Access Control

FortiClient 7.2

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

FORTINET®

March 12, 2024
FortiClient 7.2 Access Control
04-720-877387-20240312

TABLE OF CONTENTS

Deployment options

You can deploy FortiClient in one of the following scenarios:

- FortiClient in the Fortinet Security Fabric on page 4. This scenario allows FortiClient to participate in the Fortinet Security Fabric.
- FortiClient with EMS on page 6. In this scenario, FortiClient does not participate in the Security Fabric.

FortiClient in the Fortinet Security Fabric

In this scenario, FortiClient Zero Trust Telemetry connects to EMS to receive a profile of configuration information as part of an endpoint policy. EMS is connected to the FortiGate to participate in the Fortinet Security Fabric. EMS sends FortiClient endpoint information to the FortiGate.

The FortiGate can also receive dynamic endpoint group lists from EMS and use them to build dynamic firewall policies. EMS sends group updates to FortiOS, and FortiOS uses the updates to adjust the policies based on those groups.

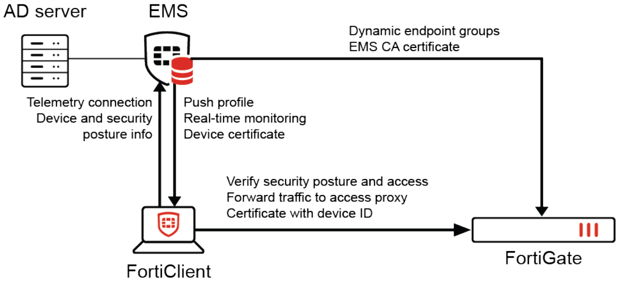
FortiClient can also receive a device certificate from EMS that it can use to securely encrypt and tunnel TCP and HTTPS traffic through HTTPS to the FortiGate.

FortiGate does not provide configuration information for FortiClient and the endpoint. An administrator must configure FortiClient using an EMS endpoint policy.

Following is a summary of how the Zero Trust Telemetry connection works in this scenario. The following assumes that EMS is already connected to the FortiGate as a participant in the Security Fabric:

1. EMS sends its CA certificate to the FortiGate.
2. FortiClient Telemetry attempts connection to EMS. Based on the EMS configuration, FortiClient may receive an SSL certificate from EMS to verify the connection. If the certificate is valid, FortiClient Telemetry connects to EMS. If the certificate is invalid, FortiClient may allow or deny connection to the EMS based on configured invalid certificate action.
3. FortiClient receives the following from EMS:
   - Licensing.
   - Profile of configuration information as part of an endpoint policy.
   - Device certificate that includes the FortiClient UID. FortiClient installs the received certificate to the current user certificate store for Chrome and Edge browser, and installs it to the browser certificate store for Firefox. This feature may not be available for Firefox.
4. FortiClient sends security posture information to EMS, including third-party software information, running processes, network information, and so on.
5. EMS dynamically groups the endpoint based on the information it received, using the configured Zero Trust tagging rules.
6. FortiOS pulls the dynamic endpoint group information from EMS. The FortiOS administrator can use this data to build dynamic firewall policies.

7. When the endpoint initiates TCP or HTTPS traffic, FortiClient works as a local proxy gateway to securely encrypt and tunnel the traffic through HTTPS to the FortiGate, using the certificate received from EMS.
8. The FortiGate retrieves the UID to identify the device and check other information using the endpoint information that EMS provided to the FortiGate. The FortiGate allows or denies the access as applicable.
9. EMS sends dynamic endpoint group updates to FortiOS. FortiOS uses the updates to adjust the policies based on those groups.



FortiClient follows the endpoint profile configuration that it receives from EMS. EMS locks FortiClient settings so that the endpoint user cannot manually change FortiClient configuration.

Only EMS can control the connection between FortiClient and EMS. You can only disconnect FortiClient when you are logged into EMS.

The EMS server's IP addresses are embedded in FortiClient deployment packages created in EMS. This allows the endpoint to connect FortiClient Telemetry to the specified EMS server.

EMS sends the following endpoint information to FortiOS:

- User profile:
  - Logged-in username
  - Full name
  - Email address
  - Phone number
- User avatar
- Social network account IDs
- MAC address
- OS type
- OS version
- FortiClient version
- FortiClient UUID

FortiGate also opens a websocket with EMS. EMS adds a new FcmNotify daemon to handle the websocket connection. EMS notifies the FortiGate if any of the following device information has changed. FortiOS loads the updated information:

- System information
- User avatar
- Vulnerabilities
- Zero Trust tags

EMS also sends the following endpoint information to FortiAnalyzer:

- Telemetry/system information
- User avatar

- Software inventory
- Processes
- Network statistics
- Classification tags

FortiClient directly sends the following information to FortiAnalyzer:

- Logs
- Windows host events

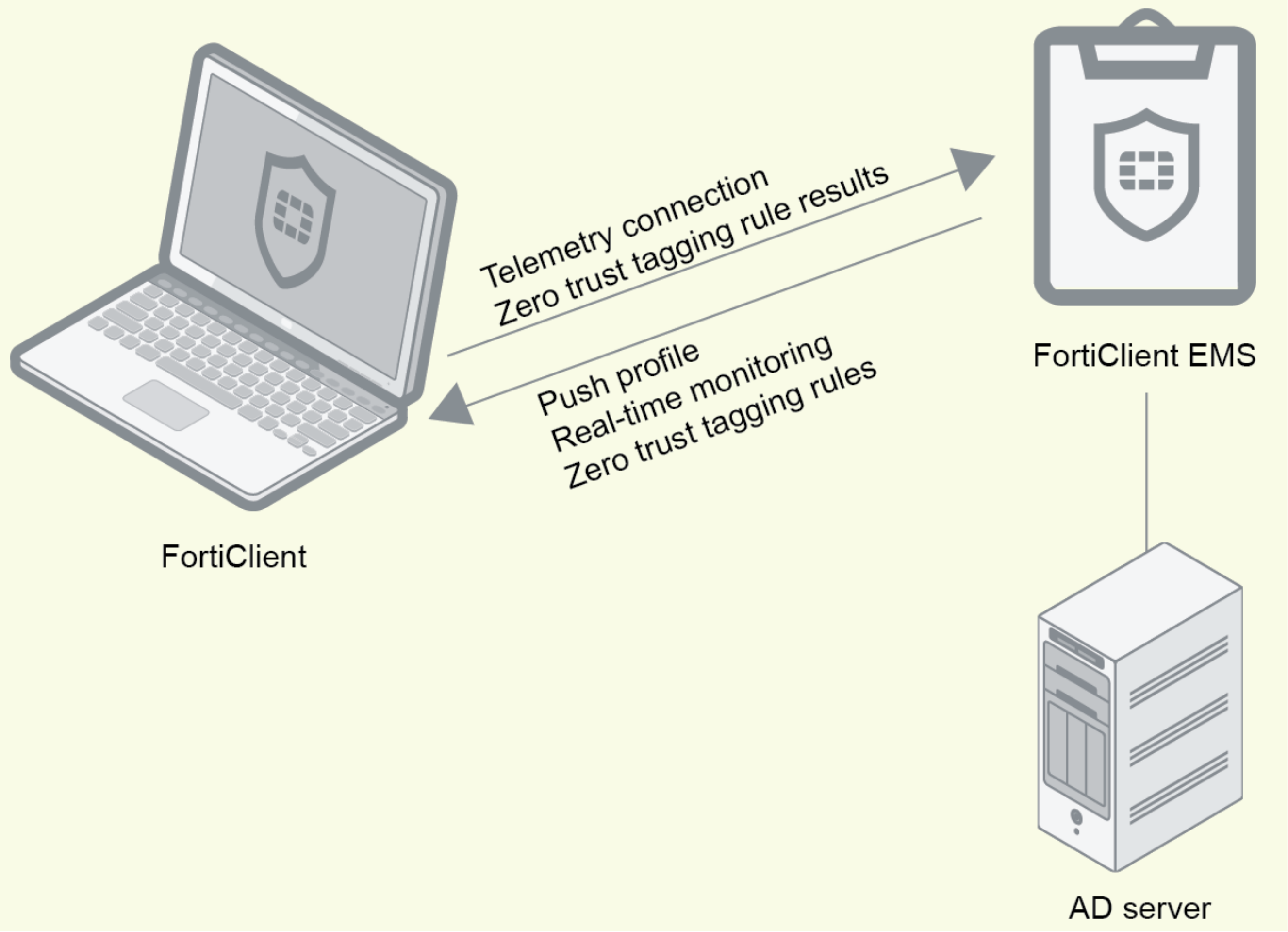
See Creating or editing Security Fabric connectors .

For details on configuring FortiOS to pull endpoint tags and their corresponding endpoint lists from EMS, see FortiOS dynamic policies using EMS dynamic endpoint groups.

FortiClient with EMS

In this scenario, EMS provides FortiClient endpoint provisioning. FortiClient connects Telemetry to EMS to receive configuration information in an endpoint profile as part of an endpoint policy from EMS. EMS also sends Zero Trust tagging rules to FortiClient and uses the results from FortiClient to dynamically group endpoints in EMS. Only EMS can control the connection between FortiClient and EMS. You must make any changes to the connection from EMS, not FortiClient. When FortiClient is connected to EMS, EMS locks FortiClient settings so that the endpoint user cannot change any configuration. To disconnect FortiClient from EMS, the EMS administrator must deregister the endpoint in EMS.

In this scenario, EMS and FortiClient cannot participate in the Security Fabric, since a FortiGate is not present.


Telemetry connection
Zero trust tagging rule results
Push profile
Real-time monitoring
Zero trust tagging rules
FortiClient EMS
FortiClient
AD server

How FortiClient Telemetry connects to EMS

When initially installing FortiClient on an endpoint, FortiClient registers to the EMS that created the deployment package.

After the FortiClient endpoint reboots, rejoins the network, or encounters a network change, FortiClient uses the following methods in the following order to locate an EMS for Telemetry connection:

1. Manually entering the IP address, which means that the endpoint user enters the EMS IP address into FortiClient.
2. Telemetry server list:
   FortiClient Telemetry searches for IP addresses in its subnet in the Telemetry server list. It connects to the EMS in the list that is in the same subnet as the host system.

   If FortiClient cannot find any EMS servers in its subnet in the Telemetry server list, it attempts to connect to the first reachable EMS in the list, starting from the top. FortiClient maintains the list order as configured in the Telemetry server list.
3. Remembered Telemetry server list. You can configure FortiClient to remember server IP addresses when you connect Telemetry to EMS. Later FortiClient can use the remembered IP addresses to automatically connect Telemetry to EMS.

Silent registration

When silent registration is enabled, FortiClient connects and reconnects Telemetry to EMS without any user interaction. FortiClient does not notify the user about the connection, and the user is not required to confirm the connection.

By default, silent registration is enabled in endpoint profiles in EMS. If desired, you can disable silent registration in EMS.

Reregistration

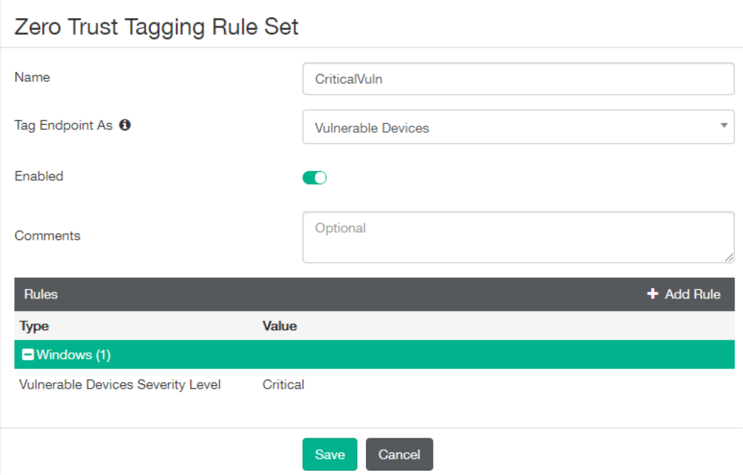
The EMS administrator can assign an endpoint policy that includes a Telemetry server list to endpoints. Receiving the Telemetry server list triggers FortiClient to connect to an EMS server using the order in How FortiClient Telemetry connects to EMS on page 8, even if FortiClient Telemetry is already connected to EMS.

Configuring EMS profile to allow or block endpoint from VPN tunnel connection based on the applied Zero Trust tag

You can configure a profile to allow or block an endpoint from connecting to a VPN tunnel based on its applied Zero Trust tag. This feature is only available for Windows endpoints. This example describes configuring an endpoint profile to prohibit Windows endpoints with critical vulnerabilities from connecting to VPN.

To configure an endpoint profile to prohibit endpoints with critical vulnerabilities from connecting to VPN:

1. Create a Zero Trust tagging rule set that tags endpoints with critical vulnerabilities with the "Vulnerable Devices" tag:
   1. Go to *Zero Trust Tags* > *Zero Trust Tagging Rules*.
   2. Click *Add*.
   3. In the *Tag Endpoint As* field, create a new "Vulnerable Devices" tag.
   4. Toggle *Enabled* to on.
   5. Click *Add Rule*.
   6. For Windows devices, from the *Rule Type* dropdown list, select *Vulnerable Devices*.
   7. From the *Severity Level* dropdown list, select *Critical*.
   8. Click *Save*.
   9. Click *Save* again.



Zero Trust Tagging Rule Set

Name	CriticalVuln
Tag Endpoint As	Vulnerable Devices
Enabled	●
Comments	Optional

Rules

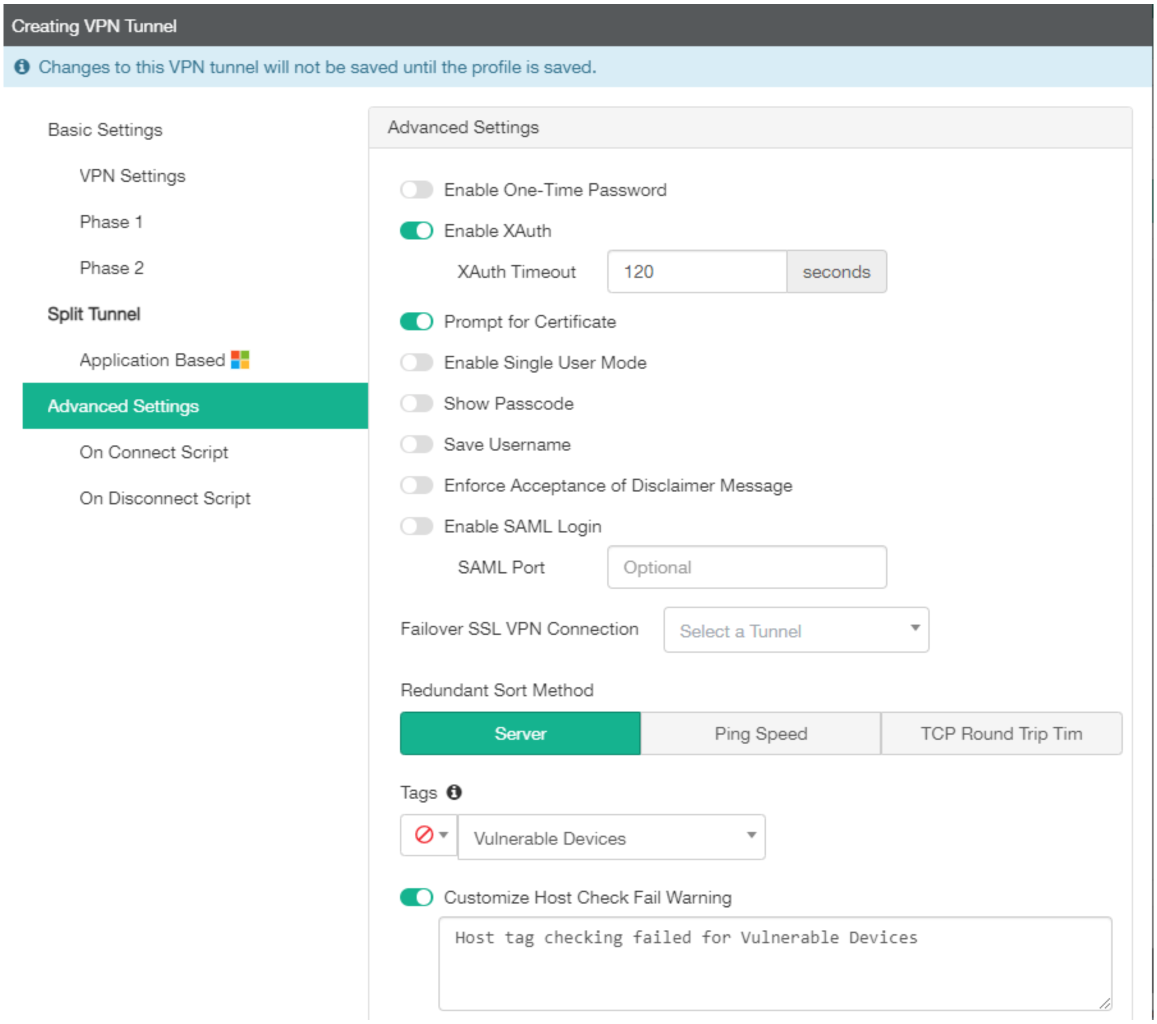
Type	Value
Windows (1)	
Vulnerable Devices Severity Level	Critical

2. Configure the options on the endpoint profile:
   1. Go to *Endpoint Profiles* > *Remote Access*.
   2. Edit the desired profile, or create a new one.
   3. Enable *Enable Secure Remote Access*.
   4. Select an existing VPN tunnel, or create a new one by clicking *Add Tunnel*.
   5. Select *Manual*, then click *Next*.
   6. In *Advanced Settings*, under *Tags*, select *Prohibit*.
   7. From the *Select a Tag* dropdown list, select *Vulnerable Devices*.
   8. Enable *Customize Host Check Fail Warning*.

i. Enter a message to display to users when their connection to the VPN tunnel is prohibited due to critical vulnerabilities on their device.

j. Configure other fields as desired.

k. Save the configuration.

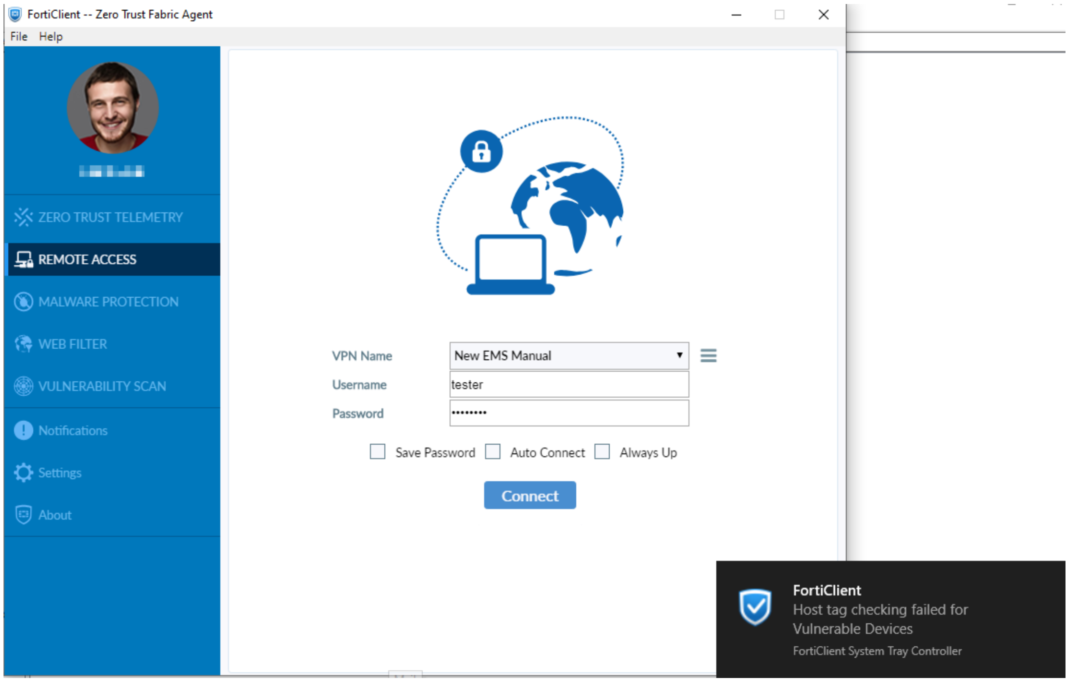


Changes to this VPN tunnel will not be saved until the profile is saved.

Enable One-Time Password: off
Enable XAuth: on
XAuth Timeout: 120 seconds
Prompt for Certificate: on
Enable Single User Mode: off
Show Passcode: off
Save Username: off
Enforce Acceptance of Disclaimer Message: off
Enable SAML Login: off
SAML Port: Optional
Failover SSL VPN Connection: Select a Tunnel
Redundant Sort Method: Server
Tags: Vulnerable Devices
Customize Host Check Fail Warning: on

```
Host tag checking failed for Vulnerable Devices
```

After the next communication between EMS and FortiClient, endpoints with this profile applied are unable to connect to this VPN tunnel if they have critical vulnerabilities. The following shows the notification that the end user sees when their connection to the VPN tunnel is prohibited due to critical vulnerabilities on their device. After the end user fixes the vulnerabilities, FortiClient allows them to establish the VPN connection.



VPN Name: New EMS Manual

Username: tester

Password: ••••••••

□ Save Password □ Auto Connect □ Always Up

FortiClient
Host tag checking failed for Vulnerable Devices
FortiClient System Tray Controller

Change log

Date	Change Description
2023-01-31	Initial release.

www.fortinet.com