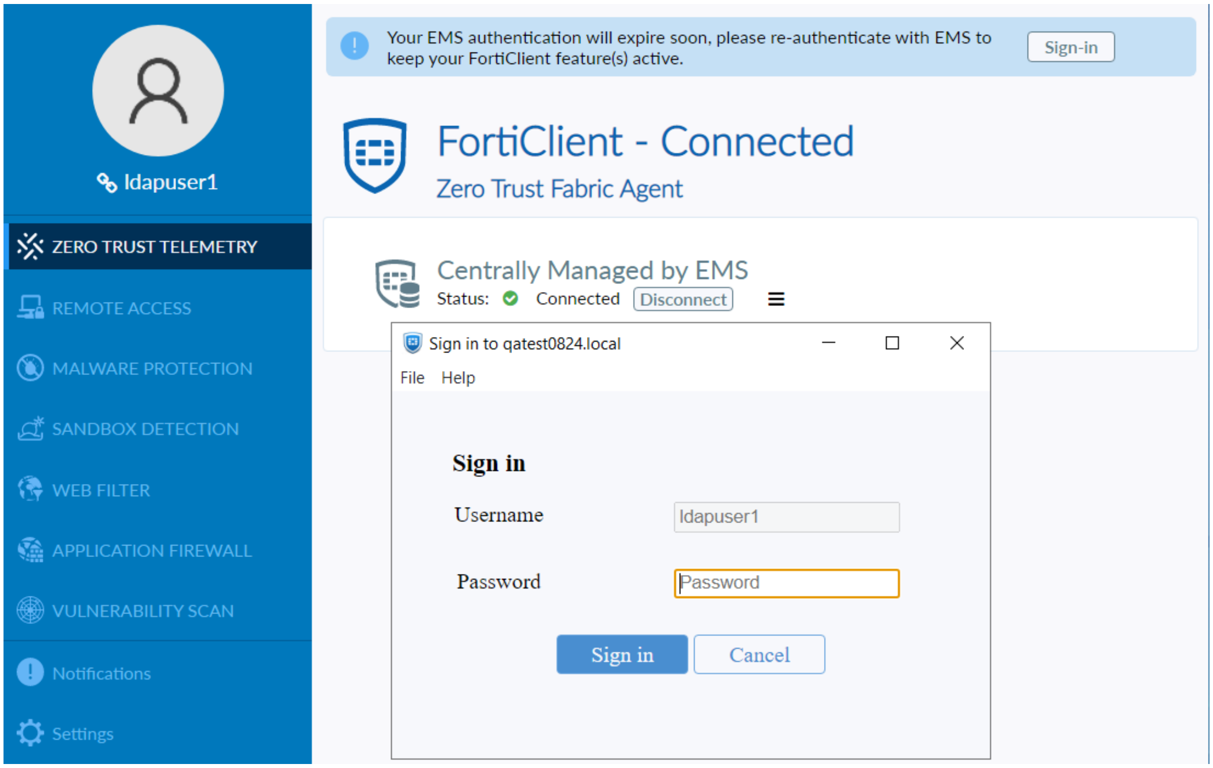
You can enforce users to reauthenticate their identities at a configured timeout interval. If the user does reauthenticate before the timeout, the endpoint unregisters from EMS. In this example, the endpoint is registered to EMS with an invitation code using LDAP authentication.

To enforce reauthentication for an onboarding user:

1. In EMS, go to *System Settings* > *EMS Settings*.
2. Enable *Enforce User Verification*.
3. Enable *User Verification Period*, and enter the desired number of days. This example sets the period to seven days. Click *Save*.

To reauthenticate your identity in FortiClient:

1. A notification appears on FortiClient five days before the reauthentication timeout. Click *Sign-in* to initiate reauthentication.
2. FortiClient displays an authentication dialog. The *Username* field is grayed out to prevent the user from reauthenticating as a different user. In the *Password* field, enter your password.



Your EMS authentication will expire soon, please re-authenticate with EMS to keep your FortiClient feature(s) active.

FortiClient - Connected

Zero Trust Fabric Agent

Centrally Managed by EMS

Status: Connected

Sign in to qatest0824.local

Sign in

Username: ldapuser1

Password: Password

3. Click *Sign in*. If you provide the correct password, FortiClient remains connected to EMS, and the warning disappears until the next reauthentication cycle. If reauthentication fails, the Telemetry status displays as *Not reachable*, the verified user logs off, and FortiClient displays a dialog to initiate the onboarding process. For a new onboarding process, the *Username* field is available.

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.

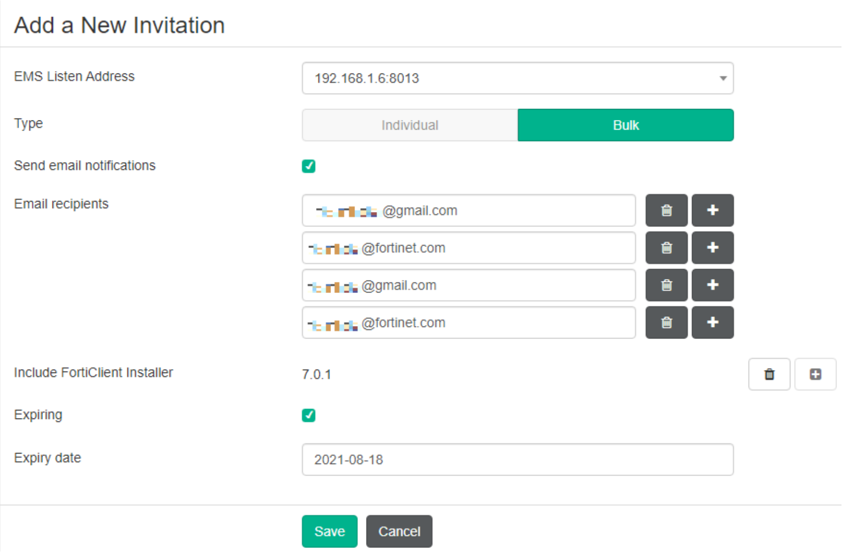
You can enforce that only endpoints that were invited using an invitation email can connect to and be managed by EMS using the *Enforce invitation-only registration for* option in *System Settings* > *EMS Settings*.

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.



Add a New Invitation

EMS Listen Address: 192.168.1.6:8013

Type: Individual / **Bulk** (selected)

Send email notifications: ☑

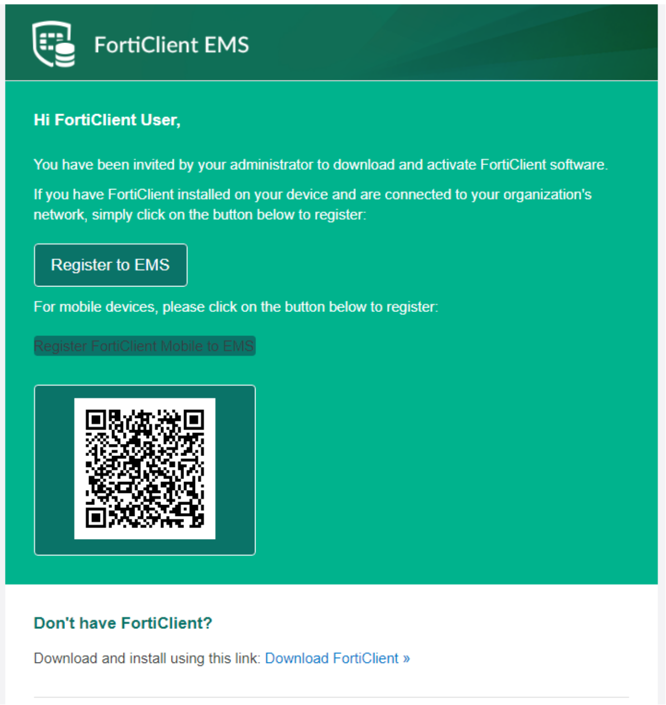
Email recipients:
[redacted]@gmail.com
[redacted]@fortinet.com
[redacted]@gmail.com
[redacted]@fortinet.com

Include FortiClient Installer: 7.0.1

Expiring: ☑

Expiry date: 2021-08-18

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.



FortiClient EMS

Hi FortiClient User,

You have been invited by your administrator to download and activate FortiClient software.

If you have FortiClient installed on your device and are connected to your organization's network, simply click on the button below to register:

For mobile devices, please click on the button below to register:

Don't have FortiClient?

Download and install using this link: Download FortiClient »

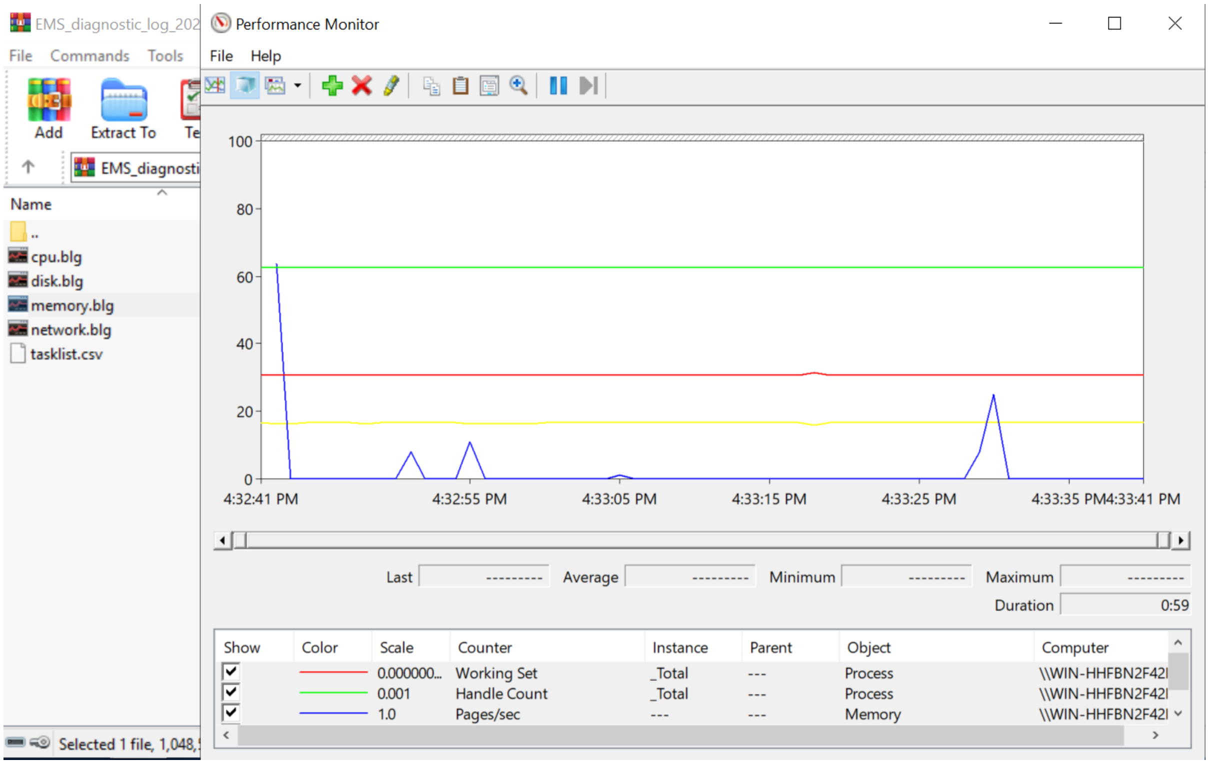
Diagnostic tool - 7.0.1

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.



Last --------- Average --------- Minimum --------- Maximum ---------

Duration 0:59

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	0.000000...	Working Set	_Total	---	Process	\\WIN-HHFBN2F42I
☑	🟩	0.001	Handle Count	_Total	---	Process	\\WIN-HHFBN2F42I
☑	🟦	1.0	Pages/sec	---	---	Memory	\\WIN-HHFBN2F42I

FortiClient Cloud Chromebook support - 7.0.1

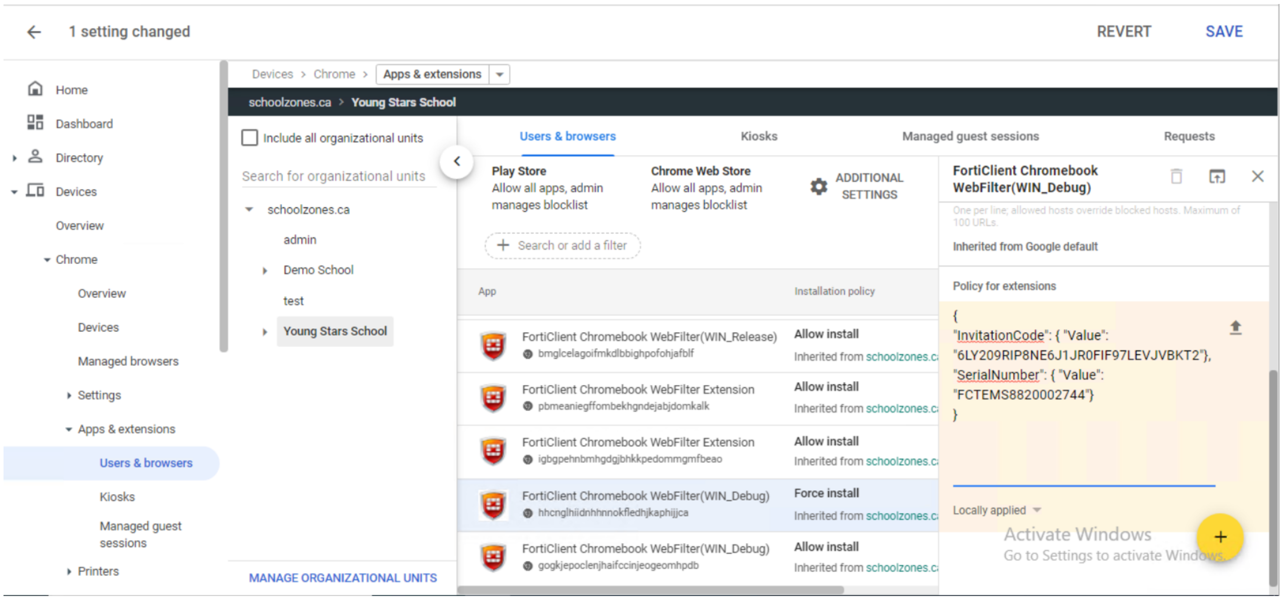
FortiClient Chromebook endpoints can connect to FortiClient Cloud. When using FortiClient Cloud, FortiClient Chromebook endpoints communicate with the FortiClient Cloud proxy and FortiClient Cloud redirects traffic to the correct FortiClient Cloud host.

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"}
}
```


1 setting changed
REVERT
SAVE
Home
Dashboard
Directory
Devices
Overview
Chrome
Overview
Devices
Managed browsers
Settings
Apps & extensions
Users & browsers
Kiosks
Managed guest sessions
Printers
Devices > Chrome > Apps & extensions
schoolzones.ca > Young Stars School
Include all organizational units
Search for organizational units
schoolzones.ca
admin
Demo School
test
Young Stars School
MANAGE ORGANIZATIONAL UNITS
Users & browsers
Kiosks
Managed guest sessions
Requests
Play Store
Allow all apps, admin manages blocklist
Chrome Web Store
Allow all apps, admin manages blocklist
ADDITIONAL SETTINGS
Search or add a filter
FortiClient Chromebook WebFilter(WIN_Debug)
One per line; allowed hosts override blocked hosts. Maximum of 100 URLs.
Inherited from Google default
Policy for extensions
Locally applied
Activate Windows
Go to Settings to activate Windows.

App	Installation policy
FortiClient Chromebook WebFilter(WIN_Release) bmglcelagoifmkdlbbighpofohjafblf	Allow install Inherited from schoolzones.ca
FortiClient Chromebook WebFilter Extension pbmeaniegffombekhgndejabjdomkalk	Allow install Inherited from schoolzones.ca
FortiClient Chromebook WebFilter Extension igbgpehnbmhgdgjbhkkpedommgmfbeao	Allow install Inherited from schoolzones.ca
FortiClient Chromebook WebFilter(WIN_Debug) hhcnglhiidnhhnnokfledhjkaphijjca	Force install Inherited from schoolzones.ca
FortiClient Chromebook WebFilter(WIN_Debug) gogkjepoclenjhaifccinjeogeomhpdb	Allow install Inherited from schoolzones.ca

```
{
"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. This feature is only available for FortiClient (Windows).
- 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.

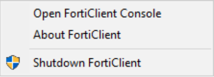
To prohibit end users from shutting down FortiClient:

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:

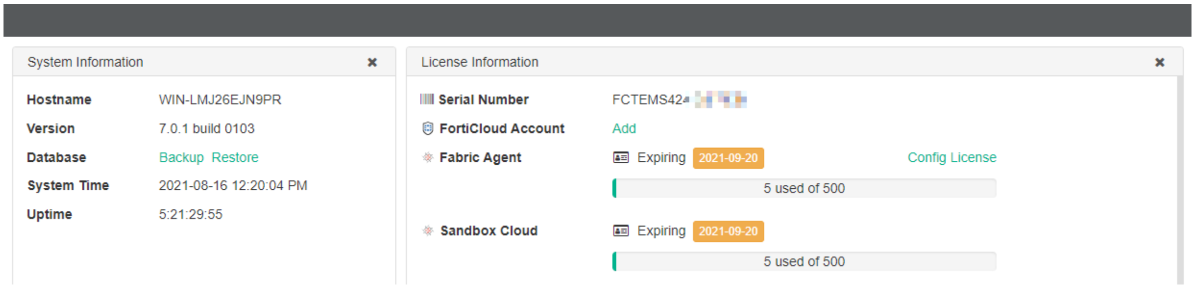
1. In EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Select the desired profile.
3. On the *System Settings* tab, enable *Allow User to Shutdown When Registered to EMS*.
4. On the *XML Configuration* tab, ensure that the `<system><ui><allow_shutdown_when_registered>` element is configured as `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.

The following shows examples of how the licensing information display on the EMS and FortiClient GUI. The *License Information* widget on the EMS Dashboard displays the license information, including the license expiry date. In this example, the license expires on September 20, 2021.



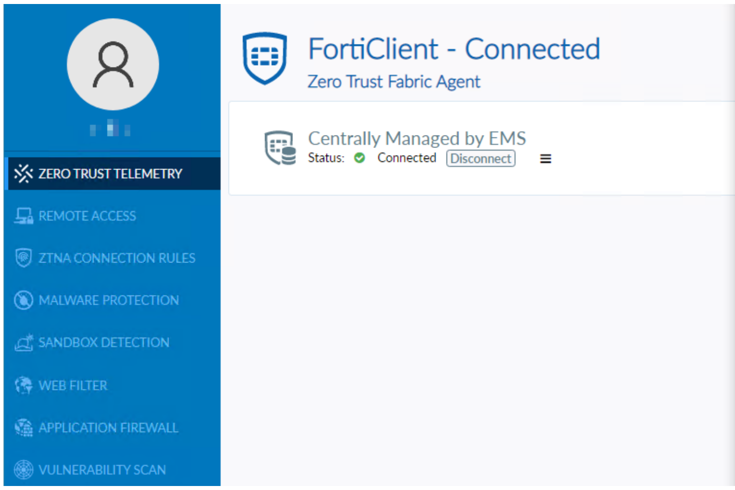
System Information

Hostname	WIN-LMJ26EJN9PR
Version	7.0.1 build 0103
Database	Backup Restore
System Time	2021-08-16 12:20:04 PM
Uptime	5:21:29:55

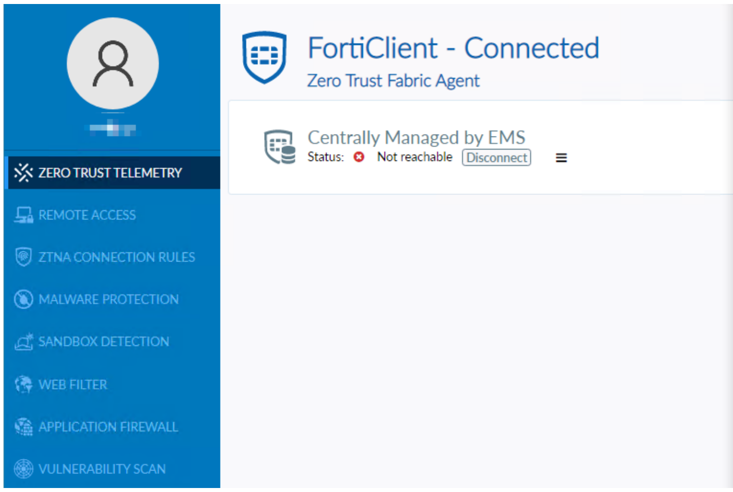
License Information

Serial Number	FCTEMS42[redacted]	
FortiCloud Account	Add	
Fabric Agent	Expiring 2021-09-20 5 used of 500	Config License
Sandbox Cloud	Expiring 2021-09-20 5 used of 500	

The following screenshot shows the FortiClient GUI on an endpoint that is connected to EMS. The FortiClient GUI displays all licensed features.



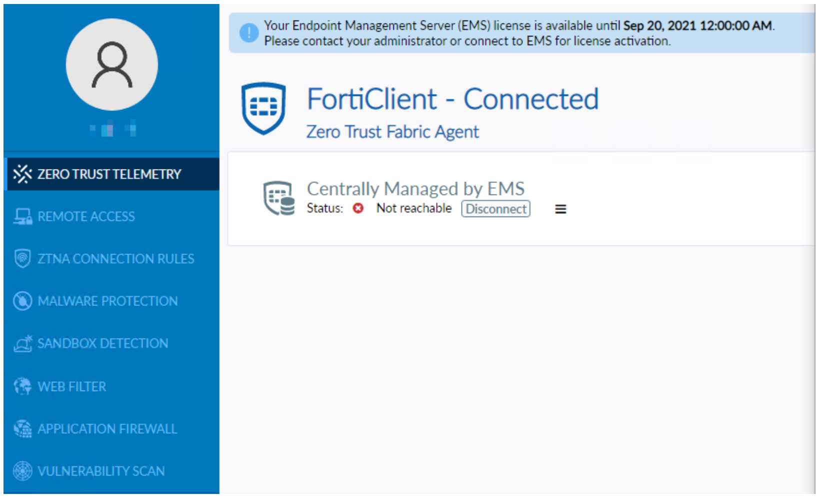
When the endpoint cannot reach EMS, all licensed features still display on the FortiClient GUI.



FortiClient - Connected
Zero Trust Fabric Agent

Centrally Managed by EMS
Status: Not reachable

Even when the endpoint cannot reach EMS, the FortiClient GUI displays a license expiry warning when it is close to the expiry date. The licensed features still display in the FortiClient GUI until the license expiry date.


Your Endpoint Management Server (EMS) license is available until **Sep 20, 2021 12:00:00 AM**.
Please contact your administrator or connect to EMS for license activation.

FortiClient - Connected
Zero Trust Fabric Agent

Centrally Managed by EMS
Status: Not reachable

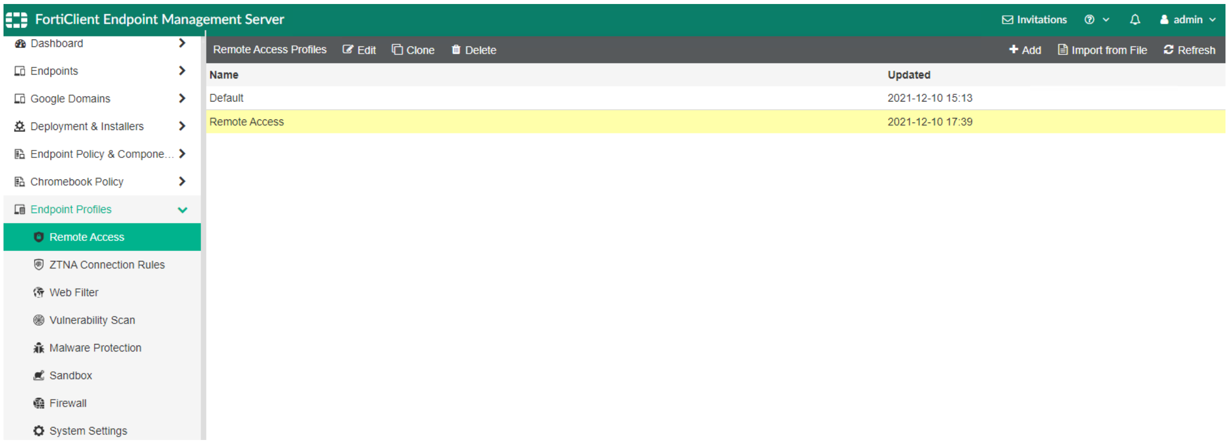
Separate endpoint profiles - 7.0.3

FortiClient EMS 7.0.3 introduces separate endpoint profiles to allow for a simpler and modular approach to endpoint profile management. You now configure separate Remote Access profiles, ZTNA Connection Rules profiles, Web Filter profiles, and so on. You then configure different profile combinations as part of an endpoint policy to deploy to endpoints.

For example, consider that you have two endpoint groups: Groups A and B. You want Group A and Group B to share identical FortiClient settings, except that Group A's antivirus scheduled scan is on a weekly basis, while Group B's is on a monthly basis. In 7.0.2 and earlier versions, you would need to create two endpoint profiles with the desired scan schedules on the *Malware Protection* tabs. All other settings on the profile's other tabs are identical between the two profiles. You would configure two endpoint policies that are configured with the two profiles. At a later point in time, if you wanted to configure a new VPN tunnel for both groups, you would need to configure the VPN tunnel on both endpoint profiles.

To accommodate this configuration in 7.0.3 and later versions, you would configure two Malware Protection profiles with the desired scan schedules to apply to the two groups, as well as two endpoint policies that are configured with the two profiles. Since all other FortiClient settings are identical across the two groups, you would configure the same Remote Access profile, Web Filter profile, Vulnerability Scan profile, and so on, for both policies. At a later point in time, if you wanted to configure a VPN tunnel for both groups, you would only need to do so in the shared Remote Access profile, rather than redundantly modifying multiple profiles.

You can view the new separate profiles in *Endpoint Profiles*. You can edit, clone, and delete profiles without affecting other profile types.

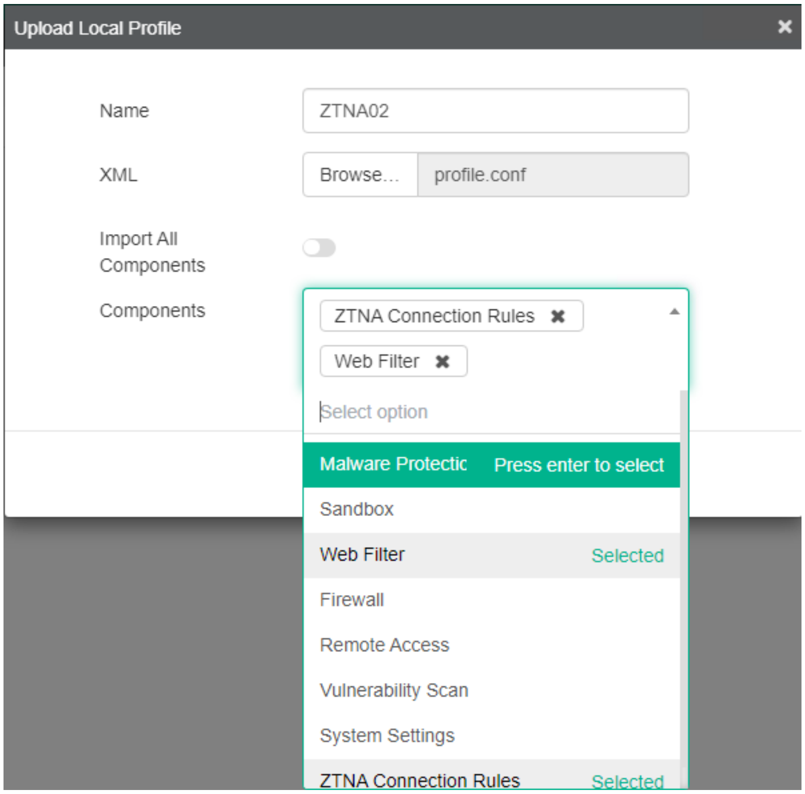


Name	Updated
Default	2021-12-10 15:13
Remote Access	2021-12-10 17:39

To import a profile:

1. Go to *Endpoint Profiles*.
2. Select the desired profile type.
3. Click *Import from File*.
4. In the *Name* field, enter the desired name.
5. In the *XML* field, browse to and upload the desired profile.

6. Do one of the following:
   a. To import all profile components, enable *Import All Components*.
   b. To import selected components, select the desired components from the *Components* dropdown list.



Upload Local Profile

Name: ZTNA02

XML: Browse... profile.conf

Import All Components

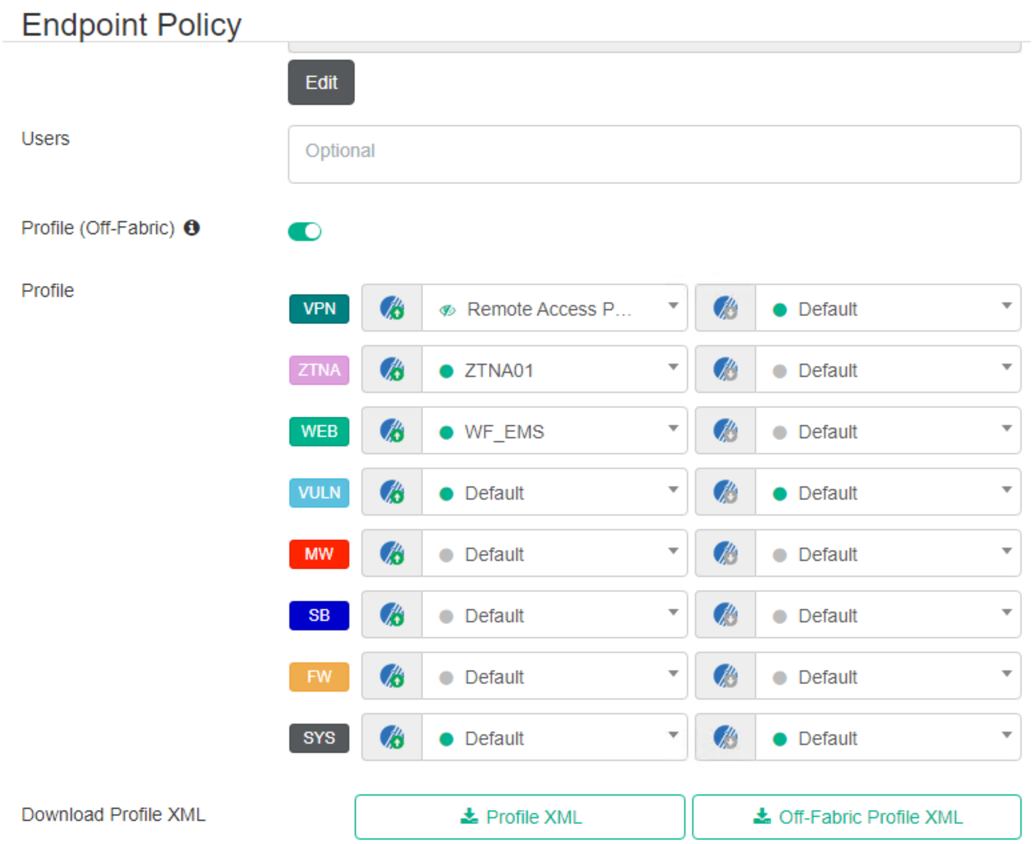
Components: ZTNA Connection Rules ✖ Web Filter ✖

7. Click *Upload*.

To assign endpoint profiles to a policy:

1. Go to *Endpoint Policy & Components* > *Manage Policies*.
2. Create a new policy or edit an existing policy.
3. If desired, enable *Profile (Off-Fabric)*.
4. Configure the desired profiles for the desired features.

5. You can use the *Profile XML* and *Off-Fabric Profile XML* buttons to download on- and off-net profiles in XML format.



Endpoint Policy

Edit

Users: Optional

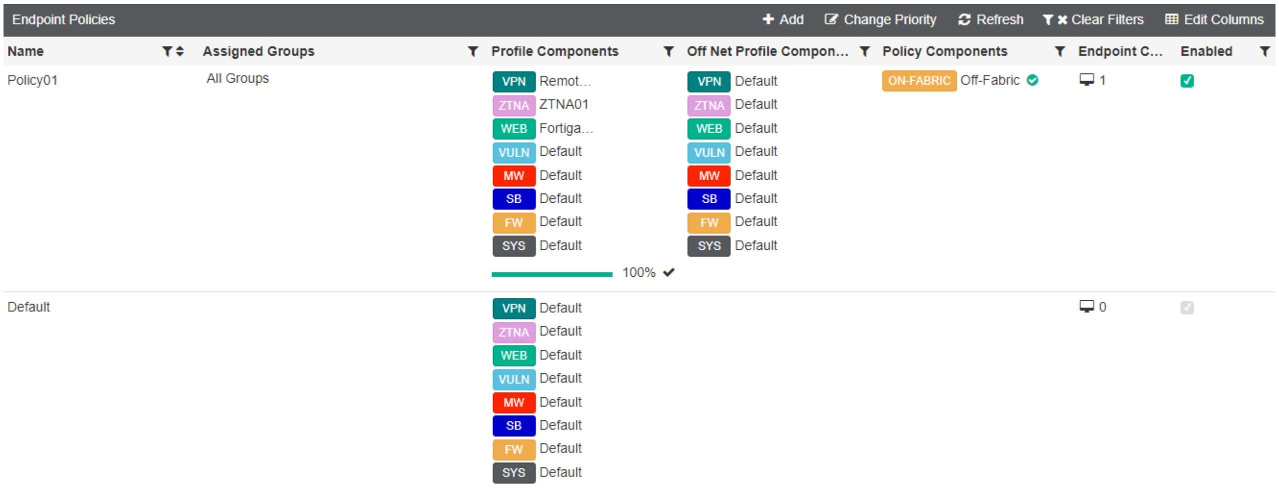
Profile (Off-Fabric) ℹ

Profile

VPN	Remote Access P...	● Default
ZTNA	● ZTNA01	● Default
WEB	● WF_EMS	● Default
VULN	● Default	● Default
MW	● Default	● Default
SB	● Default	● Default
FW	● Default	● Default
SYS	● Default	● Default

Download Profile XML: Profile XML | Off-Fabric Profile XML

6. Click *Save*. You can view each policy's assigned profiles for each feature under *Profile Components* and *Off Net Profile Components*.



Endpoint Policies — + Add | Change Priority | Refresh | Clear Filters | Edit Columns

Name	Assigned Groups	Profile Components	Off Net Profile Compon...	Policy Components	Endpoint C...	Enabled
Policy01	All Groups	VPN Remot... ZTNA ZTNA01 WEB Fortiga... VULN Default MW Default SB Default FW Default SYS Default 100% ✓	VPN Default ZTNA Default WEB Default VULN Default MW Default SB Default FW Default SYS Default	ON-FABRIC Off-Fabric ✓	1	☑
Default		VPN Default ZTNA Default WEB Default VULN Default MW Default SB Default FW Default SYS Default			0	☑

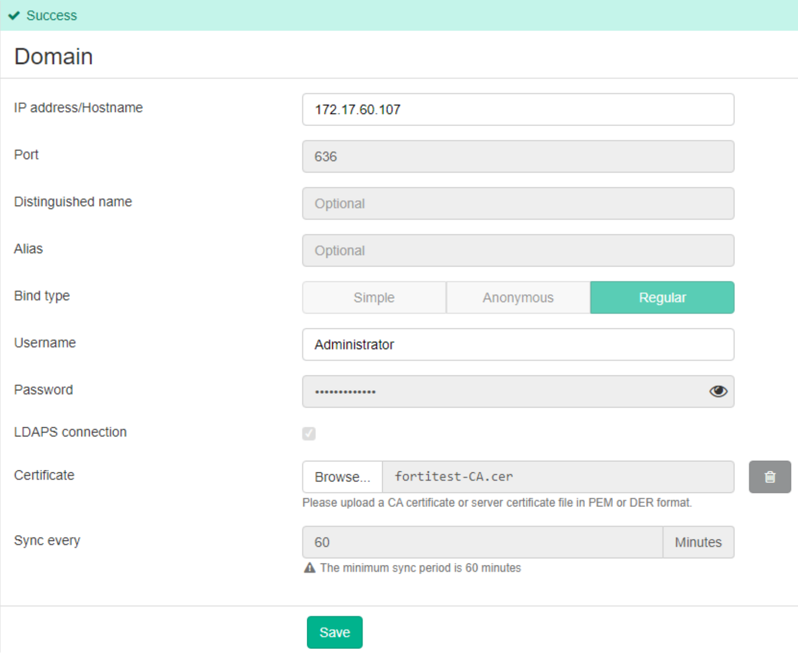
For a Chromebook policy, you can only assign Web Filter and System Settings profiles.

Active Directory LDAPS connection certificate provisioning - 7.0.3

You can upload Certificate Authority (CA) and server certificates to LDAPS connections in EMS. With this feature, you can upload CA and server certificates to the Windows Server virtual machine hosting EMS in FortiClient Cloud.

To import a domain with LDAPS to EMS:

1. Go to *Endpoints* > *Manage Domains* > *Add a domain*.
2. By default, LDAPS is enabled and the defined port is 636. In the *Certificate* field, browse to and upload a CA certificate in PEM or DER format.
3. Fill out other fields as desired.
4. Click *Test*.



✓ Success

Domain

IP address/Hostname: 172.17.60.107

Port: 636

Distinguished name: Optional

Alias: Optional

Bind type: Simple | Anonymous | [✓ Regular]

Username: Administrator

Password: •••••••••••••

LDAPS connection: ☑

Certificate: Browse... fortitest-CA.cer

Please upload a CA certificate or server certificate file in PEM or DER format.

Sync every: 60 Minutes

⚠ The minimum sync period is 60 minutes

Save

5. After the test succeeds, click *Save*.
6. Go to *Endpoints* > *Managed Domains* to confirm that EMS imported the domain, LDAPS is enabled, and all other details synced correctly.

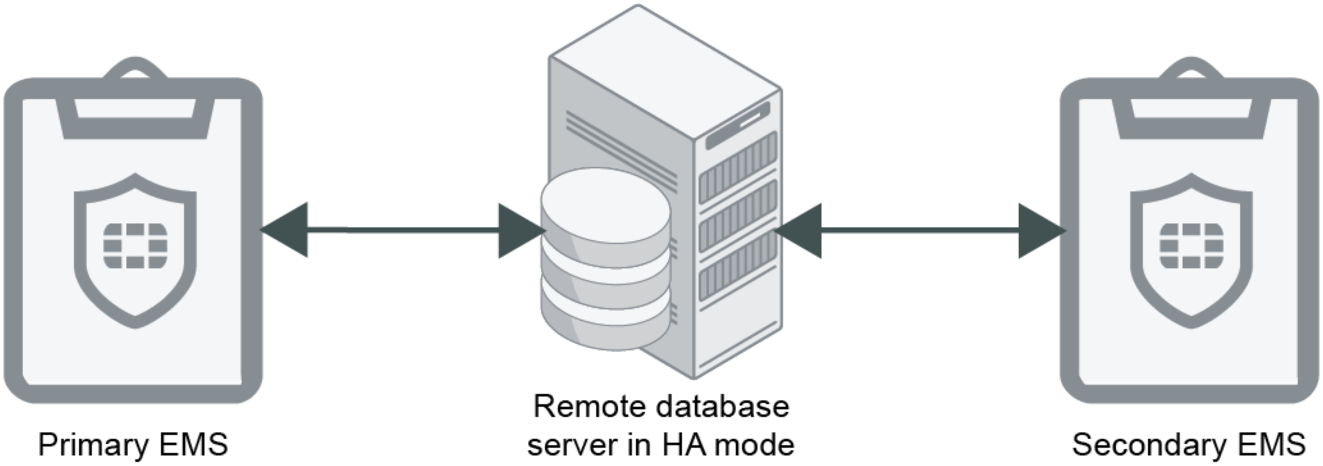
Redundancy using SQL Server - 7.0.3

The following describes redundancy or high availability (HA) options for EMS where endpoint information is synced between multiple EMS nodes running in active-passive HA mode. Consider a scenario where two EMS nodes, EMS A and EMS B, run in HA mode with EMS A as the primary node and EMS B as the secondary node. Both EMS nodes are connected to the same remote database server. Endpoints are connected to EMS A. If EMS A fails, EMS B is promoted to become the primary node, and endpoints automatically register to EMS B.

EMS HA mode supports configuring multiple EMS servers with one SQL Server. SQL Server should be running on a remote, separate Windows server. If you want to add database HA support, you can configure a SQL Server failover cluster. For SQL Server failover cluster setup, see Create a New Always On Failover Cluster Instance (Setup).

This guide focuses on configuring HA for EMS services. It assumes that you have completed SQL Server failover cluster setup as Create a New Always On Failover Cluster Instance (Setup) describes.

The example setup has two EMS nodes and one database server.



Note the following:

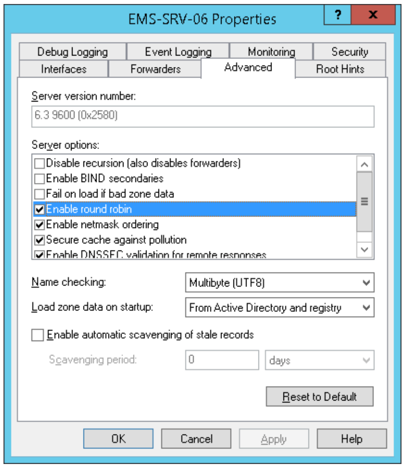
- For file synchronization between HA nodes, you must enable FILESTREAMS on the SQL Server Database Engine instance. See Enable and configure FILESTREAM.
- EMS running in HA mode must always configure a fully qualified domain name (FQDN), and FortiClient endpoints must point to a DNS server that has enabled DNS round robin or supports DNS failover, so that endpoints can always connect to the correct primary EMS server. Endpoint users must ensure that endpoints do not cache the DNS result for more than 30 seconds so that FortiClient can resolve the FQDN to the new primary EMS server with a new IP address in case EMS failover happens quickly.
- If logged in to an EMS server as a domain user, add the domain user to the local logon as a service. Otherwise, EMS services may not start up properly.

To configure DNS round robin on the database server:

By configuring DNS round robin, you can configure load balancing by pointing the same hostname to multiple servers with different IP addresses in DNS.

1. Open DNS Manager.
2. Right-click the server name, then select *Properties*.
3. On the *Advanced* tab, under *Server options*, click *Enable round robin*.

4. Click *Apply*.



EMS-SRV-06 Properties

Server version number: 6.3 9600 (0x2580)

Server options:
- ☐ Disable recursion (also disables forwarders)
- ☐ Enable BIND secondaries
- ☐ Fail on load if bad zone data
- ☑ Enable round robin
- ☑ Enable netmask ordering
- ☑ Secure cache against pollution
- ☑ Enable DNSSEC validation for remote responses

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

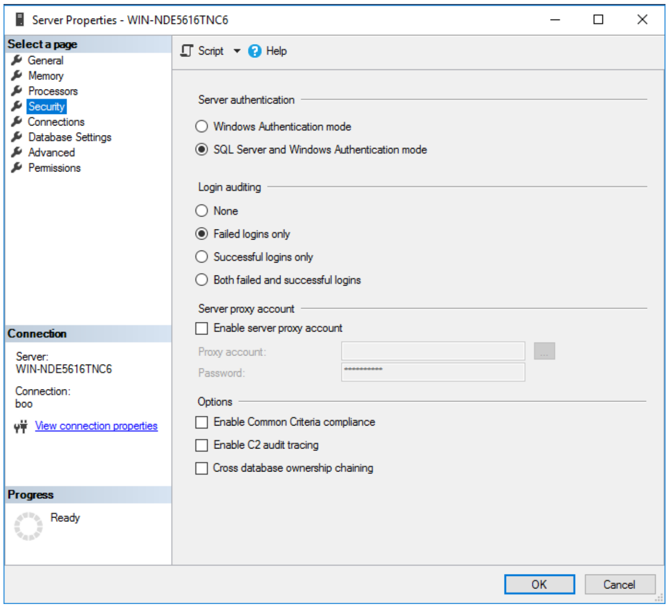
Scavenging period: 0 days

To configure SQL Server options on the remote database server:

The example uses SQL Server security login to connect to the remote database server to create the EMS database during EMS installation. You must enable certain SQL Server options before installing EMS.

If the SQL Server has multiple databases configured, ensure that each database is listening on a different port.

1. Open Microsoft SQL Server Management Studio as an administrator.
2. CoIn the *Object Explorer* pane, select *Connect* > *Database Engine*.
3. In the *Connect to Server* dialog, enter your credentials and connect to the database server.
4. In the *Object Explorer* pane, right-click the server, then select *Properties*.
5. In the *Server Properties* dialog, go to *Security*.
6. Under *Server authentication*, select *SQL Server and Windows Authentication mode*.



Server Properties - WIN-NDE5616TNC6

Server authentication
- ○ Windows Authentication mode
- ● SQL Server and Windows Authentication mode

Login auditing
- ○ None
- ● Failed logins only
- ○ Successful logins only
- ○ Both failed and successful logins

Server proxy account
- ☐ Enable server proxy account

Proxy account:
Password: **********

Options
- ☐ Enable Common Criteria compliance
- ☐ Enable C2 audit tracing
- ☐ Cross database ownership chaining

Connection

Server:
WIN-NDE5616TNC6

Connection:
boo

7. Create a SQL login user:
   a. Right-click *Security*, then select *New* > *Login*.
   b. In the *Login name* field, enter the desired username. In this example, the username is "cbreaux".

c. Select *SQL Server authentication*.

d. In the *Password* and *Confirm password* fields, enter the desired password. In this example, the password is "MyPassword".

e. Disable *Enforce password policy*.

f. Go to *Server Roles*.

g. Select *sysadmin*, then click *OK*.

8. On the EMS node, open SQL Server Management Studio and attempt to connect to the remote database with the SQL user that you created to ensure that the node can connect to the database server using the credentials.

To install EMS:

Joining EMS nodes to a domain is unnecessary, as you will use a SQL user account to connect to the database instance on the remote SQL Server database server.

1. Install EMS on the primary node by running the following command:

```
FortiClientEndpointManagementServer_7.0.3.0173_x64.exe SQLServer=WIN-NDE5616TNC6
     SQLUser=cbreaux SQLUserPassword=MyPassword SQLPort=1445 InstallSQL=0 ScriptDB=1
     BackupDir=\\EMSServer38\backup\ DBInitialSize=31MB DBInitialLogSize=4MB
     DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

In this command, the remote database server name is entered in the `SQLServer` field. This field also supports entering FQDNs.

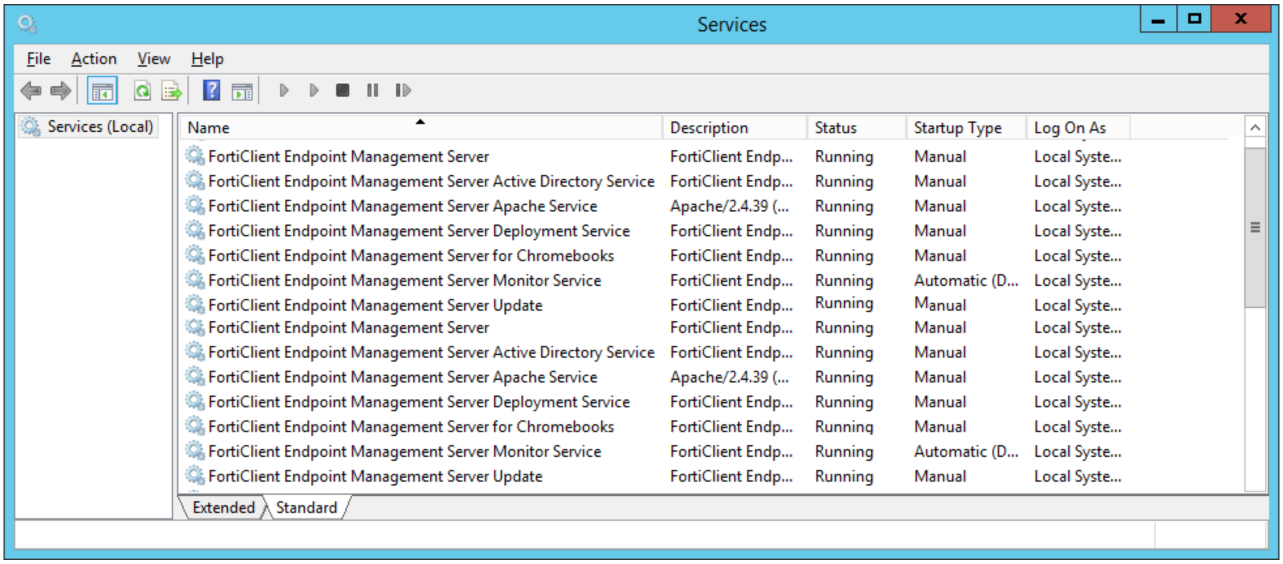
`ScriptDB=1` indicates that this is the primary node.

`BackUpDir=UNC_PATH\\backup` indicates the shared backup directory on the local EMS server or any other accessible servers. The following lists requirements for the backup directory:

- The backup directory must not be on the remote database server.
- The backup directory must not be local to the SQL server, as SQL Server applies access control lists to the encryption key file and prevents Apache running on the other server to delete the key file.
- The SQL server should require at least write permissions to the backup directory. The EMS servers should have read/write permissions for the backup directory.

Ensure that you specify `SQLPort` to match the database that you want to use for your EMS server.

After installation completes, all EMS services should be running. In HA, the FortiClient Endpoint Management Server Monitory Service can be considered as the heartbeat.



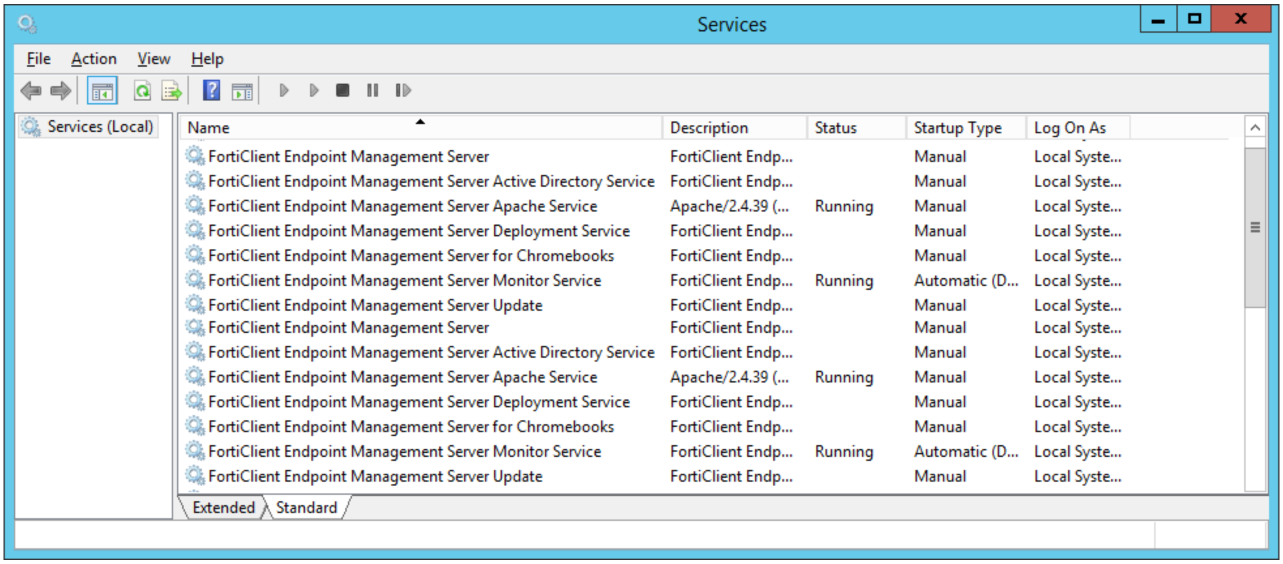
Name	Description	Status	Startup Type	Log On As
FortiClient Endpoint Management Server	FortiClient Endp...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Active Directory Service	FortiClient Endp...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Apache Service	Apache/2.4.39 (...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Deployment Service	FortiClient Endp...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server for Chromebooks	FortiClient Endp...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Monitor Service	FortiClient Endp...	Running	Automatic (D...	Local Syste...
FortiClient Endpoint Management Server Update	FortiClient Endp...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server	FortiClient Endp...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Active Directory Service	FortiClient Endp...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Apache Service	Apache/2.4.39 (...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Deployment Service	FortiClient Endp...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server for Chromebooks	FortiClient Endp...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Monitor Service	FortiClient Endp...	Running	Automatic (D...	Local Syste...
FortiClient Endpoint Management Server Update	FortiClient Endp...	Running	Manual	Local Syste...

2. Install EMS on the secondary node by running the following command:

```
FortiClientEndpointManagementServer_7.0.3.0173_x64.exe SQLServer=WIN-NDE5616TNC6
     SQLUser=cbreaux SQLUserPassword=MyPassword SQLPort=1445 InstallSQL=0 ScriptDB=0
     BackupDir=\\EMSServer38\backup\ DBInitialSize=31MB DBInitialLogSize=4MB
     DBGrowth=11MB DBLogGrowth=11% DBLoginTimeout=31 DBQueryTimeout=61
```

   `ScriptDB=0` indicates that this is the secondary node.

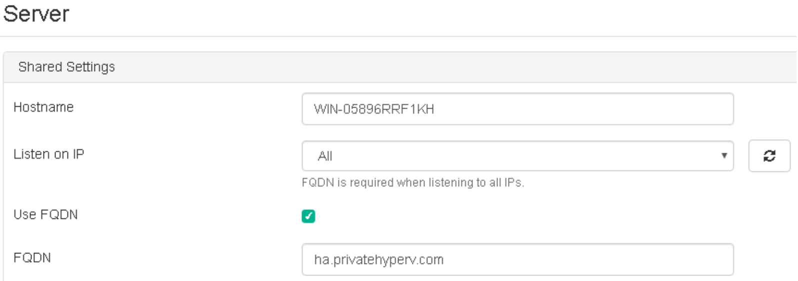
   After installation completes, only the FortiClient Endpoint Management Server Monitor Service and FortiClient Endpoint Management Server Apache Service should be running on the secondary node.



Name	Description	Status	Startup Type	Log On As
FortiClient Endpoint Management Server	FortiClient Endp...		Manual	Local Syste...
FortiClient Endpoint Management Server Active Directory Service	FortiClient Endp...		Manual	Local Syste...
FortiClient Endpoint Management Server Apache Service	Apache/2.4.39 (...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Deployment Service	FortiClient Endp...		Manual	Local Syste...
FortiClient Endpoint Management Server for Chromebooks	FortiClient Endp...		Manual	Local Syste...
FortiClient Endpoint Management Server Monitor Service	FortiClient Endp...	Running	Automatic (D...	Local Syste...
FortiClient Endpoint Management Server Update	FortiClient Endp...		Manual	Local Syste...
FortiClient Endpoint Management Server	FortiClient Endp...		Manual	Local Syste...
FortiClient Endpoint Management Server Active Directory Service	FortiClient Endp...		Manual	Local Syste...
FortiClient Endpoint Management Server Apache Service	Apache/2.4.39 (...	Running	Manual	Local Syste...
FortiClient Endpoint Management Server Deployment Service	FortiClient Endp...		Manual	Local Syste...
FortiClient Endpoint Management Server for Chromebooks	FortiClient Endp...		Manual	Local Syste...
FortiClient Endpoint Management Server Monitor Service	FortiClient Endp...	Running	Automatic (D...	Local Syste...
FortiClient Endpoint Management Server Update	FortiClient Endp...		Manual	Local Syste...

To configure EMS:

1. On the primary node, log in to EMS.
2. Go to *System Settings > Server*.
3. Enable *Use FQDN*.
4. In the *FQDN* field, enter the desired FQDN.



Server

Shared Settings

Hostname: WIN-05896RRF1KH

Listen on IP: All

FQDN is required when listening to all IPs.

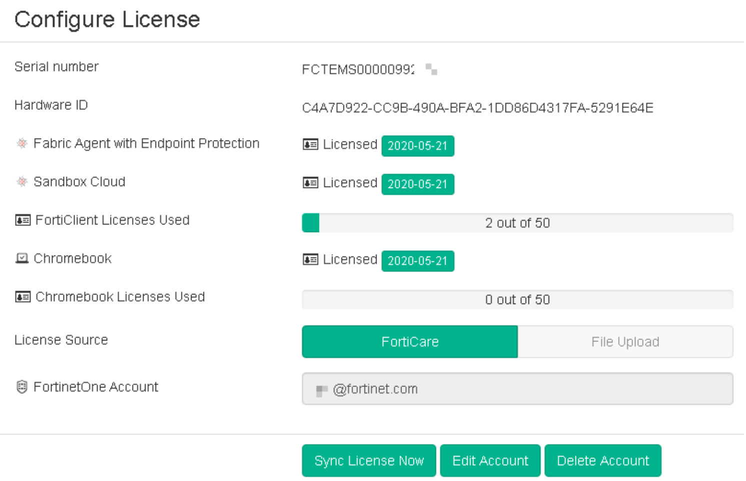
Use FQDN: ☑

FQDN: ha.privatehyperv.com

5. Go to *System Settings > EMS Settings*. Configure the *High Availability Keep Alive Internal* field with a value between 5 and 30 seconds.
6. Go to *Dashboard > Status*. Confirm that the System Information widget displays that EMS is running in HA mode. If running in HA mode, the widget also lists the HA primary and secondary nodes and their statuses.
7. Update the EMS licensing:
   a. Go to *License Information widget > Configure License*.
   b. For *License Source*, select *FortiCare*.
   c. In the *FortiCloud Account* field, enter your FortiCloud account ID or email address.

d. In the *Password* field, enter your FortiCloud account password.

e. Click *Login & Update License*. Once your account information is authenticated, EMS updates the *Configure License* page with the serial number and license information that it retrieved from FortiCloud.

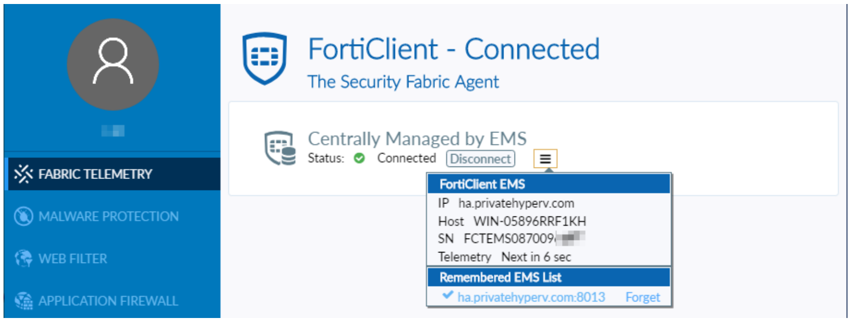


Configure License

Serial number	FCTEMS0000099[redacted]
Hardware ID	C4A7D922-CC9B-490A-BFA2-1DD86D4317FA-5291E64E
Fabric Agent with Endpoint Protection	Licensed 2020-05-21
Sandbox Cloud	Licensed 2020-05-21
FortiClient Licenses Used	2 out of 50
Chromebook	Licensed 2020-05-21
Chromebook Licenses Used	0 out of 50
License Source	FortiCare / File Upload
FortinetOne Account	[redacted]@fortinet.com

To validate the HA configuration:

1. Go to *Manage Installers > Deployment Packages*. Create a deployment package to deploy FortiClient to endpoints. See Adding a FortiClient deployment package.
2. On an endpoint, download the deployment package from the download link.
3. Install FortiClient on the endpoint.
4. Ensure that FortiClient can register to the EMS server successfully using the FQDN.
5. Simulate HA by stopping FortiClient Endpoint Management Server Monitor Service on the primary node. Ensure that the secondary node is now the EMS primary server.
6. Ensure that FortiClient can still register to the EMS server successfully using the FQDN.



[redacted]

FortiClient - Connected

The Security Fabric Agent

Centrally Managed by EMS

Status: Connected

FortiClient EMS

IP ha.privatehyperv.com

Host WIN-05896RRF1KH

SN FCTEMS087009[redacted]

Telemetry Next in 6 sec

Remembered EMS List

✓ ha.privatehyperv.com:8013

To upgrade EMS in HA mode:

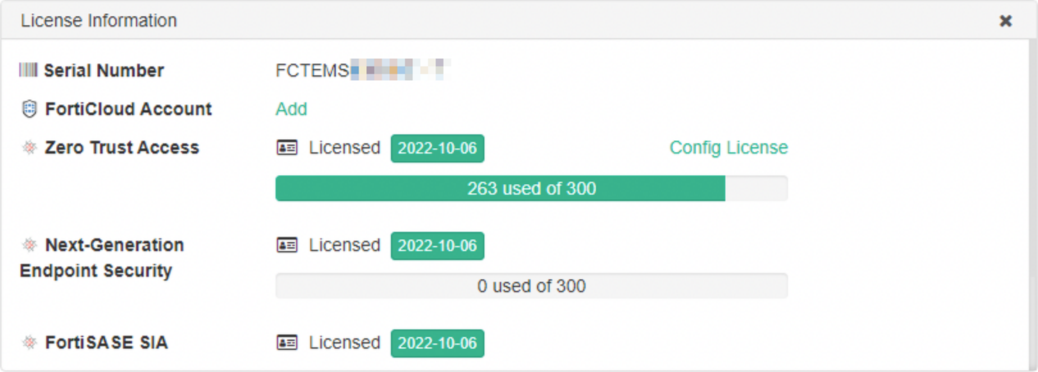
1. Stop all services in all secondary EMS servers to avoid failover while the primary EMS server is upgrading.
2. Upgrade the primary server while it is running.
3. After successfully upgrading the primary server, upgrade the secondary EMS servers. If you have multiple secondary EMS servers, you can upgrade them one by one, or simultaneously.

User-based licensing - 7.0.6

FortiClient Cloud 22.1, which runs EMS 7.0.6, introduces a user-centric registration and license computation process as an alternative to the previous device-centric process. For user- based licenses, you can manually remove or exclude users from management to free up license seats. Each user-based license allows the user to register three devices. If a user registers a fourth device, they consume two licenses.

Only FortiClient Cloud supports this feature. On-premise EMS does not support this feature.

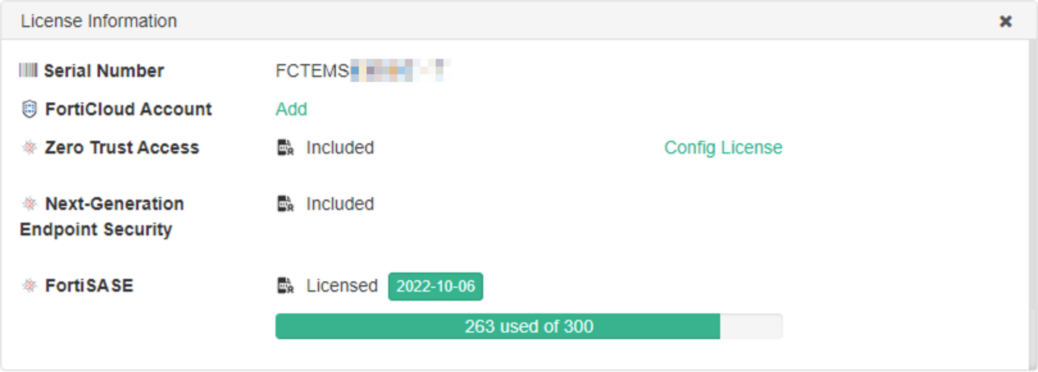
The following shows the 21.4 *License Information* widget, where you can see information for the Zero Trust Access, Next-Generation Endpoint Security, and FortiSASE licenses:



License Information

Serial Number	FCTEMS[redacted]	
FortiCloud Account	Add	
Zero Trust Access	Licensed 2022-10-06 263 used of 300	Config License
Next-Generation Endpoint Security	Licensed 2022-10-06 0 used of 300	
FortiSASE SIA	Licensed 2022-10-06	

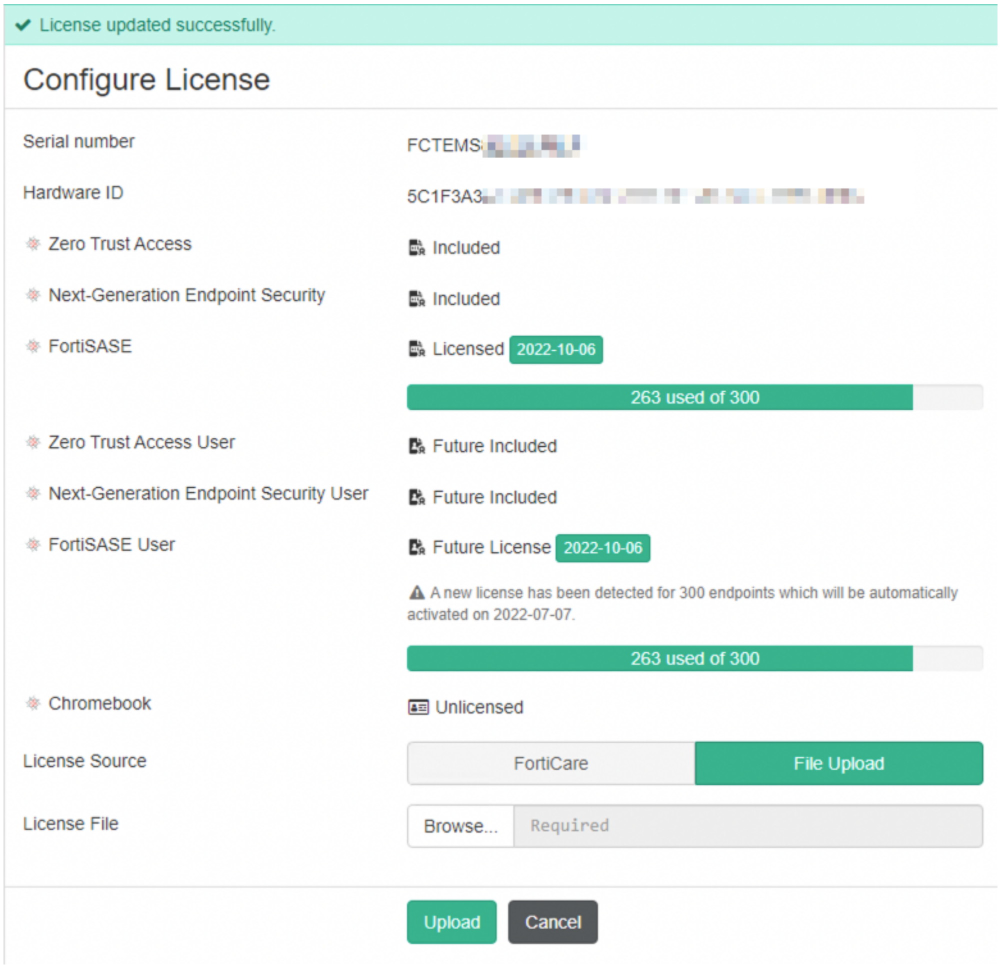
After upgrade to 22.1, the *License Information* widget continues to display information for the same licenses:



License Information

Serial Number	FCTEMS[redacted]	
FortiCloud Account	Add	
Zero Trust Access	Included	Config License
Next-Generation Endpoint Security	Included	
FortiSASE	Licensed 2022-10-06 263 used of 300	

When you load a user-based license to FortiClient Cloud 22.1, the *Configure License* page displays both the device- and user-based licenses. For example, in the following screenshot, the *Zero Trust Access* field indicates the device-based license, while the *Zero Trust Access User* field indicates the equivalent user-based license. You cannot concurrently use both license types on one FortiClient Cloud instance. Therefore, FortiClient Cloud uses the device-based license until it expires, but displays the user-based license as *Future Included* to indicate that it will become active when the device-based license expires:

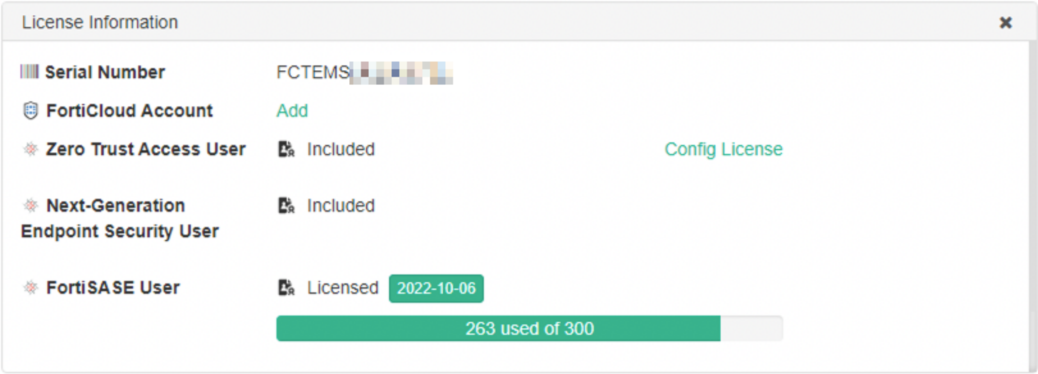


✔ License updated successfully.

Configure License

Serial number	FCTEMS[redacted]
Hardware ID	5C1F3A3[redacted]
Zero Trust Access	Included
Next-Generation Endpoint Security	Included
FortiSASE	Licensed 2022-10-06 263 used of 300
Zero Trust Access User	Future Included
Next-Generation Endpoint Security User	Future Included
FortiSASE User	Future License 2022-10-06 ⚠ A new license has been detected for 300 endpoints which will be automatically activated on 2022-07-07. 263 used of 300
Chromebook	Unlicensed
License Source	FortiCare [● File Upload]
License File	Browse... Required

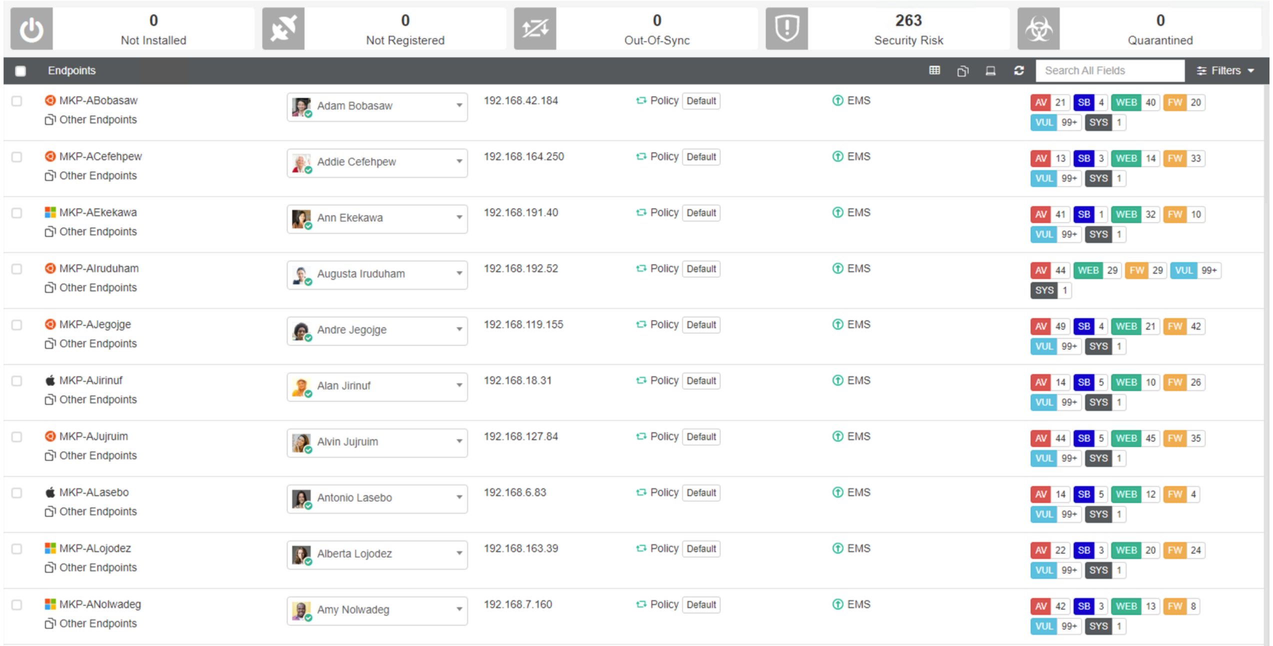
After the device-based license expires, FortiClient Cloud uses the user-based license:



License Information ×

Serial Number	FCTEMS[redacted]	
FortiCloud Account	Add	
Zero Trust Access User	Included	Config License
Next-Generation Endpoint Security User	Included	
FortiSASE User	Licensed 2022-10-06 263 used of 300	

The following shows the endpoint list using the user-based licensing:



0 Not Installed	0 Not Registered	0 Out-Of-Sync	263 Security Risk	0 Quarantined

Endpoints					Search All Fields · Filters
MKP-ABobasaw Other Endpoints	Adam Bobasaw	192.168.42.184	Policy Default	EMS	AV 21 SB 4 WEB 40 FW 20 VUL 99+ SYS 1
MKP-ACefehpew Other Endpoints	Addie Cefehpew	192.168.164.250	Policy Default	EMS	AV 13 SB 3 WEB 14 FW 33 VUL 99+ SYS 1
MKP-AEkekawa Other Endpoints	Ann Ekekawa	192.168.191.40	Policy Default	EMS	AV 41 SB 1 WEB 32 FW 10 VUL 99+ SYS 1
MKP-AIruduham Other Endpoints	Augusta Iruduham	192.168.192.52	Policy Default	EMS	AV 44 WEB 29 FW 29 VUL 99+ SYS 1
MKP-AJegojge Other Endpoints	Andre Jegojge	192.168.119.155	Policy Default	EMS	AV 49 SB 4 WEB 21 FW 42 VUL 99+ SYS 1
MKP-AJirinuf Other Endpoints	Alan Jirinuf	192.168.18.31	Policy Default	EMS	AV 14 SB 5 WEB 10 FW 26 VUL 99+ SYS 1
MKP-AJujruim Other Endpoints	Alvin Jujruim	192.168.127.84	Policy Default	EMS	AV 44 SB 5 WEB 45 FW 35 VUL 99+ SYS 1
MKP-ALasebo Other Endpoints	Antonio Lasebo	192.168.6.83	Policy Default	EMS	AV 14 SB 5 WEB 12 FW 4 VUL 99+ SYS 1
MKP-ALojodez Other Endpoints	Alberta Lojodez	192.168.163.39	Policy Default	EMS	AV 22 SB 3 WEB 20 FW 24 VUL 99+ SYS 1
MKP-ANolwadeg Other Endpoints	Amy Nolwadeg	192.168.7.160	Policy Default	EMS	AV 42 SB 3 WEB 13 FW 8 VUL 99+ SYS 1

FortiGuard Forensics service - 7.0.6

FortiClient Cloud 22.1, which runs EMS 7.0.6, introduces the FortiGuard Endpoint Forensic Analysis service, which provides remote endpoint analysis to help you respond to and recover from cyber incidents. An EMS administrator can request detailed analysis of the endpoint from the forensics team if they observe high risk applications, malware, intrusion attempts, malicious emails, high-risk traffic, lateral movement, and so on, on that endpoint. For each engagement, forensic analysts from Fortinet’s FortiGuard Labs remotely assist in collecting, examining, and presenting digital evidence, including a final detailed report.

This feature requires the FortiGuard Endpoint Forensic Analysis license. The following instructions assume that you have purchased the license and registered it to your FortiCloud account. You can have a maximum of five forensic analysis requests in progress at a given time.

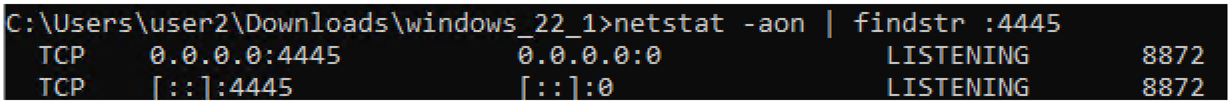
The following instructions give an example of requesting analysis on a Windows endpoint.

To request forensic analysis on an endpoint:

1. Enable *FortiGuard Forensics Analysis*:
   - **a.** In FortiClient Cloud, go to *System Settings* > *Feature Select*.
   - **b.** Enable *FortiGuard Forensics Analysis*. Click *Save*.
   - **c.** Go to *Endpoint Profiles* > *System Settings*.
   - **d.** On the desired profile, enable *Forensics License*. Click *Save*.
2. Request analysis:
   - **a.** Go to *Endpoints* > *All Endpoints*.
   - **b.** Select the desired endpoint.
   - **c.** On the *Summary* tab, under *Forensic Analysis*, click *Request Analysis*.

   d. FortiClient Cloud displays a questionnaire. Enter details as necessary, then click *Next*.
   e. Click *Click to Download* to download the forensic installer, then click *Finish*.

3. Run the downloaded installer on the endpoint to install the forensic analysis application. The installer package includes a readme document that includes instructions to install, verify, and uninstall the forensics agent. To install the agent, open Command Prompt, go to the desired directory, and enter `enwindows.exe -c`.
4. Verify that the agent is running by entering `netstat -aon | findstr :4445`. The following shows expected output for this command:

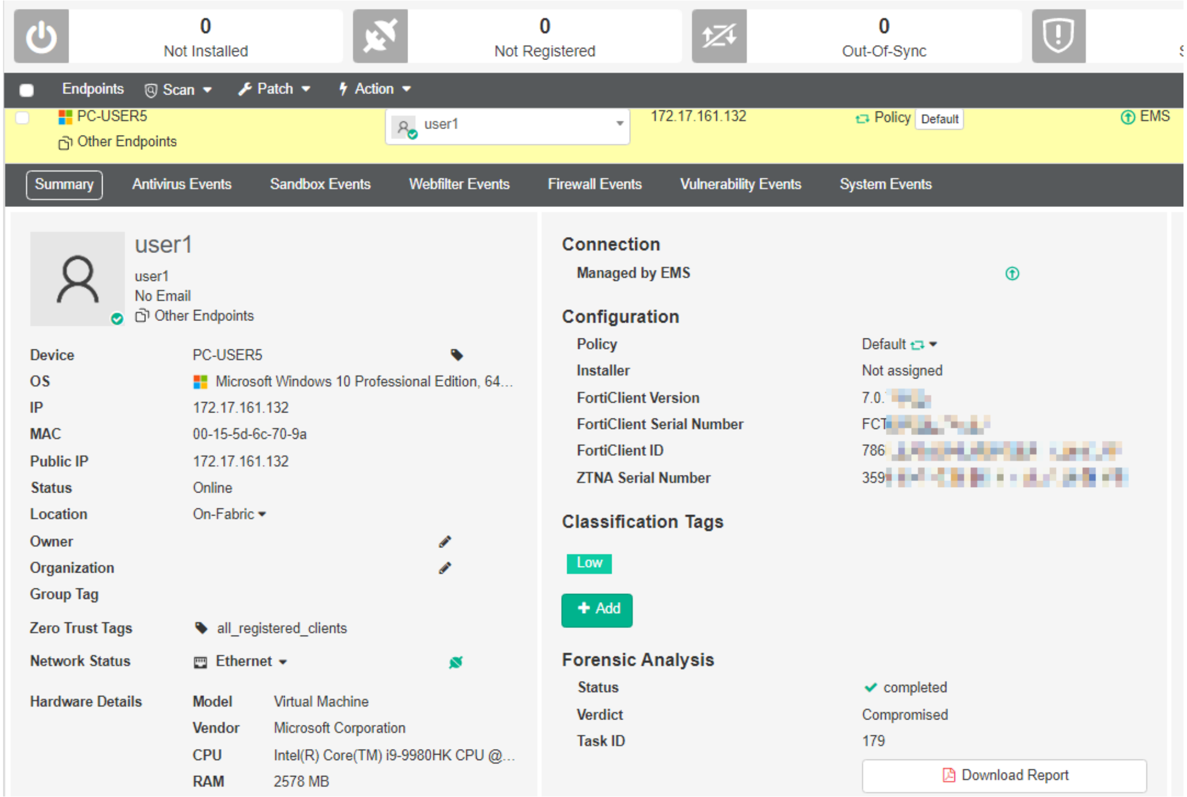


```
C:\Users\user2\Downloads\windows_22_1>netstat -aon | findstr :4445
  TCP    0.0.0.0:4445           0.0.0.0:0              LISTENING       8872
  TCP    [::]:4445              [::]:0                 LISTENING       8872
```

5. Keep the endpoint connected to the Internet and online for the next three days. The forensics team remotely connects to the endpoint and obtains required logs and events information from the endpoint for these three days.
6. You can uninstall the application after the analysis completes by entering `enwindows.exe -r`.
7. When a request is successfully created in EMS, a new task is created in FortiSOAR. After the forensics team completes analysis, the task is updated in the FortiSOAR portal to include the updated status and verdict. The team uploads the analysis report as an attachment. The following shows the status mapping between FortiSOAR and FortiClient Cloud:

FortiSOAR	FortiClient Cloud
Assign	Inprogress
Accepted	Inprogress
Onhold	Pending
Skipped	Inprogress
Failed	Failed
Cancelled	Cancelled
Completed	Completed

In FortiClient Cloud, you can download the report by going to *Endpoints > All Endpoints*, selecting the desired endpoint, then clicking *Download Report*.



PC-USER5 · user1 · 172.17.161.132 · Policy Default · EMS
Other Endpoints

user1
user1
No Email
Other Endpoints

Device	PC-USER5
OS	Microsoft Windows 10 Professional Edition, 64…
IP	172.17.161.132
MAC	00-15-5d-6c-70-9a
Public IP	172.17.161.132
Status	Online
Location	On-Fabric
Owner	
Organization	
Group Tag	
Zero Trust Tags	all_registered_clients
Network Status	Ethernet
Hardware Details	Model: Virtual Machine Vendor: Microsoft Corporation CPU: Intel(R) Core(TM) i9-9980HK CPU @… RAM: 2578 MB

Connection

Managed by EMS

Configuration

Policy	Default
Installer	Not assigned
FortiClient Version	7.0.[redacted]
FortiClient Serial Number	FCT[redacted]
FortiClient ID	786[redacted]
ZTNA Serial Number	359[redacted]

Classification Tags

Low

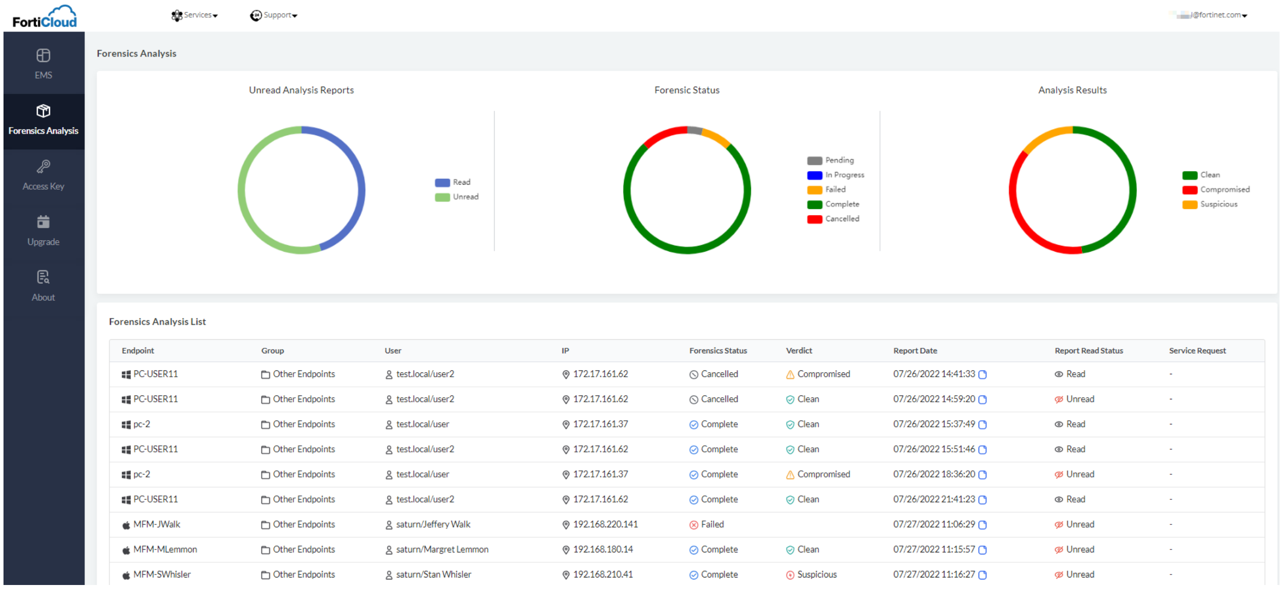
+ Add

Forensic Analysis

Status	✓ completed
Verdict	Compromised
Task ID	179

Download Report

You can also view the forensic analysis status and report on the *Forensics Analysis* tab in the portal.



Forensics Analysis List

Endpoint	Group	User	IP	Forensics Status	Verdict	Report Date	Report Read Status	Service Request
PC-USER11	Other Endpoints	test.local/user2	172.17.161.62	Cancelled	Compromised	07/26/2022 14:41:33	Read	-
PC-USER11	Other Endpoints	test.local/user2	172.17.161.62	Cancelled	Clean	07/26/2022 14:59:20	Unread	-
pc-2	Other Endpoints	test.local/user	172.17.161.37	Complete	Clean	07/26/2022 15:37:49	Read	-
PC-USER11	Other Endpoints	test.local/user2	172.17.161.62	Complete	Clean	07/26/2022 15:51:46	Read	-
pc-2	Other Endpoints	test.local/user	172.17.161.37	Complete	Compromised	07/26/2022 18:36:20	Unread	-
PC-USER11	Other Endpoints	test.local/user2	172.17.161.62	Complete	Clean	07/26/2022 21:41:23	Read	-
MFM-JWalk	Other Endpoints	saturn/Jeffery Walk	192.168.220.141	Failed		07/27/2022 11:06:29	Unread	-
MFM-MLemmon	Other Endpoints	saturn/Margret Lemmon	192.168.180.14	Complete	Clean	07/27/2022 11:15:57	Unread	-
MFM-SWhisler	Other Endpoints	saturn/Stan Whisler	192.168.210.41	Complete	Suspicious	07/27/2022 11:16:27	Unread	-

Azure SQL managed instance support - 7.0.8

You can deploy EMS using an Azure SQL managed instance. Azure provides two SQL-based offerings: Azure SQL managed instances and Azure SQL databases, which are incompatible with each other. EMS only supports Azure

SQL managed instances. Azure SQL databases do not provide all features that EMS requires.

For more information about this feature, see Azure SQL managed instance support.

Index

The following index provides a list of all new features added to FortiClient and EMS 7.0. The index allows you to quickly identify the version where the feature first became available in FortiClient and EMS.

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 6 • EMS distributes SSL deep inspection CA certificates 7.0.1 on page 31
2021-08-11	Added Dual stack IPv4 and IPv6 for SSL VPN 7.0.1 on page 22.
2021-08-16	Added: • SSL VPN security improvements on page 23 • Zero Trust tagging rules enhancement 7.0.1 on page 32 • Sending invitation emails on page 50 • Diagnostic tool 7.0.1 on page 52 Updated EMS distributes SSL deep inspection CA certificates 7.0.1 on page 31.
2021-08-17	Added Provisioning ZTNA TCP forwarding rules via EMS 7.0.1 on page 35, FortiClient license and EMS communication enhancements on page 54, and FortiGuard Outbreak Alerts service 7.0.1 on page 36.
2021-08-26	Added FortiClient Cloud Chromebook support 7.0.1 on page 53.
2021-09-22	Updated Dual stack IPv4 and IPv6 for SSL VPN 7.0.1 on page 22.
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 24.
2021-10-14	Updated Improved TCP forwarding performance 7.0.1 on page 6.
2021-10-26	Added Antiransomware file backup and restoration 7.0.2 on page 8.
2022-01-18	Added Overview on page 5 and Index on page 72.
2022-02-25	Added for release of 7.0.3: • Logging to FortiAnalyzer Cloud 7.0.3 on page 8 • FQDN-based ZTNA TCP forwarding services 7.0.3 on page 10 • Browser as external user agent for ZTNA user authentication 7.0.3 on page 13 • FortiGate-powered host check for free VPN client 7.0.3 on page 26 • Tag management and visibility improvement 7.0.3 on page 37 • Separate endpoint profiles 7.0.3 on page 56 • Active Directory LDAPS connection certificate provisioning 7.0.3 on page 60 • Redundancy using SQL Server 7.0.3 on page 60
2022-04-27	Added FortiGuard Outbreak Alerts support for tagging endpoints for specific vulnerabilities 7.0.4 on page 38 for release of 7.0.4.
2022-07-05	Added for release of 7.0.6: • Individual onboarding process 7.0.6 on page 40

Date	Change description
	- User-based licensing 7.0.6 on page 66
2022-08-23	Added FortiGuard Forensics service 7.0.6 on page 68.
2022-08-31	Added ZTNA certificate serial number mismatch 7.0.7 on page 20 for release of 7.0.7.
2022-11-08	Added Autoconnect on login as an Azure AD user 7.0.7 on page 29.
2023-03-15	Added FDS update support for antiransomware behavior rules 7.0.3 on page 15.
2023-03-21	Added Azure SQL managed instance support 7.0.8 on page 70.
2023-03-28	Updated FortiClient license and EMS communication enhancements on page 54.

www.fortinet.com