FORTINET

Administration Guide

FortiClient 7.2.7

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

December 12, 2024
FortiClient 7.2.7 Administration Guide
04-727-858748-20241212

TABLE OF CONTENTS

Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection to end user devices. As the endpoint is the ultimate destination for malware that seeks credentials, network access, and sensitive information, ensuring that your endpoint security combines strong prevention with detection and mitigation is critical.

This document is written for FortiClient (Windows) 7.2.7. FortiClient (macOS) 7.2.7 and FortiClient (Linux) 7.2.7 do not support all features that this document describes.

FortiClient, FortiClient EMS, and FortiGate

You can use FortiClient with EMS and FortiGate or with EMS only. You apply FortiClient licensing to EMS.

When you connect FortiClient only to EMS, EMS manages FortiClient. However, FortiClient cannot participate in the Fortinet Security Fabric.

When using FortiClient with EMS and FortiGate, FortiClient integrates with the Security Fabric to provide endpoint awareness, compliance, and enforcement by sharing endpoint telemetry regardless of device location, such as corporate headquarters or a café. At its core, FortiClient automates prevention of known and unknown threats through its built-in host-based security stack and integration with FortiSandbox. FortiClient also provides secure remote access to corporate assets via VPN with native multifactor authentication coupled with single sign on.

FortiClient works cooperatively with the Security Fabric. FortiClient achieves this by:

- Extending the Security Fabric down to the endpoints to secure them via security profiles
- Sharing endpoint telemetry to increase awareness of where systems, users, and data reside within an organization
- Enabling proper segmentation implementation to protect these endpoints

At regular intervals, FortiClient sends Zero Trust telemetry data to EMS. This visibility coupled with built-in controls from EMS allows the security administrator to construct a policy to deny access to endpoints with known vulnerabilities or to quarantine compromised endpoints with a single click.

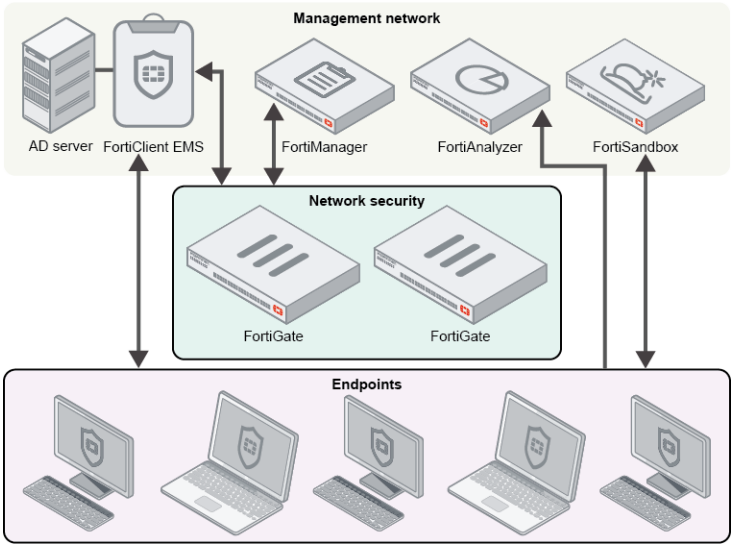
See Getting started with FortiClient on page 17.

Fortinet product support for FortiClient

The following Fortinet products work together to support FortiClient:

- FortiClient EMS
- FortiManager
- FortiGate

- FortiAnalyzer
- FortiSandbox



FortiClient EMS

FortiClient EMS runs on a Windows server. EMS manages FortiClient endpoints by deploying FortiClient (Windows) and endpoint policies to endpoints, and the endpoints can connect FortiClient Telemetry to EMS. FortiClient endpoints can connect to EMS to participate in the Fortinet Security Fabric. FortiClient endpoints connect to EMS for real-time management.

For information on EMS, see the *FortiClient EMS Administration Guide*.

FortiManager

FortiManager provides central FortiClient management for FortiGates that FortiManager manages. When endpoints are connected to managed FortiGates, you can use FortiManager to monitor endpoints from multiple FortiGates.

For information on FortiManager, see the *FortiManager Administration Guide*.

FortiGate

FortiGate provides network security. EMS defines compliance verification rules for connected endpoints and communicates the rules to endpoints and the FortiGate. The FortiGate uses the rules and endpoint information from EMS to dynamically adjust security policies. When using FortiManager, FortiGates communicate between EMS and FortiManager.

For information on FortiGate, see the *FortiOS documentation*.

FortiAnalyzer

FortiAnalyzer can receive logs and Windows host events directly from endpoints connected to EMS, and you can use FortiAnalyzer to analyze the logs and run reports. FortiAnalyzer receives other FortiClient data from EMS.

For information on FortiAnalyzer, see the *FortiAnalyzer Administration Guide*.

FortiSandbox

FortiSandbox offers capabilities to analyze new, previously unknown, and undetected virus samples in real time. Files sent to it are scanned first, using similar antivirus (AV) engine and signatures as are available on FortiOS and FortiClient. If the file is not detected but is an executable file, it is run in a Microsoft Windows virtual machine (VM) and monitored. The file is given a rating or score based on its activities and behavior in the VM.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from FortiSandbox, and applies them locally to all realtime and on-demand AV scanning.

FortiClient supports connection to an on-premise FortiSandbox appliance or FortiClient Cloud Sandbox (PaaS). For more information, see the *FortiSandbox Administration Guide*.

FortiClient standalone and licensed version feature comparison

When not connected to EMS, FortiClient offers a limited feature set. The following chart shows the modules available for FortiClient for different OSes:

Module	Free VPN-only standalone FortiClient	Licensed FortiClient			
	Windows, Windows Server, macOS, and Linux	Windows	Windows Server	macOS	Linux
Zero Trust Telemetry	No	Yes	Yes	Yes	Yes
Compliance	No	Yes	Yes	Yes	Yes
Sandbox Detection (including connection to FortiClient Cloud Sandbox (PaaS))	No	Yes	No	Yes	Yes

Module	Free VPN-only standalone FortiClient	Licensed FortiClient			
	Windows, Windows Server, macOS, and Linux	Windows	Windows Server	macOS	Linux
					FortiClient (Linux) cannot connect to FortiClient Cloud Sandbox (PaaS) or query or submit samples to FortiSandbox. It can only download and use the FortiSandbox signature file.
AntiVirus	No	Yes	Yes	Yes	Yes
Web Filter	No	Yes	Yes	Yes	Yes
Application Firewall	No	Yes	No	Yes	No
Remote Access	Only supports a limited version of the Remote Access feature. The following is supported: • IPsec and SSL VPN with user authentication • Certificate authentication • Multifactor authentication using FortiToken You can only download the free VPN client from FNDN or FortiClient.com. For details, see Standalone VPN client on page 75.	Yes	Yes	Yes	Yes. For IPsec VPN, FortiClient (Linux) only supports IKEv2.
Vulnerability Scan	No	Yes	Yes	Yes	Yes
Central management	No	Yes	Yes	Yes	Yes
24x7 support	No	Yes	Yes	Yes	Yes

In 7.2.7, you apply FortiClient licensing to EMS. EMS supports free and paid licensing models. See FortiClient EMS.

Endpoint communication security

FortiClient connects to EMS using Telemetry to:

- Obtain license information
- Send endpoint and management information to EMS
- Receive endpoint configuration
- Receive endpoint commands, the results of which it can send to EMS
- Other similar tasks

The connection from FortiClient to EMS uses TCP and TLS 1.3. During the SSL connection setup, EMS sends a server certificate to FortiClient. The certificate that EMS sends to FortiClient is the one configured in *EMS Settings* > *Shared Settings* > *Endpoint Control certificate*. See Adding an SSL certificate to FortiClient EMS.

In 7.0.1 and earlier versions, FortiClient checks the certificate subject name received from EMS to confirm its validity. In 7.0.2, the certificate validation follows industry standards:

- Domain or fully qualified domain name (FQDN) that FortiClient is connecting to matches the domain to which the certificate is issued.
  - Validation process correctly handles wildcards in the domain name in the certificate.
  - Validation process considers both the common name (CN) in the subject or subject alternative name (SAN).
- The certificate expiry date is in the future. The certificate has not expired.
- The certificate issuer or the root certificate in the certificate chain is from a publicly trusted certificate authority (CA). Trusted CAs are read from the operating system.

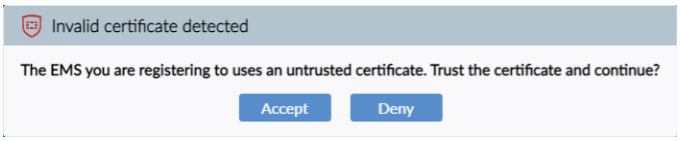
The new endpoint communication security feature allows the EMS administrator to configure endpoint profiles to take different actions based on the validity of the certificate that FortiClient receives from EMS. The EMS administrator configures this feature by enabling *Use SSL certificate for Endpoint Control* in EMS and configuring the desired *Invalid Certificate Action* for each endpoint profile.

When *Use SSL certificate for Endpoint Control* is enabled, FortiClient 7.0.1 and earlier versions cannot connect to EMS. Following the recommended upgrade path as detailed in the following procedure is recommended to ensure that endpoints can connect to EMS. See Recommended upgrade path on page 12.

The following describes the behavior when *Use SSL certificate for Endpoint Control* is enabled:

- If the EMS server certificate is valid, FortiClient silently connects without displaying a message. This is the same connection behavior from 7.0.1 and earlier versions.
- If the EMS server certificate is invalid:
  - If the *Invalid Certificate Action* is configured as *Warn*, FortiClient displays a warning message to the end user. The message warns the user that the EMS to which FortiClient is attempting to connect to has provided an invalid server certificate. The message offers options to allow or deny the connection:
    - If the user allows the connection, FortiClient connects to EMS and remembers the certificate for this EMS. FortiClient no longer prompts the user each time that it connects to this EMS.
    - If the user denies the connection, FortiClient does not connect to EMS by canceling the connection. The next time that the user tries to connect to the same EMS and the server certificate is still invalid, FortiClient

displays the same message again.



- If the *Invalid Certificate Action* is configured as *Allow*, FortiClient connects to EMS.
- If the *Invalid Certificate Action* is configured as *Deny*, FortiClient does not connect to EMS.

When *Use SSL certificate for Endpoint Control* is disabled, EMS sends the FortiCare certificate for endpoint control connections to FortiClient. FortiClient considers this certificate invalid and follows the configured *Invalid Certificate Action*.

Recommended upgrade path

Existing FortiClient and EMS users may have a mixture of 7.2.0 and older versions in production. The endpoint security improvement feature is available for EMS 7.2.0 and later versions. The EMS administrator configures this feature by enabling *Use SSL certificate for Endpoint Control* in EMS and configuring the desired *Invalid Certificate Action* for each endpoint profile. When the endpoint security improvement feature is enabled in EMS, only FortiClient 7.2.0 and later versions can connect. Therefore, upgrading all FortiClient endpoints to 7.2.0 is recommended.

When *Use SSL certificate for Endpoint Control* is enabled on EMS, FortiClient 7.0.1 and earlier versions cannot connect to EMS. Following the recommended upgrade path as detailed in the following procedure is recommended to ensure that endpoints can connect to EMS.

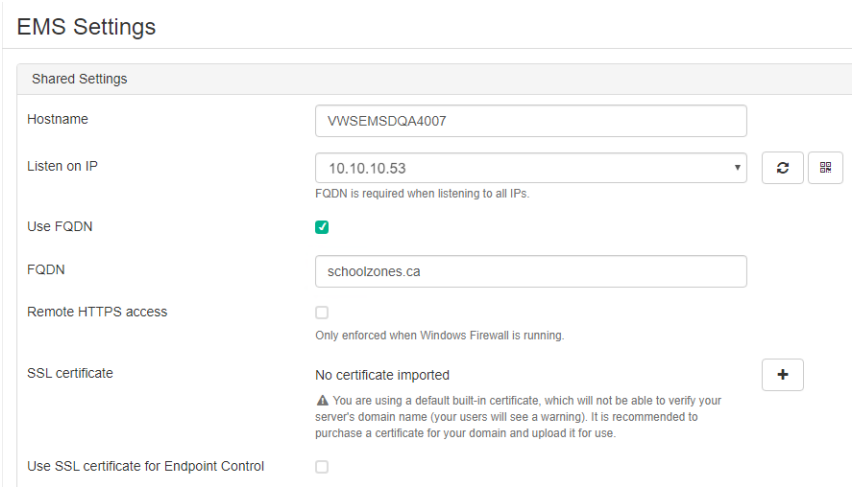
Following is the recommended upgrade path for when FortiClient and/or EMS older than 7.2.0 exists in production. You must complete the following steps:

1. Upgrade EMS to 7.2.0.
2. Upgrade FortiClient to 7.2.0.
3. Apply a valid certificate to EMS.
4. Configure the invalid certificate action as warn.

To upgrade EMS to 7.2.0:

1. Upgrade EMS to 7.2.7 as the Upgrade Path describes.
2. Go to *System Settings* > *EMS Settings*.

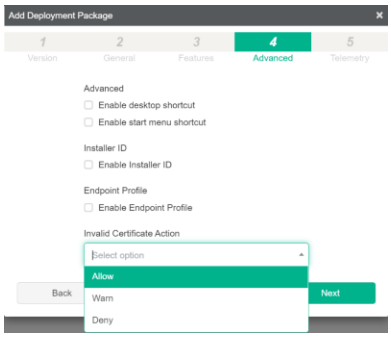
3. Disable *Use SSL certificate for Endpoint Control*.



4. Go to *Endpoint Profiles* > *Manage Profiles*.
5. Select a *System Settings* profile.
6. Configure *Invalid Certificate Action* as *Allow*.
7. Save the configuration.
8. Repeat steps 4-7 for all profiles.

To upgrade FortiClient to 7.2.0:

1. Create an installer:
   a. In EMS, go to *Deployment & Installers* > *FortiClient Installer*.
   b. Click *Add*.
   c. On the *Version* tab, you can choose to create a deployment package that uses an official installer or custom installer. Do one of the following:
      i. If you want to use an official installer, do the following:
         i. Select *Choose an official release*.
         ii. From the *Release* dropdown list, select *7.2*.
         iii. From the *Patch* dropdown list, select *7.2.0*.
      ii. If you want to use a custom installer, do the following:
         i. Select *Choose a custom installer*.
         ii. Select an existing FortiClient 7.2.0 custom installer from the *Custom Installer* dropdown list, or use the *Add Installer option* to add a new 7.2.0 installer.
   d. Click *Next*.
   e. In the *Name* and *Notes* fields, enter the desired values. Click *Next*.
   f. On the *Features* tab, enable all desired features. Click *Next*.
   g. On the *Advanced* tab, from the *Invalid Certificate Action* dropdown list, select *Allow*. Configure other fields as desired, then click *Next*.



h. Click *Finish*.

2. Create a deployment configuration:
   a. Go to *Deployment & Installers* > *Manage Deployment*.
   b. Click *Add*.
   c. In the *Endpoint Groups* field, click *Edit*. In the *Add Endpoint Groups* dialog, select all groups that contain endpoints to upgrade to 7.2.0.
   d. For *Action*, select *Install*.
   e. From the *Deployment Package* dropdown list, select the package that you created earlier.
   f. Enable *Start at a Scheduled Time* and configure the desired time.
   g. Ensure that *Enable the Deployment* is enabled.
   h. Configure other fields as desired, then save the deployment configuration.
   At the scheduled time, EMS deploys the FortiClient 7.2.0 upgrade to all endpoints groups that you configured for the deployment. FortiClient upgrades to 7.2.0 on the endpoints. After upgrade, FortiClient reconnects to EMS. FortiClient does not display an error or warning as it reconnects to EMS.

To apply a valid certificate to EMS:

1. In EMS, go to *System Settings* > *EMS Settings*.
2. You can add an SSL certificate to EMS in one of the following ways:

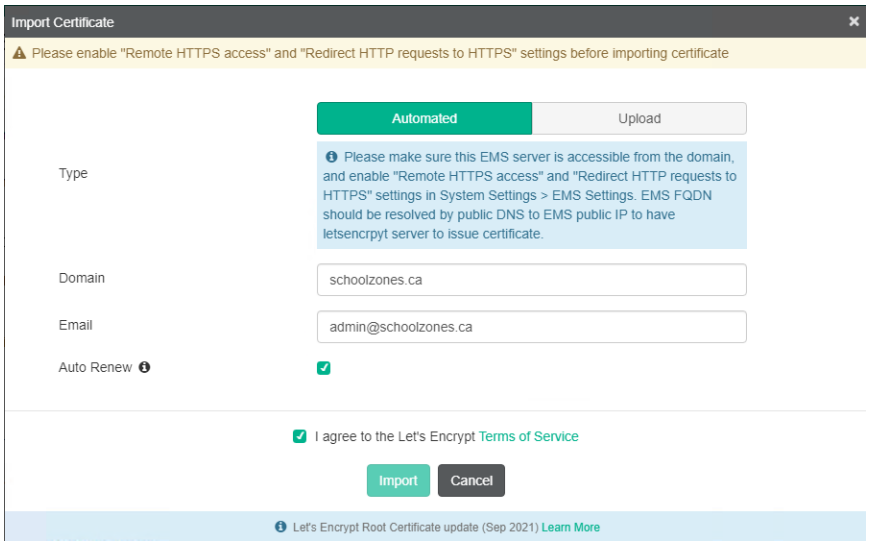
Method	Description
Automated	The Automated Certificate Management Environment (ACME), as defined in RFC 8555, is used by the public Let's Encrypt certificate authority to provide free SSL server certificates. You can configure EMS to use certificates that are managed by Let's Encrypt.
Upload	Manually upload an SSL certificate.

For either method, you must ensure that the certificate satisfies the criteria in Endpoint communication security on page 11 to ensure that communication between FortiClient and EMS is secure.

Do one of the following:

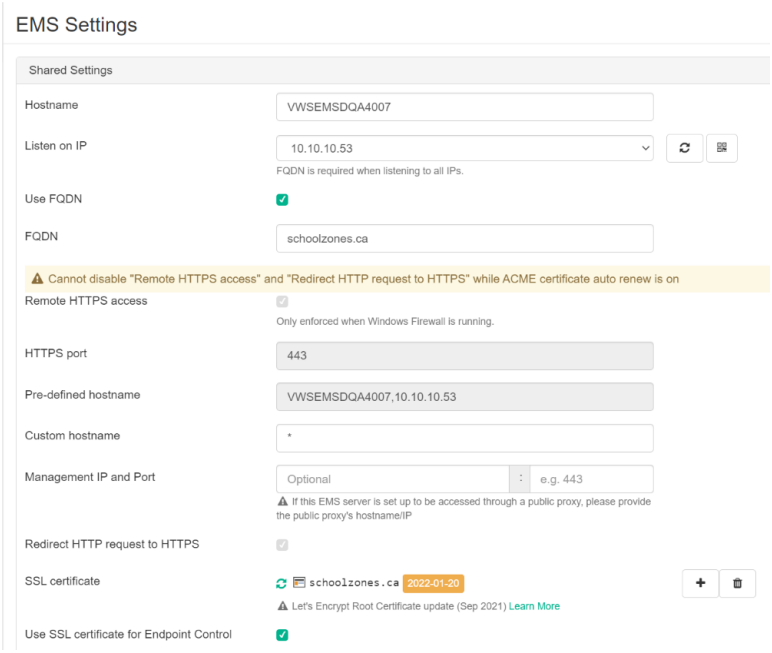
   a. Configure an automated SSL certificate:
      i. Go to *System Settings* > *EMS Settings*.
      ii. Ensure that *Remote HTTPS access* and *Redirect HTTP request to HTTPS* are enabled.
      iii. Ensure that ports 80 and 443 are accessible from the Internet by going to https://<EMS FQDN> in a browser. If the ports are accessible, the browser displays the EMS login page.
      iv. In the *SSL certificate* field, click the *Import SSL certificate* button.
      v. Select *Automated*.

vi. In the *Domain* field, enter the EMS FQDN. For the Let's Encrypt server to issue the certificate, the public DNS server must resolve the EMS FQDN to the EMS public IP address.
vii. In the *Email* field, enter a valid email address.
viii. If desired, enable *Auto Renew*. When *Auto Renew* is enabled, EMS automatically renews the certificate before expiry.
ix. Select the checkbox to agree to Let's Encrypt's terms of service. Click *Import*.



b. Manually upload an SSL certificate:
i. Go to *System Settings* > *EMS Settings*.
ii. In the *SSL certificate* field, click the *Import SSL certificate* button.
iii. Select *Upload*.
iv. In the *Certificate* field, browse to and select the desired certificate.
v. In the *Certificate Password* field, configure the desired password for the certificate.
vi. Click *Upload*.

3. After all endpoints have upgraded to FortiClient 7.2.0 and EMS is using a valid certificate, go to *System Settings* > *EMS Settings* and enable *Use SSL certificate for Endpoint Control*. When you enable this option, endpoints still running FortiClient 7.0.1 and older versions can no longer connect to this EMS. If they were previously connected, they now show as offline.



To configure the invalid certificate action as warn:

1. In EMS, go to *Endpoint Profiles* > *Manage Profiles*.
2. Select a profile.
3. On the *System Settings* tab, configure *Invalid Certificate Action* as *Warn*.
4. Save the profile.
5. After FortiClient receives the configuration change, observe if FortiClient displays a warning about the certificate being invalid. If you do not observe connection issues when *Invalid Certificate Action* is set to *Warn*, you can optionally change the setting to *Deny*.

Getting started

This section describes how to get started with FortiClient. It also includes key concepts that administrators and endpoint users should be aware of when using FortiClient.

Getting started with FortiClient

In 7.2.7, you must use FortiClient with EMS. FortiClient must connect to EMS to activate its license and become provisioned by the endpoint profile that the administrator configured in EMS. You cannot use any FortiClient features (except for VPN, as Free 30-day VPN access on page 61 describes) until FortiClient is connected to EMS and licensed.

The setup process is as follows. The EMS administrator completes some actions, and the endpoint user completes others.

1. The administrator configures a FortiClient deployment package in EMS. The administrator specifies which modules to install in the deployment package.
2. The administrator prepares to deploy FortiClient from EMS. See Provisioning preparation on page 22.
3. The administrator deploys FortiClient on the endpoint from EMS. See Provisioning on page 30. FortiClient installs on the endpoint. For installation to be successful, the endpoint must be a computer or device on your network that has Internet access and is running a supported operating system.
   After FortiClient installs on the endpoint, it immediately connects to EMS to activate its license. The endpoint user may need to confirm the connection request to complete the Telemetry connection to EMS.

   If the *Use SSL certificate for Endpoint Control* option is disabled in EMS, EMS sends a built-in EMS certificate or FortiCare SSL certificate to FortiClient. If the *Use SSL certificate for Endpoint Control* option is enabled in EMS, EMS sends an SSL certificate to FortiClient so that FortiClient can use the certificate to verify the connection. FortiClient may allow or block the connection based on the configured *Action for EMS invalid certificates*. See Advanced options on page 103.

   FortiClient is now a managed endpoint. Once licensed, FortiClient becomes provisioned by the endpoint profile configured in EMS. The modules that the administrator included in the deployment package in step 1 become available for use.

   After the endpoint profile provisions , it connects to the FortiGuard server to check for updates for the configured features.
4. The administrator manages the endpoint using EMS.FortiClient
5. If desired, the endpoint user can add a personal VPN configuration. See Configuring VPN connections on page 55.
6. The endpoint user can use the installed modules in FortiClient. Depending on what modules were installed, one, more, or all of the following tabs are available:
   - Zero Trust Telemetry
   - Malware Protection
   - Sandbox Detection
   - Web Filter
   - Application Firewall
   - Vulnerability Scan

- Remote Access
- ZTNA Connection Rules

FortiClient receives its license expiry information from EMS during initial provisioning. When FortiClient cannot reach EMS, it refers to the previously received expiry information to confirm that its license is still active. FortiClient does not need to maintain a connection to EMS to maintain its licensed status.

EMS and endpoint profiles

In EMS, administrators can configure an endpoint profile. Administrators then include the profile in an endpoint policy, which they apply to groups of endpoints. Profiles defines the configuration for FortiClient software on endpoints. The profile consists of the following sections:

- Remote Access
- ZTNA Connection Rules
- Web Filter
- Vulnerability Scan
- Malware Protection
- Sandbox
- Firewall
- System Settings
- XML Configuration

When the endpoint receives the configuration information in the endpoint profile as part of an endpoint policy, it automatically updates FortiClient settings. FortiClient settings are locked and read-only when EMS provides the configuration in a profile.

For information on configuring endpoint profiles using EMS, see the *FortiClient EMS Administration Guide*.

Telemetry connection options

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 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. This feature requires FortiOS 6.2.0 or a later version.

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. This feature requires FortiClient 7.0.0 or a later version and FortiOS 7.0.0 or later.

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, and that FortiClient and FortiOS are also 7.0.0 or a later version:

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:

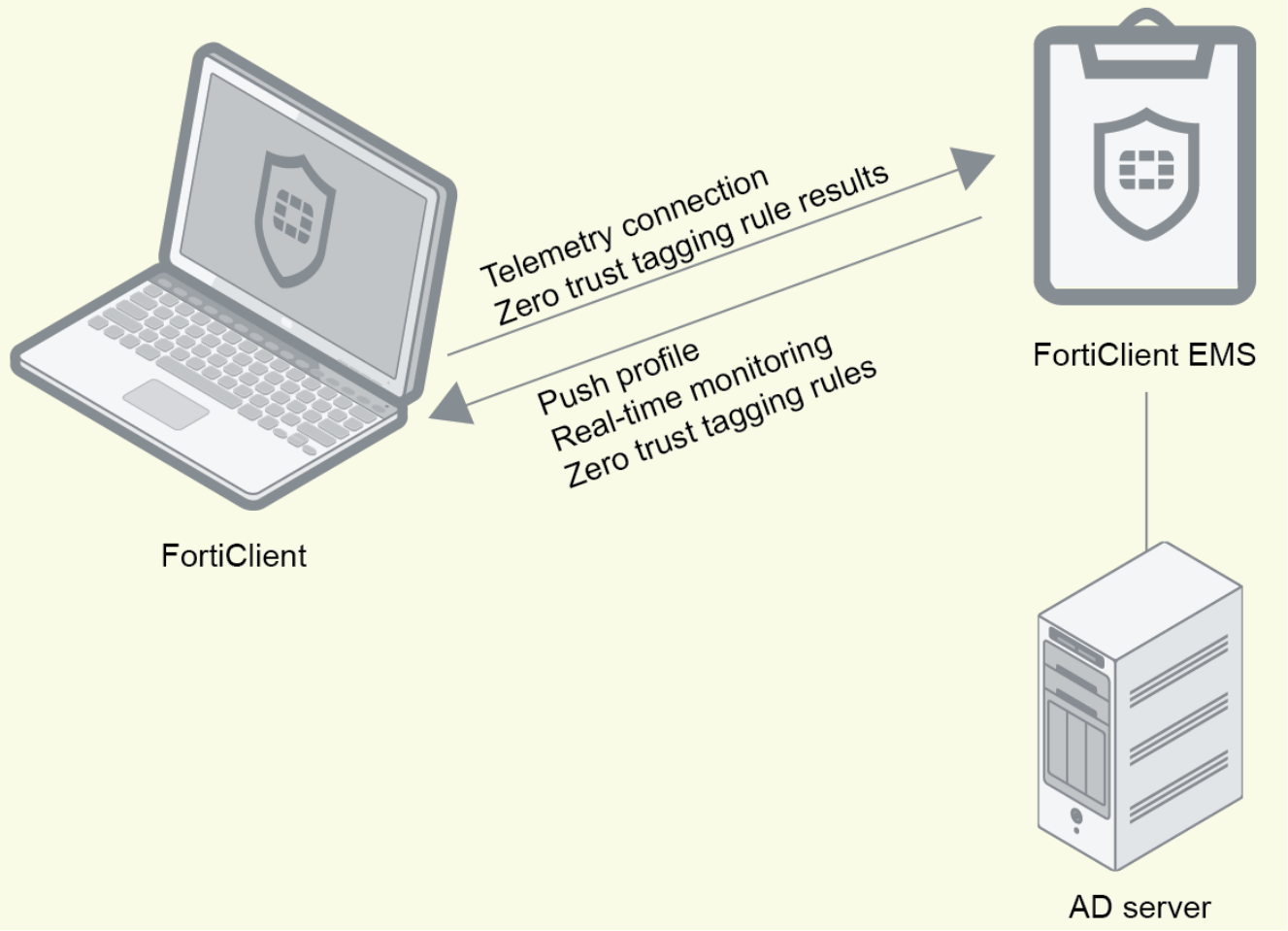
- Logs
- Windows host events

See the *FortiAnalyzer Administration Guide* for details.

For details on configuring FortiOS to pull endpoint tags and their corresponding endpoint lists from EMS, see the *FortiClient EMS Administration Guide*.

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 use 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.



EMS and automatic upgrade of FortiClient

You can use EMS to create a FortiClient installer configured to automatically upgrade FortiClient on endpoints to the latest version.

After the FortiClient installer with automatic upgrade enabled is deployed to endpoints, FortiClient is automatically upgraded to the latest version when a new version of FortiClient is available via EMS. See the *FortiClient EMS Administration Guide*.

Provisioning preparation

Before provisioning FortiClient, administrators and endpoint users should understand the installation requirements and FortiClient setup types available for installation. Administrators should also be aware of the licensing requirements.

Installation requirements

The following table lists operating system (OS) support and the minimum system requirements:

OS support	Minimum system requirements
• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (64-bit)	• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient does not support ARM-based processors. • Compatible operating system and minimum 2 GB RAM • 1 GB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dialup connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing documentation • MSI installer 3.0 or later
Microsoft Windows Server 2019 or newer	• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient does not support ARM-based processors. • Compatible operating system and minimum 512 MB RAM • 1 GB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dialup connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing documentation • MSI installer 3.0 or later

OS support	Minimum system requirements
• macOS Sequoia (version 15) • macOS Sonoma (version 14) • macOS Ventura (version 13) • macOS Monterey (version 12)	• Apple Mac computer with Intel processor or M1 or M2 chip • 1 GB of RAM • 1 GB of free hard disk drive (HDD) space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections
Linux distributions: • Ubuntu 22.04 and 24.04 • Red Hat 9 or newer • CentOS Stream 9 • Fedora 36 and later with KDE or GNOME	• Linux-compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512 MB RAM • 600 MB free hard disk space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections

For Microsoft Windows Server, FortiClient supports the Vulnerability Scan, SSL VPN, Web Filter, and antivirus (AV) features, including obtaining a Sandbox signature package for AV scanning. To use SSL VPN on a Windows Server machine, you must enable your browser to accept cookies. Otherwise, tunnel connection fails.

Licensing

FortiClient requires a license. You apply FortiClient licensing to EMS. See Windows, macOS, and Linux licenses for details.

Contact your Fortinet sales representative for information about FortiClient licenses.

Required services and ports

You must enable required ports and services for use by FortiClient and its associated applications on your server. The required ports and services enable FortiClient to communicate with servers running associated applications.

Communication	Usage	Protocol	Port	Incoming/outgoing	How to customize
FortiClient Telemetry	Endpoint management (on-premise EMS), participation in the Fortinet Security Fabric	TCP	8013	Outgoing	GUI
SYSLOG	Upload logs to syslog server	UDP	514	Outgoing	N/A
FortiSandbox	Send files to FortiSandbox for analysis	TCP	514	Outgoing	N/A
Remote access - SSL VPN	Establish VPN connection to the FortiGate	TCP	443 (default)	Outgoing	GUI
FortiAnalyzer/FortiManager	Upload logs and Windows host events to FortiAnalyzer or FortiManager	TCP	514	Outgoing	N/A
Remote access - IPsec VPN	Establish VPN connection to the FortiGate	UDP	IKE 500 ESP (IP 50) NAT-T 4500	Outgoing	N/A
FortiAuthenticator/FortiGate	Single sign on (SSO) mobility agent, FortiClient SSO	TCP	8001 (default)	Outgoing	GUI
FortiManager	Use FortiManager for FortiClient software and signature updates	TCP	80 (default)	Outgoing	GUI
SMTP/FortiGuard	Virus submission	TCP	25	Outgoing	N/A

Communication	Usage	Protocol	Port	Incoming/outgoing	How to customize
FortiPAM	Use FortiPAM for privilege access management	TCP	9191	Outgoing	N/A
FortiGuard	Cloud-based malware detection	TCP	8888	Outgoing	N/A

FortiClient can also connect to FortiClient Cloud instead of on-premise EMS for endpoint management. The following table summarizes required services for FortiClient to communicate with FortiClient Cloud:

Usage	Server URL	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient Cloud connection	forticlient-emsproxy.forticloud.com forticlient.forticloud.com	TCP	443 (default)	Outgoing	

FortiClient connects to FortiGuard to query for URL ratings for Web Filter and to download AV and vulnerability scan engine and signature updates. FortiClient can connect to legacy FortiGuard or FortiGuard Anycast. The EMS administrator configures FortiGuard server options. See Web Filter and System Settings. The following table summarizes required services for FortiClient to communicate with FortiGuard:

Usage	Server URL			Protocol	Port	Incoming/Outgoing	How to customize
	Global	U.S.	Europe				
URL rating with FortiGuard Anycast	fctguard.fortinet.net	fctusguard.fortinet.net	fcteuguard.fortinet.net	TCP	443	Outgoing	N/A The EMS administrator can configure Web Filter to use Anycast or legacy FortiGuard servers. See Web Filter.

Usage	Server URL Global	U.S.	Europe	Protocol	Port	Incoming/Outgoing	How to customize
URL rating with FortiGuard (legacy)	fgd1.fortigate.com	usfgd1.fortigate.com	N/A	UDP	8888 (default)	Outgoing	N/A The EMS administrator can configure Web Filter to use Anycast or legacy FortiGuard servers. See Web Filter.
AV/vulnerability signature update	forticlient.fortinet.net myforticlient.fortinet.net	usforticlient.fortinet.net	N/A	TCP	80	Outgoing	N/A
AV/vulnerability signature updates with FortiGuard Anycast	fctupdate.fortinet.net	fctusupdate.fortinet.net	fcteuupdate.fortinet.net	TCP	443	Outgoing	N/A

FortiClient can also connect to FortiClient Cloud Sandbox (SaaS) for integration with FortiSandbox. The following table summarizes required services for FortiClient to communicate with FortiClient Cloud Sandbox (SaaS):

Usage	Server URL	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient Cloud Sandbox (SaaS) connection	aptctrl1.fortinet.com aptctrl1.fortinet.com sends a list of Sandbox server addresses to FortiClient. There are no fixed IP addresses, FQDNs, or ports for these servers. However, the returned port is usually 514.	TCP	443 (default)	Outgoing	N/A

FortiClient (iOS) and (Android) require the following access:

Usage	Server URL	Protocol	Port	Incoming/Outgoing	How to customize
Retrieve device public IP address	myforticlient.fortinet.net	TCP	443 (default)	Outgoing	N/A

For the list of required services and ports for EMS, see the *FortiClient EMS Administration Guide*.

Firmware images and tools

Firmware images and tools are available for Windows, macOS, and Linux.

Microsoft Windows

The following files are available in the firmware image file folder:

File	Description
FortiClientTools_7.2.7.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.2.7.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_ 7.2.7.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 7.2.7.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.2.7.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.2.7 includes the FortiClient 7.2.7 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.2.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	Virus cleaner.
OnlineInstaller	Installer files that install the latest FortiClient version available.

File	Description
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools.
VPNAutomation	VPN automation tool.
VC_redist.x64.exe	Microsoft Visual C++ 2015 Redistributable Update (64-bit).
vc_redist.x86.exe	Microsoft Visual C++ 2015 Redistributable Update (86-bit).

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_7.2.7.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.2.7.xxxx_ x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_ 7.2.7.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.2.7.xxxx_x64.exe	Free VPN-only installer (64-bit).

macOS

The following file is available in the firmware image file folder:

File	Description
FortiClientTools_7.2.7.xxxx_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.2.7.xxx_macosx.dmg	Free VPN-only installer.

The following file is available on FortiClient.com:

File	Description
FortiClient_7.2.7.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.2.7.xxx_macosx.dmg	Free VPN-only installer.

EMS 7.2.7 includes the FortiClient 7.2.7 standard installer.

Linux

The following files are available in the firmware image file folder:

File	Description
forticlient_7.2.7.xxxx_amd64.deb	Standard installer package for Ubuntu.
forticlient_7.2.7.xxxx_x86_64.rpm	Standard installer package for Red Hat and CentOS.
forticlient_server_7.2.7.xxxx_amd64.deb	Headless (no GUI, CLI-only) installer for Ubuntu.
forticlient_server_7.2.7.xxxx_x86_64.rpm	Headless (no GUI, CLI-only) installer for Red Hat and CentOS.
forticlient_vpn_7.2.7.xxxx_amd64.deb	Free VPN-only installer for Ubuntu.
forticlient_vpn_7.2.7.xxxx_64.rpm	Free VPN-only installer Red Hat and CentOS.
forticlient_vpn_server_7.2.7.xxxx_amd64.deb	Headless (no GUI, CLI-only) free VPN-only installer for Ubuntu.
forticlient_vpn_server_7.2.7.xxxx_x86_64.rpms	Headless (no GUI, CLI-only) VPN-only installer for Red Hat and CentOS.

FortiClient.com also includes instructions for installing (Linux).

Obtaining FortiClient installation files

The EMS administrator will provide a download link to the FortiClient installation files. Download the installation file for your OS from the provided link.

You can also obtain the FortiClient installation files from FortiClient.com.

Provisioning

You can install FortiClient on a single computer using the installation wizard or deploy it to multiple Microsoft Windows systems using Microsoft Active Directory (AD).

FortiClient prevents uninstallation only for non-administrator users.

Manually installing FortiClient on computers

The following section describes how to install FortiClient on a computer running a Microsoft Windows, macOS, or Linux operating system.

Microsoft Windows

The following instructions guide you though the installation of FortiClient on a Microsoft Windows computer. For more information, see the *FortiClient (Windows) Release Notes*.

To check FortiClient's digital signature, right-click the installation file and select *Properties*. In this menu you can set file attributes, run the compatibility troubleshooter, view the digital signature and certificate, install the certificate, set file permissions, and view file details.

Installing FortiClient requires being logged in to the device as a user that belongs to the Administrators user group. During initial installation, FortiClient is restricted to *Program Files* and you cannot change the install path.

Once installed, FortiClient has system privileges. FortiClient performs upgrades that EMS triggers using the system account and does not require other user permissions.

To install FortiClient (Windows):

1. Double-click the FortiClient executable file. The *Setup Wizard* launches.
2. In the *Welcome to the FortiClient Setup Wizard* screen, perform the following actions:
   a. Click the *License Agreement* button, and read the license agreement. You have the option to print the EULA in this License Agreement screen. Click *Close* to return to the installation wizard.
   b. Select the *Yes, I have read and accept the license* checkbox.
3. Click *Next* to continue. The *Destination Folder* screen displays.
4. (Optional) Click *Change* to choose an alternate folder destination for installation.
5. Click *Next* to continue.

A dialog displays during a new FortiClient installation and when upgrading from an older FortiClient version that does not have the AV feature installed.

Uninstalling conflicting antivirus (AV) software before installing FortiClient or enabling the real-time protection (RTP) feature is recommended. Alternatively, you can disable the conflicting software's AV feature. When FortiClient connects to EMS, if the EMS-assigned endpoint profile has RTP enabled and a third party AV product is installed, FortiClient disables RTP.

See the Microsoft knowledge base for caveats on installing AV software. See the Microsoft Anti-Virus exclusion list.

6. Click *Next*. The *Ready to install FortiClient* screen displays.
7. Complete the installation:
   a. Click *Install*.
   b. Click *Finish*. On a new FortiClient installation, you do not need to reboot your system. When upgrading the FortiClient version, you must restart your system for the configuration changes made to FortiClient to take effect. Select *Yes* to restart your system or select *No* to manually restart later. FortiClient updates signatures and components from the FDN.
   c. FortiClient attempts to connect FortiClient Telemetry to EMS.
   d. To launch FortiClient, double-click the desktop shortcut.

Microsoft Server

You can install FortiClient on a Microsoft Windows Server. You can use the regular FortiClient Windows image for Server installations.

Check the *FortiClient (Windows) 7.2.7 Release Notes* for supported Microsoft Windows Server versions.

Refer to the Microsoft knowledge base for caveats on installing AV software in a server environment. See the Microsoft Anti-Virus exclusion list.

macOS

The following instructions guide you though the manual installation of FortiClient on a macOS computer. For more information, see the *FortiClient (macOS) Release Notes*.

After manually running the FortiClient installer on a macOS computer, you must enable certain permissions and perform other actions for FortiClient to work properly. This topic provides instructions on the necessary configurations. The process is as follows:

1. Install FortiClient on a macOS computer using the installer file. See To install FortiClient on a macOS computer: on page 32.
2. Activate system extensions. See To activate system extensions: on page 32.

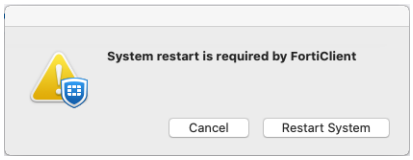
3. (macOS 11 Big Sur and 10.15 Catalina only) Enable full disk access. See To enable full disk access: on page 35.
4. Enable notifications. See To enable notifications: on page 36.

Depending on what features are enabled on EMS, installing FortiClient (macOS) may require admin credentials to handle prompts for system keychain changes and granting permissions under *Security & Privacy*.

For FortiClient upgrade, system certificates and security permissions remain unchanged, so no special user privileges are required.

To install FortiClient on a macOS computer:

1. Double-click the FortiClient_7.2.7.xx_macosx .dmg installer file. The *FortiClient for macOS* dialog displays.
2. Double-click *Install*. The *Welcome to the FortiClient Installer* dialog displays.
3. (Optional) Click the lock icon in the upper-right corner to view certificate details and click *OK* to close the dialog. Click *Continue*.
4. Read the Software License Agreement and click *Continue*. You have the option to print or save the Software Agreement in this window. You are prompted to *Agree* with the terms of the license agreement.
5. If you agree with the terms of the license agreement, click *Agree* to continue the installation.
6. Depending on your system, you may be prompted to enter your system password.
7. After the installation completes successfully, Click *Close* to exit the installer. FortiClient has been saved to the *Applications* folder.
8. If using macOS Mojave (version 10.14), you must reboot the macOS device after installing FortiClient (macOS). FortiClient (macOS) displays the following prompt after installation. Click *Restart System*:



9. Double-click the FortiClient icon to launch the application. The application loads to your desktop.

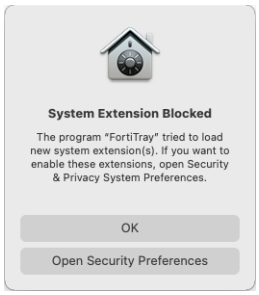
To activate system extensions:

After you perform an initial install of FortiClient, the device prompts you to allow some settings for FortiClient processes. You must have administrator credentials for the macOS machine to configure these changes.

After you grant permissions for extensions and daemons, you do not need to grant permissions again when upgrading to new FortiClient versions.

1. After installation completes, the device displays a prompt to grant permissions to the FortiClient VPN configuration manager. This allows FortiClient to monitor network events on this device. Click *Allow*.

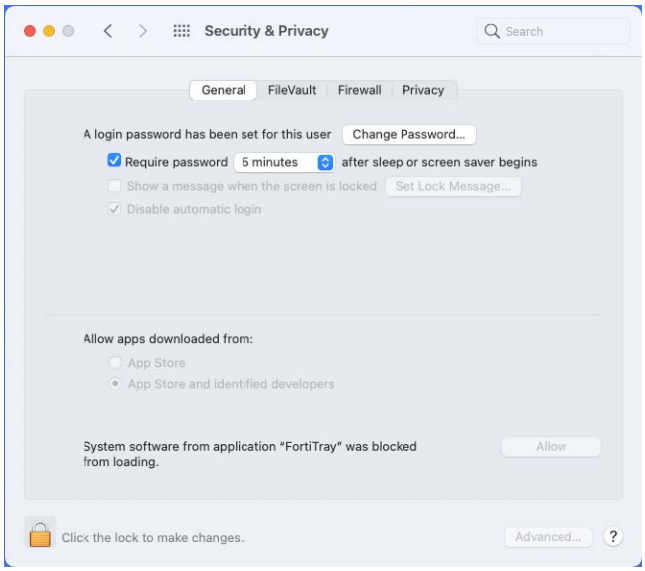
2. The system also displays the following warning that FortiTray extensions are blocked. This prevents FortiTray from loading.



To enable the FortiTray extension, do the following:

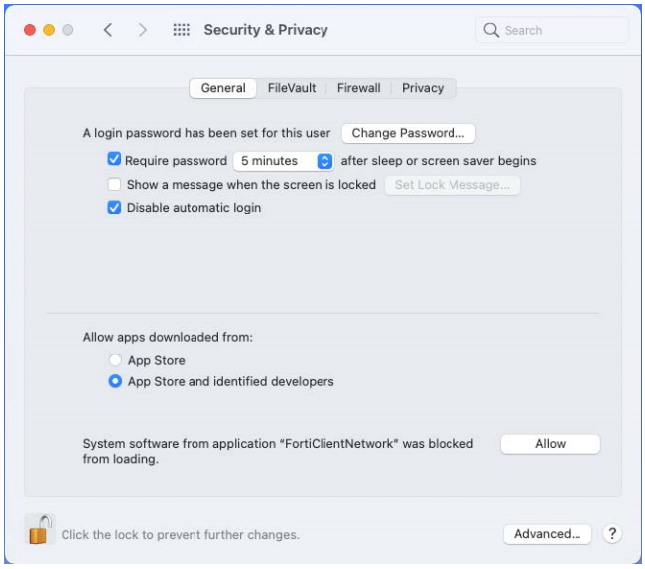
a. Go to *System Preferences* > *Security & Privacy*.

b. Click the *Allow* button beside *System software from application "FortiTray" was blocked from loading*.

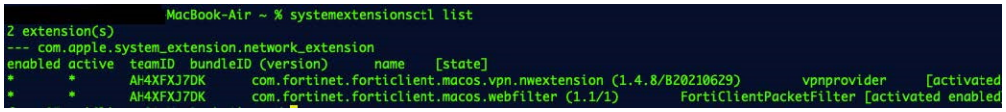


3. For Web Filter and Application Firewall to work properly, you must enable the FortiClientNetwork extension. This extension may also be necessary to connect to SSL VPN after connecting FortiClient to SSL VPN. The FortiClient team ID is AH4XFXJ7DK. Do the following:

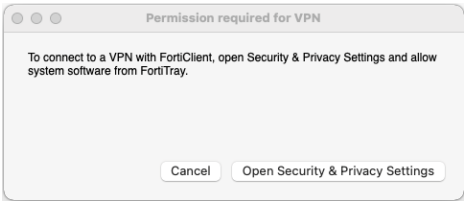
a. Go to *System Preferences* > *Security & Privacy*.
b. Click the *Allow* button beside *System software from application "FortiClientNetwork" was blocked from loading*.



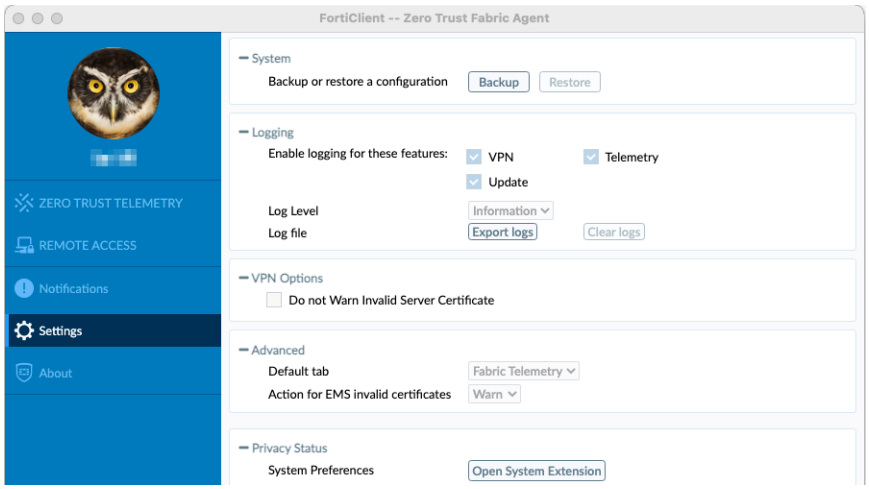
4. Verify the statuses of the extensions by running the `systemextensionsctl list` command in the macOS terminal. The following provides example output when the extension is enabled:



If you do not grant permission to the FortiTray extension or the VPN configuration manager after installing FortiClient, macOS displays a popup whenever you attempt to connect to a VPN tunnel. You cannot establish a VPN tunnel until you grant permissions to the FortiTray extension and VPN configuration manager.



You can also go to the *Settings* tab and click *Open System Extension* under *Privacy Status*. This shows if any FortiClient extensions still require permissions.

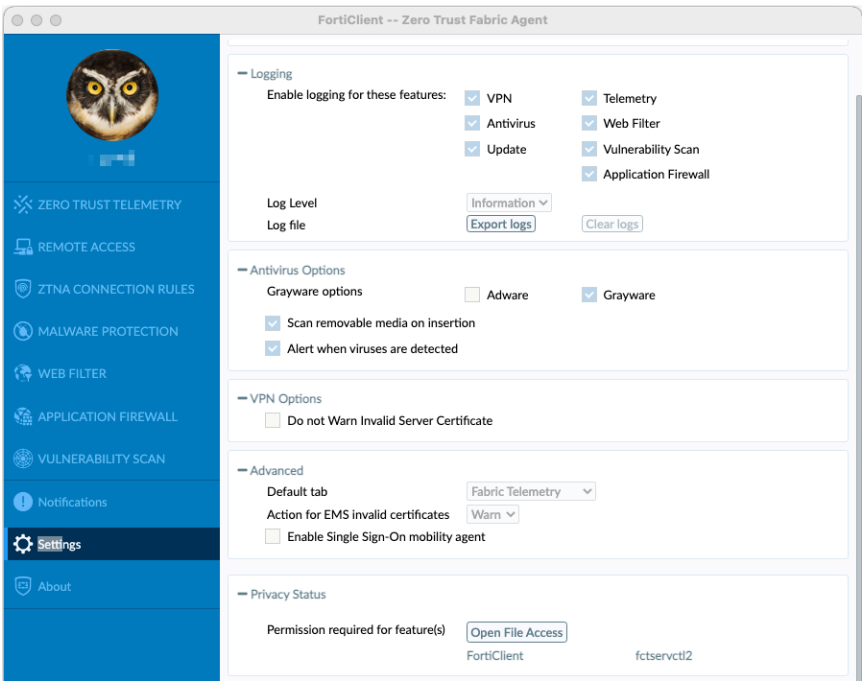


To enable full disk access:

macOS 11 Big Sur and 10.15 Catalina include security setting changes, which require you to enable full disk access for FortiClient services. If you do not grant full disk access to FortiClient services, FortiClient only provide partial protection of files in the /Applications directory. The first time that FortiClient detects an attempt to run an executable file located in another protected location on the endpoint as malware protection, macOS denies FortiClient access and prompts the user to grant full disk access.

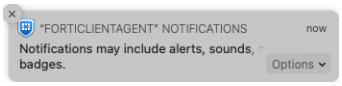
1. Go to *System Preferences* > *Security & Privacy* tab, and select *Full Disk Access*
2. To make changes, click lock icon on the bottom left, enter your credentials, and *Unlock*.
3. Select the following services to grant them full disk access:
   - fctservctl2
   - FortiClient

If you did not grant full disk access permissions for the daemons, you can check their status on the *Settings* tab under *Privacy Status*. Click *Open File Access* to grant permissions for the daemons. If you do not configure this, macOS displays a popup asking for permissions each time that you use a feature related to one of the daemons, such as scanning for viruses.

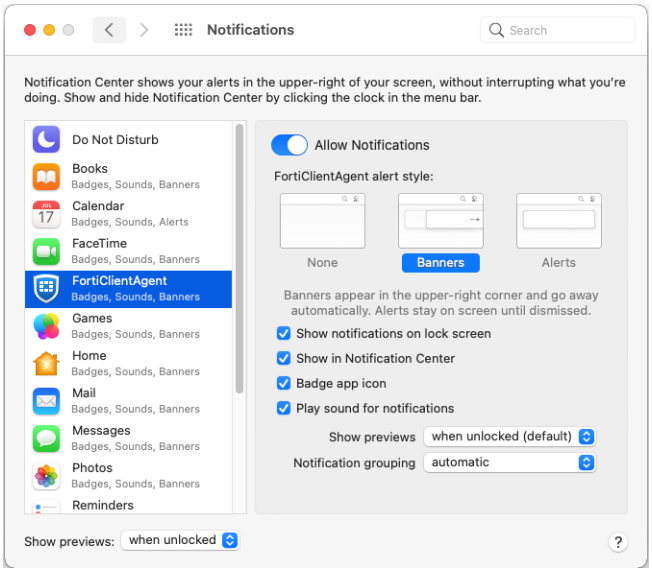


To enable notifications:

After initial installation, macOS prompts the user to enable FortiClient (macOS) notifications.



1. Go to *System Preferences* > *Notifications* > *FortiClientAgent*.
2. Toggle *Allow Notifications* on.



Additional steps may be required if using Web Filter or RTP with FortiClient (macOS). See the *FortiClient (macOS) Release Notes* for details.

Linux

The following instructions guide you though the installation of FortiClient on a Linux computer running Ubuntu, Red Hat, or CentOS. For more information, see the *FortiClient (Linux) Release Notes*.

Various CLI commands are available for FortiClient (Linux) 7.2.7. See FortiClient (Linux) CLI commands on page 123.

Installing FortiClient (Linux) requires root or sudo privileges. Once FortiClient (Linux) is installed, it has root/sudo privileges. So FortiClient (Linux) performs upgrades that FortiClient EMS triggers using the root privilege.

Installing FortiClient (Linux) using a downloaded installation file

To install on Red Hat or CentOS 8:

1. Obtain a FortiClient Linux installation rpm file.
2. In a terminal window, run the following command:
   `$ sudo dnf install <FortiClient installation rpm file> -y`
   `<FortiClient installation rpm file>` is the full path to the downloaded rpm file.

If running Red Hat 7 or CentOS 7, replace `dnf` with `yum` in the command in step 2.

To install on Ubuntu:

1. Obtain a FortiClient Linux installation deb file.
2. Install FortiClient using the following command:
   `$ sudo apt-get install <FortiClient installation deb file>`
   `<FortiClient installation deb file>` is the full path to the downloaded deb file.

Installing FortiClient (Linux) from repo.fortinet.com

To install on Red Hat or CentOS:

1. Add the repository:
   ```
   sudo yum-config-manager --add-repo
        https://repo.fortinet.com/repo/forticlient/7.2/centos/8/os/x86_64/fortinet.repo
   ```
2. Install FortiClient:
   ```
   sudo yum install forticlient
   ```

To install on Fedora:

1. Add the repository:
   ```
   sudo dnf config-manager --add-repo
        https://repo.fortinet.com/repo/forticlient/7.2/centos/8/os/x86_64/fortinet.repo
   ```
2. Install FortiClient:
   ```
   sudo yum install forticlient
   ```

To install on Ubuntu 18.04 LTS and 20.04 LTS:

1. Install the gpg key:
   ```
   wget -O - https://repo.fortinet.com/repo/forticlient/7.2/ubuntu/DEB-GPG-KEY | sudo apt-key add -
   ```
2. Add the following line in `/etc/apt/sources.list`:
   ```
   deb [arch=amd64] https://repo.fortinet.com/repo/forticlient/7.2/ubuntu/ /stable multiverse
   ```
3. Update package lists:
   ```
   sudo apt-get update
   ```
4. Install FortiClient:
   ```
   sudo apt install forticlient
   ```

To install on Ubuntu 22.04 LTS:

1. Install the gpg key:
   ```
   wget -O - https://repo.fortinet.com/repo/forticlient/7.2/debian/DEB-GPG-KEY | gpg --dearmor | sudo tee /usr/share/keyrings/repo.fortinet.com.gpg
   ```
2. Create `/etc/apt/sources.list.d/repo.fortinet.com.list` with the following content:
   ```
   deb [arch=amd64 signed-by=/usr/share/keyrings/repo.fortinet.com.gpg] https://repo.fortinet.com/repo/forticlient/7.2/debian/ stable non-free
   ```
3. Update package lists:
   ```
   sudo apt-get update
   ```
4. Install FortiClient:
   ```
   sudo apt install forticlient
   ```

Installation folder and running processes

The FortiClient installation folder is `/opt/forticlient`. In case there are issues or you need to report a bug, FortiClient logs are available in `/var/log/forticlient`.

Installing FortiClient on infected systems

The FortiClient installer always runs a quick AV scan on the target host system before proceeding with the complete installation. If the system is clean, installation proceeds as usual.

Any virus found during this step is quarantined before installation continues.

In case a virus on an infected system prevents downloading the new FortiClient package, use the following process:

1. Boot into “safe mode with networking”. The FortiClient installer requires this mode to download the latest signature packages from the Fortinet Distribution Network.
2. Run the FortiClient installer.

This scans the entire file system. A log file is generated in the logs subdirectory. If a virus is found, it is quarantined. When complete, reboot into normal mode and run the FortiClient installer to complete the installation.

Windows does not allow FortiClient installation to complete in safe mode. An error message is generated. Rebooting into normal mode is necessary to complete the installation.

Installing FortiClient as part of cloned disk images

If you configure computers using a cloned hard disk image, you must remove the unique identifier from the FortiClient application. You will encounter problems if you deploy multiple FortiClient applications with the same identifier.

This section describes how to include a custom FortiClient installation in a cloned hard disk image but remove its unique identifier. On each computer configured with the cloned hard disk image, the FortiClient application generates its own unique identifier the first time the computer is started.

To install FortiClient as part of cloned disk images:

1. Install the FortiClient application.
2. Right-click the FortiClient icon in the system tray and select *Shutdown FortiClient*.
3. From the folder where you expanded the FortiClientTools.zip file, run RemoveFCTID.exe. The RemoveFCTID tool requires administrative rights.

Do not include the RemoveFCTID tool as part of a logon script.

4. Shut down the computer.

Do not reboot the Windows operating system on the computer before you create the hard disk image. The FortiClient identifier is created before you log on.

5. Create the hard disk image and deploy it as needed.

Installing FortiClient using the CLI

You can install FortiClient using the CLI. When an EMS administrator creates a FortiClient installer as Adding a FortiClient deployment package describes, EMS creates .exe and .msi installers. You can use either to install FortiClient:

Installer file	Description
`.exe`	Includes custom modifications as configured when creating the deployment package. You can double-click the file to run the installer, or install FortiClient in the CLI.
`.msi`	You must use the .msi installer in combination with the .mst file., as the .msi file does not include any custom modifications configured when creating the deployment package. If using the .msi file, you must install FortiClient using the CLI so that you can provide the accompanying .mst file. Otherwise, the custom modifications are unavailable to FortiClient after installation.

The following table summarizes the installation options available when using the CLI. All of the following options are available if you use the .exe file. If you use the .msi file with the .mst file, not all of the following options are available, as you are constrained by the CLI options that Windows Installer permits. See Command-Line Options.

Option	Description
`/quiet`	Installation is in quiet mode and requires no user interaction.
`/passive`	Installation is in unattended mode, showing only the progress bar.
`/norestart`	Does not restart the machine after installation is complete.
`/promptrestart`	Prompts you to restart the machine if necessary.
`/forcerestart`	Always restarts the machine after installation.
`/uninstallfamily`	Uninstalls FortiClient. With this option, the FortiClient installer detects whatever version of FortiClient is installed and uninstalls it. For example, a FortiClient 7.2.7 installer can detect and uninstall an installed copy of FortiClient 7.0.0.
`/log <path to log file>`	Creates a log file in the specified directory with the specified name.

The following example installs FortiClient build 1131 in quiet mode, does not restart the machine after installation, and creates a log file with the name "example" in the c:\temp directory, using the .exe file:

```
FortiClientSetup_7.2.7.1131_x64.exe /quiet /norestart /log c:\temp\example.log
```

The following example installs FortiClient using the .msi and .mst files, and creates a log file with the name "output":

```
msiexec.exe /i "FortiClient.msi" TRANSFORMS="FortiClient.mst" /log output.log
```

Centralized FortiClient deployment

You can centrally deploy FortiClient to multiple endpoints. See:

- FortiClient EMS on page 40
- Deploying FortiClient using Microsoft AD servers on page 40
- Intune Deployment Guide

FortiClient EMS

You can deploy FortiClient to multiple endpoints using deployment configurations in EMS. See Deployment & Installers.

Deploying FortiClient using Microsoft AD servers

There are multiple ways to deploy FortiClient MSI packages to endpoints including using AD servers. See Firmware images and tools on page 27.

The following instructions are based on Microsoft Windows Server 2008. If you are using a different version of Microsoft Server, your MMC or snap-in locations may differ.

Deploying FortiClient with Microsoft AD

To deploy FortiClient with Microsoft AD:

1. On your domain controller, create a distribution point.
2. Log into the server computer as an administrator.
3. Create a shared network folder where the FortiClient MSI installer file is distributed from.
4. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient MSI installer package into this share folder.
5. Select *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
6. After selecting your domain, right-click to select a new organizational unit (OU).
7. Move all the computers you want to distribute the FortiClient software to into the newly-created OU.
8. Create a group policy object (GPO), then create the FortiClient installer package:
   a. Select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in opens. Select the OU you just created. Right-click it, *Select Create a GPO* in this domain, and link it here. Give the new GPO a name then select *OK*.
   b. Expand the GPO container and find the newly created GPO. Right-click the GPO and select *Edit*. The Group Policy Management Editor MMC Snap-in opens.
   c. Expand *Computer Configuration* > *Policies* > *Software Settings*. Right-click *Software Settings* and select *New* > *Package*.
   d. Select the path of your distribution point and FortiClient installer file and then select *Open*. Select *Assigned* and select *OK*. The package is then generated.
9. If you want to expedite the installation process, on the server and client computers, force a GPO update. The software is installed on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

Uninstalling FortiClient with Microsoft AD

To uninstall FortiClient with Microsoft AD:

1. On your domain controller, select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in opens. Expand the Group Policy Objects container and right-click the Group Policy Object you created to install FortiClient and select *Edit*. The *Group Policy Management Editor* opens.
2. Select *Computer Configuration* > *Policy* > *Software Settings* > *Software Installation*. You can see the package used to install FortiClient.
3. Right-click the package and select *All Tasks* > *Remove*. Choose *Immediately* to uninstall the software from users and computers, or *Allow* users to continue to use the software but prevent new installations. Select *OK*. The package deletes.
4. If you want to expedite the uninstall process on both the server and client computers, force a GPO update as shown in the previous section. The software is uninstalled on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and uninstall the software then.

Uninstalling FortiClient

1. The EMS administrator deregisters the endpoint. See the *FortiClient EMS Administration Guide*.
2. In FortiClient, on the *Zero Trust Telemetry* tab, disconnect from EMS. The endpoint is no longer managed by EMS.

3. Uninstall FortiClient using the Windows Add/Remove Programs application.

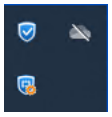
Upgrading FortiClient

For information about supported upgrade paths for FortiClient, see the *FortiClient and FortiClient EMS Upgrade Paths*.

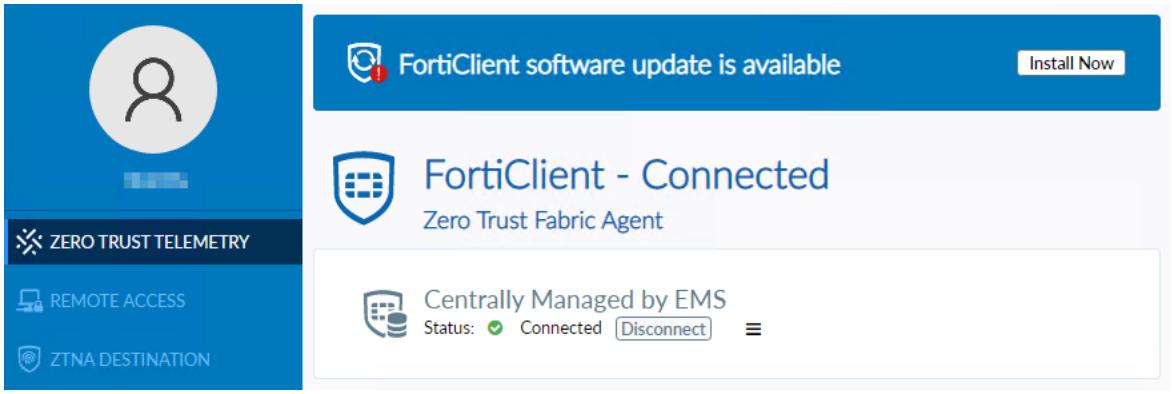
An administrator controls FortiClient upgrades for you. See EMS and automatic upgrade of FortiClient on page 21. Depending on the EMS configuration, you may be able to schedule the installation and/or reboot time. FortiClient upgrades only require a system reboot when it requires a driver upgrade.

To upgrade FortiClient:

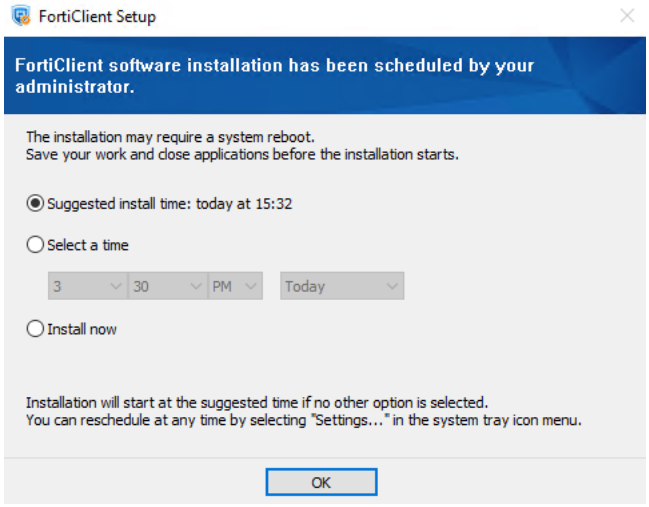
1. Consider that the EMS administrator schedules a FortiClient deployment. After the endpoint downloads the FortiClient deployment package, do one of the following to open the setup dialog:
   a. A FortiClient installation icon appears in the system tray. Double-click the icon.



   b. On the *Zero Trust Telemetry* and *About* tabs, FortiClient displays a notification banner regarding the available update. Click *Install Now*.

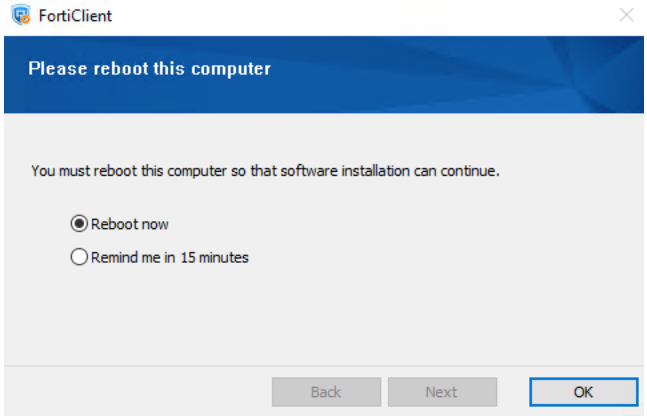


2. Select an option in the setup dialog to schedule the installation.

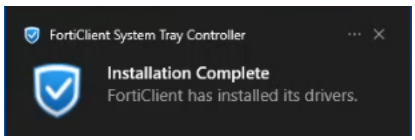


Once installation begins, you can double-click the tray icon to see the progress. If you choose not to schedule the upgrade on the endpoint, the upgrade proceeds at the time that the EMS administrator has configured. See Creating a deployment configuration.

3. After installation completes, if FortiClient requires a driver upgrade, a reboot prompt displays. You can also open the prompt from the tray icon. You can reboot now or select *Remind me in 15 minutes*. The reboot prompt reappears in 15 minutes if you select this option. You can only defer the reboot for 15 minutes once.



The system tray tooltip displays the amount of time left before the reboot will occur, and FortiClient displays warnings before the 15 minutes elapses. Attempts to open the GUI before rebooting open the reboot prompt instead of the GUI. After system reboot, drivers update and the installation process completes. The endpoint shows a tray notification stating *Installation Complete*.



Verifying ports and services and connection between EMS and FortiClient

Ports and services

If your FortiClient is installed on a domain-joined endpoints and your administrator has followed the instructions in Preparing the AD server for deployment, you can use the following CLI command to verify the SMB and RPC services are bound to ports 445 and 135, respectively:

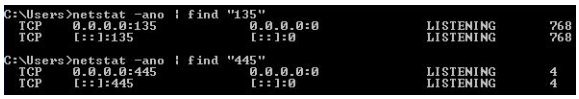
```
netstat -ano | find "<port number>"
```

`a`: displays all connections and listening ports

`n`: displays addresses and port numbers in numerical form

`o`: displays process ID (PID) associated with each connection

The following shows that Windows is listening to port TCP/135 and TCP/445 on a particular interface: 0.0.0.0 in this case. The PIDs are 768 and 4.



You can confirm the process by finding the returned PIDs on the Task Manager Details tab.

You can also use this command on the EMS server. See the *FortiClient EMS Administration Guide*.

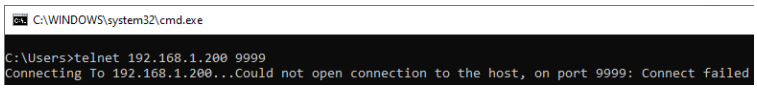
Connectivity between EMS and FortiClient

In addition to the services running correctly, there must be connectivity between EMS and the endpoint. This section defines connectivity as a route and traffic on a given port. You can use Command Prompt and the built-in Telnet application to verify this. Ensure that Telnet is enabled on your device by going to *Control Panel* > *Turn Windows features on or off*, and ensuring that the *Telnet Client* checkbox is selected. In this example, 192.168.1.200 is the EMS server IP address, and 8013 is the port that is being checked:

```
telnet 192.168.1.200 8013
```

If the command is successful, Command Prompt returns _. Since the service on 8013 is not Telnet, this is the expected result.

If the command is unsuccessful, Command Prompt returns a warning that the connection could not be opened.



User details

You can view and edit user details by clicking the user avatar in the upper left corner of FortiClient. Depending on your EMS configuration, FortiClient may display a notification where you can also specify your user details.

Viewing user details

When an administrator configures FortiClient to send logs to FortiAnalyzer or FortiManager, some user details are visible in FortiAnalyzer, FortiManager, and FortiOS. See Sending logs and Windows host events to FortiAnalyzer or FortiManager on page 102.

Click the user avatar in the upper left corner of FortiClient to view the following information:

Option	Description
Full name	Displays the endpoint user's name if added by the endpoint user.
Phone	Displays the endpoint user's phone number if added by the endpoint user. See Retrieving user details from cloud applications on page 46 and Adding your phone number and email address manually on page 47.
Email	Displays the endpoint user's email address if added by the endpoint user. See Retrieving user details from cloud applications on page 46 and Adding your phone number and email address manually on page 47.
Get personal info from	Displays the source of the endpoint user's personal information and the last time the information was updated. The options are user-specified, from the OS, and from cloud applications: LinkedIn, Google, and Salesforce. Depending on the EMS configuration, not all options may be available. You can click *User Input* to select an image or take a webcam photo to use as the user avatar. You can provide information to FortiClient from an account for a cloud application, such as a Linkedin, Google, or Salesforce account. After the endpoint user logs into the account, FortiClient attempts to retrieve the following information when available: name, avatar, phone number, and email address. See Retrieving user details from cloud applications on page 46. By default, FortiClient displays user details from the endpoint OS and sends this information to EMS. If you provide details using one of the methods above, FortiClient displays those details and sends that information to EMS instead.
Status	Displays whether the endpoint is online or offline, on- or off-fabric. See On-/off-fabric status with EMS on page 52.
Hostname	Displays the hostname of the endpoint where FortiClient is installed.

Option	Description
Domain	Displays the name of the domain to which the endpoint is connected, if applicable.
Zero Trust Tags	Displays the tags that have been applied to the endpoint depending on the Zero Trust tagging rules configured in EMS. Tags may or may not be visible depending on the EMS configuration.
FortiGuard Outbreak Detections	Displays the tags that have been applied to the endpoint depending on the FortiGuard outbreak detection rules configured in EMS. Tags may or may not be visible depending on the EMS configuration.

Retrieving user details from cloud applications

You can direct FortiClient to retrieve information about you from one of the following cloud applications, if you have an account. Depending on the EMS configuration, not all options may be available:

- LinkedIn
- Google
- Salesforce

FortiClient attempts to retrieve the following information after you log in:

- Username
- Phone number
- Email address
- Picture

FortiClient displays the retrieved information. The information is encrypted and only FortiClient can access it. FortiClient does not retrieve or save the password for your social media account.

Consider a situation where two users, User A and User B, use the same computer:

1. User A logs into the computer and provides their social media information in FortiClient.
2. FortiClient retrieves and displays User A's social media information while User A is logged in.
3. User A logs out of the computer.
4. User B logs into the computer.
5. FortiClient no longer displays User A's social media information. If User B previously provided their social media information, this automatically displays. Otherwise FortiClient displays the avatar for User B's OS account. If it was not previously provided, User B provides their social media information, which displays in FortiClient.
6. User B logs out and User A logs in. FortiClient displays User A's social media information.

If User A or B do not log out of their account and instead lock the screen or switch accounts, FortiClient may display either user's social media information to both users.

Although FortiClient can retrieve the endpoint user's username from cloud applications, the retrieved username does not display in FortiClient. Instead, the retrieved username is included in FortiClient logs with the phone number and email address. You can view log content in FortiOS, FortiAnalyzer, and FortiManager. See Sending logs and Windows host events to FortiAnalyzer or FortiManager on page 102.

You can manually specify an avatar for FortiClient to use and edit the phone number and email address. See Specifying the user avatar manually on page 47 and Adding your phone number and email address manually on page 47.

1. Click the user avatar in the upper left corner of FortiClient.
2. Click one of the following links:
   - *Linkedin*
   - *Google*
   - *Salesforce*
3. A browser window opens. Log into your account.
4. Click *Allow* to grant FortiClient permission to use your information.

Adding your phone number and email address manually

Although FortiClient can retrieve information from a cloud application account, you can manually add or edit a phone number or email address in FortiClient.

The phone number can be a maximum of 30 characters and can include any of the following characters: *0123456789-+x*

To add a phone number and email address manually:

1. Click the user avatar in the upper left corner of FortiClient.
2. Click *Add Phone*, enter the phone number, and press *Enter*.
3. Click *Add Email*, enter the email address, and press *Enter*.

To edit a phone number or email address:

1. Click the user avatar in the upper left corner of FortiClient.
2. Click the phone number or email address, edit the information, and press *Enter*.

Specifying the user avatar manually

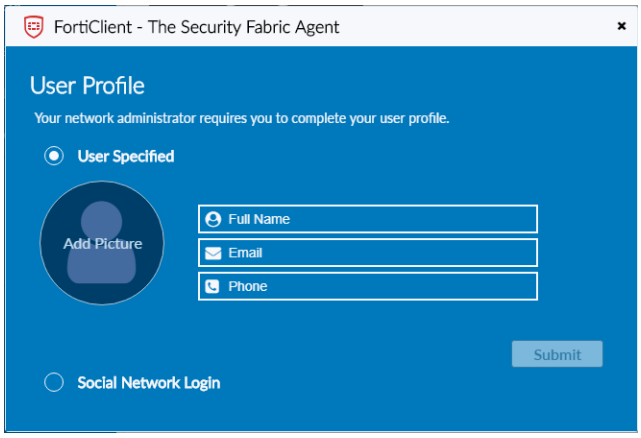
Although FortiClient can retrieve an avatar from Windows, an AD server, or a cloud application, you can add an avatar to FortiClient by taking a photo or uploading an avatar .

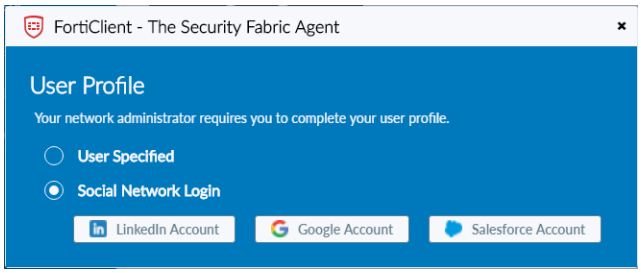
1. Click the user avatar in the upper left corner of FortiClient.
2. Under *Get personal info from*, click *User Input*.

3. Take a photo using the webcam, or select an existing image file.

User Profile notification

Depending on your EMS configuration, FortiClient may display a notification where you can also specify your user details. You can enter your identity information manually or log in to your LinkedIn, Google, or Salesforce account for FortiClient to retrieve the information from that account. Not all options may be available depending on your EMS configuration. If you close the notification without specifying your identity, the notification displays every ten minutes until you submit your identity information.





Zero Trust Telemetry

The *Zero Trust Telemetry* tab displays whether FortiClient Telemetry is connected to EMS. You can use the *Zero Trust Telemetry* tab to manually connect FortiClient Telemetry to EMS and to disconnect FortiClient Telemetry from EMS.

FortiClient Telemetry

FortiClient can use a server IP address/FQDN or invitation code to connect FortiClient Telemetry to EMS or an invitation code to connect Telemetry to FortiClient Cloud.

Telemetry data

When FortiClient Telemetry is connected to EMS, FortiClient collects the following data about the endpoint and its workload and sends it to EMS:

- Hardware information, such as MAC addresses
- Software information, such as the OS version on the endpoint
- Identification information, such as username, avatar, and hostname
- Vulnerability information that the vulnerability scanning module reports

When EMS is participating in the Security Fabric, the Security Fabric uses the information to understand the endpoint and its workload to better protect it.

Connecting FortiClient Telemetry after installation

After FortiClient software installation completes on an endpoint, you can connect FortiClient to EMS. After FortiClient Telemetry connects to EMS, FortiClient receives an endpoint policy from EMS. A system tray bubble message displays once the download is complete. The endpoint policy may contain an endpoint profile of configuration information as well as a Telemetry server list.

You can use these processes to connect Telemetry to EMS after the FortiClient endpoint reboots, rejoins the network, or encounters a network change.

To automatically connect to an on-premise EMS:

FortiClient may automatically launch and connect Telemetry to the EMS server that created the installed deployment package.

1. When FortiClient locates EMS, the *Connecting FortiClient Telemetry* dialog displays when EMS requests the FortiClient telemetry connection key. The following options are available:

Endpoint User	Displays the name of the endpoint user logged into the endpoint.
Logged into Domain	Displays the domain name if applicable.
Hostname	Displays the endpoint name.
FortiClient Telemetry Connection Key	Enter the connection key.
Remember FortiClient Telemetry Connection Key	Select for FortiClient to remember the connection key.
Remember this Endpoint Management Server (EMS)	Select for FortiClient to remember the IP address of the EMS you are connecting Telemetry to. See Remembering gateway IP addresses on page 51.

2. Click *OK* to connect FortiClient Telemetry to the identified EMS.

To manually connect FortiClient to on-premise EMS:

1. Based on your EMS configuration, you will do one of the following:
   a. If your FortiClient automatically launches after installation and prompts you for credentials, such as Active Directory credentials, enter the credentials. This connects FortiClient to EMS.
   b. If your FortiClient does not automatically launch after installation, do the following:
      i. Launch FortiClient.
      ii. On the *Zero Trust Telemetry* tab, in the *Register with Zero Trust Fabric* field, manually enter the EMS IP address or invitation code.
      iii. If multitenancy is enabled on EMS and you must register to a specific site, click the *Switch to IP connect* button, then enter the site name in the *Site Name* field. If multitenancy is enabled on EMS but you do not provide a site name, FortiClient connects to the default site.

To connect to FortiClient Cloud:

1. After initial installation, FortiClient should automatically register to FortiClient Cloud. If FortiClient did not automatically register to FortiClient Cloud, enter the invitation code in the *Register with Zero Trust Fabric* field on the *Zero Trust Telemetry* tab in FortiClient. Your EMS administrator should have provided the code to you.
2. Click *Connect*. FortiClient is managed by FortiClient Cloud.

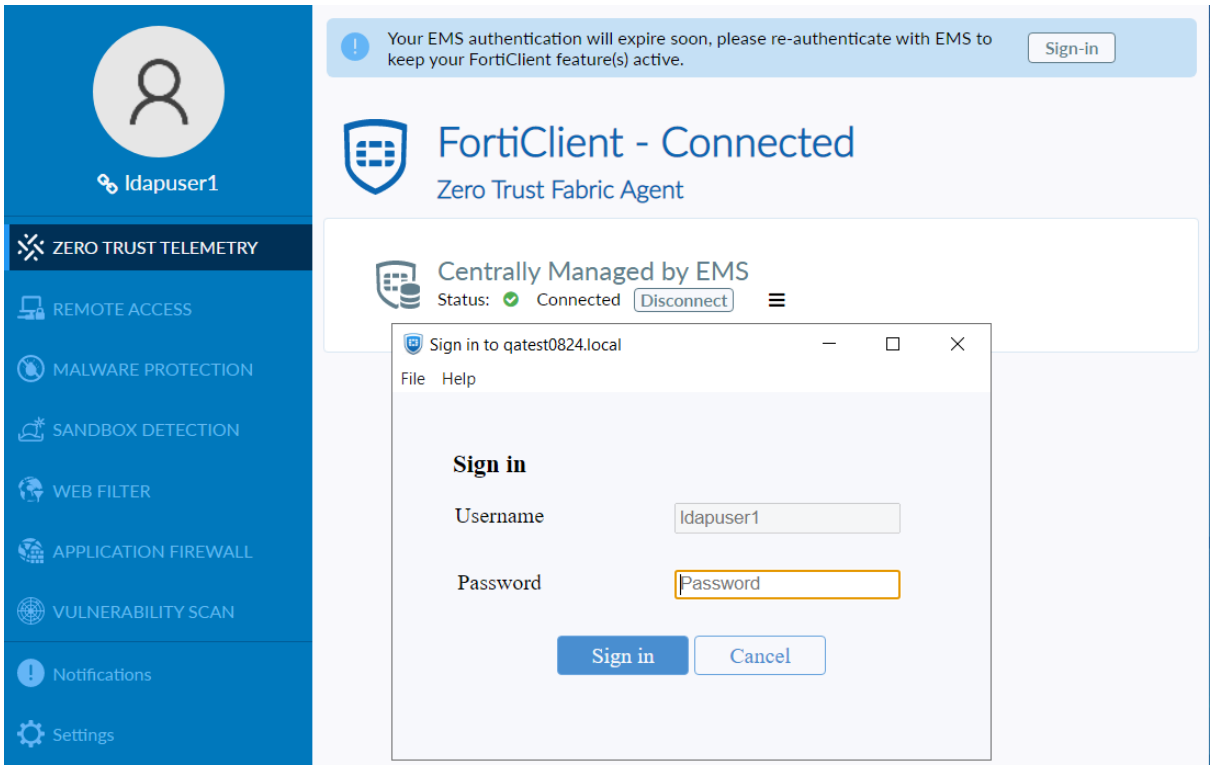
Reauthenticating your identity

If your EMS administrator has configured a reauthentication timeout, you may need to periodically reauthenticate to maintain your connection to EMS. This is configured using the *User Verification Period* field in EMS. See Configuring EMS settings.

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.



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.

Remembering gateway IP addresses

When you confirm Telemetry connection to EMS, you can instruct FortiClient to remember the EMS IP address. If a connection key is required, FortiClient remembers the connection key too. FortiClient can remember up to 20 IP addresses for EMS.

The remembered IP addresses display in the local gateway IP list. FortiClient can use the remembered gateway IP addresses to automatically connect to EMS.

See Forgetting a gateway IP address on page 52.

To remember a gateway IP address:

1. In the *Connecting FortiClient Telemetry* dialog, select the *Remember this Endpoint Management Server (EMS)* checkbox.
2. Click *Accept*. FortiClient remembers the IP address and password, if applicable.

Forgetting a gateway IP address

When you instruct FortiClient to forget an IP address for EMS, FortiClient Telemetry does not use the IP address to automatically connect to EMS when rejoining the network.

To forget a gateway IP address:

1. On the *Zero Trust Telemetry* tab, click the menu icon beside the *Disconnect* button.
2. In the *Remembered Server List*, click *Forget* beside the IP addresses you no longer want FortiClient to remember.

Disconnecting FortiClient Telemetry

You must disconnect FortiClient Telemetry from EMS to connect to another EMS or to disable and uninstall FortiClient.

An EMS administrator may disconnect FortiClient for you. This is sometimes referred to as deregistering FortiClient. When an EMS administrator disconnects FortiClient Telemetry for you, the Telemetry server list is also removed from FortiClient.

To disconnect FortiClient Telemetry:

1. On the *Zero Trust Telemetry* tab, click *Disconnect*. A confirmation dialog displays.
2. Click *Yes* to disconnect FortiClient Telemetry from EMS.

After you disconnect FortiClient Telemetry from EMS, FortiClient Telemetry automatically connects with EMS when you rejoin the network.

Compliance with EMS and FortiOS

In FortiClient 7.2.7, compliance depends on EMS and FortiOS. This feature is only available if using FortiClient 7.2.7 with EMS 7.2.7 and FortiOS 7.2.7.

The administrator can define Zero Trust tagging rules in EMS based on criteria such as certificates, the logged in domain, files present, OS versions, running processes, and registry keys. When a FortiClient endpoint registers to EMS, EMS dynamically groups the endpoint based on the Zero Trust tagging rules. FortiOS can receive the dynamic endpoint groups from EMS and use them to create dynamic firewall policies. The endpoint may be unable to access the network based on the Zero Trust tagging rules.

See the *FortiClient EMS Administration Guide*.

On-/off-fabric status with EMS

Endpoints must connect FortiClient Telemetry to EMS for FortiClient to use an on-fabric, off-fabric, or offline status.

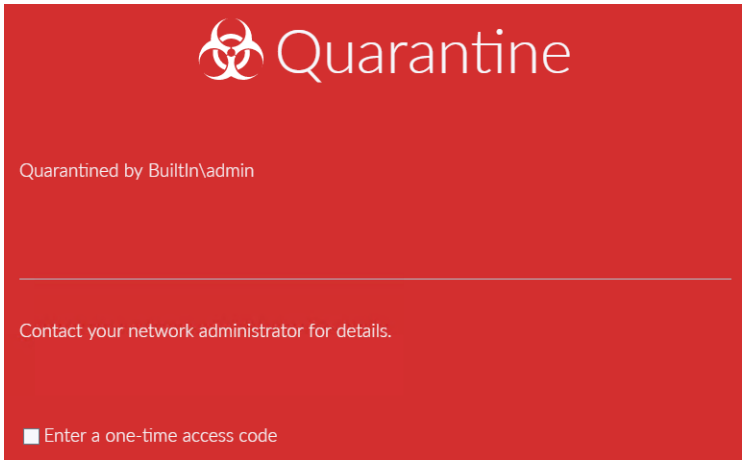
When FortiClient connects Telemetry to EMS, FortiClient determines whether the endpoint has an on- or off-fabric status. See On-fabric Detection Rules.

Logging to FortiAnalyzer

When FortiClient endpoints are on-fabric and logging to FortiAnalyzer is configured, FortiClient logs are sent to FortiAnalyzer. However, when FortiClient endpoints are off-fabric, and FortiAnalyzer is not reachable, FortiClient logs are held for the log retention period, and sent to FortiAnalyzer when FortiClient is on-fabric again. By default, FortiClient logs are held for 90 days. You can control the log retention period by using the `<log_retention_days>` element in the XML configuration. See the *FortiClient XML Reference Guide*.

Quarantined endpoints

In certain situations, an administrator may quarantine an endpoint. When an endpoint is quarantined, the following page displays, and the endpoint user loses network access. Contact your system administrator for assistance.



If the EMS administrator customized the quarantine message, the message may display differently than the example above. In the following example, the EMS administrator has added a phone number to the message.

After the endpoint is quarantined, you can select the *Enter a one-time access code* checkbox and enter the code to access the FortiClient GUI. You can obtain the access code from the EMS administrator.

After using the code to access the FortiClient GUI, you can remove the endpoint from quarantine by clicking the *Unquarantine* button.

Remote Access

FortiClient supports both IPsec and SSL VPN connections to your network for remote access. Administrators can use EMS to provision VPN configurations for FortiClient and endpoint users can configure new VPN connections using FortiClient.

When configuring and forming VPN connections, note that in FortiClient the user password is saved only for the user who entered it. It is not accessible in FortiClient to the device's other users. All other information is visible in FortiClient when other users are logged into the same device.

Configuring VPN connections

You can configure SSL and IPsec VPN connections using FortiClient.

Configuring an SSL VPN connection

To configure an SSL VPN connection:

1. On the *Remote Access* tab, click *Configure VPN*.
2. Select *SSL-VPN*, then configure the following settings:

Connection Name	Enter a name for the connection.
Description	(Optional) Enter a description for the connection.
Remote Gateway	Enter the remote gateway's IP address/hostname. You can configure multiple remote gateways by separating each entry with a semicolon. If one gateway is not available, the VPN connects to the next configured gateway.
Customize port	Change the port. The default port is 443.
Enable Single Sign On (SSO) for VPN Tunnel	Enable SAML SSO for the VPN tunnel. For this feature to function, the administrator must have configured the necessary options on the Service Provider and Identity Provider. See SAML support for SSL VPN.
Use external browser as user-agent for saml user authentication	FortiClient can use a browser as an external user-agent to perform SAML authentication for SSL VPN tunnel mode, instead of the FortiClient embedded login window. If a user has already authenticated using SAML in the default browser, they do not need to reauthenticate in the FortiClient built-in browser. Available if *Enable Single Sign On (SSO) for VPN Tunnel* is enabled. See Using a browser as an external user-agent for SAML authentication in an SSL VPN connection.

Client Certificate	Select *Prompt on connect* or the certificate from the dropdown list.
Authentication	Select *Prompt on login* or *Save login*. The *Disable* option is available when *Prompt on connect* or a certificate is configured for *Client Certificate*.
Username	If you selected *Save login*, enter the username to save for the login.
Enable Dual-stack IPv4/IPv6 address	Enable or disable FortiClient to establish a dual stack SSL VPN tunnel to allow both IPv4 and IPv6 traffic to pass through. See Dual stack IPv4 and IPv6 support for SSL VPN.
+	Select the add icon to add a new connection.
-	Select a connection and then select the delete icon to delete a connection.

3. Click *Save* to save the VPN connection.

FortiClient supports split DNS tunneling for SSL VPN portals, which allows you to specify which domains the DNS server specified by the VPN resolves, while the DNS specified locally resolves all other domains. This requires configuring split DNS support in FortiOS. Microsoft Windows 8.1 does not support this feature.

If using FortiClient on a Windows Server 2016 machine, ensure that you disable IE Enhanced Security. Otherwise, SSL VPN may not function as configured.

Configuring an IPsec VPN connection

FortiClient connects to IPsec VPN only when it is connected to EMS and EMS is part of a Fortinet Security Fabric with a FortiGate. Otherwise, FortiClient cannot connect to the IPsec VPN tunnel.

FortiClient (Linux) does not support creating personal IPsec VPN tunnels.

To configure an IPsec VPN connection:

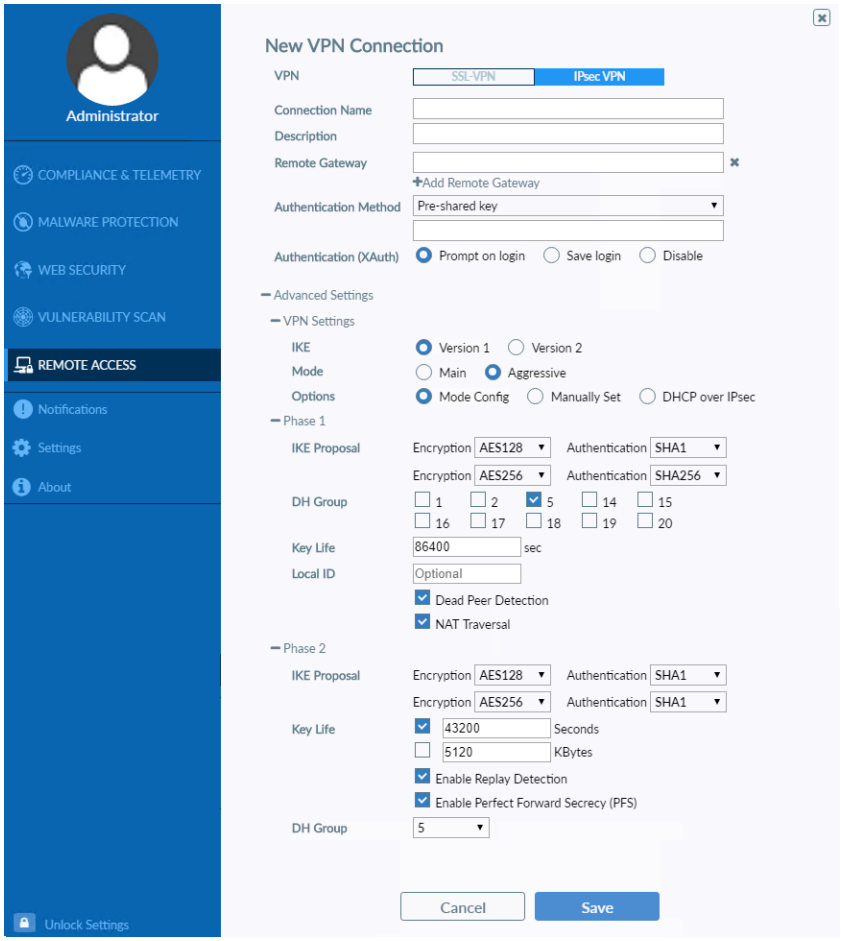
1. On the *Remote Access* tab, click *Configure VPN*.
2. Select *IPsec VPN*, then configure the following settings:

Connection Name	Enter a name for the connection.
Description	(Optional) Enter a description for the connection.
Remote Gateway	Enter the remote gateway IP address/hostname. You can configure multiple remote gateways. If one gateway is not available, the VPN connects to the next configured gateway.
Authentication Method	Select *X.509 Certificate* or *Pre-shared Key* in the dropdown list. When you select *x.509 Certificate*, select *Prompt on connect* or a certificate from the list.

Authentication (XAuth)	Select *Prompt on login*, *Save login*, or *Disable*. Available if IKE version 1 is selected.
Authentication (EAP)	Select *Prompt on login*, *Save login*, or *Disable*. Available if IKE version 2 is selected.
Failover SSL VPN	If the IPsec VPN connection fails, FortiClient attempts to connect to the specified SSL VPN tunnel.
Enable Single Sign On (SSO) for VPN Tunnel	Enable SAML SSO for the VPN tunnel. For this feature to function, the administrator must have configured the necessary options on the service and identity providers (IdP).
Customize port	Enter the port number that FortiClient uses to communicate with the FortiGate, which acts as the SAML service provider.
Username	If you selected *Save login*, enter the username to save for the login.
Advanced Settings	Configure VPN settings, phase 1, and phase 2 settings.
VPN Settings	
IKE	Select Version 1 or Version 2.
Mode	Available if IKE version 1 is selected. Select one of the following: • *Main*: Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*: Phase 1 parameters are exchanged in a single message with authentication information that is not encrypted. Although *Main* mode is more secure, you must select *Aggressive* mode if there is more than one dialup phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier (local ID).
Options	Select one of the following: • *Mode Config*: IKE Mode Config can configure host IP address, domain, DNS and WINS addresses. • *Manually Set*: Manual key configuration. If one of the VPN devices is manually keyed, the other VPN device must also be manually keyed with the identical authentication and encryption keys. Enter the DNS server IP address and the IP address and subnet values to assign. Select the checkbox to enable split tunneling. • *DHCP over IPsec*: DHCP over IPsec can assign an IP address, domain, DNS and WINS addresses. Select the checkbox to enable split tunneling.
Phase 1	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required.

		You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
	IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the dropdown lists.
	DH Group	Select one or more Diffie-Hellman groups. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups results in failed negotiations.
	Key Life	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172,800 seconds.
	Local ID	Enter the local ID (optional). This local ID value must match the peer ID value given for the remote VPN peer's peer options.
	Dead Peer Detection	Select this checkbox to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.
	NAT Traversal	Select the checkbox if a NAT device exists between the client and the local FortiGate unit. The client and the local FortiGate unit must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Phase 2		Select the encryption and authentication algorithms that are proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals you specify must match configuration on the remote peer.
	IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the dropdown lists.
	Key Life	The *Key Life* setting sets a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.
	Enable Replay Detection	Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them.
	Enable Perfect Forward Secrecy (PFS)	Select the checkbox to enable perfect forward secrecy (PFS). PFS forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time.

	DH Group	Select one Diffie-Hellman (DH) group. This must match the DH group the remote peer or dialup client uses.
+		Select the add icon to add a new connection.
-		Select a connection and then select the delete icon to delete a connection.



3. Click *Save* to save the VPN connection.

Connecting VPNs

You can connect VPN tunnels to FortiGate:

Connecting to SSL or IPsec VPN

Depending on the FortiClient configuration, you may also have permission to edit an existing VPN connection and delete an existing VPN connection.

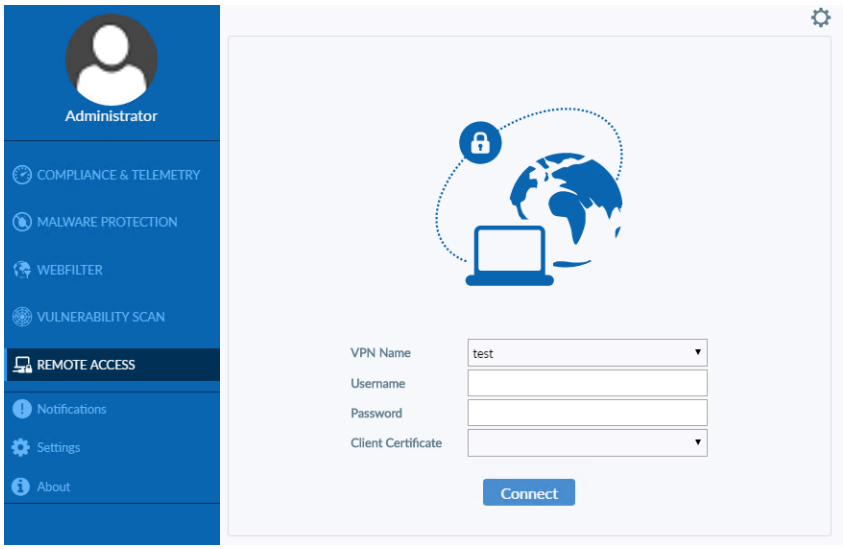
Internet Explorer's SSL and TLS settings should be the same as those on the FortiGate.

For FortiClient (macOS), VPN connections requriing FIDO2 authentication is only supported with FortiOS 7.0.1 and later versions.

To connect to SSL or IPsec VPN:

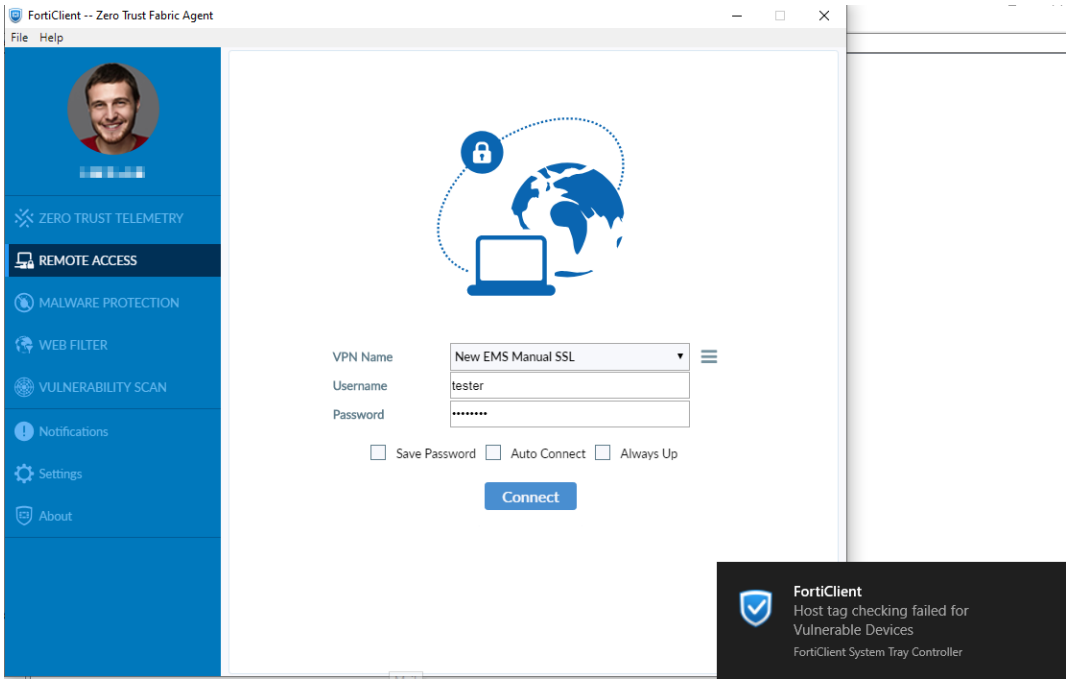
1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
   Optionally, you can right-click the FortiTray icon in the system tray and select a VPN configuration to connect.

   Provisioned VPN connections are listed under *Corporate VPNs*. Locally configured VPN connections are listed under *Personal VPNs*.



2. Enter your username and password.
3. If a certificate is required, select a certificate. If the VPN tunnel was configured to require a certificate, you must select a certificate. If no certificate is required, the option is hidden in FortiClient. Your administrator may have configured FortiClient to automatically locate a certificate for you.
4. Click the *Connect* button. Depending on the configuration received from EMS, you may also need to accept a disclaimer message to establish the connection.
   When connected, FortiClient displays the connection status, duration, and other relevant information. You can browse your remote network. Click the *Disconnect* button when you are ready to terminate the VPN session.

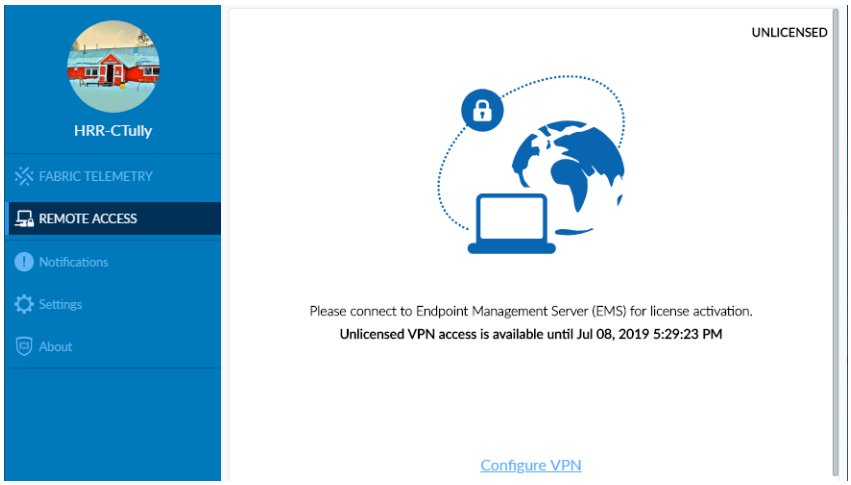
   Based on the Zero Trust tagging rules that your EMS administrator has configured, your endpoint may be unable to connect to VPN. The following shows the notification that the you see when your connection to the VPN tunnel is prohibited due to the applied Zero Trust tags. After you fix the vulnerabilities, FortiClient is allowed to establish the VPN connection.



Free 30-day VPN access

For 30 days after initial FortiClient installation, you can configure and establish a VPN connection to a FortiGate, allowing the endpoint to reach an EMS behind a FortiGate. This is especially useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license.

The following shows the GUI in this scenario. You can see that the user can access the VPN feature until July 8, 2019, meaning that they initially installed FortiClient 30 days earlier, on June 8, 2019. If the user does not use a VPN tunnel to activate their FortiClient license by 5:29 PM on July 8, as shown, FortiClient revokes the VPN access and all FortiClient features, including VPN, stop working.



Following successful registration to EMS, FortiClient receives a full license if available from EMS. EMS enables all FortiClient features that are configured on the assigned endpoint profile and were included when installing FortiClient.

If FortiClient was registered to EMS and licensed for VPN, then becomes unregistered, the free 30-day VPN access becomes available again.

If FortiClient goes offline after registering to EMS, FortiClient features remain enabled for 30 days. You can still establish a VPN connection to the FortiGate in this scenario.

Connecting VPN with FortiToken Mobile

VPN connections may require network authentication that uses a token from FortiToken Mobile, an application that runs on Android and iOS devices. For information about FortiToken Mobile, see the Fortinet Document Library.

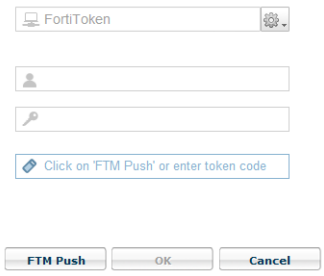
You can configure FortiGate to let you push a token from FortiToken Mobile to FortiGate to complete network authentication when connecting VPNs. When configured, you can select the push token option by clicking *FTM Push* in FortiClient. This notifies the FortiGate that you choose to use the push token option. Following this, you receive a notification of the authentication request on your device that has FortiToken Mobile installed. On your device, you can tap the notification and follow the instructions to allow or deny the authentication requests.

If a push token is not configured, you must enter a token code from FortiToken Mobile into FortiClient when connecting VPNs.

You must have available the device with FortiToken Mobile installed to complete this procedure.

To connect VPN with FortiToken Mobile using push notifications:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
2. Enter your username and password and click the *Connect* button. The *Click on 'FTM Push' or enter token code* box displays.



3. Click *FTM Push*. Your device with FortiToken Mobile installed receives a notification.
4. On your device with FortiToken Mobile installed, tap the notification and follow the instructions to allow the authentication request and complete network authentication without typing the token code. You can also deny the authentication request, or do nothing and let the notification request expire.

To connect VPN with FortiToken Mobile by entering a token code:

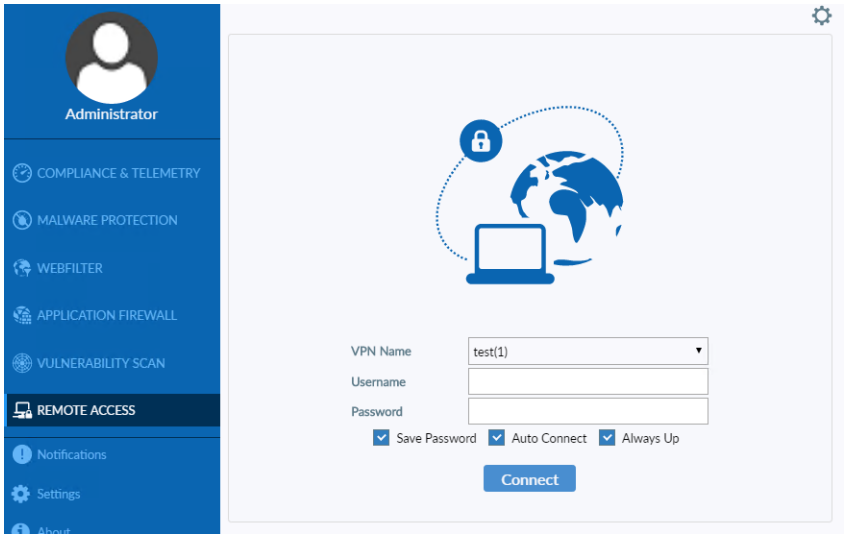
1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
2. Enter your username and password and click the *Connect* button. The *Enter token code* box displays.
3. Enter the token code from FortiToken Mobile and click *OK* to complete network authentication.

Save password, auto connect, and always up

When an administrator uses EMS to configure a profile for FortiClient, the administrator can configure an IPsec or SSL VPN connection to FortiGate and enable the following features:

Feature	Description
Save Password	Allows the user to save the VPN connection password in FortiClient. Disabling *Save Password* deselects *Auto Connect* and *Always Up*.
Auto Connect	When FortiClient launches, the VPN connection automatically connects. Automatic connection to the VPN tunnel may fail if the endpoint boots up with a user profile set to automatic logon. See Appendix E - VPN autoconnect on page 132 for configuration examples. Enabling autoconnect enables *Save Password*. Autoconnect tunnels pushed from EMS have *Save Password* and *Auto Connect* enabled and grayed out.
Always Up (keep alive)	When selected, the VPN connection is always up. If the connection fails, possibly due to network errors, FortiClient attempts to reconnect. If credentials (username and password) are saved, FortiClient attempts to reconnect silently. If credentials are insufficient (for instance, multifactor authentication is required or password is not saved), FortiClient prompts for credentials. Enabling always up enables *Save Password*.

After FortiClient Telemetry connects to EMS, FortiClient receives a profile from EMS that contains IPsec and/or SSL VPN connections to FortiGate. The following example shows an SSL VPN connection named *test(1)*.



If the VPN connection fails, a popup displays to inform you about the connection failure while FortiClient continues trying to reconnect VPN in the background.

Depending on the VPN configuration, the popup may include a *Cancel* button. If you click the *Cancel* button, FortiClient stops trying to reconnect VPN.

Access to certificates in Windows Certificates Stores

On a Windows system, you can view certificates by using an MMC (Microsoft Management Console) snap-in called Certificates console. For more information, see the following Microsoft TechNet articles:

- *Add the Certificates Snap-in to an MMC*
- *Display Certificate Stores*

The Certificates console offers the following snap-in options:

- My user account
- Service account
- Computer account

You can select one or more snap-in options, which display in the Certificates console. FortiClient typically searches for certificates in one of the following accounts:

- User account – contains certificates for the logged on user
- Computer account – contains certificates for the local computer

If the certificate is in the local computer account, FortiClient can typically access the certificate. A certificate from the local computer account may be used to establish an IPsec VPN connection, regardless of whether the logged on user is an administrator or a non-administrator. For SSL VPN and IPsec VPN, the administrator needs to grant permission to users who are non-administrators to access the private key of the certificate. Otherwise, non-administrators cannot use the certificate in the computer account to establish SSL VPN connections. This restriction does not apply to any user with administrator level permission.

If the certificate is in the user account, FortiClient can access the certificate, if the user has already successfully logged in, and the same user imported the certificate. In all other scenarios, FortiClient may be unable to access the certificate.

The following table summarizes when FortiClient can (yes) and cannot (no) locate the certificate for users who are logged into the endpoint and connecting VPN tunnels:

Account	Connect VPN using FortiClient GUI or FortiTray	
	Logged in user with admin privilege	Logged in user with non-admin privilege
User account	Yes, certificate found, if the same administrator user imported the certificate	Yes, certificate found, if the same user imported the certificate
Computer account	Yes, certificate found	IPsec VPN: Yes, certificate found, if access permission granted to private key SSL VPN: Yes, certificate found, if access permission granted to private key
SmartCard	Yes, certificate found, if same user that was logged on at the time card was inserted	Yes, certificate found, if same user that was logged on at the time card was inserted

When a user imports a certificate into the user account, a different logged on user cannot access the same certificate.

A certificate on a smart card is imported into the user account of the logged on user. As a result, the same conditions apply as with the user account.

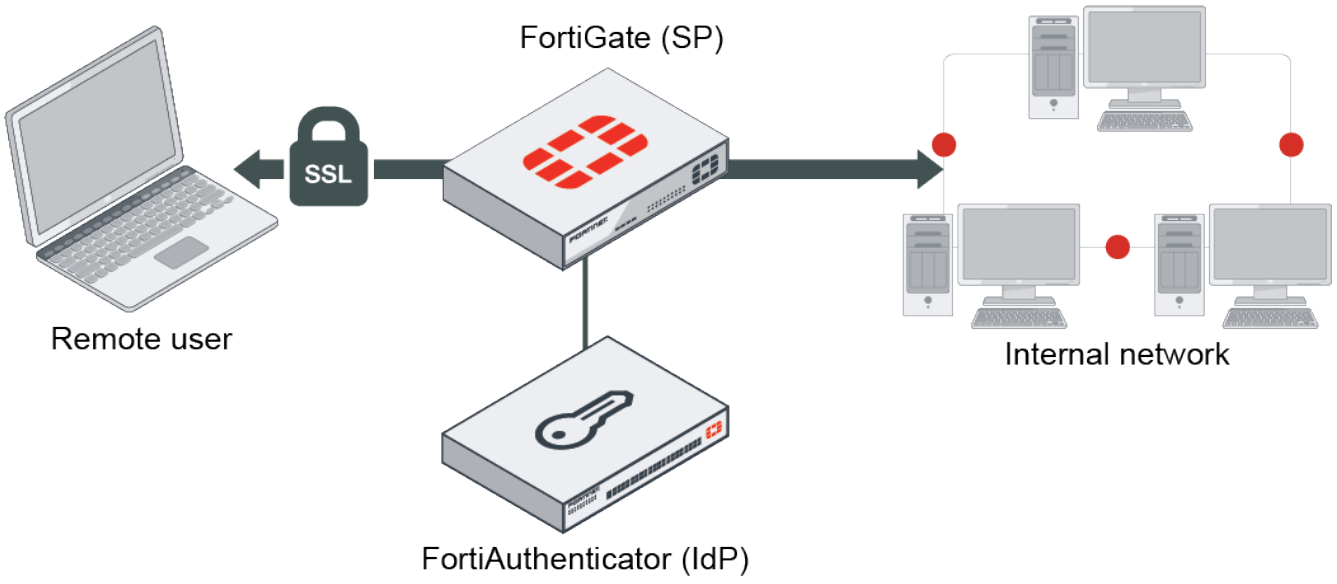
FortiClient (Linux) does not support smart card.

The following table summarizes when FortiClient can (yes) and cannot (no) locate the certificate before a user logs into the endpoint:

Account	Unknown user before logging into Windows
User account	No certificate found
Computer account	Yes certificate found
SmartCard	No certificate found

SAML support for SSL VPN

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



This process is as follows:

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

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

To configure the FortiGate as the SP:

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

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

2. Add the SAML user to the user group:

```
config user group
   edit "saml_grp"
      set member "saml-user"
   next
end
```

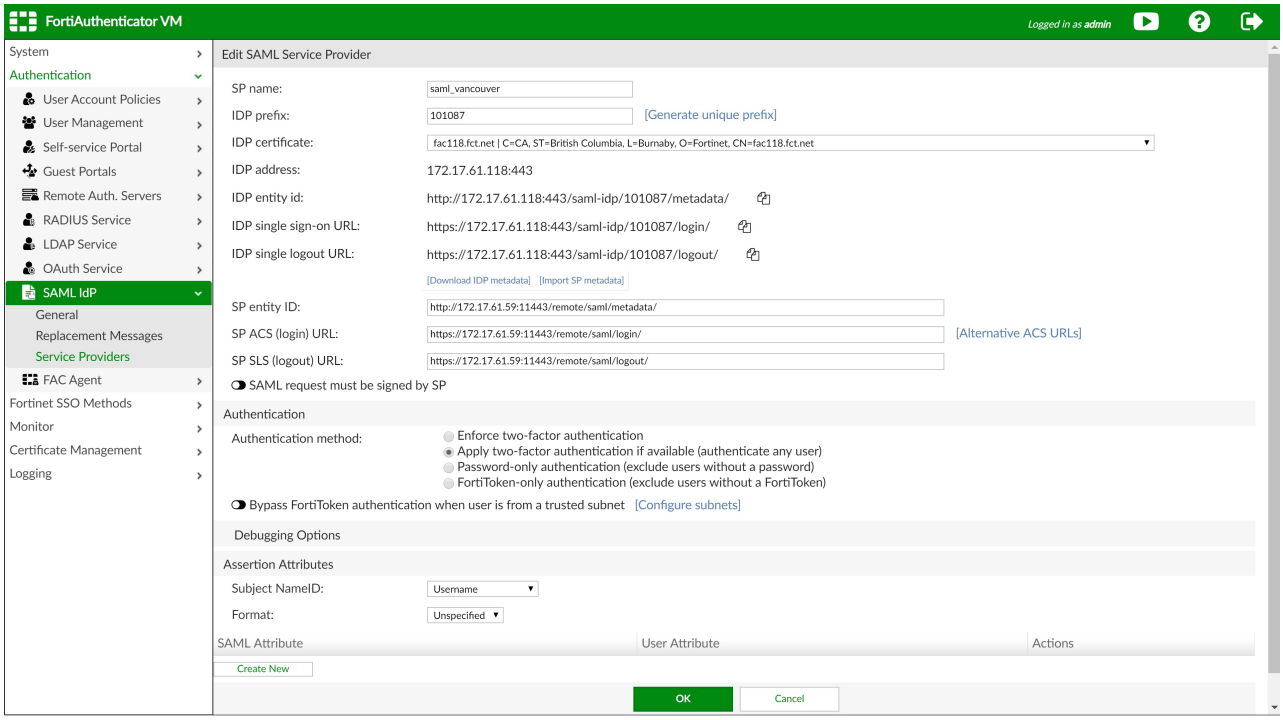
3. Set the SAML group in SSL VPN settings:

```
config vpn ssl settings
```

```
    config authentication-rule
      edit 1
        set groups "saml-group"
        set portal "full-access"
      next
    next
end
```

To configure FortiAuthenticator as the IdP:

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



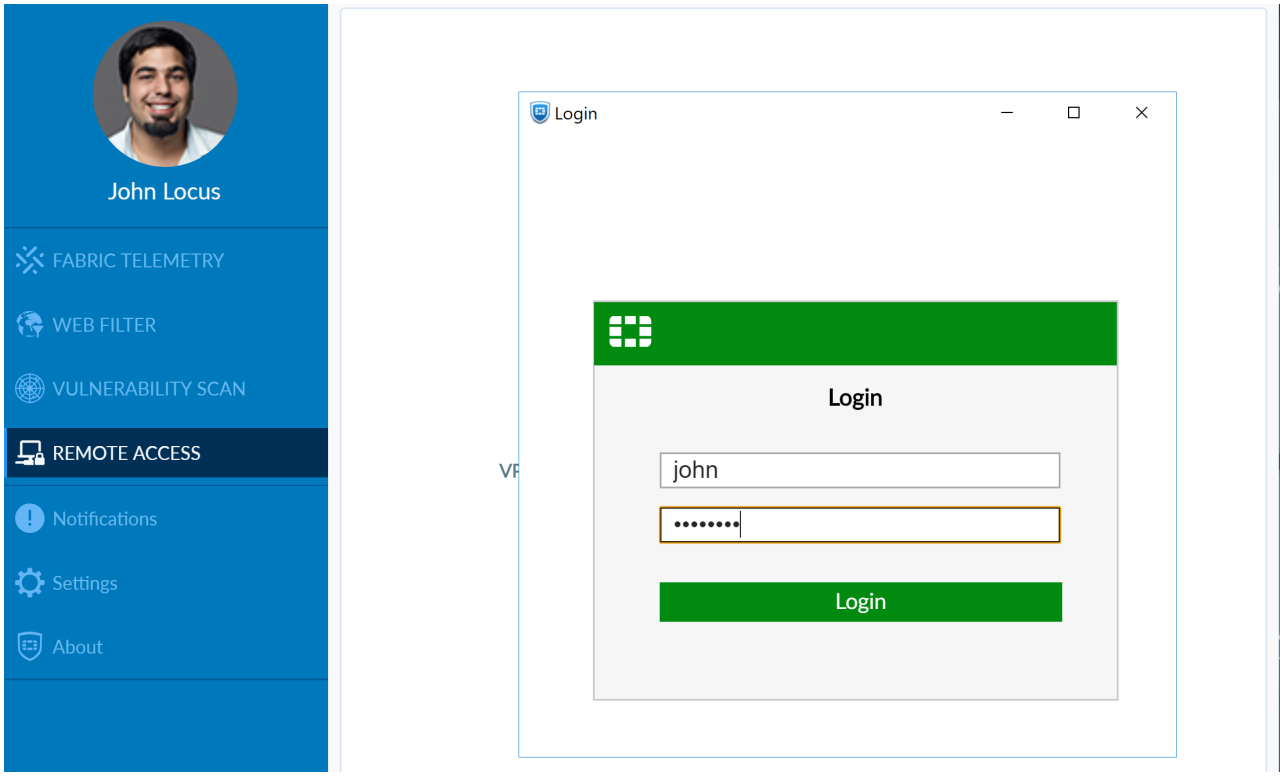
4. To add a local user, go to *Authentication* > *User Management* > *Local User*, then click *Create New*. Configure the local user as desired.
5. To import RADIUS users, go to *Authentication* > *User Management* > *Remote User* > *RADIUS Users*. Import the desired RADIUS server.
6. To import LDAP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

To configure SAML SSO authentication for FortiClient:

- To configure SAML SSO authentication for a corporate VPN tunnel in EMS, go to Endpoint Profiles and select the desired profile. On the *XML Configuration* tab, configure `<sso_enabled>1</sso_enabled>` for the desired tunnel. EMS 6.4.0 does not support GUI implementation for this feature.
- To configure SAML SSO authentication for a personal VPN tunnel in FortiClient, on the *Remote Access* tab, edit or create a new VPN tunnel. Select the *Enable Single Sign On (SSO) for VPN Tunnel* checkbox.

To connect to a VPN tunnel using SAML authentication:

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



FortiClient provides an option to the end user to save their VPN login password with or without SAML configured. When using SAML, this feature relies on persistent sessions being configured in the IdP, discussed as follows:

- Azure
- Okta

If the IdP does not support persistent sessions, FortiClient cannot save the SAML password. The end user must provide the password to the IdP for each VPN connection attempt.

The FortiClient save password feature is commonly used along with autoconnect and always-up features as well.

Advanced features (Windows)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient profile options in EMS to ensure the FortiClient profile settings do not overwrite your custom XML settings. See the *FortiClient XML Reference Guide*.

Activating VPN before Windows logon

When using VPN before Windows logon, the user is offered a list of preconfigured VPN connections to select from on the Windows logon screen. This requires that the Windows logon screen is not bypassed. As such, if VPN before Windows logon is enabled, it is required to also select the *Users must enter a user name and password to use this computer* checkbox in the *User Accounts* dialog.

To activate VPN before Windows logon:

1. In FortiClient, create the VPN tunnels of interest or receive the VPN list of interest from FortiClient EMS.
2. Ensure that VPN is enabled before logon to the FortiClient *Settings* page.
3. On the Windows system, start an elevated command line prompt.
4. Enter `control passwords2` and press `Enter`. Alternatively, you can enter `netplwiz`.
5. Check the checkbox for *Users must enter a user name and password to use this computer*.
6. Click *OK* to save the setting.

VPN before logon is unrelated to auto-connect or always-up and is a one-time connection made so the domain controller can be reached prior to login. This is often leveraged in conjunction with a user password reset. For the remote device to sync the new password, it must contact the domain controller which is often unreachable outside of a VPN connection.

VPN before logon authentication supports:

- Smart cards
- Machine certificates without usernames
- Username and password
- Two-factor authentication
- LDAP
- RADIUS

Connecting VPNs before logging on (AD environments)

The VPN `<options>` tag holds global information controlling VPN states. The VPN connects first, then logs on to Active Directory (AD)/domain.

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
      <options>
        <show_vpn_before_logon>1</show_vpn_before_logon>
        <use_windows_credentials>1</use_windows_credentials>
      </options>
      <connections>
        <connection>
          <name>psk_90_1</name>
          <type>manual</type>
          <ike_settings>
            <prompt_certificate>0</prompt_certificate>
            <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
            <redundantsortmethod>1</redundantsortmethod>
            <auth_data>
              <certificate>
                <common_name>
```

```
                <match_type>
                  <![CDATA[wildcard]]>
                </match_type>
                <pattern>
                  <![CDATA[*]]>
                </pattern>
              </common_name>
              <issuer>
                <match_type>
                  <![CDATA[simple]]>
                </match_type>
                <pattern>
                  <![CDATA[Certificate  Authority]]>
                </pattern>
              </issuer>
            </certificate>
          </auth_data>
          ...
        </ike_settings>
      </connection>
    </connections>
  </ipsecvpn>
 </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. The fragment includes all closing tags, but omits some important elements to complete the VPN configuration. For a list of all available elements, see the *FortiClient XML Reference Guide*.

<redundantsortmethod> value	Effect
1	Sets the IPsec VPN connection as ping response-based. The VPN connects to the FortiGate that responds the most quicky.
0	Default value. The IPsec VPN connection is priority-based. Priority-based configurations try to connect to the FortiGate starting with the first in the list.

Creating redundant IPsec VPNs

To use IPsec VPN resiliency/redundancy, configure a list of VPN gateways within the <server> tag, separating entries with semicolons, then specify a sort method with the <redundantsortmethod> tag:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
      <options>
        ...
      </options>
      <connections>
        <connection>
          <name>psk_90_1</name>
          <type>manual</type>
          <ike_settings>
            <prompt_certificate>0</prompt_certificate>
```

```
                <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                <redundantsortmethod>1</redundantsortmethod>
                ...
            </ike_settings>
         </connection>
      </connections>
   </ipsecvpn>
</vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. The fragment includes all closing tags, but omits some important elements to complete the VPN configuration. For a list of all available elements, see the *FortiClient XML Reference Guide*.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response-based. The VPN connects to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority-based. Priority-based configurations try to connect to the FortiGate starting with the first in the list.

Creating priority-based SSL VPN connections

SSL VPN only supports priority-based configurations for resiliency/redundancy. To use SSL VPN resiliency/redundancy, configure a list of VPN gateways within the `<server>` tag, separating entries with semicolons:

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            ...
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
               <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
               ...
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. The fragment includes all closing tags, but omits some important elements to complete the VPN configuration. For a list of all available elements, see the *FortiClient XML Reference Guide*.

For SSL VPN, all FortiGates must use the same TCP port.

Advanced features (macOS)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient profile options in EMS to ensure the FortiClient profile settings do not overwrite your custom XML settings. See the *FortiClient XML Reference Guide*.

Creating redundant IPsec VPNs

To use VPN resiliency/redundancy, configure a list of FortiGate or EMS IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
         <options>
            ...
         </options>
         <connections>
            <connection>
               <name>psk_90_1</name>
               <type>manual</type>
               <ike_settings>
                  <prompt_certificate>0</prompt_certificate>
                  <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                  <redundantsortmethod>1</redundantsortmethod>
                  ...
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

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

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response-based. The VPN connects to the FortiGate or EMS which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority-based. Priority-based configurations tries to connect to the FortiGate or EMS starting with the first in the list.

```
            </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.

For SSL VPN, all FortiGate or EMS units must use the same TCP port.

Creating priority-based SSL VPN connections

SSL VPN supports priority-based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            ...
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
               <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
               ...
            </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.

For SSL VPN, all FortiGate or EMS must use the same TCP port.

VPN tunnel and script

This feature supports autorunning a user-defined script after connecting or disconnecting the configured VPN tunnel. The scripts are batch scripts in Windows and shell scripts in macOS. They are defined as part of a VPN tunnel configuration on EMS's XML format FortiClient profile. The profile is pushed down to FortiClient from EMS as part of an endpoint policy. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel is executed.

Windows

Mapping a network drive after tunnel connection

The script maps a network drive and copies some files after the tunnel connects.

```
<on_connect>
   <script>
      <os>windows</os>
      <script>
         <script>
```

```
            <![CDATA[ net use x: \\192.168.10.3\ftpshare /user:CMoltisanti md c:\test copy
                 x:\PDF\*.* c:\test ]]>
         </script>
      </script>
   </script>
</on_connect>
```

Always use `#username#/#password#` inline with the batch command, as follows:

```
net use \\myserver\fileshare /user:#username# #password#
```

Do not assign `#username#/#password#` to variables, like the following:

```
SET user=#username#
SET pwd=#password#
net use \\myserver\fileshare /user:%user% %pwd%
```

Deleting a network drive after tunnel disconnection

The script deletes the network drive after the tunnel disconnects.

```
<on_disconnect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[ net use x: /DELETE ]]>
         </script>
      </script>
   </script>
</on_disconnect>
```

macOS

Mapping a network drive after tunnel connection

The script maps a network drive and copies some files after the tunnel connects.

```
<on_connect>
   <script>
      <os>mac</os>
      <script>
         /bin/mkdir /Volumes/installers
         /sbin/ping -c 4 192.168.1.147 > /Users/admin/Desktop/dropbox/p.txt
         /sbin/mount -t smbfs //kimberly:RigUpTown@ssldemo.fortinet.com/installers
              /Volumes/installers/ > /Users/admin/Desktop/dropbox/m.txt
         /bin/mkdir /Users/admin/Desktop/dropbox/dir
         /bin/cp /Volumes/installers/*.log /Users/admin/Desktop/dropbox/dir/.
      </script>
   </script>
</on_connect>
```

Deleting a network drive after tunnel disconnection

The script deletes the network drive after the tunnel disconnects.

```
<on_disconnect>
   <script>
      <os>mac</os>
      <script>
         /sbin/umount /Volumes/installers
         /bin/rm -fr /Users/admin/Desktop/dropbox/*
      </script>
   </script>
</on_disconnect>
```

Internal resource lookup with IPv6 enabled on NIC interface

Lookup by name to internal resources may fail when IPv6 is enabled on the NIC interface. To resolve this issue, you can do one of the following.

To disable ParallelAandAAA capability:

1. In Registry Editor, go to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters*.
2. Set "`DisableParallelAandAAAA "=dword:00000001`.

To enable SMHNR:

Use this method only for an SSL VPN full tunnel. This method is not supported if using split tunnel.

1. In Local Group Policy Editor, go to *Computer Configuration* > *Administrative Templates* > *Network* > *DNS Client* > *Turn off smart multi-homed name resolution*.
2. Click *policy setting*.
3. Set to *Disabled*, then click *OK*.
4. In Registry Editor, go to *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient*.
5. Set "`DisableSmartNameResolution"=dword:00000000`

Standalone VPN client

Windows and macOS

There is a VPN-only installer for Windows and macOS. You can also create a VPN-only installer using FortiClient EMS.

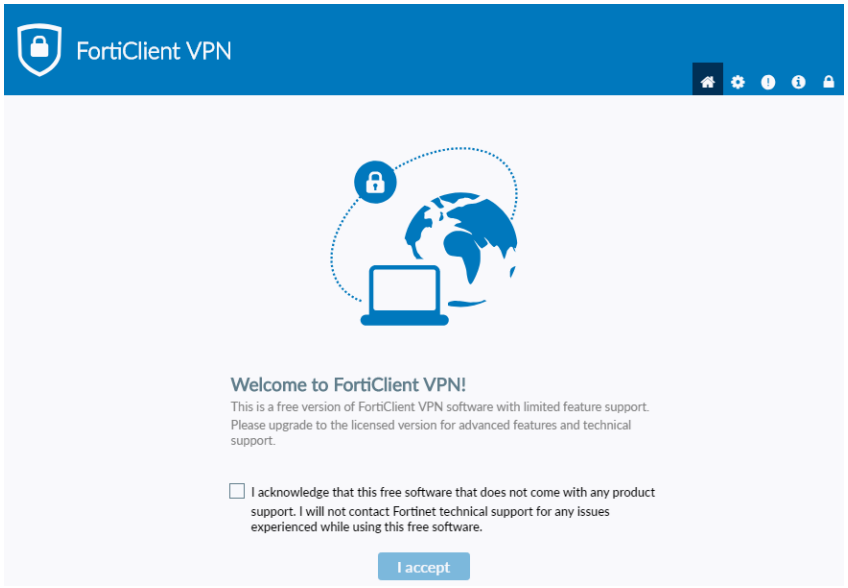
For FortiGate administrators, a free version of FortiClient VPN is available which supports basic IPsec and SSL VPN and does not require registration with EMS. This version does not include central management, technical support, or some advanced features. The free VPN-only client does support SAML.

Full-featured FortiClient 7.2.7 requires registration to EMS. Each endpoint registered with EMS requires a license seat on EMS.

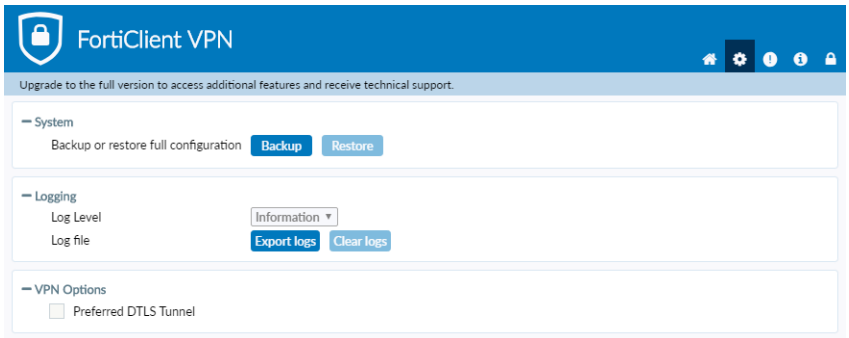
The FortiClient VPN installer differs from the installer for full-featured FortiClient. You can only download the free VPN client from FNDN or FortiClient.com.

The free VPN client supports the single sign on mobility agent.

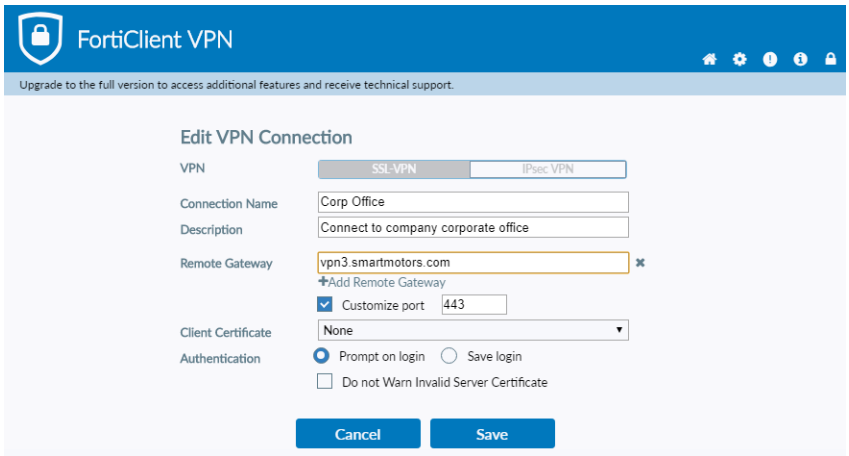
When the free VPN client is run for the first time, it displays a disclaimer. You cannot configure or create a VPN connection until you accept the disclaimer:



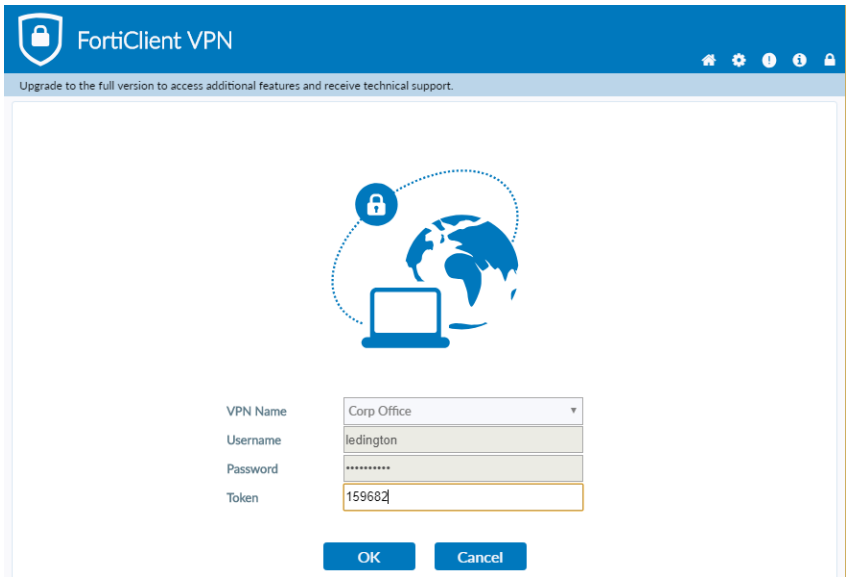
Only the VPN feature is available. You can access the *Settings*, *About*, and *Notifications* pages from a toolbar.



Configuring settings for a new VPN connection on the free VPN client resembles doing the same on a full FortiClient installation:



You can establish a VPN connection from the homepage:



Linux

An SSL VPN tunnel client standalone installer for Linux operating systems is available from FNDN. See the *FortiOS Release Notes*.

ZTNA Destination

You can use FortiClient to create a secure encrypted connection to protected applications without using VPN. Acting as a local proxy gateway, FortiClient works with the FortiGate application proxy feature to create a secure connection via HTTPS using a certificate received from EMS that includes the FortiClient UID. The FortiGate retrieves the UID to identify the device and check other endpoint information that EMS provides to the FortiGate, which can include other identity and posture information. The FortiGate allows or denies the access as applicable. See Zero Trust Network Access (ZTNA) for FortiOS configuration requirements. For TCP forwarding to non-web-based applications, you must define ZTNA connection rules in FortiClient as follows.

For Linux devices, ZTNA certificate provisioning requires Trusted Platform Module 2.0.

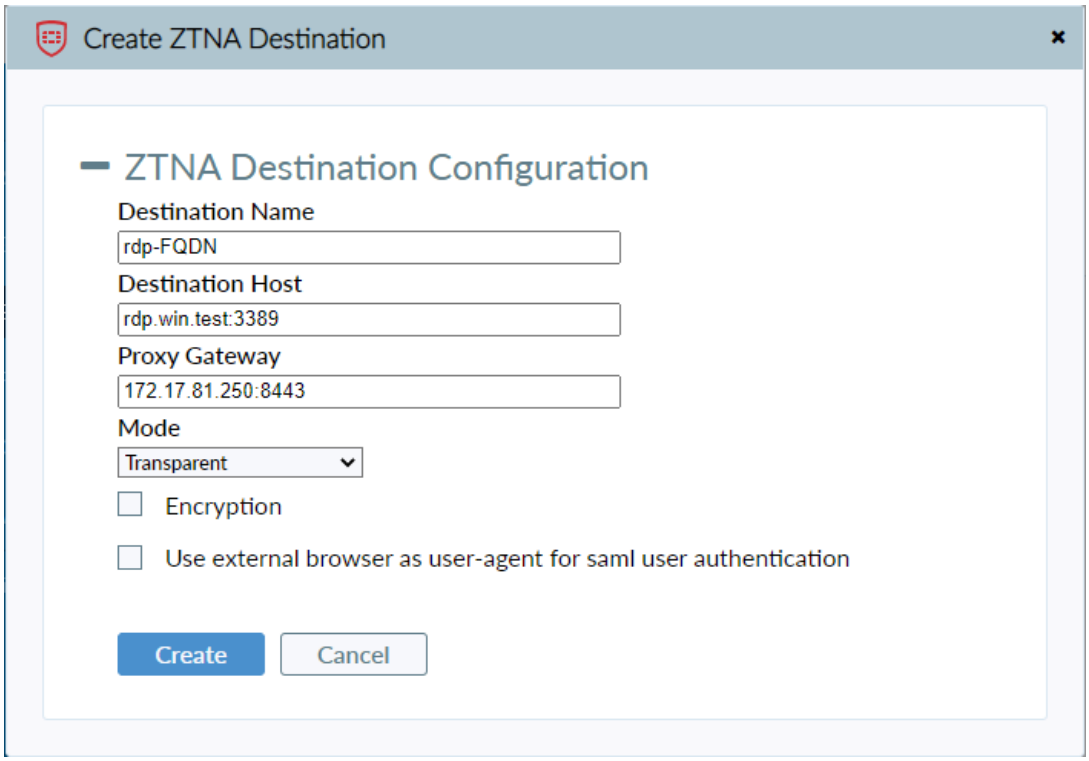
It is recommended for FortiClient to receive ZTNA destinations from EMS as configured by the EMS administrator. See the FortiClient EMS Administration Guide.

You cannot use ZTNA destinations and TCP forwarding on a Windows 7 endpoint.

To add a ZTNA destination:

1. On the *ZTNA Destination* tab, click *Add Destination*.
2. In the *Destination Name* field, enter the desired name.
3. In the *Destination Host* field, enter the IP address/FQDN and port of the destination host in the format <IP address or FQDN>:<port>. This field does not support entering a hostname. For example, you could enter demo.fortinet.com:22 as the destination host value.
4. In the *Proxy Gateway* field, enter the FortiGate access IP address and port in the same format. For example, you could enter 21.14.22.11:80 as the proxy gateway value.
5. From the *Mode* dropdown list, select *Transparent*.
6. Enable or disable *Encryption*. By default, *Encryption* is disabled. When *Encryption* is enabled, traffic between FortiClient and the FortiGate is always encrypted, even if the original traffic has already been encrypted. When *Encryption* is disabled, traffic between FortiClient and the FortiGate is not encrypted.
7. If desired, enable *Use external browser as user-agent for saml user authentication*. FortiClient can use a browser as an external user-agent to perform SAML authentication.

8. Click *Create*.



Malware Protection

The Malware Protection tab includes the following features:

The *Malware Protection* tab displays in FortiClient when FortiClient is installed with *Additional Security Features* selected.

Antivirus

FortiClient includes an antivirus (AV) component to scan system files, executable files, removable media, dynamic-link library (DLL) files, and drivers. FortiClient also scans for and removes rootkits. In FortiClient, file-based malware, malicious websites, phishing, and spam URL protection are part of the AV component. FortiClient's AV component supports twelve levels of nested compressed files for scanning. For compressed files, FortiClient supports a maximum file size of 1 GB for antivirus scanning. For a compressed file with a size larger than 1 GB, FortiClient will scan it after decompression.

Updating the AV database

FortiClient informs you if the AV database is out of date. FortiClient automatically updates signatures. However, if you see the signatures are outdated, you can go to *About* to download updates from FortiGuard. See Viewing FortiClient engine and signature versions on page 83.

Scanning with AV on-demand

You can perform on-demand AV scanning. You can scan specific files or folders, and you can submit a file for analysis.

Scanning now

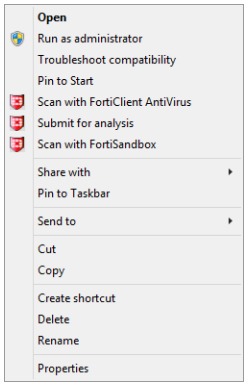
1. On the *Malware Protection* tab, go to *AntiVirus Protection*.
2. Beside the *Scan Now* button, use the dropdown list to select *Quick Scan*, *Full Scan*, *Custom Scan*, or *Removable media Scan*.

Quick Scan	Runs the rootkit detection engine to detect and remove rootkits. It looks for threats by scanning executable files, DLLs, and drivers that are currently running.

Full Scan	Runs the rootkit detection engine to detect and remove rootkits. It then looks for threats by performing a full system scan on all files, executable files, DLLs, and drivers.
Custom Scan	Runs the rootkit detection engine to detect and remove rootkits. It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.
Removable Media Scan	Runs the rootkit detection engine to detect and remove rootkits. It scans all connected removable media, such as USB drives.

Scanning files or folders

Right-click the file or folder and select *Scan with FortiClient AntiVirus* from the menu.



Submitting files to FortiGuard for analysis

You can send up to five files a day to FortiGuard for analysis.

You do not receive feedback for files submitted for analysis. The FortiGuard team can create signatures for any files that are submitted for analysis and determined to be malicious.

1. On your workstation, right-click a file or executable, and select *Submit for analysis* from the menu. A dialog displays that identifies the number of files submitted.
2. Confirm the location of the file that you want to submit, and click the *Submit* button.

Viewing AntiVirus scan results

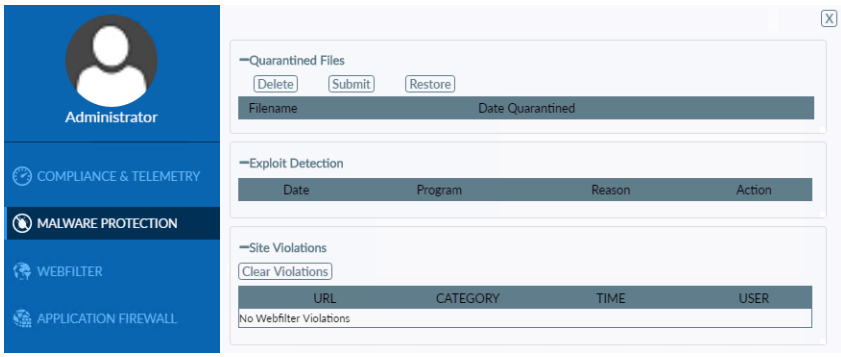
You can view quarantined threats, site violations, alerts, and RTP events.

For details on viewing quarantined threats, see Viewing quarantined files on page 87.

Viewing site violations

On the *Site Violations* page, you can view site violations and submit sites to be recategorized.

1. On the *Malware Protection* tab, click *X Threats Detected*.



Site Violations displays the following options:

URL	Website URL.
CATEGORY	Web filter category the site belongs to.
TIME	Date and time of the site violation.
USER	User who attempted to access the site.

2. Click *Close*.

Viewing alerts

When FortiClient AV detects a virus while attempting to download a file via a web browser, a warning displays.

Select *View recently detected virus(es)* to collapse the virus list. Right-click a file in the list to access the following context menu. If EMS is managing FortiClient, these options are disabled:

Delete	Delete a quarantined or restored file.
Quarantine	Quarantine a restored file.
Restore	Restore a quarantined file.
Submit Suspicious File	Submit a file to FortiGuard as a suspicious file.
Submit as False Positive	Submit a quarantined file to FortiGuard as a false positive.
Add to Exclusion List	Add a restored file to the exclusion list. FortiClient does not scan any files in the exclusion list.
Open File Location	Open the file location on your workstation.

Depending on the settings received from EMS, virus alert dialog may or may not display when you attempt to download a virus in a web browser.

Viewing RTP events

When an AV RTP event has occurred, you can view these events in FortiClient.

1. From the *Malware Protection* tab, select *Threats Detected*.
2. Select *Real-time Protection events (x)*.
   The `realtime_scan.log` opens in the default viewer.
   Example log output:

```
Realtime scan result:
time: Wed Jan 9 09:52:18 2019, Realtime Protection Started, AV_ENGINE:6.00012 MDARE_
     ENGINE:2.00068 AV_SIG:1.00000 AV_EXT_SIG:1.00000 MDARE_SIG:1.00000
time: Wed Jan 9 09:52:42 2019, virus found: EICAR_TEST_FILE, action: Quarantined,
     C:\Users\Administrator\Downloads\5adfd0ce-278a-4697-8a97-624b307df63c.tmp
```

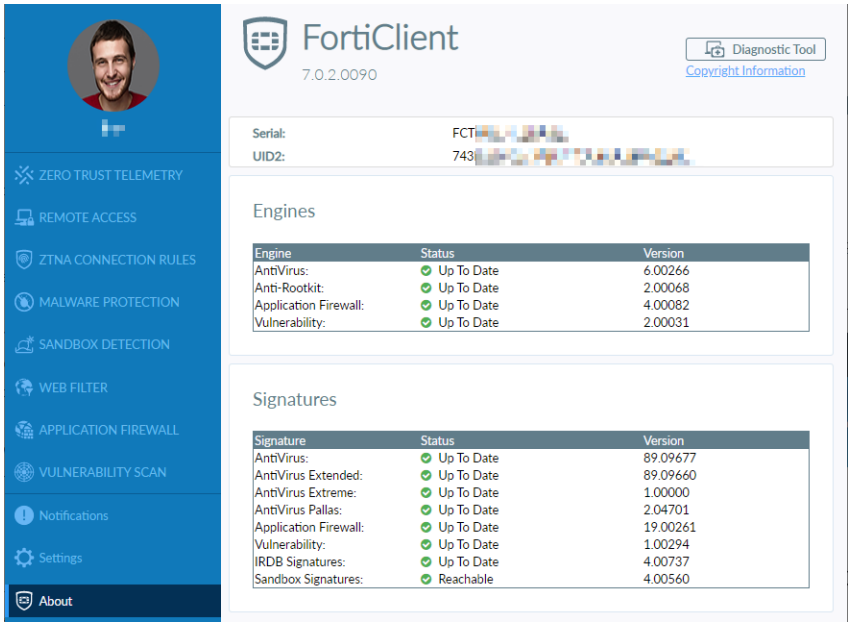
Viewing FortiClient engine and signature versions

You can view the current FortiClient version, engine, and signature information.

When EMS manages FortiClient, you can use a FortiManager for FortiClient software and signature updates. When configuring the profile using EMS, select *Use FortiManager for Client Signature Update* to enable the feature, and enter your FortiManager IP address. You can failover to FDN when FortiManager is unavailable.

To view FortiClient engine and signature versions:

1. Go to *About*.



2. Hover the mouse over the *Status* field to see the date and time FortiClient last updated the selected item.
3. Click *Close*.

Cloud Based Malware Protection

The cloud-based malware protection feature helps protect endpoints from high risk file types from external sources such as the Internet or network drives by querying FortiGuard to determine whether files are malicious. The following describes the process for cloud-based malware protection:

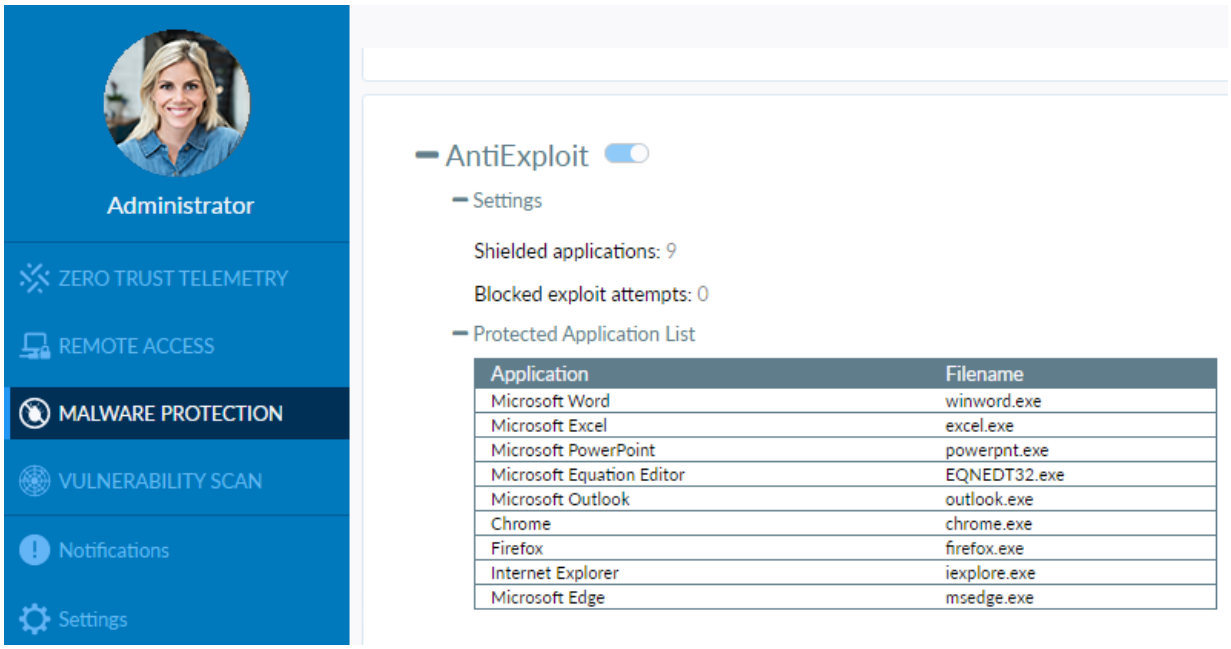
1. A high risk file is downloaded or executed on the endpoint.
2. FortiClient generates a SHA1 checksum for the file.
3. FortiClient sends the checksum to FortiGuard (FQDN with port 8888) to determine if it is malicious against the FortiGuard checksum library.
4. If the checksum is found in the library, FortiGuard communicates to FortiClient that the file is deemed malware. By default, FortiClient quarantines the file.

This feature only submits high risk file types such as .exe, .doc, .pdf, and .dll to FortiGuard. The list of high risk file types is the same as the list of file types submitted to Sandbox by default. See the *FortiClient EMS Administration Guide* for details.

For details on seeing quarantined files, see Viewing quarantined files on page 87.

AntiExploit

The antiexploit detection feature helps protect vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox) and Microsoft Office applications, against exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, the compromised application process is terminated. The antiexploit detection feature also helps protect against memory-based attacks and drive-by download attacks. It also detects and blocks unknown and known exploit kits. It is a signature-less solution. The anti-exploit detection feature protects applications from any activities that can be harmful, regardless if legitimate applications or malicious code are causing them.



Due to a feature enhancement, antiexploit detection now supports the following applications:

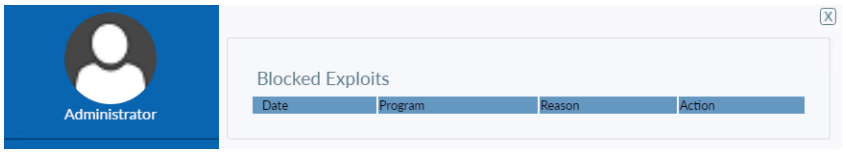
- Microsoft applications:
  - Word
  - Excel
  - PowerPoint
  - Equation Editor
  - Outlook
- Browsers:
  - Chrome
  - Firefox
  - Internet Explorer
  - Microsoft Edge

The antiexploit detection feature is available only for FortiClient (Windows).

Viewing detected exploit attempts

You can view the exploit attempts FortiClient has blocked. See .

1. On the *Malware Protection* tab, click *Blocked exploit attempts*.
   In this page you can view the date and description of a blocked exploit attempt.



This page displays the following information:

Date	Date of the detected exploit attempt.
Program	Program that attempted the detected exploit attempt.
Reason	Reason the detected exploit attempt was blocked.
Action	Action FortiClient took in response to the detected exploit attempt.

2. Click *Close*.

Evaluating the anti-exploit detection feature

The anti-exploit detection feature blocks malicious content from exploiting vulnerabilities in applications. To test or verify this feature, you can use the Metasploit Framework module. This module requires Windows 7 x86, Firefox, and Adobe Flash Player.

Consider running the exploit with and without enabling the anti-exploit detection feature in FortiClient. FortiClient blocks such an exploit and displays a bubble message in FortiTray to notify the endpoint user.

In newer product versions, vendors resolve most publicly announced exploits. The FortiClient Vulnerability Scan feature can identify, report, and apply patches for supported applications. See Vulnerability Scan on page 95.

Removable media access

FortiClient controls access to removable media devices, such as USB drives. FortiClient can allow, block, or monitor access to removable media devices, as configured by the EMS administrator.

Antiransomware

Antiransomware protects specific files, folders, or file types from unauthorized changes. After detecting ransomware behavior on the endpoint, FortiClient restores files that the detected ransomware encrypted. FortiClient automatically updates antiransomware signatures and engines as available from FortiGuard Distribution Servers. See Anti-Ransomware.

Quarantined files

Various features on the *Malware Protection* tab can quarantine files that pose a threat to the endpoint. This section describes viewing the quarantined files and the actions you can take with the quarantined files:

Viewing quarantined files

To view quarantined files:

1. On the *Malware Protection* tab, click *Threats Detected*. This option is available under *AntiVirus Protection* and *Cloud Based Malware Protection*. You can also click *Zero-Day* on the *Sandbox Detection* tab.
   You can view the original file location, virus name, and logs, and submit the suspicious file to FortiGuard. You cannot restore or delete the quarantined file.
   FortiClient organizes quarantined files into the following sections:
   - *Quarantined Files*: files that AntiVirus Protection has quarantined
   - *Cloud Protection Quarantined Files*: files that Cloud Based Malware Protection has quarantined
   - *Sandbox Quarantined Files*: files that Sandbox Detection has quarantined
2. The following information displays:

Filename	Names of the quarantined files.
Date Quarantined	Dates and time the files were quarantined.

3. Select a file from the list to view detailed information about the file and click *Details*.

Submit	Click submit for FortiGuard analysis.
Filename	Name of the quarantined file.
Original Location	Location of the file before scanning.
Date Quarantined	Date and time the file was quarantined.
Submitted	Displays *Not Submitted* when the selected file has not been submitted to FortiGuard for analysis by clicking the *Submit* button. Displays *Submitted* after clicking the *Submit* button.
Status	Status of the file, such as *Quarantined*.
Virus Name	Name of the detected virus.
Quarantined File Name	Name of the file after it was quarantined.
Log File Location	Location of the log file for the scan.
Quarantined By	FortiClient feature that quarantined the file.
Close	Click to close the details dialog.

4. Click *Close*.

FortiClient sends quarantined file information to EMS. If the EMS administrator whitelists the file (in the case of a false positive), EMS sends the whitelist information to FortiClient. After FortiClient receives the whitelist information, it releases the file from quarantine. See the *FortiClient EMS Administration Guide* for details.

Submitting quarantined files for scanning

To submit quarantined files to FortiSandbox for scanning:

1. On the *Malware Protection* tab, click *Threats Detected*. This option is available under *AntiVirus Protection* and *Cloud Based Malware Protection*. You can also click *Zero-Day* on the *Sandbox Detection* tab.
2. Select the file and click *Submit*.

Sandbox Detection

FortiClient supports integration with FortiSandbox, including on-premise FortiSandbox appliances and FortiClient Cloud Sandbox (SaaS). When configured, FortiSandbox automatically scans files downloaded on the endpoint or from removable media attached to the endpoint or mapped network drives. FortiClient also automatically scans files downloaded with an email client on the endpoint or from the Internet. In each case, if the file is not detected locally, and FortiSandbox integration is configured, FortiClient sends the file to the FortiSandbox for further analysis. Endpoint users can also manually submit files to FortiSandbox for scanning.

You can block access to files until FortiClient returns the FortiSandbox scanning result.

When scanning is complete, FortiClient can quarantine/deny access to infected files or alert and notify the endpoint user of infected files without quarantining the files. If FortiSandbox sends a verdict to FortiClient indicating that the file is malicious, FortiClient also sends the results to EMS.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from FortiSandbox, and applies them locally to all realtime and on-demand AV scanning.

FortiClient can send a maximum of 300 files daily to FortiClient Cloud Sandbox (SaaS). If multiple files are submitted around the same time, FortiClient sends one file to FortiClient Cloud Sandbox (SaaS), waits until it receives the verdict for that file, then sends the next file to FortiClient Cloud Sandbox (SaaS).

The file size limit for submission to FortiSandbox is 200 MB.

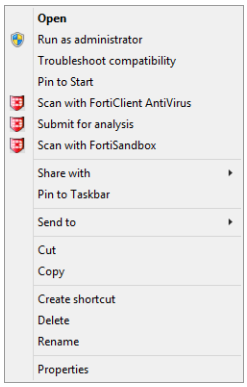
If configured by the EMS administrator, FortiClient submits files with specified extensions to FortiSandbox. See the *FortiClient EMS Administration Guide* for details.

FortiSandbox integration does not require FortiClient real-time protection to be enabled. If using a separate real-time antimalware application, FortiClient cannot send files that this application has quarantined to FortiSandbox.

Scanning with FortiSandbox on-demand

You can send files to FortiSandbox for scanning on-demand when FortiSandbox is enabled and online.

Right-click a file and select *Scan with FortiSandbox* from the menu.



Viewing FortiSandbox scan results

Go to the *Sandbox Detection* tab. The following information displays:

Submitted	Number of files submitted to FortiSandbox for scanning.
Zero-day	Number of detected zero-day files. Click to view details about the files.
Clean	Number of files determined clean after FortiSandbox scanning.
Pending	Number of files waiting for FortiSandbox scanning.

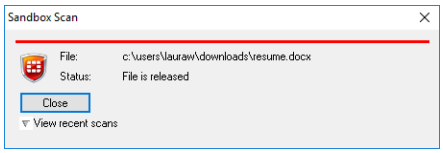
The *Zero-day File Details* section displays the name, status, and date and time quarantined for each zero-day file. Click a file to view the following information:

Original Location	Original location of the file on the local machine.
Submission Type	Whether the file was submitted to FortiGuard.
Virus Name	Name of the detected virus.
Quarantined File Name	Name of the quarantined file.

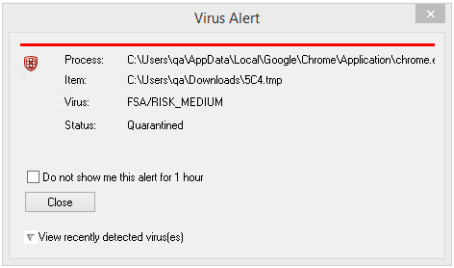
For details on viewing quarantined files, see Quarantined files on page 87.

Using the popup window

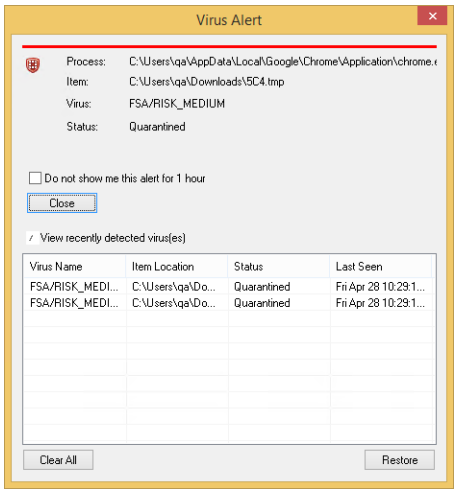
As FortiSandbox scans and releases files, a popup displays to inform you. You can view the recent scans by clicking the *View recent scans* option.



When FortiSandbox detects a virus and quarantines a file, the *Virus Alert* window displays.



You can use the *Virus Alert* window to view information about the recently scanned files by clicking the *View recently detected virus(es)* option.



Web & Video Filter

Web Filter allows you to block, allow, warn, and monitor web traffic based on URL category or custom URL filters. When a domain is detected, the URL is sent to FortiGuard for categorization. FortiClient then takes action based on the returned category. You can create a custom URL filter exclusion list that overrides the FortiGuard category.

Since FortiClient cannot perform deep inspection and instead leverages certificate inspection for HTTPS websites, FortiClient also cannot present a block page with a trusted connection. This is seen as a browser certificate warning. To avoid this, there are two options:

- Leverage the web browser plugin for HTTPS web filtering. See Web browser plugin for HTTPS web filtering on page 92.
- Action On HTTPS Site Blocking. See the *FortiClient EMS Administration Guide*.

FortiClient inspects all web traffic, not just traffic that a web browser generates. This means you may get web filter certificate warnings or popup messages for other applications, such as Outlook.

Video Filter helps protect you by filtering sensitive video contents from websites like YouTube. The EMS administrator configures Video Filter settings and deploys them to FortiClient.

If FortiClient cannot contact FortiGuard, FortiClient blocks all web traffic by default. To configure FortiClient to allow web traffic when FortiGuard is unreachable, see the *FortiClient XML Reference Guide*.

Web browser plugin for HTTPS web filtering

The EMS administrator can enable a web browser plugin for HTTPS web filtering on the endpoint. This improves detection and enforcement of Web Filter rules on HTTPS sites. After FortiClient receives the update from EMS that enables the plugin, the browser installs the plugin extension automatically. When FortiClient telemetry disconnects or EMS disables the plugin, the browser removes the plugin automatically after the next browser restart.

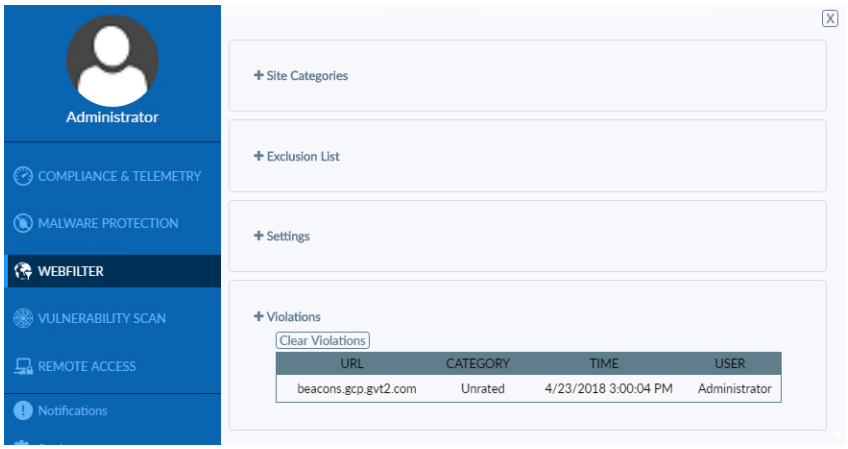
FortiClient only supports the web browser plugin for the Google Chrome, Mozilla Firefox, and Microsoft Edge browsers on Windows platforms.

Viewing violations

You can view web filtering violations in FortiClient.

On the *Web Filter* tab, click the *Settings* icon.

Alternately, you can click *Sites Blocked (in last 7 days)*.

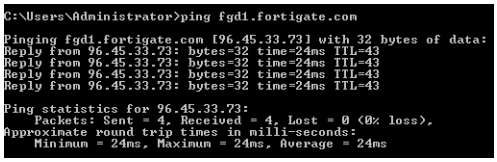


The following information displays under *Violations*.

URL	Website URL.
Category	Website subcategory.
Time	Date and time the website was accessed.
User	Name of the user generating the traffic. Hover the cursor over the column to view the complete entry in the popup bubble message.

Troubleshooting Web Filter

If Web Filter is not functioning as configured, this may be because FortiClient cannot contact FortiGuard. Open Command Prompt and run `ping fgd1.fortigate.com`. If FortiClient can contact FortiGuard, it should output the following:



If you have confirmed that FortiClient can contact FortiGuard but Web Filter still does not work as configured, ensure the necessary ports are open. FortiClient requires port 8888 or 53 to be open for FortiGuard URL rating. See Required services and ports on page 23.

Application Firewall

FortiClient can recognize the traffic generated by a large number of applications.

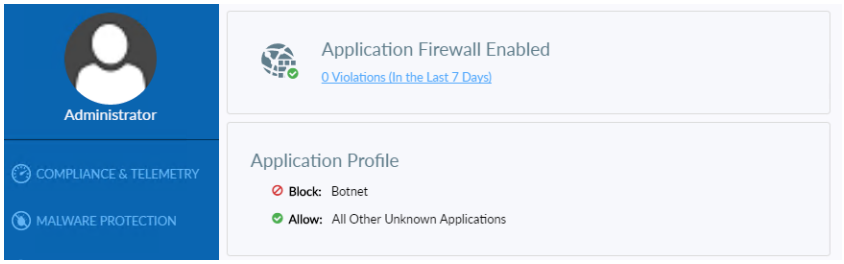
Viewing blocked applications

On the *Application Firewall* tab, click the *<number> Violations (In the Last 7 Days)* link.

A page of all blocked applications displays.

Viewing application firewall profiles

You can view the application firewall profile on the *Application Firewall* tab.



Vulnerability Scan

FortiClient includes a vulnerability scan component to check endpoints for known vulnerabilities. The vulnerability scan results can include:

- List of vulnerabilities detected
- How many detected vulnerabilities are rated as critical, high, medium, or low threats
- Links to more information, including links to the FortiGuard Center
- One-click link to install patches and resolve as many identified vulnerabilities as possible
- List of patches that require manual installation to resolve vulnerabilities

FortiClient can detect known vulnerabilities for many software. For the software list, see Appendix B - Vulnerability patches on page 115.

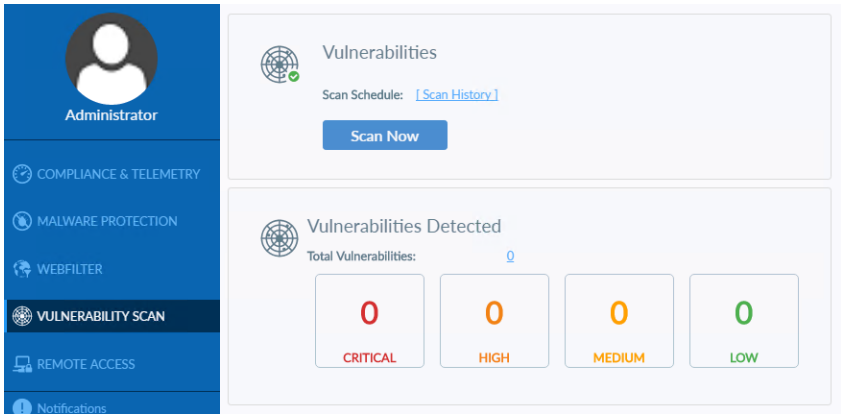
Vulnerability scan provides EMS with a list of all software installed on the endpoint, including vendor and version information. See the *FortiClient EMS Administration Guide*.

Scanning on-demand

You can scan on-demand. When the scan is complete, FortiClient displays a summary of vulnerabilities found on the endpoint. If any detected vulnerabilities require you to manually install remediation patches, the list of affected software also displays.

To scan on-demand:

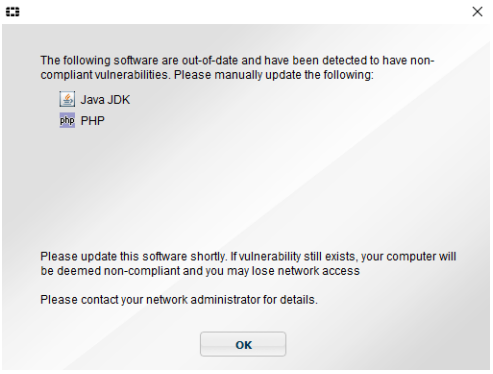
1. On the *Vulnerability Scan* tab, click the *Scan Now* button.



FortiClient scans the endpoint for known vulnerabilities, and a summary of vulnerabilities found on the system displays.

If any detected vulnerabilities require you to manually install remediation patches, a dialog displays that informs you what software should be updated. If you fail to update the identified software, you may lose access to the network. If

you lose access to the network, contact your system administrator for assistance. Following is an example of the dialog:



2. If applicable, read the list of software that requires manual installation of software patches, and click *OK*. See Manually fixing detected vulnerabilities on page 98.

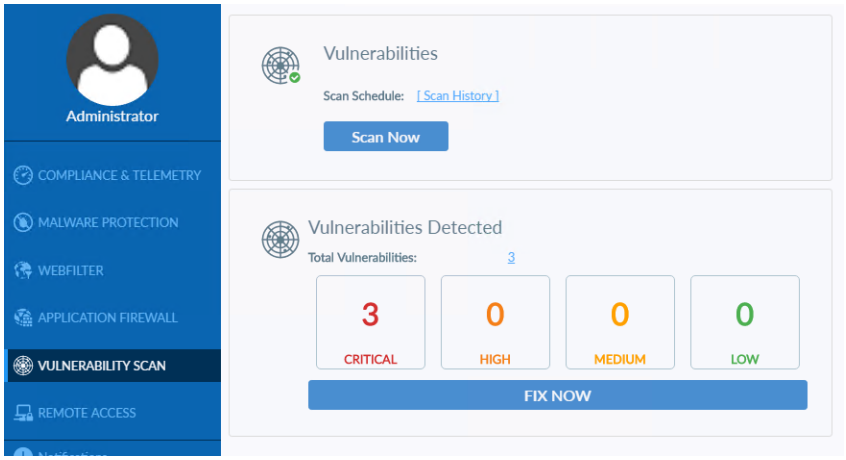
Automatically fixing detected vulnerabilities

The *Vulnerability Scan* tab identifies vulnerabilities on the endpoint that should be fixed by installing software patches. You can automatically install software patches by clicking the *Fix Now* link or review detected vulnerabilities before installing software patches.

Any software patches that cannot be automatically installed are listed on the *Vulnerability Scan* tab and you should manually download and install software patches for the vulnerable software.

You may be unable to automatically fix vulnerabilities. An administrator may have the vulnerabilities automatically fixed for you.

On the *Vulnerability Scan* tab, under *Vulnerabilities Detected*, click *Fix Now* to automatically install software patches to fix the detected vulnerabilities.

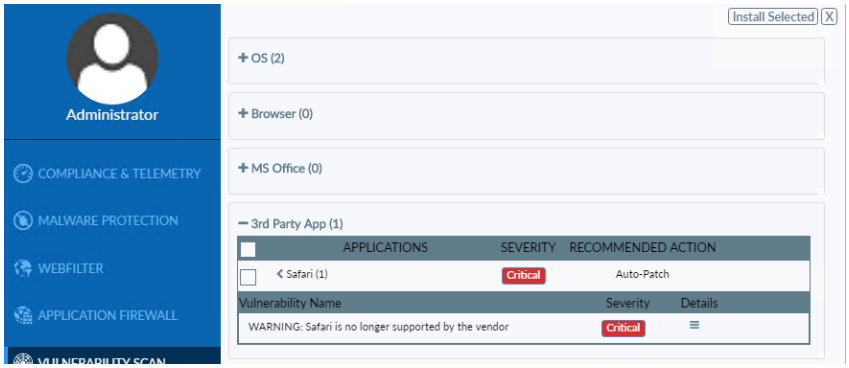


FortiClient installs the software patches. You may need to reboot the endpoint to complete installation.

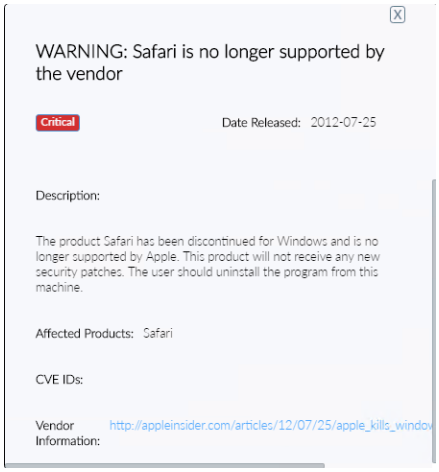
Reviewing detected vulnerabilities before fixing

To review detected vulnerabilities before fixing:

1. In the *Vulnerability Scan* tab, beside *Vulnerabilities Detected*, click the <*number*> link to review information about vulnerabilities before installing patches.
   A page of details displays.
2. Click each category with vulnerabilities to view its details. For example, click the *3rd Party App* category to view details about detected third party application vulnerabilities.



3. Expand the application to view its vulnerabilities.
4. Click the *Details* icon for each vulnerability to view its details and click *Close* to close the detailed view.



5. In each category, select the checkbox for the software for which you want to install patches.
   For example, in the *OS* category, expand *Operating System*, and select the checkbox beside the vulnerabilities for which you want to install patches.
   You may be unable to choose which patches to install, depending on your FortiClient configuration. You are also unable to select the checkbox for any software that requires manual installation of patches.
6. Click the *Install Selected* button to install patches.
   FortiClient installs the patches. You may need to reboot the endpoint to complete installation.

Manually fixing detected vulnerabilities

In some cases, FortiClient cannot automatically install software patches, and you must manually download and install software patches. After each scan, the *Vulnerability Scan* tab lists any software that requires you to manually download and install software patches. See also Scanning on-demand on page 95.

If a software vendor has ceased to provide patches for its software, the software is tagged as obsolete in the signatures used by the Vulnerability Scan feature, and you must uninstall the software to fix detected vulnerabilities. The obsolete tag is visible in the details. See Viewing details about vulnerabilities on page 98.

To manually fix detected vulnerabilities:

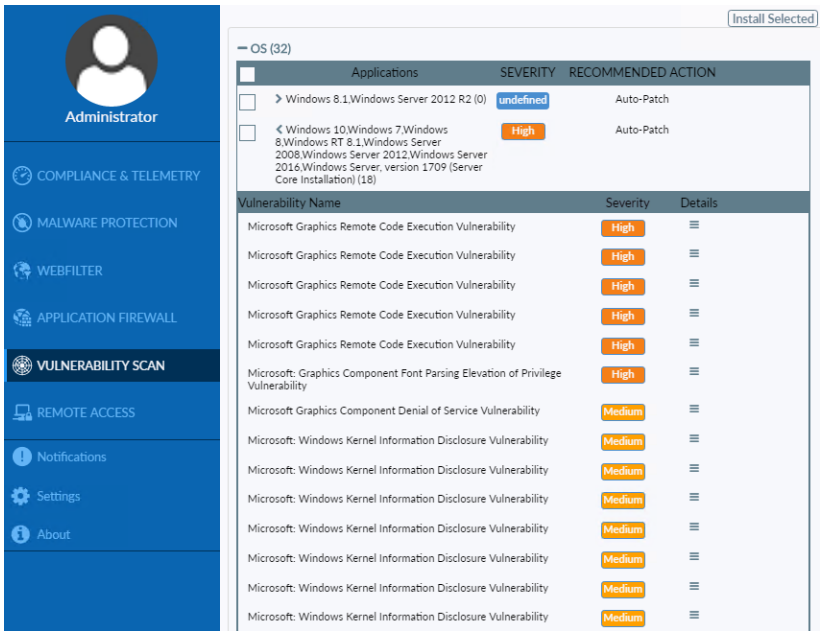
1. On the *Vulnerability Scan* tab, identify the software that requires manual fixing.
   Any software with detected vulnerabilities that requires you to manually download and install software patches is displayed in the *Vulnerabilities Detected* area.
2. Download the latest software patch for each software from the Internet, and install it on the endpoint.
3. After you install the software for all remaining vulnerabilities, go to the *Vulnerability Scan* tab, and click the *Scan Now* button to instruct FortiClient to confirm the vulnerabilities are fixed.
   If the manual fixes were successful, the *Vulnerability Scan* tab displays *Vulnerabilities Detected: None* after the scan completes.

Viewing details about vulnerabilities

To view details about vulnerabilities:

1. On the *Vulnerability Scan* tab, any software with detected vulnerabilities that requires you to manually download and install software patches displays in the *Vulnerabilities Detected* area.
2. View more details on all vulnerabilities by clicking the number of total vulnerabilities detected.
3. Expand the desired section. Vulnerabilities are divided into *OS, Browser, MS Office, 3rd Party App, Service, User Config*, and *Others*.

4. Expand the desired application. Click the *Details* icon beside the desired vulnerability.



If the detected vulnerability requires you to manually download and install a fix, it is communicated in the *Recommended Action* section. In addition, the following information may display: *The fix for the vulnerability must be manually installed from: <link>*.

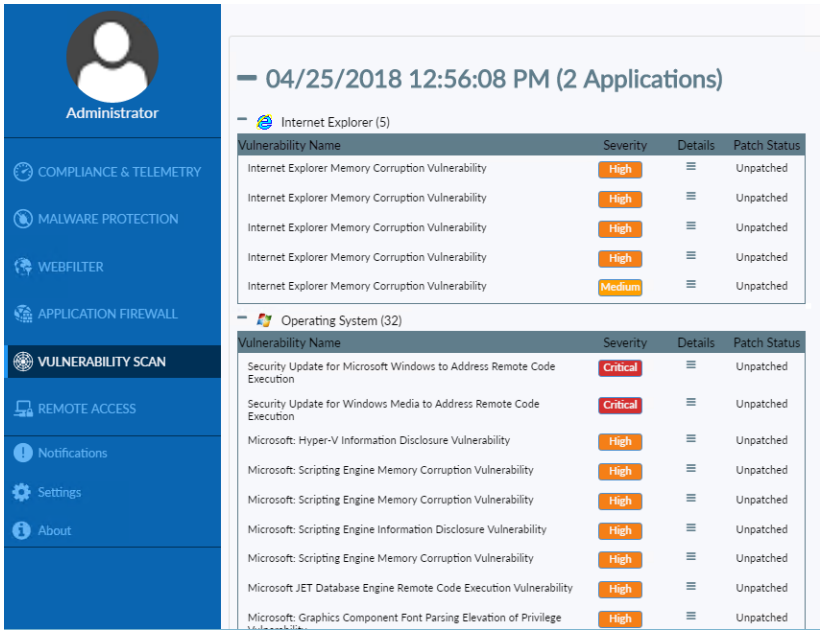
5. Click *Close*.

Viewing vulnerability scan history

You can view the history of the last seven vulnerability scans and patches. You can view the history to see what software was identified as vulnerable and whether patches for the vulnerabilities were installed.

To view vulnerability scan history:

1. In FortiClient, click the *Vulnerability Scan* tab.
2. Click *Scan History*. The vulnerability patch history displays by date. Click each date and software name to expand it and view details or contract it and hide details.



3. Click *Close* to return to the *Vulnerability Scan* tab.

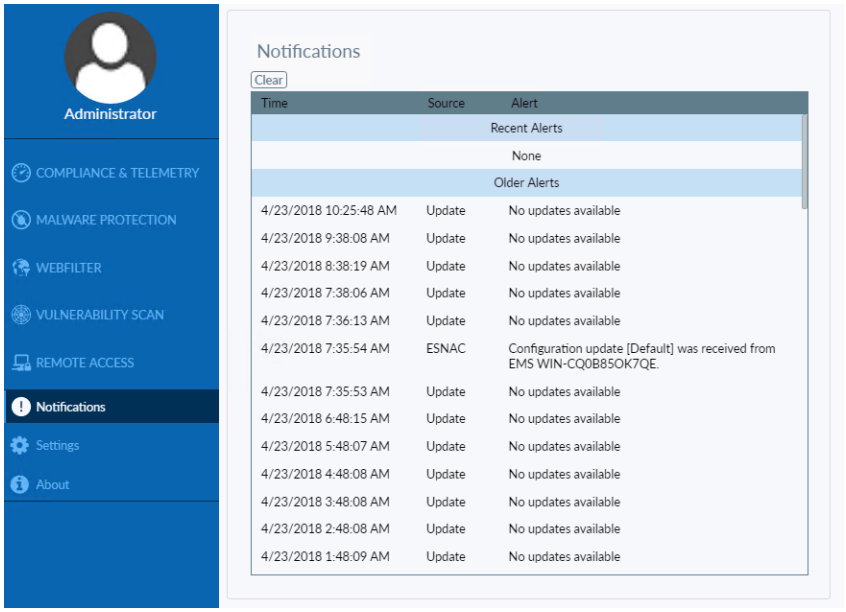
Notifications

Click the *Notifications* tab in FortiClient to view notifications.

Event notifications include:

- AV events, including scheduled scans and detected malware.
- Sandbox Detection events, including detected malware.
- Telemetry events, including configuration updates received from EMS.
- Web Filter events, including blocked website access attempts.
- System events, including signature and engine updates and software upgrades.

Click *Threat Detected* to view quarantined files, site violations, and RTP events.



Settings

This section describes the options on the *Settings* page. There are settings that EMS locks that you cannot change.

System

You can back up the FortiClient configuration to an XML file, and restore the FortiClient configuration from an XML file.

1. Go to *Settings*.
2. Expand the *System* section, then select *Backup* or *Restore* as needed.
   When performing a backup, you can select the file destination, password requirements, and add comments as needed.

Logging

Sending logs and Windows host events to FortiAnalyzer or FortiManager

Sending logs to FortiAnalyzer or FortiManager requires the following:

- FortiClient
- EMS
- FortiAnalyzer or FortiManager

When FortiClient connects Telemetry to EMS, the endpoint can upload logs and Windows host events directly to FortiAnalyzer or FortiManager units on port 514 TCP.

FortiClient logs and Windows host events display in the FortiClient administrative domain in FortiAnalyzer.

FortiClient Telemetry must connect to EMS for FortiClient to upload logs and Windows host event logs directly to FortiAnalyzer or FortiManager.

Exporting the log file

To export the log file:

1. Go to *Settings*.
2. Expand the *Logging* section, and click *Export logs*.
3. Select a location for the log file, enter a name for the log file, and click *Save*.

VPN options

You cannot configure these options when FortiClient is connected to EMS. The EMS administrator can configure these options from the EMS GUI or using XML configuration.

To configure VPN options:

1. Go to *Settings* and expand the *VPN Options* section.
2. Configure the following options:

Option	Description
Enable VPN before logon	Enable selecting a VPN connection before logging into the system.
Preferred DTLS Tunnel	If enabled, FortiClient uses DTLS if it is enabled on the FortiGate and tunnel establishment is successful. If not enabled on the FortiGate or tunnel establishment does not succeed, TLS is used. DTLS tunnel uses UDP instead of TCP and can increase throughput over VPN. When disabled, FortiClient uses TLS, even if DTLS is enabled on FortiGate.
Do not Warn Invalid Server Certificate	Select if you do not want to be warned if the server presents an invalid certificate.

3. Click *Save*.

Advanced options

To configure advanced options:

1. Go to *Settings*, and expand the *Advanced* section.
2. Configure the following settings, and click *OK*:

Default tab	Select the default tab to display when opening FortiClient.
Action for EMS invalid certificates	Select the action to take when FortiClient attempts to connect to EMS with an invalid certificate: • **Warn**: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to EMS, or terminate the connection attempt. FortiClient remembers the user's decision for this EMS, but displays the warning prompt if FortiClient attempts to connect to another EMS (using a different EMS FQDN/IP address and certificate) with an invalid certificate. • **Allow**: allows FortiClient to connect to EMS with an invalid certificate. • **Deny**: block FortiClient from connecting to EMS with an invalid certificate.
Enable Single Sign-On mobility agent	Enable SSO.

Enable Privilege Access Management	Enable privilege access management (PAM). This enables FortiClient to communicate with FortiPAM. In the *Local Server Port* field, enter the port for FortiClient to use to communicate with FortiPAM. The default port for this communication is 9191. If you change this value, ensure that you also change it in FortiPAM.
Disable proxy (troubleshooting only)	Disable proxy when troubleshooting FortiClient.

FortiPAM agent client executable integrity check

FortiClient supports the FortiPAM integrity check feature that allows you to check wither the privilege access management (PAM) client has been tampered with or not while launching an application.

The FortiPAM administrator defines the verification method to use. Once the secret is launched, FortiPAM sends verification information to the fortivrs through info response. FortiClient then verifies the certificate or checksum. If verification fails, the launch stops and an error displays. This feature supports the following verification methods:

Method	Description

Executable hash	FortiPAM supports the following hash value types for the PAM agent integrity check:
	• MD5
	• SHA1
	• SHA256
	You can use the Certutil tool to calculate the hash checksum value for the installed launcher applications such as PuTTy, RDP, VNC, TightVNC, or WinSCP.
	1. When secrets launch, PAM informs FortiClient that integrity check is enabled and provides it with the hash value configured in package.
	2. FortiClient compare this hash value with the launcher application hash value:
	  • If the hash values match, the secret launches.
	  • If the hash values do not match, *"The required software to launch is not installed on the computer. Click here to download"* displays.
	FortiClient calculates all hash values MD5/SHA1/SHA256 for the installed application and launches the secret if it matches any hash value.

Certificate	When secrets launch, the PAM agent verifies the application integrity using its digital certificate. FortiClient verifies if the application certificate authority (CA) certificate is available in the Windows certificate store as a trusted root CA. If a known public CA signed the certificate and the certificate is available on the Windows certificate store, the secret launches. If the private CA configured in the FortiPAM integrity check package that PuTTy signed, the PAM agent considers it as a valid certificate and the secret launches. If a public CA did not sign the certificate or the FortiPAM-configured certificate is unavailable in the Windows certificate store, it is not valid and a prompt to download the application configured on FortiPAM displays and the secret launch stops.

You can configure *Package Download Option* as follows:

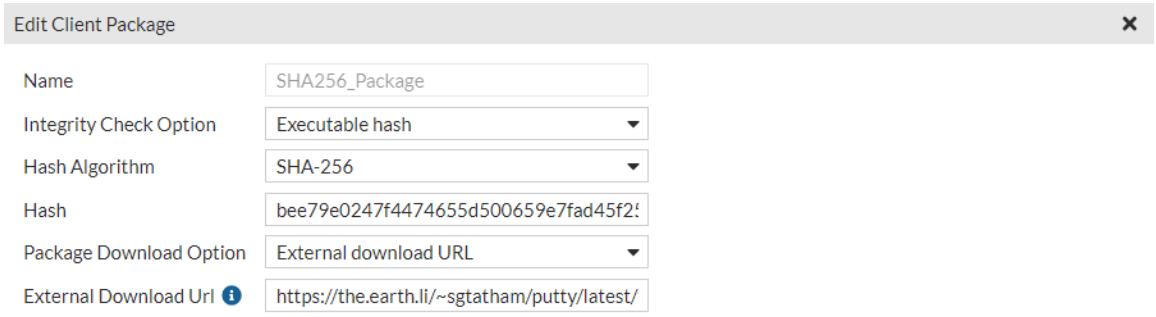
Package download option	Description
External Download URL	Enter launcher application's external download URL link.
Internal Download URL	Upload launcher application directly to the package.

If verification fails, *"The required software to launch is not installed on the computer. Click here to download"* displays. Clicking *"here"* downloads the launcher application. You can install this application and use it for launching secrets.

The FortiPAM agent can only perform integrity checks on native secrets such as RDP, Putty, VNC, TightVNC, and WinSCP.

To configure PAM agent integrity check using executable hash when launching PuTTY:

1. Configure FortiPAM:
   a. In FortiPAM, go to *Secret Settings* > *Integrity Check*.
   b. Create a client software package using PuTTy's SHA 256 executable hash.
   c. In the *Hash* field, enter the PuTTY.exe file's hash value. Do not enter the PuTTy.msi file's hash value.
   d. From the *Package Download Option* dropdown list, select *External download URL*.
   e. In the *External Download Url* field, enter the PuTTy.exe file's external download URL. Click *OK* and save.



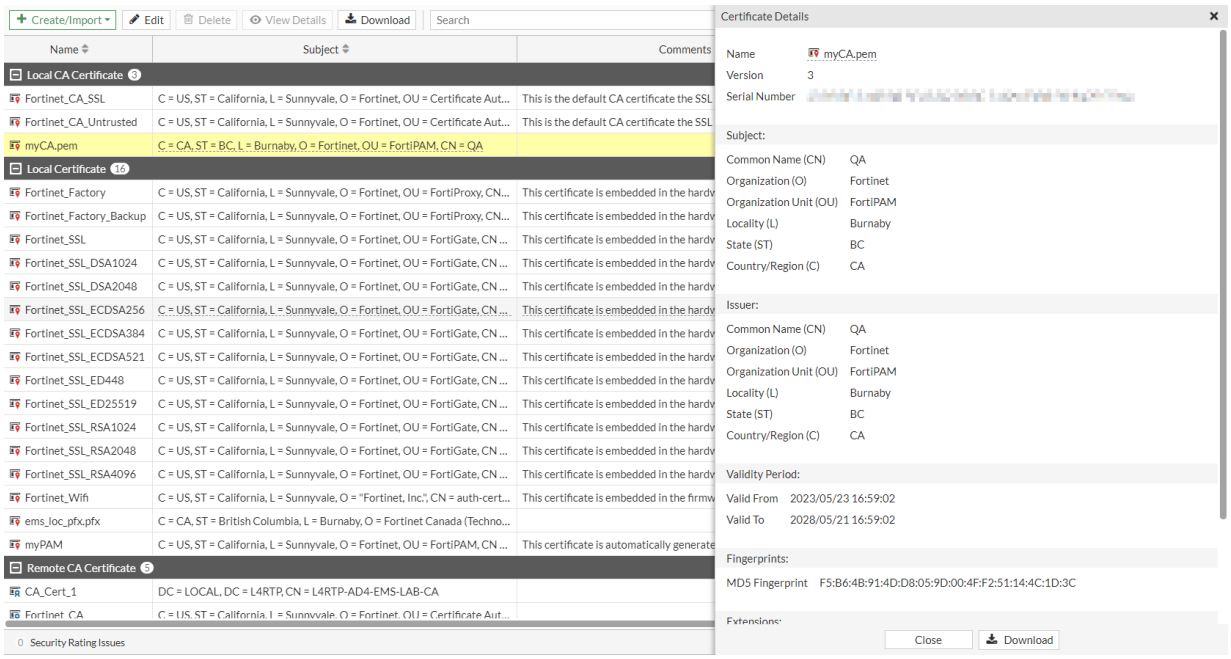
   f. Configure the PuTTy launcher:
      i. Go to *Secret Settings* > *Launchers* > *PuTTy*.
      ii. Enable *Client Software*.
      iii. From the dropdown list, select the desired client software package. Save.
   g. Configure the template:
      i. Go to *Secret Settings* > *Templates* > *FortiGate SSH Password Template*.
      ii. Under *Launcher*, click *Create*.
      iii. From the *Launcher Name* dropdown list, select *PuTTY*.
      iv. In the *Launcher Port* field, enter the port number.
      v. Enable *Integrity Check*. Click *OK* and save the template.
2. Install FortiClient with PAM enabled.
3. Register to EMS.
4. Go to *Settings* > *Advanced*. Ensure that PAM is enabled.
5. Log in to FortiPAM as a standard user from the endpoint.
6. Go to *Secrets* > *Secret List*.
7. Click *Launch Secret* to launch the PuTTy secret through the PuTTy application. The PuTTy session establishes.
8. Go to C:\Program Files\Fortinet\FortiClient\logs\trace\fortivrs_session_1_1.log to verify the integrity check-related logs. From the example logs, you can observe that FortiClient calculates MD5, SHA1 and SHA256 checksums and then compares them with the executable hash in the FortiPAM integrity check package:

```
[2023-08-09 09:51:47.7398329] [12376:6272] [fortivrs 2316    info] startProgram:
cmdline2-1: C:\Program Files\PuTTY\putty.exe admin@172.19.200.253 -P 22
[2023-08-09 09:51:47.7435547] [12376:6272] [fortivrs 2316    info]
PerformHashCheck: Program Path(C:\Program Files\PuTTY\putty.exe), HashMethod: 1,
Calculated HashSum: 14080A3E4E877BE235F06509B2A4B6A9
[2023-08-09 09:51:47.7465327] [12376:6272] [fortivrs 2316    info]
PerformHashCheck: Program Path(C:\Program Files\PuTTY\putty.exe), HashMethod: 2,
Calculated HashSum: 868866BD51F1AC744991C08EDA6446222A0CCDAE
[2023-08-09 09:51:47.7506061] [12376:6272] [fortivrs 2316    info]
PerformHashCheck: Program Path(C:\Program Files\PuTTY\putty.exe), HashMethod: 3,
Calculated HashSum:
35C9DF3A348AE805902A95AB8AD32A6D61EF85CA8249AE78F1077EDD2429FE6B
[2023-08-09 09:51:47.7513043] [12376:6272] [fortivrs 2316    info]
PerformIntegrityCheck: (exe-hash):: Program Path(C:\Program Files\PuTTY\putty.exe),
HashSum Matched for SHA256
[2023-08-09 09:51:47.7556323] [12376:6272] [fortivrs 2316    info] startProgram:
Program Started, pid: 9868, session: 9540
[2023-08-09 09:51:47.7569721] [12376:12572] [fortivrs 2316    info]
updateFortiVRS0: Send Client Update to FortiVRS[0], res_code(3)
[2023-08-09 09:51:47.7607448] [12376:12560] [fortivrs 2316    info]
SendUpdatetoFortiVRS0: SendUpdatetoFortiVRS0 success!.
```

When the integrity check fails due to a tampered PuTTY application (executable hash value mismatch between the PuTTY.exe file and the hash in FortiPAM), *"The required software to launch is not installed on the computer. Click here to download"* displays. Click *here* to download the PuTTY.exe application to the endpoint. Install the application and relaunch the secret. Secret launching succeeds with the newly downloaded application.

To configure PAM agent integrity check using certificate when launching RDP signed by private CA:

1. Configure FortiPAM:
   a. In FortiPAM, go to *System* > *Certificates* > *Create/Import* > *Certificate* > *Import Certificate* > *Certificate* and upload the certificate and key files. Enter and confirm the password, then click *Create* and *OK*. The uploaded certificate displays under *Local CA Certificates*.



b. Go to *Secret Settings* > *Integrity Check*.

c. Create a client software package using the certificate.

d. From the *CA Certificate* dropdown list, select the uploaded certificate.

e. From the *Package Download Option* dropdown list, select *Internal download URL*.

f. In the *Package* field, upload the mstsc.exe file that the private CA signed. Click *OK* and save.

g. Configure the RDP launcher:

  i. Go to *Secret Settings* > *Launchers* > *Remote Desktop-Windows*.

  ii. Enable *Client Software*.

  iii. From the dropdown list, select the desired client software package. Save.

h. Configure the template:

  i. Go to *Secret Settings* > *Templates* > *FortiGate SSH Password Template*.

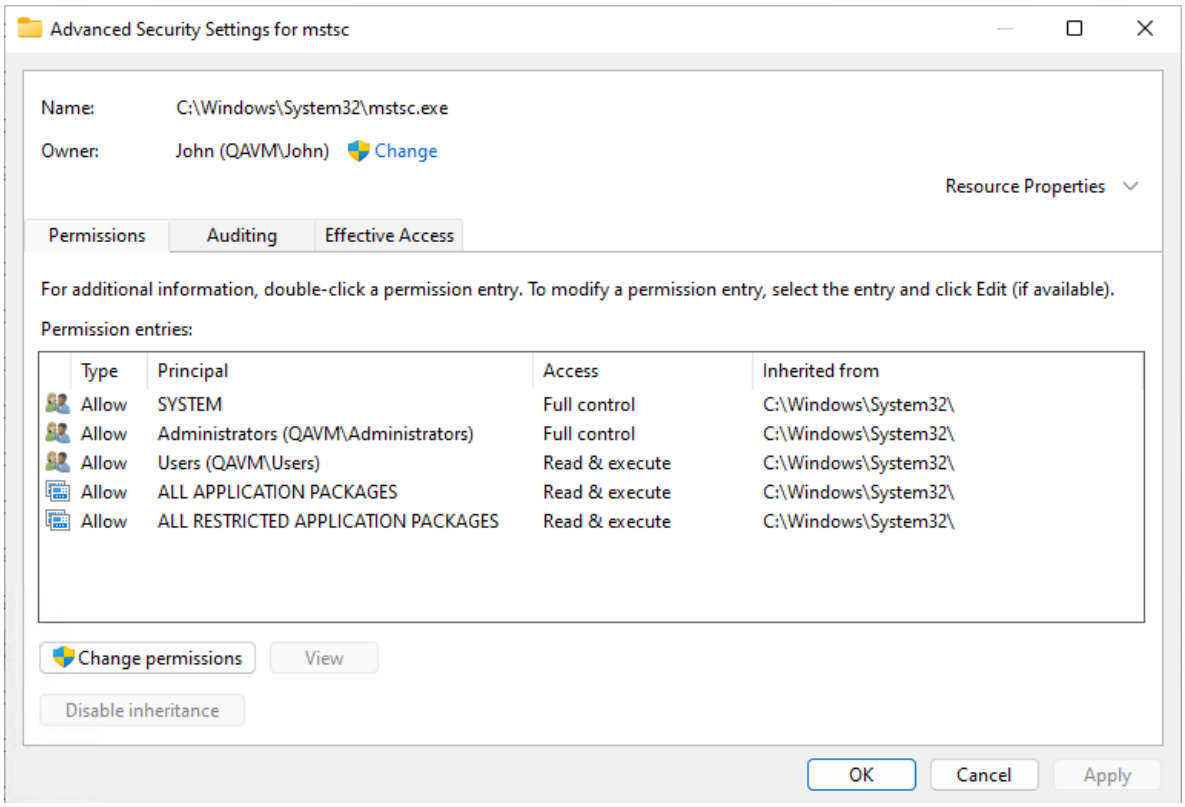
  ii. Under *Launcher*, click *Create*.

  iii. From the *Launcher Name* dropdown list, select *Remote Desktop-Windows*.

  iv. In the *Launcher Port* field, enter the port number.

  v. Enable *Integrity Check*. Click *OK* and save the template.

2. On the Windows endpoint, go to C:\Windows\System32 and replace the mstsc.exe signed by the public CA with the mstsc.exe file signed by the private CA (myCA.pem). To replace the file, change the permissions on the mstsc.exe file signed by public CA by going to *Properties* > *Security* > *Advanced*, clicking *Change* beside *Owner*, and entering the user account that is currently logged in, and clicking *OK*. Click *Apply* and *OK* to save the permission. Then replace the file with the mstsc.exe signed by private CA.



3. Install FortiClient with PAM enabled.
4. Register to EMS.
5. Go to *Settings* > *Advanced*. Ensure that PAM is enabled.
6. Log in to FortiPAM as a standard user from the endpoint.
7. Go to *Secrets* > *Secret List*.
8. Click *Launch Secret* to launch the RDP secret through the RDP application. The RDP session establishes after verifying the mstsc.exe file certificate. Since the RDP application is signed by a private CA, the application certificate is considered valid and the secret launches.
9. Go to C:\Program Files\Fortinet\FortiClient\logs\trace\fortivrs_session_1_1.log to verify the integrity check-related logs. From the example logs, you can observe that the RDP application (mstsc.exe) file certificate is verified and then secret session is launched:

```
[2023-08-15 13:56:16.9145914 UTC-07:00] [15228:15280] [fortivrs 2434    info]
startProgram: cmdline2-1: ndirsystem32\mstsc.exe /V:172.19.200.243:3389
/noConsentPrompt
[2023-08-15 13:56:16.9150111 UTC-07:00] [15228:15280] [fortivrs 2434    info]
PerformIntegrityCheck: Secret does not exist at path: ndirsystem32\mstsc.exe
[2023-08-15 13:56:16.9154416 UTC-07:00] [15228:15280] [fortivrs 2434    info]
startProgram: cmdline3: C:\Windows\mstsc.exe /V:172.19.200.243:3389
/noConsentPrompt
[2023-08-15 13:56:16.9158138 UTC-07:00] [15228:15280] [fortivrs 2434    info]
PerformIntegrityCheck: Secret does not exist at path: C:\Windows\mstsc.exe
[2023-08-15 13:56:16.9160824 UTC-07:00] [15228:15280] [fortivrs 2434    info]
startProgram: cmdline4: C:\Windows\system32\mstsc.exe /V:172.19.200.243:3389
/noConsentPrompt
```

```
[2023-08-15 13:56:16.9628112 UTC-07:00] [15228:15280] [fortivrs 2434    info]
IntegrityCheck::PhpVerifyFile: WinVerifyTrust_I Status Code: 0x800b010a
[2023-08-15 13:56:16.9639246 UTC-07:00] [15228:15280] [fortivrs 2434    info]
PerformIntegrityCheck: (cert):: Program Path(C:\Windows\system32\mstsc.exe),
Certificate Verified
```

FortiTray

When FortiClient is running on your system, you can select the FortiTray icon in the Windows system tray to perform various actions. The FortiTray icon is available in the system tray even when FortiClient is closed.

- Default menu options:
  - Open FortiClient
  - View *About* tab in FortiClient
  - Shut down FortiClient
- Dynamic menu options, depending on configuration:
  - Connect to a configured IPsec VPN or SSL VPN connection
  - Display the AV scan window (if a scheduled scan is currently running)
  - Display the Vulnerability scan window (if a vulnerability scan is running)

If you hover the cursor over the FortiTray icon, you receive various notifications including the FortiClient version, AV signature version, and AV engine version.

When EMS has locked the configuration, the option to shut down FortiClient from FortiTray is grayed out.

To establish a VPN connection from FortiTray:

1. Select the Windows System Tray.
2. Right-click the *FortiTray* icon, and select a VPN connection configuration.
3. Enter your username and password in the authentication window, and click *OK* to connect.

Diagnostic Tool

You can access the FortiClient Diagnostic Tool from FortiClient. Go to *About*.

On FortiClient (Windows), you can also access the Diagnostic Tool from the *Start* menu.

You can use the FortiClient Diagnostic Tool to generate a debug report, then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report and email the report to customer support to help with troubleshooting.

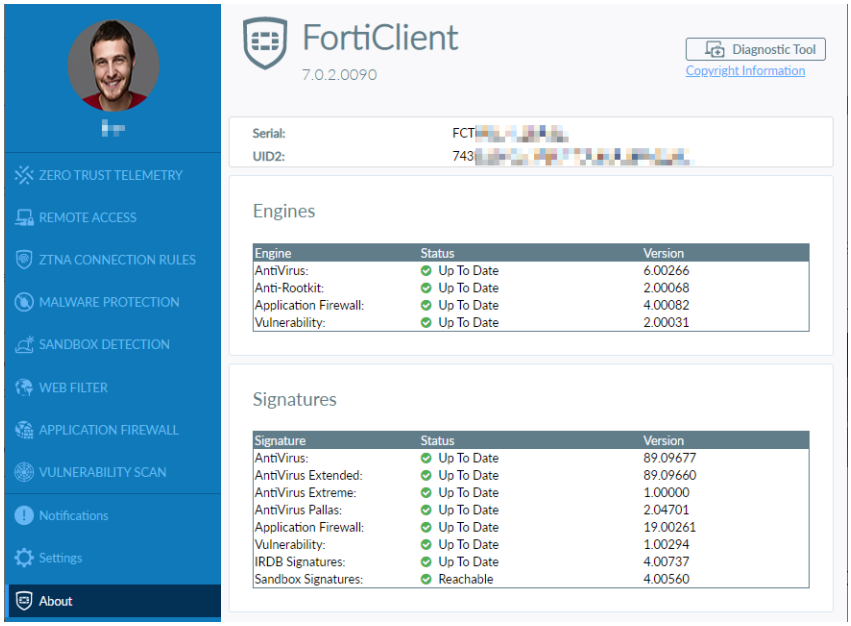
The FortiClient Diagnostic Tool does not record sensitive information. It contains information about the endpoint such as:

- Windows operating system version
- Windows software updates
- Names and versions of installed software
- Names and versions of installed drivers
- FortiClient configuration
- FortiClient logs

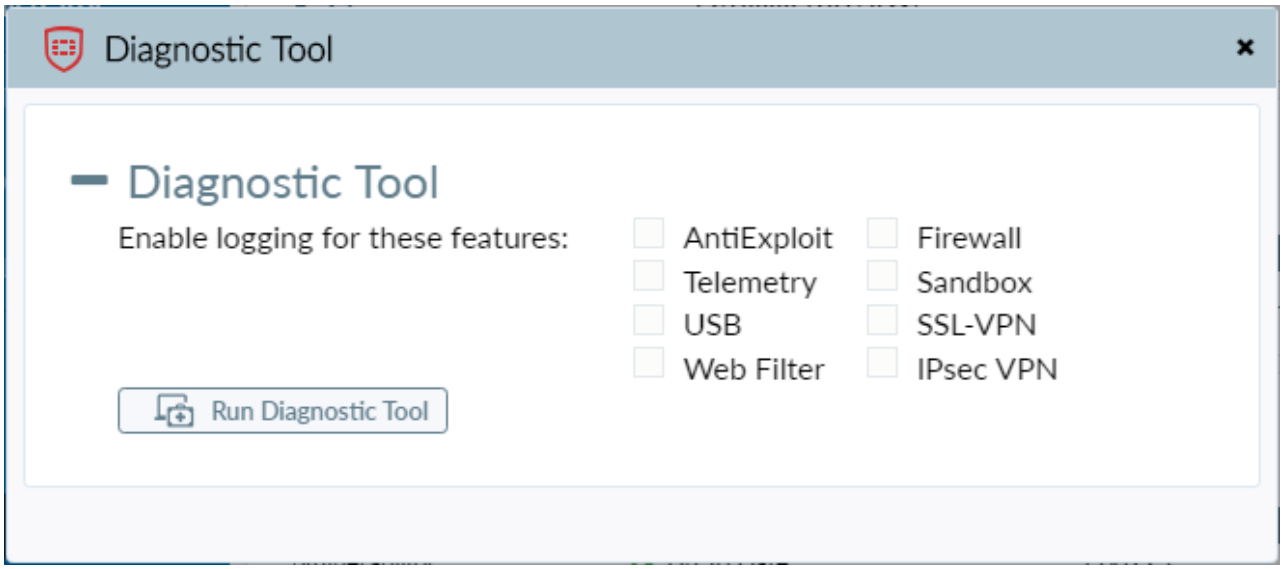
Before sending the package that the FortiClient Diagnostic Tool created to the FortiClient team, you can open and read the package.

To access the FortiClient Diagnostic Tool:

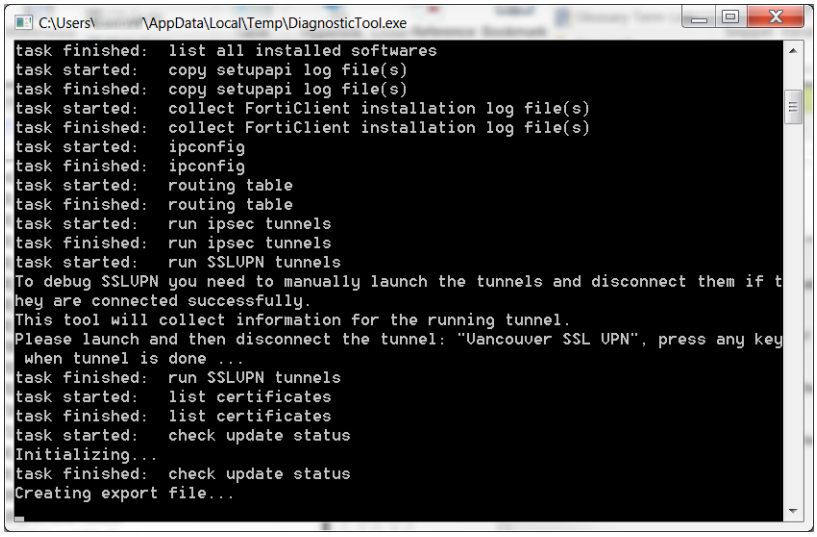
1. Go to *About*.



2. Click the *Diagnostic Tool* button in the top right corner. The FortiClient Diagnostic Tool dialog displays.



3. The dialog displays the features selected by the EMS administrator. Click *Run Diagnostic Tool*.
4. Click *Run Tool*. A window displays the provided status information.



5. (Optional) When prompted, launch and disconnect the VPN tunnels for which you want to collect information. The Diagnostic Tool creates a *Diagnostic_Result* file and displays it in a folder on the endpoint. The default folder location is *C:\Users <username>\AppData\Local\FortiClient\tmp*.
6. Click *Close*.

Forensic analysis

The FortiGuard Endpoint Forensic Analysis service provides remote endpoint analysis to help your organization respond to and recover from cyber incidents. For each engagement, forensic analysts from Fortinet's FortiGuard Labs remotely assist in collecting, examining, and presenting digital evidence, including a final detailed report.

See Requesting forensic analysis.

Appendix A - API

You can operate FortiClient VPNs using the COM-based FortiClient API. You can use the API only with IPsec VPN. The API does not support SSL VPN.

Overview

The FortiClient COM library provides functionality to:

- Retrieve a list of VPN tunnels configured in the FortiClient application.
- Start and stop any configured VPN tunnel.
- Send XAuth credentials.
- Retrieve status information:
  - Configured tunnel list
  - Active tunnel name
  - Connection status
  - Idleness status
  - Remaining key life
- Respond to FortiClient-related events:
  - VPN connect
  - VPN disconnect
  - VPN is idle
  - XAuth authentication requested

For more information, see the vpn_com_examples ZIP file located in the VPN automation file folder in the FortiClientTools file.

API reference

The following tables provide API reference values:

`Disconnect(bstrTunnelName As String)`	Close the named VPN tunnel.
`GetRemainingKeyLife(bstrTunnelName As String, pSecs As Long, pKBytes As Long)`	Retrieve the named connection remaining key life. Whether key life time (pSecs) or data (pKBytes) are significant depends on the detailed settings in the FortiClient application.
`SendXAuthResponse (tunnelName As String, userName As String, password As String, savePassword As Boolean)`	Send XAuth credentials for the named connection: • Username, password • True if password should be saved

`GetTunnelList()`	Retrieve the list of all connections configured in the FortiClient application.
`IsConnected (bstrTunnelName As String) As Boolean`	Return `True` if the named connection is up.
`IsIdle (bstrTunnelName As String) As Boolean`	Return `True` if the named connection is idle.

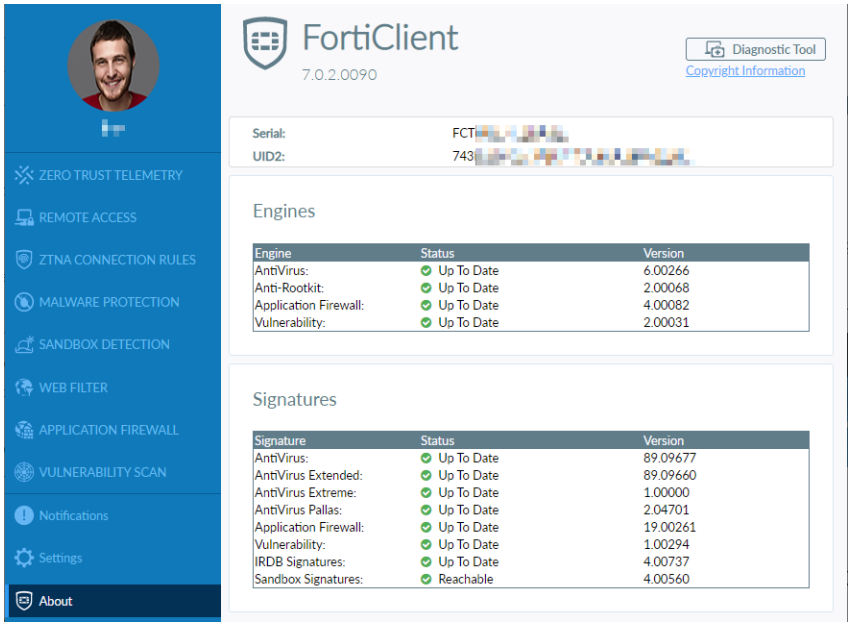
`OnDisconnect(bstrTunnelName As String)`	Connection disconnected.
`OnIdle(bstrTunnelName As String)`	Connection idle.
`OnXAuthRequest(bstrTunnelName As String)`	The VPN peer on the named connection requests XAuth authentication.

Appendix B - Vulnerability patches

FortiClient checks many applications for vulnerabilities. FortiClient can automatically patch vulnerabilities from some applications, but not all applications. For some applications, you must manually patch vulnerabilities.

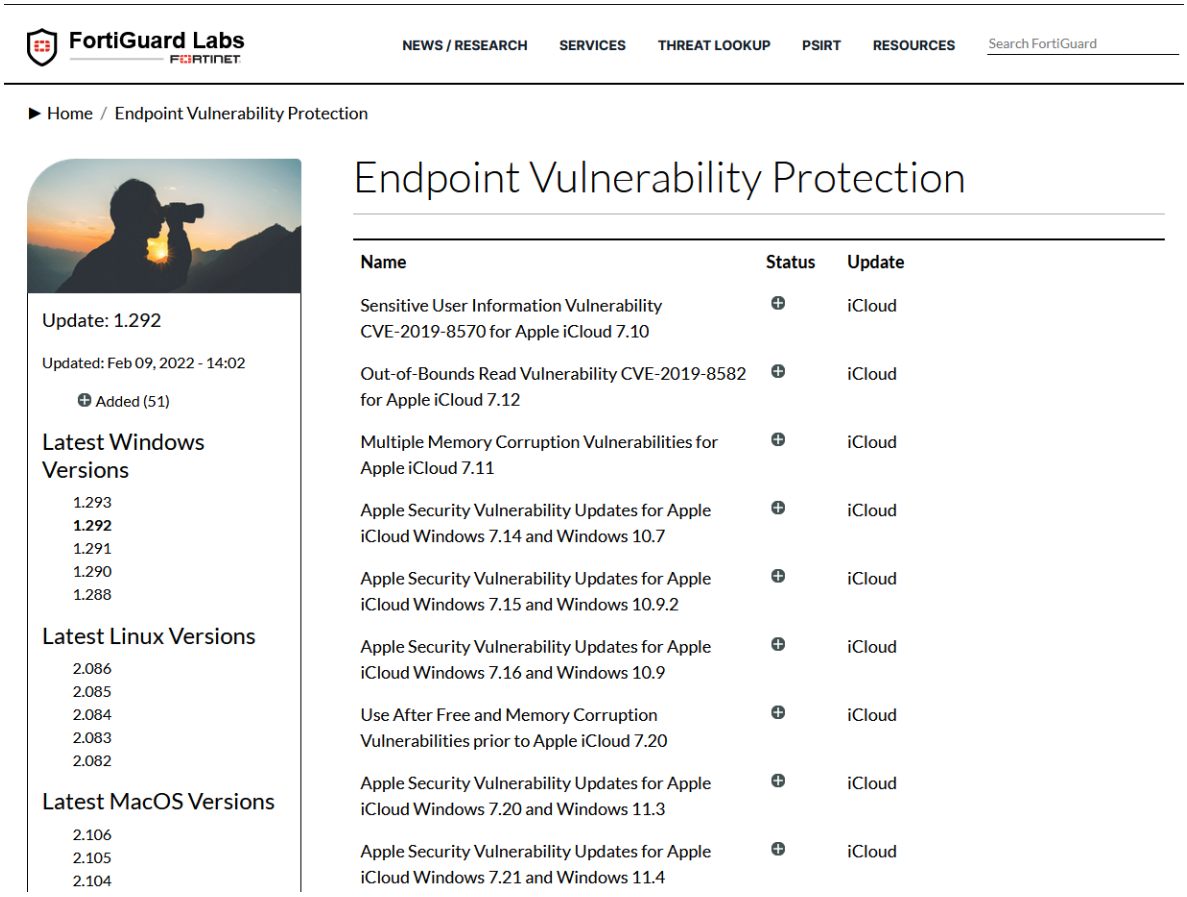
To view vulnerability signature information:

1. In FortiClient, go to *About* to check the vulnerability signature version number. In the example, the version number is 1.00294.



2. Go to Endpoint Vulnerability Protection Service.
3. At the bottom of the page, click the desired vulnerability signature version. The vulnerabilities added for that

signature version are listed.



Appendix C - Processes

This section identifies the processes used by FortiClient (Windows) and FortiClient (macOS).

FortiClient (Windows) processes

The following table identifies the processes in Task Manager that FortiClient (Windows) uses:

Name	Description	Purpose
	FortiClient Virus Feedback Service	Used by antivirus (AV) and FortiClient to submit samples to FortiGuard
FCVbltScan.exe	FortiClient Vulnerability Scan Daemon	FortiClient Vulnerability Scan engine
FortiAvatar.exe	FortiClient User Avatar Agent	Used by FortiClient and FortiClient Telemetry to obtain avatar images for users
ipsec.exe	FortiClient IPsec VPN Service	Remote Access for IPsec VPN
FortiClient.exe	FortiClient Console	FortiClient GUI
FortiClient_Diagnostic_Tool.exe	FortiClient Diagnostic Tool	Diagnostic Tool
av_task.exe	FortiClient Antivirus Scanner	FortiClient AV
AzureToken.exe	FortiClient Azure token agent	Token information verification
EPCUserAvatar.exe	FortiClient user avatar agent	Update avatar information
fcappdb.exe	FortiClient Application Database Service	Application Firewall
fcaptmon.exe	FortiClient Sandbox Agent	Sandbox Detection
FCAuth.exe	FortiClient authentication	Authentication

Name	Description	Purpose
FCCOMInt.exe	FortiClient COM interface	COM server for starting and stopping IPsec VPN tunnels. Facilitates interaction with FortiGate appliances or FortiManager for policy enforcement and updates.
FCConfig.exe	FortiClient Configuration Daemon	Configuration update
FCDBLog.exe	FortiClient Logging Daemon	Logging
FCHelper64.exe	FortiClient System Helper	FortiClient ensures 32-bit processes can access 64-bit resources
fcmonitor.exe	FortiClient Application Control Agent	Monitoring and maintaining monitoring and maintaining the functionality of FortiClient on the system
FctSecSvr.exe	FortiClient WSC Services	FortiClient integration into Windows Security Center
fmon.exe	FortiClient Realtime AntiVirus Protection	AV
fortiae.exe	FortiClient Anti-Exploit	Anti-Exploit engine
FortiClientConsole.exe	FortiClient Security Console	FortiClient integration into Windows Security Center
FortiClientSecurity.exe	FortiClient Security	FortiClient integration into User Account Control
FortiElevate.exe	FortiClient Elevation	Allows FortiClient or related services to perform actions that require elevated privileges (e.g., modifying system settings, installing updates, or applying network configurations).
FortiESNAC.exe	FortiClient Network Access Control	FortiClient Telemetry
fortifws.exe	FortiClient Firewall Service	Application Firewall
FortiGuardAgent.exe	forticlint web filter service	Web Filter service
FortiProxy.exe	FortiClient Proxy Service	AV and Web Filter
FortiScand.exe	FortiClient Scan Server	Offloading AV scanning to a separate process
FortiSettings.exe	FortiClient Settings Service	Used by FortiClient settings

Name	Description	Purpose
FortiSSLVPNdaemon.exe	FortiClient SSLVPN daemon	Remote Access for SSL VPN
FortiSSLVPNsys.exe	FortiClient SSLVPN shadow mode connector	SSLVPN
FortiTcs.exe	FortiClient ZTNA service	ZTNA service
FortiTray.exe	FortiClient System Tray Controller	FortiTray
FortiUSBmon.exe	FortiClient USB monitor protection	Removable media access control.
FortiVPN.exe	FortiClient VPN Controller	Schedules, controls, and monitors VPN connections
fortivrs.exe	FortiClient Video Record Daemon	provides PAM functionality
FortiVPN.exe	FortiClient VPN Controller	Schedules, controls, and monitors VPN connections
FortiWF.exe	FortiClient Web Filter Service	Used by Web Filter
FSSOMA.exe	Single sign on mobility agent	User authentication
scheduler.exe	FortiClient Scheduler	Windows ensures FortiClient services are running when needed
submitv.exe	FortiClient Virus Feedback Service	Used by antivirus (AV) and FortiClient to submit samples to FortiGuard
update_task.exe	FortiClient Auto-Update Agent	Communication with FortiGuard servers for signature updates
vcm2.exe	vulnerability engine	FortiClient Vulnerability Scan Engine

FortiClient (macOS) processes

FortiClient (macOS) uses the following processes:

- The process for the FortiClient main GUI is located at `/Application/FortiClient.app/Contents/MacOS/FortiClient`
- The process for FortiTray controller is located at `/Application/FortiClient.app/Contents/Resources/runtime.helper/FortiClient Agent.app/MacOS/FortiClientAgent`

- The process for FortiClient upgrade GUI is located at `/Application/FortiClient.app/Contents/Resources/runtime.helper/FortiClient Update.app/Contents/MacOS/FortiClientUpdate`

The following table identifies the processes in the following location used by FortiClient (macOS):

`/Library/Application Support/Fortinet/FortiClient/bin`:

Name	Purpose
fctservctl	FortiClient Service Controller
epctrl	FortiClient endpoint control daemon
ftgdagent	Web Filter
fmon	AV scan main program
scanunit	AV scan scanner
vulscan	Vulnerability scan
fctappfw	Firewall service
fssoavgent_launchagent	FSSO agent
fssoavgent_launchdaemon	FSSO daemon
fctctld	VPN controller
sslvpnd	SSL VPN Daemon
racoon	IPsec VPN Service
racoonctl	IPsec VPN Controller
fctupdate	FortiClient update tool
fctupgrade	FortiClient upgrade tool

Appendix D - CLI commands

FortiClient (Windows) CLI commands

FortiClient supports the following CLI installation options with FortiESNAC.exe for endpoint control:

```
Usage:
c:\Program Files\Fortinet\FortiClient\FortiESNAC.exe -r|--register <address/invitation> [-
p|--port <port>] [-v|--vdom <site>]
c:\Program Files\Fortinet\FortiClient\FortiESNAC.exe -u|--unregister
c:\Program Files\Fortinet\FortiClient\FortiESNAC.exe -d|--details

Options:
  -h --help Show the help screen
  -r --register Register using an EMS address or an invitation code
  -p --port EMS port, ignored if registering by invitation code (Optional, 8013 by default)
  -v --vdom EMS site, ignored if registering by invitation code (Optional, "Default" by
default)
  -u --unregister Unregister from the current EMS
  -k --key Key for registering/deregistering from EMS if required.
                  Will prompt for user input if key verification fails or no key is given.
  -m --remember Remember the given connection key specified by -k|--key when registering to
EMS
                  (Optional, will not remember the key by default)
  -d --details Show telemetry details and status
```

FortiClient (macOS) CLI commands

The following summarizes the CLI commands available for FortiClient (macOS) 7.2.7:

Endpoint control

FortiClient 7.2.7 must establish a Telemetry connection to EMS to receive license information. FortiClient features are only enabled after connecting to EMS.

Usage

You can access endpoint control features through the `epctrl` CLI command. This command offers the end user the ability to connect or disconnect from EMS and check the connection status. You can access usage information by using the following commands:

```
➜  ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -h
FortiClient Endpoint Control

Usage:
```

```
  /Library/Application Support/Fortinet/FortiClient/bin/epctrl -r|--register
<address/invitation> [-p|--port <port>] [-s|--site <site>] [-k|--key <key>] [-m|--remember]
  /Library/Application Support/Fortinet/FortiClient/bin/epctrl -u|--unregister [-k|--key
<key>]
  /Library/Application Support/Fortinet/FortiClient/bin/epctrl -d|--details
  /Library/Application Support/Fortinet/FortiClient/bin/epctrl -t|--trust accept|deny
  /Library/Application Support/Fortinet/FortiClient/bin/epctrl -a|--auth

Options:
  -h --help        Show the help screen
  -r --register    Register using an EMS address or an invitation code
  -p --port        EMS port, ignored if registering by invitation code (Optional, 8013 by
default)
  -s --site        EMS site, ignored if registering by invitation code (Optional, "Default"
by default)
  -u --deregister  Deregister from the current EMS
  -k --key         Key for registering/deregistering from EMS if required. Will prompt for
user input if key verification fails or no key is given
  -m --remember    Remember the given connection key specified by -k|--key when registering
to EMS (Optional, will not remember the key by default)
  -t --trust       Trust or deny a pending invalid EMS certificate
  -a --auth        Initializes the authentication process if user authentication is enabled
on EMS
  -d --details     Show telemetry details and status
```

Connecting to on-premise EMS

FortiClient can connect to on-premise EMS using the following commands. If EMS is listening on the default port, 8013, you do not need to specify the port number. If EMS is listening on another port, such as 8444, you must specify the port number with the EMS IP address. The example illustrates both use cases.

Connecting to on-premise EMS using an invitation code (SAML configured)

```
➜ ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -r <invitation_code>
SAML URL: {SAML_url}
Username: Connected!
```

Connecting to on-premise EMS using IP address and default port

```
➜ ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -r 172.18.60.251
Registering to EMS 172.17.60.251:8013.
```

Connecting to on-premise EMS using IP address and non-default port

```
➜ ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -r 172.18.60.251 -p 8444
Registering to EMS 172.17.60.251:8444.
```

Connecting to on-premise EMS with multitenancy enabled

If EMS multitenancy is enabled, you can also specify the site name. If connecting to the default site, you do not need to provide a site name. The example illustrates connecting to a site named "headquarters".

```
➜ ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -r 172.18.60.251 -s
    headquarters
```

Disconnecting from EMS

```
➜  ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -u
Deregistered
```

Specifying and remembering required connection key

EMS may require a connection key for FortiClient to connect.

```
➜ ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -r 172.18.60.251 -k
    <connection_key> -m
➜ ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -u -k <connection_key>
```

Trusting or denying pending invalid EMS certificate

```
➜ ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -t accept|deny
```

Initializing authentication process if EMS has enabled user authentication

```
➜ ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -a
```

Showing telemetry details and status

The following example shows output when FortiClient is not connected to EMS:

```
➜  ~ /Library/Application\ Support/Fortinet/FortiClient/bin/epctrl -d

====================================
 FortiClient License Details
====================================
Last EMS Access Time:  Never Accessed
License Expiry:        Unlicensed
VPN Expiry:            Wed Feb 14 11:14:58 2024 PST

====================================
 FortiClient EMS Details
====================================
No telemetry data available.
```

FortiClient (Linux) CLI commands

FortiClient (Linux) supports an installer targeted towards the headless version of Linux server. FortiClient (Linux) 7.2.7 for servers (forticlient_server_7.2.7.xxxx) offers a command line interface and is intended to be used with the CLI-only (headless) installation. The same set of CLI commands also work with a FortiClient (Linux) GUI installation.

The following summarizes the CLI commands available for FortiClient (Linux) 7.2.7:

Endpoint control

FortiClient 7.2.7 must establish a Telemetry connection to EMS to receive license information. FortiClient features are only enabled after connecting to EMS.

Usage

You can access endpoint control features through the `epctrl` CLI command. This command offers the end user the ability to connect or disconnect from EMS and check the connection status. You can access usage information by using the following commands:

```
jameslee@sunshine:~$ forticlient epctrl -h
Endpoint Control CLI interface

Usage: forticlient epctrl [command]

Available Commands:
auth    Initializes the authentication process if user authentication is enabled on EMS
detail    Show detail of endpoint status
disconnect  Disconnect from an EMS
register  Register to a specified EMS IP, Hostname, or invitation code
trust   Trust or deny a pending invalid EMS certificate
```

Connecting to EMS or FortiClient Cloud

FortiClient can connect to on-premise EMS or FortiClient Cloud using the following commands. If EMS is listening on the default port, 8013, you do not need to specify the port number. If EMS is listening on another port, such as 8444, you must specify the port number with the EMS IP address. The example illustrates both use cases:

```
jameslee@sunshine:~$ forticlient epctrl register 172.17.60.251
Registering to EMS 172.17.60.251:8013 at site "default".

jameslee@sunshine:~$ forticlient epctrl register 172.17.60.251 -p 8444
Registering to EMS 172.17.60.251:8444.
```

If EMS multitenancy is enabled, you can also specify the site name. If connecting to the default site, you do not need to provide a site name. The example illustrates connecting to a site named "headquarters".

```
jameslee@sunshine:~$ forticlient epctrl register 172.17.60.251 -s headquarters
```

FortiClient can connect to on-premise EMS or FortiClient Cloud using an invitation code (ABCDEF123 in the example) that you received from the administrator:

```
jameslee@sunshine:~$ forticlient epctrl register ABCDEF123
```

Endpoint control status

You can check FortiClient endpoint control status details with the `detail` argument. When FortiClient is connected to EMS only, the command output is as follows:

```
jameslee@sunshine:~$ forticlient epctrl detail
====================================
FortiClient License Details
====================================
License Expiry:  Mon Oct 14 11:16:32 2024 PDT
VPN Expiry:      N/A (EMS Connected)

====================================
FortiClient EMS Details
====================================
IP:                192.168.34.30
Site:              default
```

```
Host:              ubuntu
SN:                FCTEMS123456
Status:            Connected
Last Access Time:  Thu Jun  6 11:56:35 2024 PDT

====================================
Zero Trust Tags
====================================
Ubuntu2204
```

If FortiClient is connected to EMS and notifying FortiGate, the endpoint control status displays the serial numbers and hostnames of the EMS and FortiGates as follows:

```
jameslee@sunshine:~$ forticlient epctrl detail

====================================
FortiClient License Details
====================================
License Expiry:  Mon Oct 14 11:16:32 2024 PDT
VPN Expiry:      N/A (EMS Connected)

====================================
FortiClient EMS Details
====================================
IP:                192.168.34.30
Site:              default
Host:              ubuntu
SN:                FCTEMS123456
Status:            Connected
Last Access Time:  Thu Jun  6 11:56:35 2024 PDT

====================================
Zero Trust Tags
====================================
Ubuntu2204

====================================
FortiGate Details
====================================
IP: 172.17.60.40
Host: FGVM02TM18001119
SN: FGVM02TM18001119
Status: Connected
```

When FortiClient is not connected to EMS, the endpoint control status has no Telemetry data available as shown:

```
jameslee@sunshine:~$ forticlient epctrl detail

====================================
FortiClient License Details
====================================
License Expiry:  Unlicensed
VPN Expiry:      Fri Jul  5 14:55:13 2024 PDT

====================================
FortiClient EMS Details
====================================
No telemetry data available.
```

```
====================================
Zero Trust Tags
====================================
```

Disconnecting from EMS

FortiClient can disconnect from EMS only if the configuration received from EMS allows it. You can disconnect using the `disconnect` command.

```
jameslee@sunshine:~$ forticlient epctrl disconnect
Unregistering from EMS.
```

AV scanning

You may run an AV scan from the CLI on the entire file system or on a specified directory. You can only run an AV scan as the root user. After completing an AV scan, FortiClient prints the scan results and detailed log file locations. You can run the following command to run an AV scan, where `<directory_path>` is the directory path to scan. You can perform a full scan by inputting `/` in place of `<directory_path>`.

```
forticlient fmon scan custom <directory_path>
```

The following shows an AV scan performed on the `/var` directory:

```
jameslee@sunshine:/var$ forticlient fmon scan custom /var
Signature dir : forticlient/vir_sig/
Log dir : forticlient/
Fmon on daemon mode.
Dest dir : /var
CPU number : 1
Server port : 40140
AV Engine path : forticlient/libav.so
AV Signature path : forticlient/vir_sig/vir_high:forticlient/vir_sig/vir_sandbox_sig
Load AV signature success.
<=== PID : 13821 Client Hello rc = 2185
Child : 13821 ready
===> Scan : /var/spool/anacron/cron.daily
===> Scan : /var/spool/anacron/cron.weekly
===> Scan : /var/spool/anacron/cron.monthly
===> Scan : /var/crash/_usr_bin_gedit.1001.crash
===> Scan : /var/crash/_opt_forticlient_fmon.1000.crash
===> Scan : /var/backups/apt.extended_states.1.gz
===> Scan : /var/backups/shadow.bak
===> Scan : /var/backups/dpkg.statoverride.2.gz
===> Scan : /var/backups/passwd.bak
===> Scan : /var/backups/dpkg.diversions.1.gz
===> Scan : /var/backups/apt.extended_states.0
===> Scan : /var/backups/dpkg.arch.2.gz
===> Scan : /var/backups/alternatives.tar.1.gz
===> Scan : /var/backups/dpkg.arch.0
===> Scan : /var/backups/dpkg.status.1.gz
===> Scan : /var/backups/dpkg.statoverride.0
===> Scan : /var/backups/dpkg.arch.1.gz
===> Scan : /var/backups/gshadow.bak
===> Scan : /var/backups/dpkg.diversions.2.gz
===> Scan : /var/backups/alternatives.tar.2.gz
.............................
.............................
```

```
 ..............................
 -------------- scan_dispatch_worker finished -------------

Scan started at Mon Apr 22 14:43:45 2019

Found virus : EICAR_TEST_FILE
In file : /var/eicar.com
Action : Quarantine success
Quarantine file : forticlient/quarantine/eicar.com.1

--------------- Scan summary ---------------------
Total scan files : 10947
Found virus : 1
Worker crash : 0
Worker timeout : 0
------------------------------------------------

Scan ended at Mon Apr 22 14:44:01 2019

Full results can be found in forticlient/Daemon - Mon Apr 22 14:43:45 2019.log
```

You can restore a quarantined file. This releases the file from quarantine and makes it accessible to the user.

```
jameslee@sunshine:/home/jameslee$ sudo /opt/forticlient/fchelper -r <file>
```

Vulnerability scanning

You can run a vulnerability scan from the CLI to check for vulnerable applications on the machine. You can only run a vulnerability scan as the root user. After completing a vulnerability scan, FortiClient prints the number of vulnerabilities present on the machine, their severity levels, and detailed log file locations. You can run a vulnerability scan by running the following command:

```
jameslee@sunshine:/home/jameslee$ forticlient vulscan scan
Vulnerability Scan Complete
--------------- Scan summary ---------------------
Critical : 7
High : 2
Medium : 7
Low : 0
```

You can patch existing vulnerabilities using FortiClient. FortiClient runs a vulnerability scan again after patching the vulnerabilities and prints the results. You can patch vulnerabilities as shown:

```
jameslee@sunshine:/home/jameslee$ forticlient vulscan patch
[INFo} Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig
[INFO] Decryption success!
[INFO] LoadFromDb
[INFO] Total sig : 13163
[INFO] Signature version=1.38
[INFO] Engine version=2.0.0.22
[INFO] Build install list
...

Patching vid 55441
Hit:1 http://ca.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://ca.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:4 http://ca.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
```

```
Get:5 http://ca.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Metadata [278 kB]
Get:6 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metadata [9,364 B]
Get:7 http://ca.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 48x48 Icons [66.7 kB]
Get:8 http://ca.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 64x64 Icons [123 kB]
Get:9 http://ca.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 DEP-11 Metadata [222
kB]
Get:10 http://security.ubuntu.com/ubuntu bionic-security/main DEP-11 48x48 Icons [7,788 B]
Get:11 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 Metadata
[35.7 kB]
Get:12 http://ca.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 48x48 Icons [194
kB]
Get:13 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 48x48 Icons [16.4
kB]
Get:14 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 64x64 Icons [92.2
kB]
Get:15 http://ca.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 64x64 Icons [406
kB]
Get:16 http://ca.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 DEP-11 Metadata
[2,468 B]
Get:17 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11 Metadata
[2,464 B]
Get:18 http://ca.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 DEP-11 Metadata
[7,352 B]
Fetched 1,716 kB in 3s (591 kB/s)
Reading package lists... Done
[INFO] install command is: apt-get -y install --only-upgrade firefox
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
fonts-lyx
The following packages will be upgraded:
firefox
1 upgraded, 0 newly installed, 0 to remove and 315 not upgraded.
Need to get 0 B/48.1 MB of archives.
After this operation, 7,509 kB of additional disk space will be used.
 (Reading database ... 162206 files and directories currently installed.)
Preparing to unpack .../firefox_66.0.3+build1-0ubuntu0.18.04.1_amd64.deb ...
Unpacking firefox (66.0.3+build1-0ubuntu0.18.04.1) over (59.0.2+build1-0ubuntu1) ...
Processing triggers for mime-support (3.60ubuntu1) ...
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.1) ...
Setting up firefox (66.0.3+build1-0ubuntu0.18.04.1) ...
Installing new version of config file /etc/apparmor.d/usr.bin.firefox ...
Please restart all running instances of firefox, or you will experience problems.
Processing triggers for man-db (2.8.3-2) ...
Processing triggers for gnome-menus (3.13.3-11ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
[INFO] query command is: dpkg-query --show firefox
Package version found is 66.0.3+build1-0ubuntu0.18.04.1

Patching vid 55442
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://ca.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://ca.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://ca.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
.............................
.............................
```

```
.............................
-------------- Scan summary ---------------------
Critical : 0
High : 0
Medium : 0
Low : 0
------------------------------------------------
```

FortiClient updates

You can run a FortiClient update task from the CLI once FortiClient has connected to EMS and is licensed. The update task downloads the latest FortiClient engine and signatures. You can only run an update task as the root user. Following are the command and its output:

```
root@sunshine:/home/jameslee# /opt/forticlient/update
```

```
***************Update starting**************
Sandbox test = 0
Sandbox host to test = (null)
log_level: 6
Enable custom fds server :80 failover port: 8000 failover to fdg: 1 allow sw update: 0
Updating FCTDATA: Update started forced update
[INFO] Engine version=2.0.0.22
[INFo} Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig [INFO] Decryption success!
[INFO] LoadFromDb [INFO] Total sig : 13163
[INFO] Signature version=1.38
Getting current FortiClient Components information
current av engine version: 6.2.126
av engine id: 06002000FVEN04100-00006.00126-9999999999
current av main sig full version: 67.1895
av main sig id: 06002000FVDB04000-00067.01895-9999999999
current av ext sig full version: 67.1892
...
...
user jameslee, type:7, session:0, pid:6913
user = jameslee
sandbox server not configured.
Updating FCTDATA: Update finished
[INFO] Engine version=2.0.0.22
[INFo} Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig
[INFO] Decryption success!
[INFO] LoadFromDb
[INFO] Total sig : 13163
[INFO] Signature version=1.38
Downloading done ret = 0
root@sunshine:/home/jameslee#
```

Existing signature details

You can check details of the existing FortiClient engine and signatures by running the `version` command:

```
jameslee@sunshine:/home/jameslee$ forticlient version
```

```
FortiClient Version: 7.2.7.XXXX
FortiClient Serial:  FCT123456
FortiClient UID:     3FF8BE62539...

====================================
Engines
====================================
AntiVirus:          7.00026
Vulnerability:      2.00032

====================================
Signatures
====================================
AntiVirus:          1.00000
AntiVirus Extended: Unavailable
Vulnerability:      2.00425
Sandbox:            Unavailable
ICDB:               1.00026
```

Update help

The update help option lists all options available for the update task. You can access this option as shown:

```
jameslee@sunshine:~$ /opt/forticlient/update -h
FortiClient Update

Usage:
  /opt/forticlient/update [options...]

Options:
  -h Show the help screen
  -v Enable verbose log
```

VPN

You can access VPN features through the `vpn`CLI command. This command offers the end user the ability to connect to or disconnect from VPN and perform other VPN tasks.

```
VPN CLI interface

Usage:
forticlient vpn [command]

Available Commands:
connect     Connect to a VPN
disconnect  Disconnect from VPN
edit        Configure new/existing VPN profile
list        List VPN profiles
remove      Remove VPN profile
status      Print current VPN status
view        View VPN profile
```

Option	Description
`connect <vpn_name>`	Connect to a configured VPN tunnel. Use the `--user=<username>, --password, --save-password`, `--always-up`, and `auto-connect` options to provide the username and password, save the password, or configure the tunnel to always be up or autoconnect.
`disconnect`	Disconnect from VPN.
`edit <vpn_name>`	Create or edit a VPN tunnel configuration.
`list`	List existing VPN tunnel configurations.
`remove <myvpn_name>`	Remove the VPN tunnel configuration.
`status`	Show VPN status.
`view <vpn_name>`	View a VPN tunnel configuration's details.

Connecting to VPN using the Linux CLI may not function correctly on Ubuntu if you do not configure `gnome-keyring`. See the Ubuntu Manpage.

To configure `gnome-keyring`:

1. Install `gnome-keyring`:
   ```
   sudo apt install gnome-keyring
   ```
2. Initialize and unlock the login keyring:
   ```
   killall gnome-keyring-daemon
   echo -n "your-login-password" | gnome-keyring-daemon --unlock
   ```

Appendix E - VPN autoconnect

With autoconnect enabled, when FortiClient launches, it automatically connects to a predefined VPN tunnel. As this happens automatically, you can only specify one tunnel to autoconnect to. You can leverage autoconnect to minimize security complexity when working from home. End users no longer need the extra step of providing credentials and connecting to VPN. FortiClient only attempts this connection once. If it fails due to the server being unreachable or incorrect credentials, FortiClient does not reattempt to connect until the next time the user logs in.

This guide details the settings required to add autoconnect functionality to an existing VPN connection, including the user definition and policies. If you are setting up a new VPN, see Remote access and SSL VPN full tunnel for remote user.

Autoconnect requires some stored credentials for authentication. These credentials can be:

- Username and password. See Configuring autoconnect with username and password authentication on page 132.
- Certificate (user, machine, or smartcard). See Configuring autoconnect with certificate authentication on page 135.

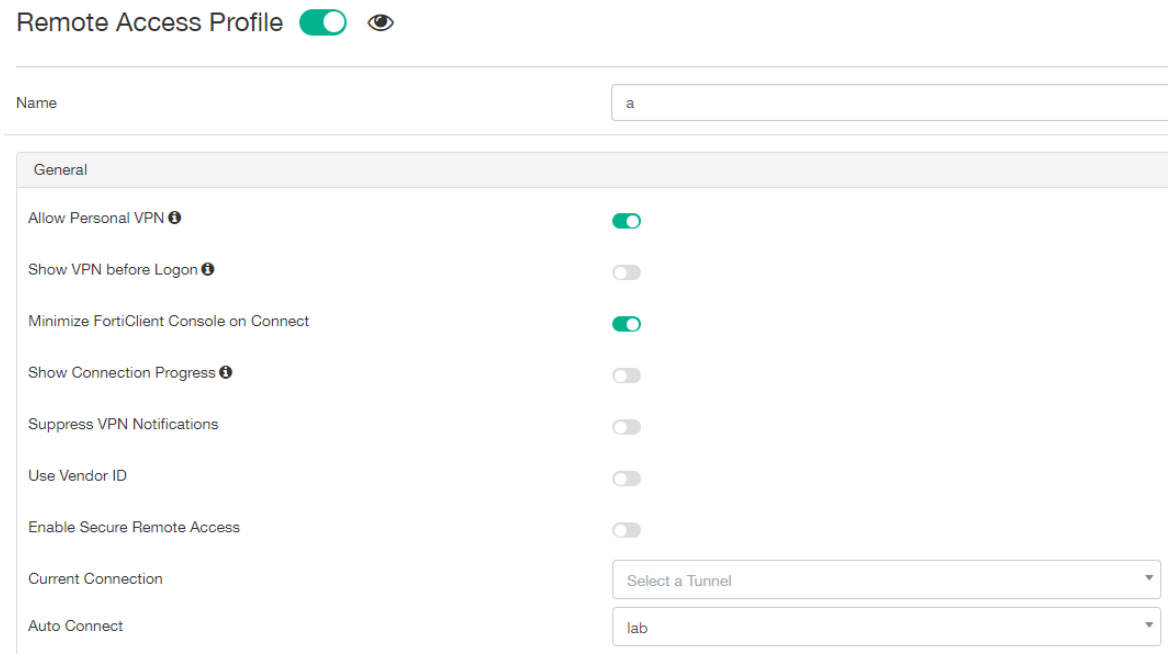
Once you have defined credentials, you must manually establish the tunnel the first time to store the provided credentials for future connections.

Configuring autoconnect with username and password authentication

To configure autoconnect with username and password authentication:

1. Configure EMS:
   a. Go to *Endpoint Profiles* > *Remote Access*.
   b. Edit the profile with the VPN tunnel that you want to configure autoconnect for.

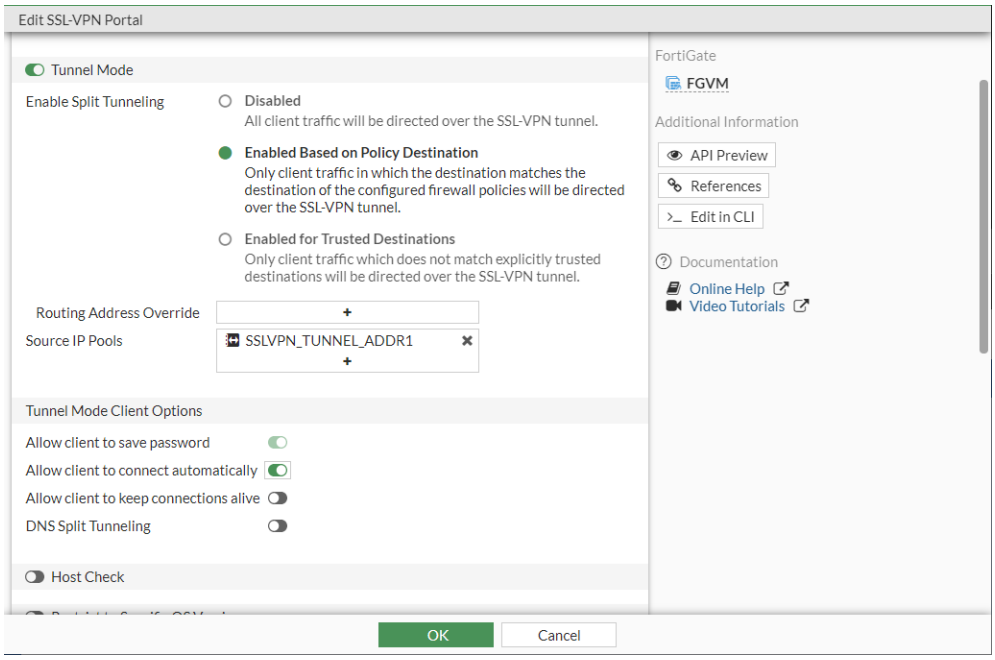
c. Under *General*, from the *Auto Connect* dropdown list, select the desired VPN tunnel.



d. Edit the tunnel:
   i. In *Advanced Settings*, enable *Show "Remember Password" Option*.
   ii. Enable *Show "Auto Connect" Option*.
   iii. Click *Save Tunnel*.

2. Configure FortiOS:
   a. Do the following for an SSL VPN tunnel:
      i. Go to *VPN* > *SSL-VPN Portals*.
      ii. For the desired portal, enable *Allow client to connect automatically*. This automatically enables *Allow client to save password*.

iii. Click *OK*.



b. Do the following for an IPsec VPN tunnel:

i. If you are using an existing tunnel, you can only configure autoconnect using the CLI. Run the following commands:

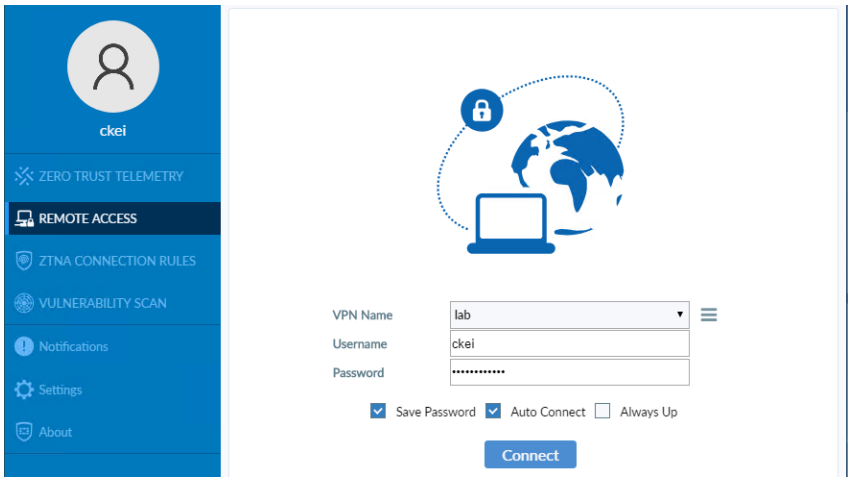
```
config vpn ipsec phase1-interface
   edit "vpn_tunnel_name"
      set save-password enable
      set client-auto-negotiate enable
   next
end
```

ii. Do the following if you are creating a new tunnel:

i. Go to *VPN* > *IPsec Wizard*.

ii. Configure the tunnel as desired. In *Client Options*, enable *Save Password* and *Auto Connect*.

3. In FortiClient, go to the *Remote Access* tab. The *Save Password* and *Auto Connect* checkboxes should display. If they do not display, you may have to connect manually to VPN once. Upon disconnect, the settings enabled in step 2 will appear below the *Password* field.



Configuring autoconnect with certificate authentication

Certificate authentication requires three certificates:

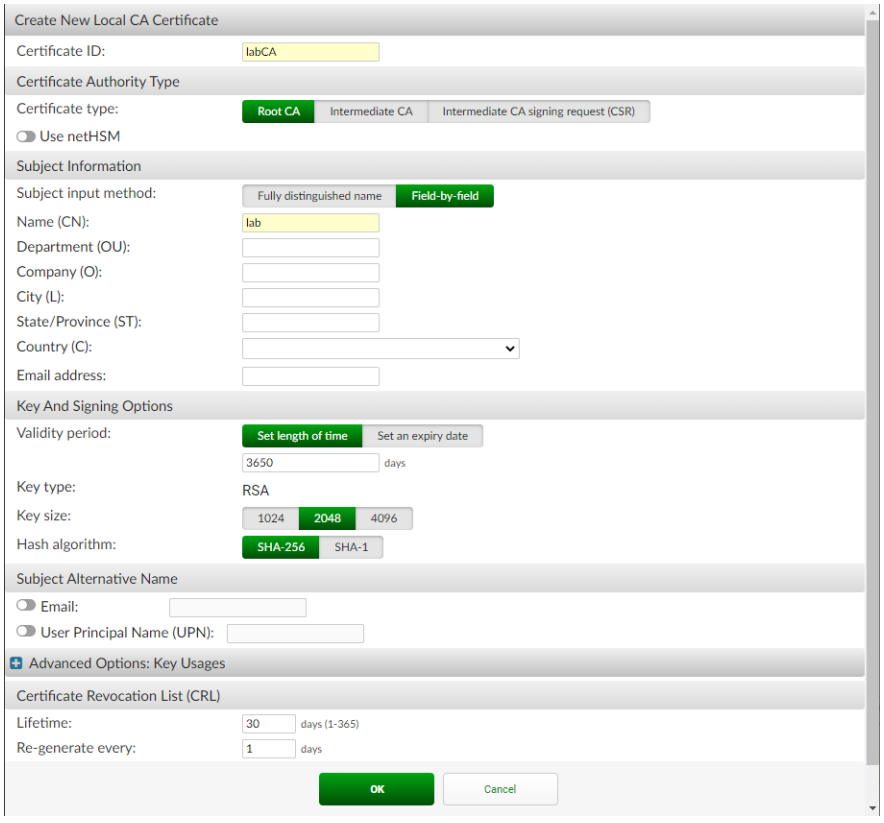
- Certificate Authority (CA) certificate
- Server certificate that the CA certificate has signed
- Client certificate that the CA certificate has signed

If the selected CA is well-known, such as Digicert or Comodo, the CA certificate may be preinstalled on the endpoint. Instead, this example uses FortiAuthenticator as a CA to sign the client and server certificates. In this example, you must import the CA certificate in FortiAuthenticator to the endpoint and FortiOS.

Creating certificates in FortiAuthenticator

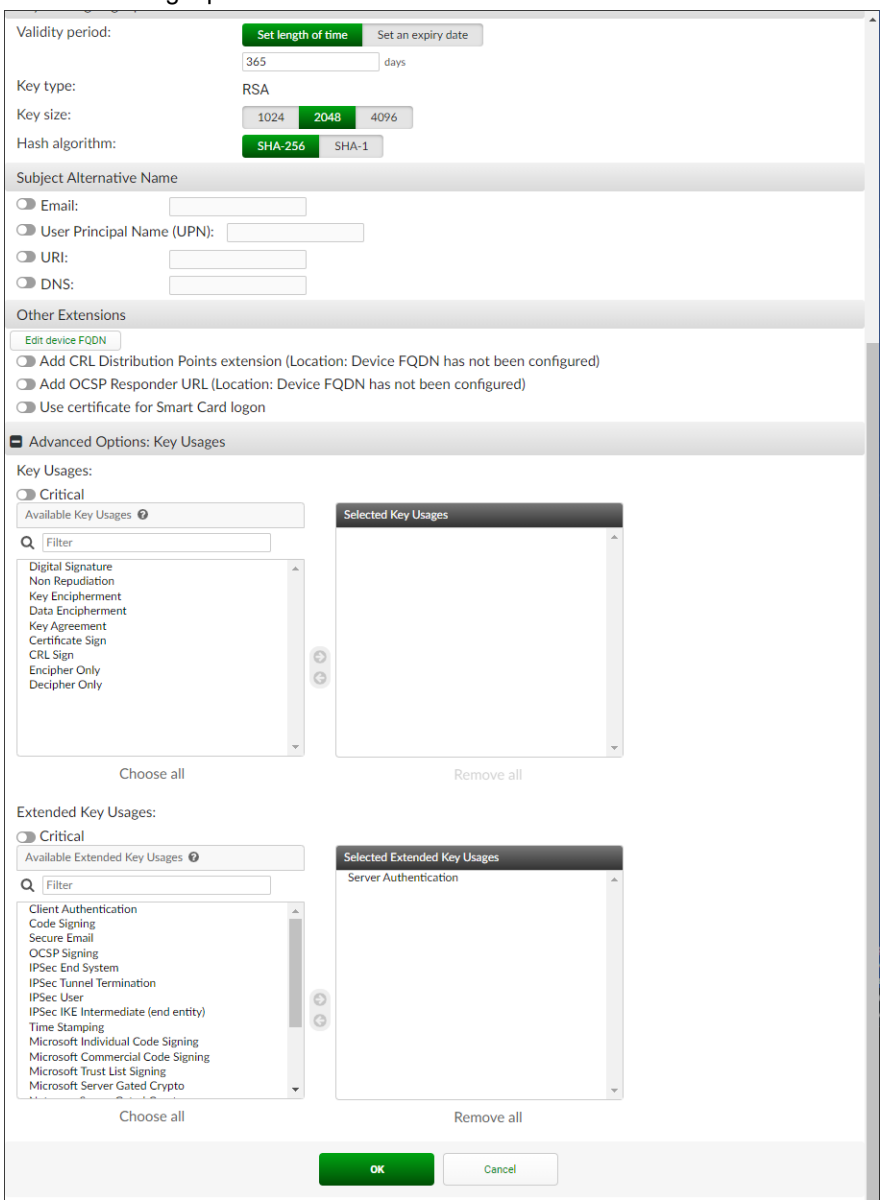
To create certificates in FortiAuthenticator:

1. Configure the CA certificate:
   a. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.
   b. Click *Create New*.
   c. Enter the desired values in the *Certificate ID* and *Name (CN)* fields.
   d. Configure other fields as desired.
   e. Click *OK*.



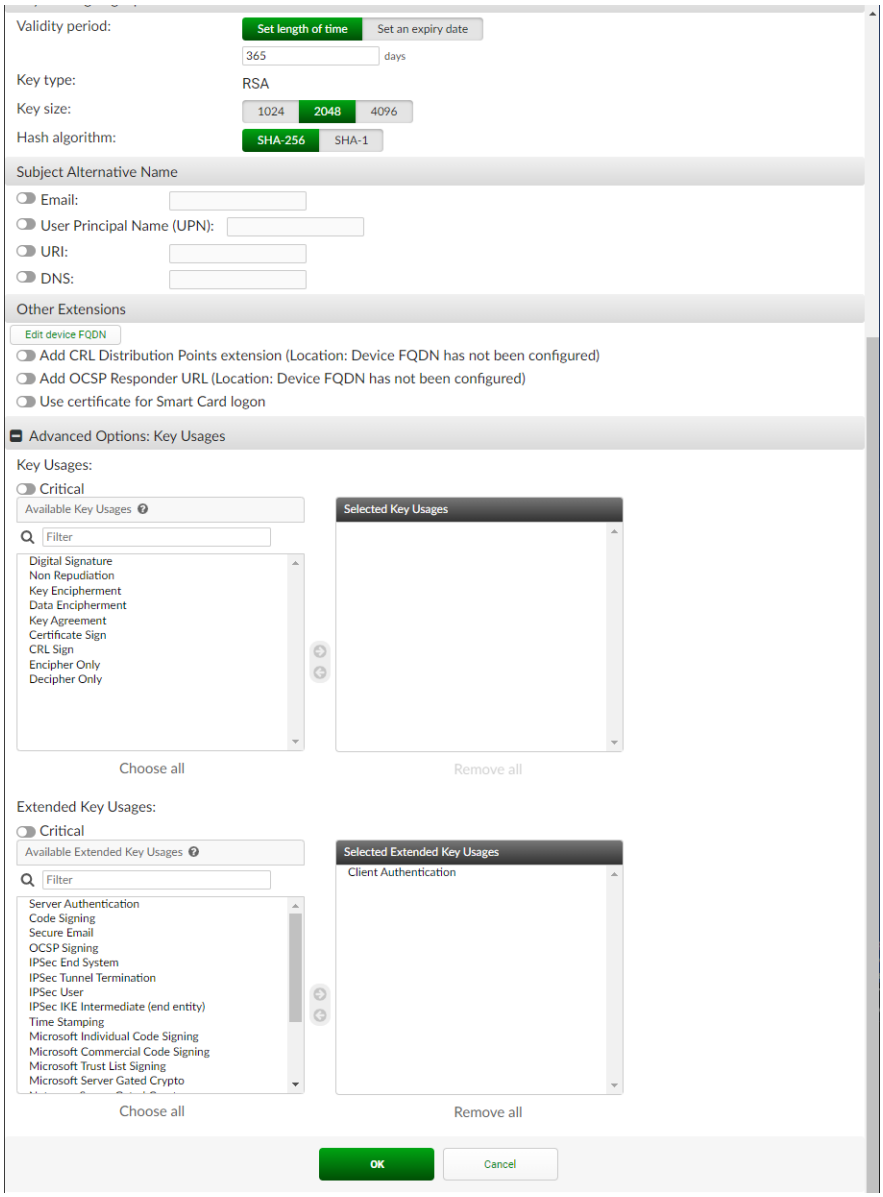
   f. On the *Local CAs* pane, select the checkbox for the newly created certificate, then click *Export Certificate*.
   g. Save the certificate in a location that you can upload it to FortiOS from.

2. Configure the server certificate:
   a. Go to *Certificate Management* > *End Entities* > *Users*.
   b. Click *Create New*.
   c. In the *Certificate ID* field, enter the desired certificate name.
   d. By default, the *Issuer* field is set to *Local CA*, and if you have only one local CA, it will be preselected in the *Certificate authority* dropdown list. Ensure that the certificate you created in step 1 is selected.
   e. In the *Name (CN)* field, enter the desired IP address. You must enter an IP address, as this is what FortiClient uses to connect to the VPN tunnel.
   f. Under *Advanced Options: Key Usages* > *Extended Key Usages*, select *Server Authentication* and move it from the left to the right pane. Click *OK*.



   g. On the *Users* pane, select the checkbox for the newly created certificate, then click *Export Key and Cert*.
   h. Enter a strong password, then click *OK*.
   i. FortiAuthenticator warns that the private key will be removed from FortiAuthenticator following the download. Save the certificate in a location that you can upload it to FortiOS from.

3. Configure the client certificate by repeating the instructions in step 2, except for step f. Instead of *Server Authentication*, select *Client Authentication* and move it from the left to the right pane.



Configuring FortiOS

To configure FortiOS:

1. Go to *System* > *Certificates*. If *Certificates* is unavailable, enable the feature in *System* > *Feature Visibility* > *Certificates*.
2. Import the CA certificate:
   a. Select *Import* > *CA Certificate*.
   b. For *Type*, select *File*.
   c. Use the *Upload* button to locate the CA certificate that you generated in Creating certificates in FortiAuthenticator on page 135.

d. Click *OK*. The uploaded certificate appears under *Remote CA Certificate* with the name CA_Cert_1. You can identify the certificate by the *Subject* column. In this example, the *Subject* column displays CN=lab.

3. Import the server certificate:
   a. Select *Import* > *Local Certificate*.
   b. For *Type*, select *PKCS #12 Certificate*.
   c. Use the *Upload* button to locate the server certificate that you generated in Creating certificates in FortiAuthenticator on page 135.
   d. Enter the password that you defined when exporting the certificate-key pair. Click *OK*.
4. To use certificate authentication, you must create PKI users in the CLI. Enter the following commands:

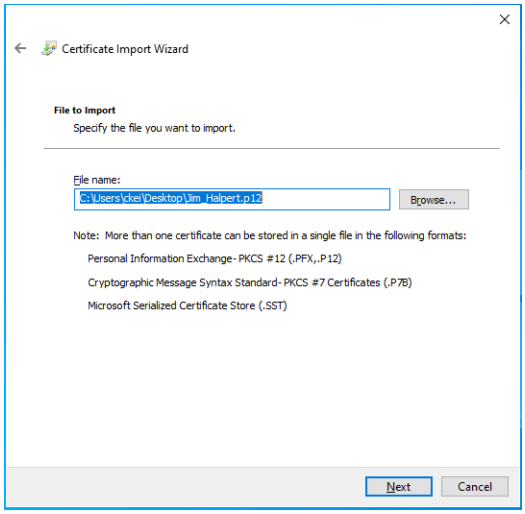
```
config user peer
   edit JimHalpert
      set ca CA_Cert_1
      set subject jhalpert
   next
end
```

5. Configure VPN settings:
   a. Go to *VPN* > *SSL-VPN Settings*.
   b. Locate *Server Certificate* and find the server certificate that you uploaded.
   c. Enable *Require Client Certificate*.
   d. Click *Apply*.

Installing certificates on the client

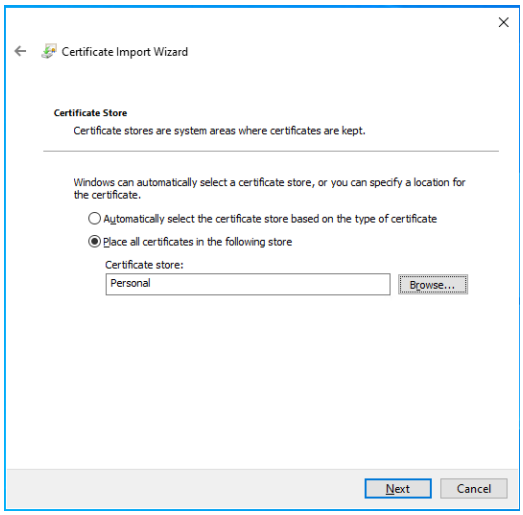
To configure a Windows client:

1. Install the user certificate:
   a. Double-click the certificate file to launch Certificate Import Wizard.
   b. For *Store Location*, select *Current User*. Click *Next*.
   c. The file name should already be accurate for the location and name. Click *Next*.



   d. In the *Password* field, provide the password that you configured in Creating certificates in FortiAuthenticator on page 135. Click *Next*.
   e. Select *Place all certificates in the following store*.

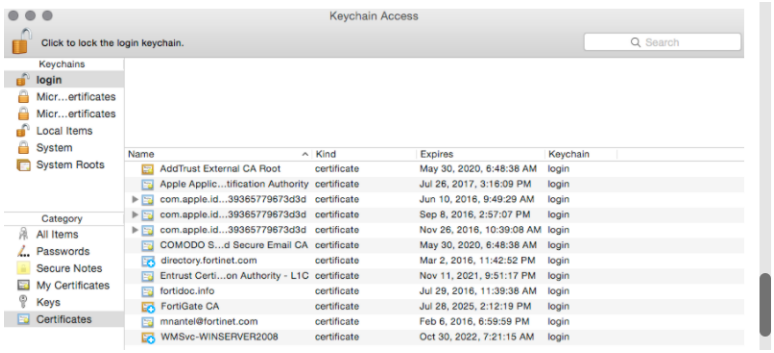
f. Browse to *Personal*. Click *OK*, then *Next*, and *Finish*.



2. Repeat step 1 to install the CA certificate. For step f, select *Trusted Root Certificate Authorities* instead of *Personal*.

To configure a macOS client:

1. Install the user certificate:
   a. Open the certificate file. Keychain Access opens.
   b. Double-click the certificate.
   c. Expand *Trust*, then select *Always Trust*.



2. Repeat step 1 to install the CA certificate.

Configuring the VPN tunnel in EMS

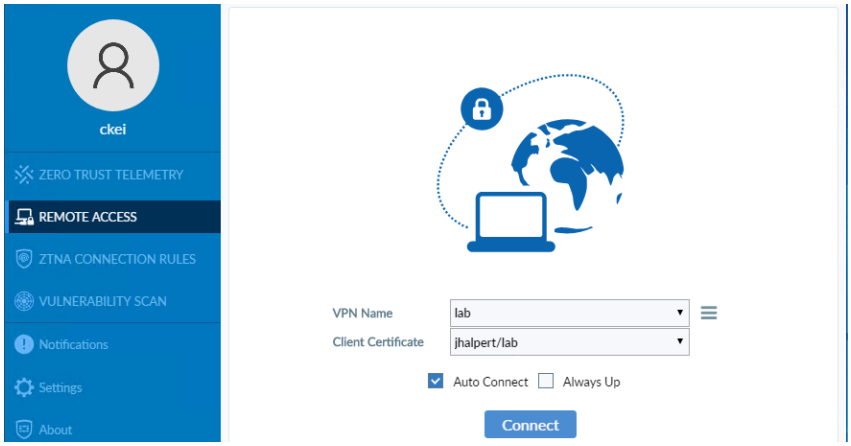
To configure the VPN tunnel in EMS:

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Select the desired profile.
3. On the *VPN* tab, select the desired VPN tunnel.
4. In *Basic Settings*, enable *Require Certificate*.
5. If you want to use only certificate authentication, disable *Prompt for Username*.
6. Click *Save Tunnel*.
7. Click *Save* to save the profile.

Connecting to the VPN tunnel in FortiClient

To connect to the VPN tunnel in FortiClient:

1. In FortiClient, go to the *Remote Access* tab.
2. From the *VPN Name* dropdown list, select the desired VPN tunnel.
3. From the *Client Certificate* dropdown list, select the newly installed certificate.
4. Enable *Auto Connect*.
5. Click *Connect* to establish connection to this VPN tunnel for the first time. This user's subsequent logons automatically bring up the VPN tunnel and use certificate authentication.



Appendix F - SSL VPN prelogon

SSL VPN prelogon allows tunnel establishment at startup time before users log on to the computer. This may be desirable in situations where remote terminals require access to the VPN hub before login regardless of the users who log in to the computer.

Because the SSL VPN tunnel must establish without user authentication, the authentication method cannot be based on username and password or on a user certificate.

Instead, this solution uses a machine certificate that a trusted certificate authority (CA) issued to allow the trusted computer to connect.

This guide details the settings required to configure SSL VPN prelogon functionality in a Windows environment where a Windows client establishes an SSL VPN tunnel with a FortiGate using a computer certificate that a Windows Active Directory (AD) issued.

SSL VPN prelogon requires the following:

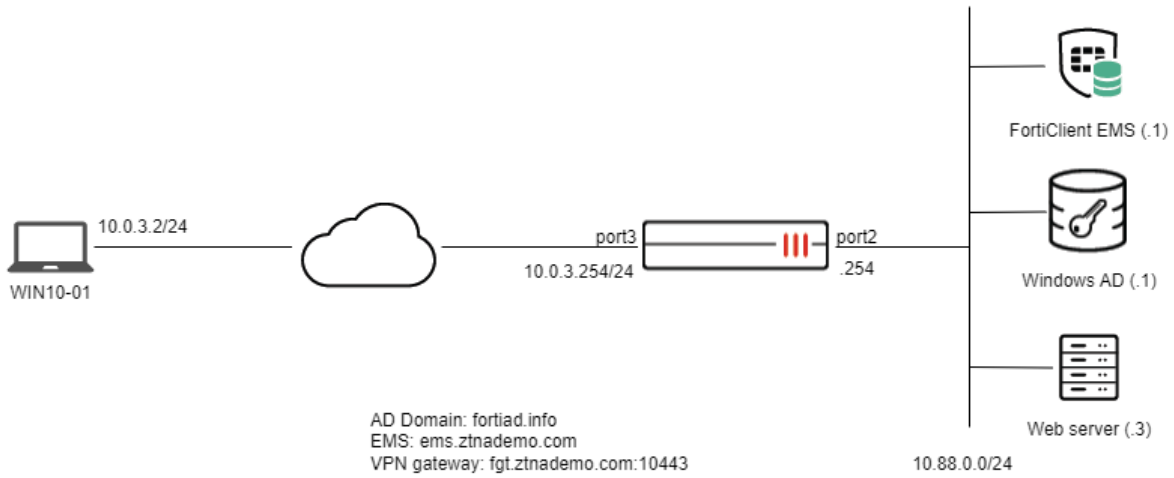
- The endpoint computer is registered to the Windows domain.
- A computer certificate that the Windows AD issued is installed on the endpoint's local machine certificate store.
- The certificate is issued to the machine name. The name appearing in the SAN field is a UPN or DNS name value matching the computer name in the AD.
- CA certificate of the root CA is installed on the FortiGate's certificate store.
- FortiClient is installed and registered with EMS to retrieve the SSL VPN tunnel configurations.

The authentication flow is as follows:

1. Upon startup, FortiClient connects to the VPN gateway using its computer certificate for authentication.
2. FortiGate inspects the certificate expiry date, issuer CA, and SAN field.
3. The FortiGate does a LDAP lookup on the Windows AD to determine if the UPN or DNS name in the SAN field of the certificate matches any computer in the domain. The match may be performed on the computer Name or UserPrincipalName.
4. Optionally, FortiGate further verifies that the FortiGate user group allows the computer memberOf attribute.

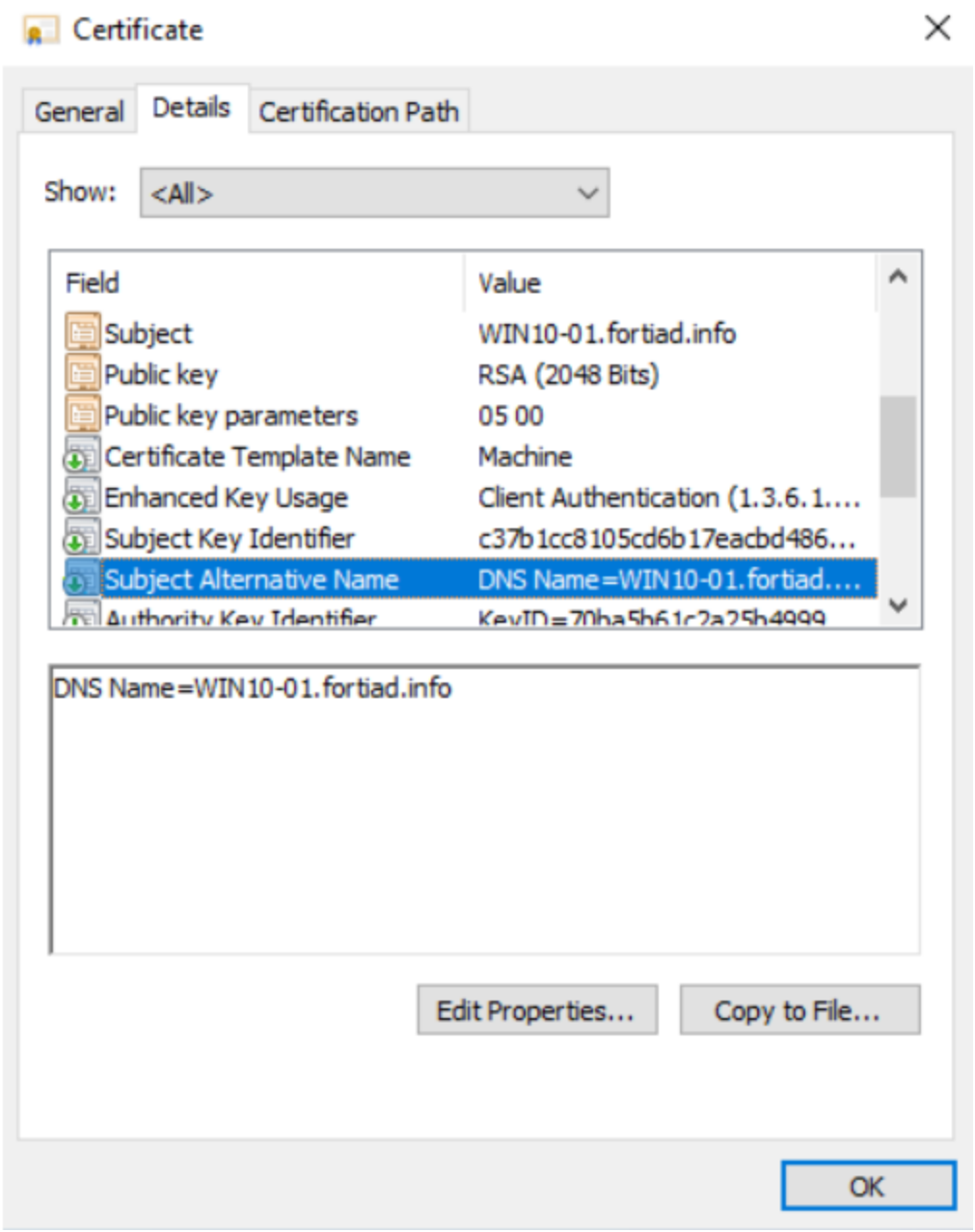
SSL VPN prelogon using AD machine certificate

This example uses the following topology:

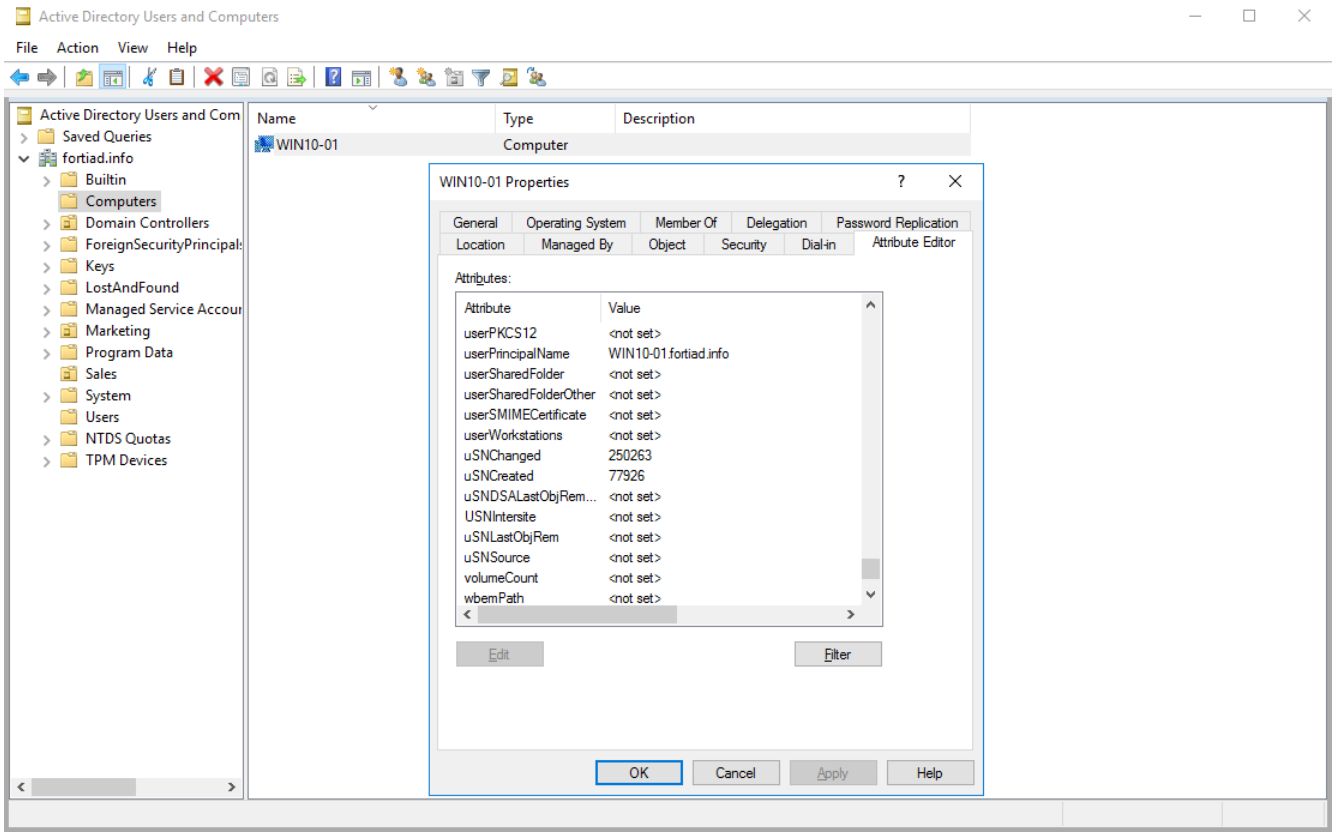


Computer/machine certificate

In this example, a group policy enables autoenrollment of computer certificates from each endpoint. The following is issued to WIN10-01. To see the certificate, open the Certificate Manager or Certificate Plug-in, and go to Local Computer\Personal\Certificates. Double-click the issued certificate and view the *Details* tab.



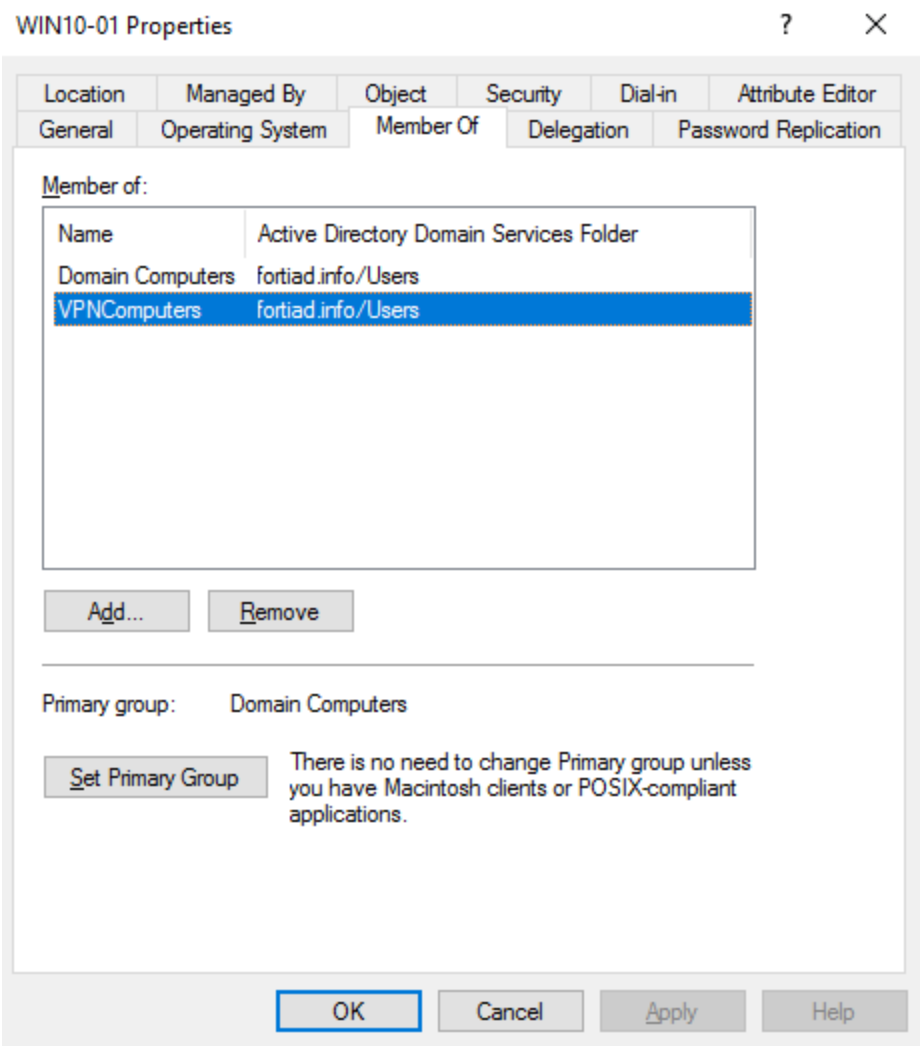
As the example shows, the Windows Active Directory (AD) issues a certificate with *DNS Name=WIN10-01.fortiad.info* in the subject alternative name (SAN) field. This matches the computer userPrincipalName on the AD:



Alternatively, you can try to issue a custom computer certificate with principal name in the SAN field, which matches the computer name field. Usually, the name field does not include the domain portion (fortiad.info in this example). Therefore, stripping the domain portion from the certificate principal name requires extra configuration on the FortiGate.

Security group

The computer WIN10-01 is a member of the VPNComputers security group, which contains all computers that are allowed access to VPN.

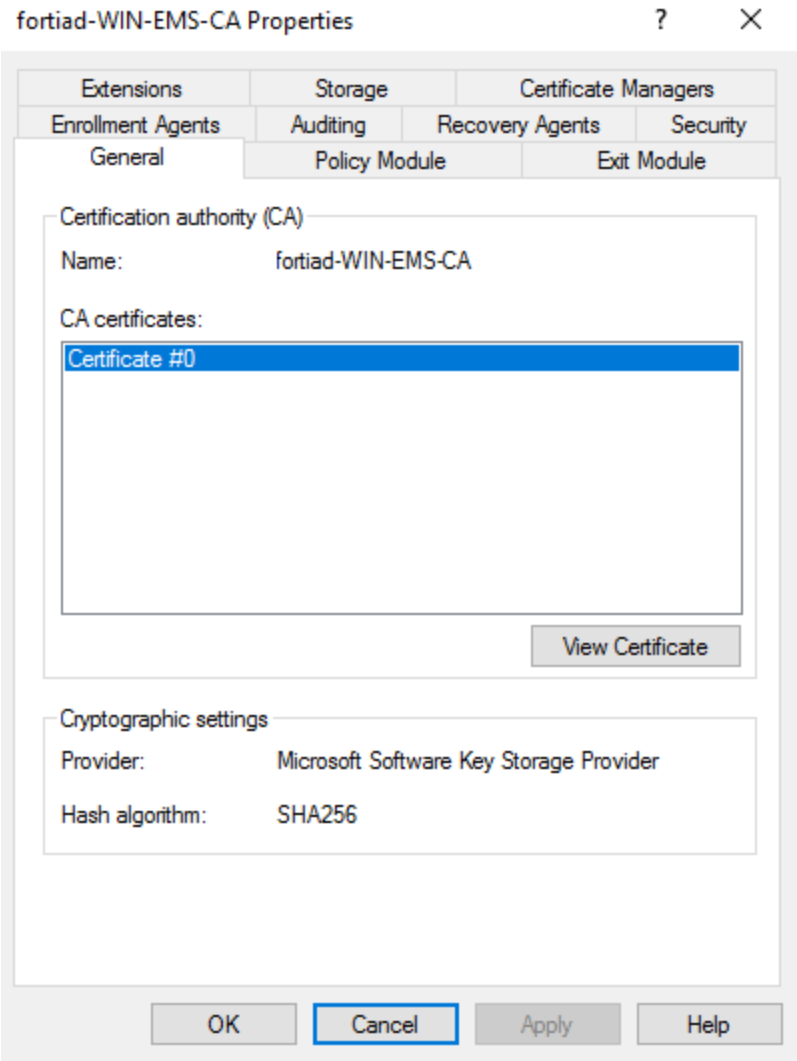


CA certificate

You must import the Active Directory (AD) certificate authority (CA) certificate into the FortiGate for the FortiGate to verify the chain of trust for the client certificate and the LDAPS connection.

To import the CA certificate:

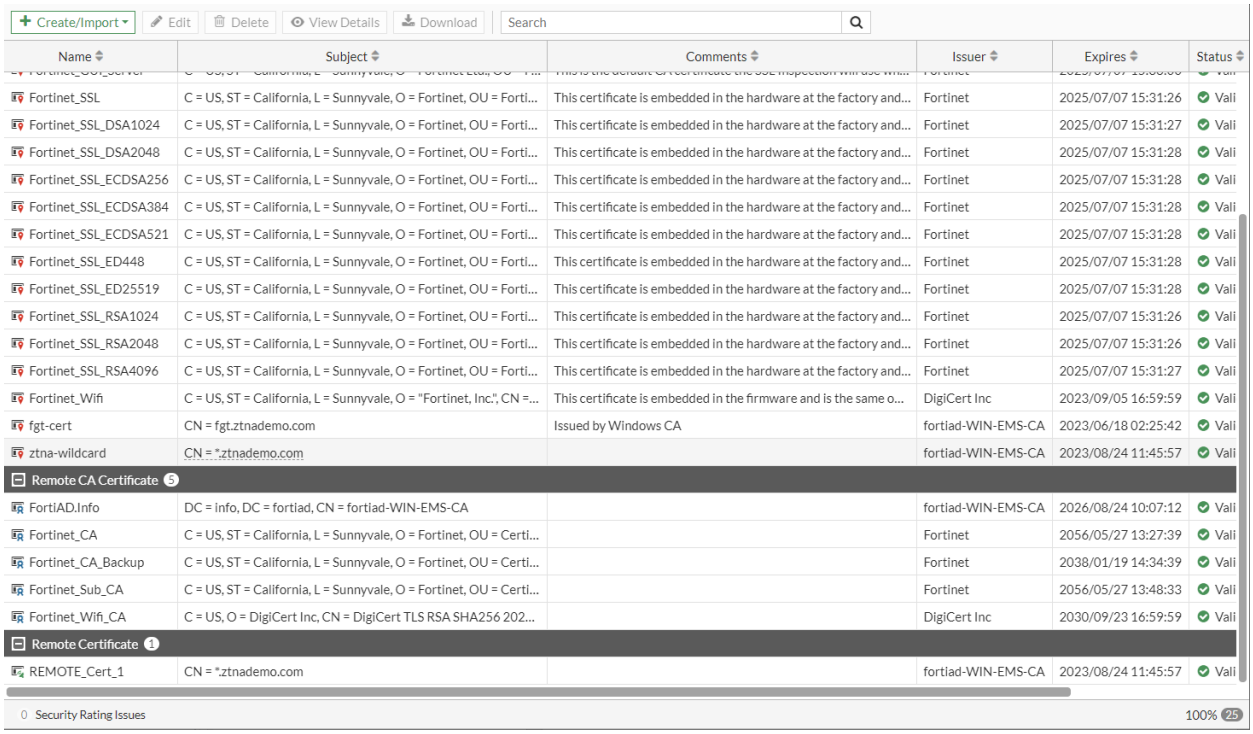
1. In the Certification Authority manager, right-click your domain, then select *Properties*.
2. On the *General* tab, click *View Certificate*.



3. On the *Details* tab, click *Copy to File...*
4. Follow the wizard to save the file as a Base-64 encoded X.509 (.CER).
5. In FortiOS, import the certificate:
   a. Go to *System* > *Certificates*.
   b. Click *Create/Import* > *CA Certificate*.
   c. For *Type*, select *File*.
   d. Click *Upload*.
   e. Select the previously saved CA certificate.
   f. Click *OK*.
   g. Once imported, run the following CLI commands to rename the certificate for easier recognition:

```
config vpn certificate ca
   rename CA_Cert_1 to FortiAD.Info
end
```

6. In *System* > *Certificates*, view the imported certificate under *Remote CA Certificate*.



Additionally, the root CA may have also issued a server certificate for the SSL VPN portal access. If so, you must import this server certificate on the FortiGate. In this example, a wildcard certificate for *.ztnademo.com was issued and installed on the FortiGate as the screenshot demonstrates.

Furthermore, you must install the CA certificate on the endpoint computer to verify the connection security with the SSL VPN gateway. You should install the CA certificate to Local Computer\Trusted Root Certification Authority\Certificates.

FortiGate authentication configuration

You must configure several components on the FortiGate to perform authentication:

Component	Description
LDAP server	The LDAP server configuration defines the connection to the Active Directory (AD) server. It also defines the subject alternate name (SAN) field in the client certificate that should be used for matching. This can be one of the following: • Othername – “Other name” in the SAN field • rfc822name – RFC822 email address in the SAN field • dnsname – DNS name in the SAN field You can define the LDAP search filter to look up and match the preferred field on the LDAP server. By default, the (userPrincipalName=%s) filter filters on the UPN field during LDAP lookup. If looking up the name is desired, change the first portion of the filter to (name=%s). See Using the SAN field for LDAP-integrated certificate authentication.

Component	Description
PKI user	A PKI user defines one or many users that are matched using client certificate. Matching against many users uses the LDAP-integrated authentication method. See Configuring a PKI user.
User group	A user group must have the LDAP server and PKI user objects defined. Optionally, select a group name to match a computer that is memberOf the LDAP group.

To configure the LDAP server:

1. In FortiOS, go to *User & Authentication* > *LDAP Servers*.
2. Click *Create*.
3. Configure the LDAP server as follows:

Field	Value/configuration
Name	LDAP-fortiad-Machine
Server IP/Name	10.88.0.1
Common Name Identifier	sAMAccountName
Distinguished Name	dc=fortiad,dc=info
Bind Type	Regular
Username	fortiad\Administrator
Password	<password>
Secure Connection	Enable. This is recommended.
Protocol	LDAPS
Certificate	FortiAD.Info. This is the certificate authority (CA) certificate imported from the CA.
Server identity check	Enable if supported.

4. Click *OK*.
5. To define the SAN-related settings, configure the bolded settings in the CLI:

```
config user ldap
    edit "LDAP-fortiad-Machine"
        set server "10.88.0.1"
        set server-identity-check enable
        set cnid "sAMAccountName"
        set dn "dc=fortiad,dc=info"
        set type regular
        set username "fortiad\\Administrator"
        set password ENC <password>
        set secure ldaps
        set ca-cert "FortiAD.Info"
```

```
        set port 636
        set account-key-upn-san dnsname
        set account-key-filter "(&(userPrincipalName=%s)(!
(UserAccountControl:1.2.840.113556.1.4.803:=2)))"
    next
end
```

To filter on the SAN field UPN and match the name field during LDAP lookup, configure the following settings instead:

```
config user ldap
    edit "LDAP-fortiad-Machine"
        set account-key-processing strip
        set account-key-upn-san othername
        set account-key-filter "(&(name=%s)(!
(UserAccountControl:1.2.840.113556.1.4.803:=2)))"
    next
end
```

The setting `set account-key-processing strip` allows the FortiGate to strip the domain portion of the othername before using it in the LDAP lookup.

To configure the PKI user:

You must configure the first PKI user from the CLI before it appears in the GUI. You must select the FortiAD.Info CA certificate to verify the chain of trust.

```
config user peer
   edit "PKI-LDAP-Machine"
      set ca "FortiAD.Info"
      set ldap-server "LDAP-fortiad-Machine"
      set ldap-mode principal-name
   next
end
```

To configure the user group:

1. Do one of the following:
   a. To configure the user group in the GUI, do the following:
      i. From *User & Authentication > User Groups*, click *Create New*.
      ii. Set *Name* to PKI-Machine-Group.
      iii. Set *Type* to *Firewall*.
      iv. Set *Members* to the PKI user PKI-LDAP-Machine.
      v. Under *Remote Groups*, click *Add*.
      vi. Select the *Remote Server LDAP-fortiad-Machine*.
      vii. From the tree, optionally select a group used for matching. Once selected, right-click the entry and click *Add Selected*.
      viii. Click *OK* to save.
      ix. Click *OK* again to save the user group object.

b. To configure the user group in the CLI, run the following commands:

```
config user group
    edit "PKI-Machine-Group"
        set member "LDAP-fortiad-Machine" "PKI-LDAP-Machine"
        config match
            edit 1
                set server-name "LDAP-fortiad-Machine"
                set group-name "CN=VPNComputers,CN=Users,DC=fortiad,DC=info"
            next
        end
    next
end
```

FortiGate SSL VPN configuration

The SSL VPN configuration is comprised of these parts:

- SSL VPN portal
- SSL VPN realm
- SSL VPN settings
- Firewall policy

To configure the SSL VPN portal:

You can use the default full-access or tunnel-access profile. Ensure that under *Tunnel mode*, split tunneling is configured and enabled based on policy destination. You can configure additional settings as needed.

To configure the SSL VPN realm:

1. Go to *System* > *Feature Visibility*.
2. Enable *SSL-VPN Realms*.
3. Click *Apply*.
4. Under *VPN* > *SSL-VPN Realms*, click *Create New*.
5. Enter the URL path pki-ldap-machine.
6. Click *OK* to save.

To configure the SSL VPN settings:

1. Go to *System* > *SSL-VPN Settings*.
2. Input the following values:

Field	Value
Enable SSL-VPN	Enable
Listen on Interface(s)	port3
Listen on Port	10443

Field	Value
Server Certificate	ztna-wildcard. The Windows certificate authority issues this wildcard server certificate.
DNS Server	Specify
DNS Server #1	10.88.0.1

3. Under *Authentication/Portal Mapping*, click *Create New* to create a new mapping.
4. Set *Users/Groups* to PKI-Machine-Group.
5. Set *Realm* to *Specify*.
6. Select the /pki-ldap-machine realm.
7. Set the portal to full-access.
8. Click *OK* to save.
9. Edit the *All Other Users/Groups* entry:
   a. Set portal to no-access.
   b. Click *OK* to save.

To configure the firewall policy:

1. From *Policy & Objects* > *Firewall Policy*, click *Create New* to create a new policy.
2. Input the following values:

Field	Value
Name	VPN-Machine
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	port2
Source	all, PKI-Machine-Group
Destination	Create an address object for the web server 10.88.0.3/32 and any other servers that must be accessed.
Schedule	always
Service	ALL
Action	ACCEPT
Log Allow Traffic	Enabled, All Sessions

3. Configure any other security profiles settings as needed.
4. Click *OK* to save.

Enabling VPN prelogon in EMS

A remote client should be registered to and managed by EMS to obtain the VPN remote access profile for connecting to the VPN. Therefore, a firewall policy must allow access to the EMS server.

You must configure a Remote Access profile in EMS to allow VPN prelogon. The first example creates a tunnel with configurations for enabling VPN prelogon with machine certificate. Users can select FortiClient VPN on the Windows logon page.

The next example takes it one step further and enables Windows to automatically connect to the tunnel on startup.

Configuring a firewall policy to allow access to EMS

To configure a firewall policy to allow access to EMS:

FortiGate should allow access on TCP/10443 (default) for client download and TCP/8013 (default) for telemetry.

1. On the FortiGate, go to *Policy & Objects* > *Virtual IPs*.
2. Click *Create New*.
3. Input the following values:

Field	Value/configuration
Name	Telemetry-VIP
Interface	port3
Type	Static NAT
External IP address/range	0.0.0.0
Map to IPv4 address/range	10.88.0.1
Services	HTTPS. Create a new service called Telemetry, which has its destination port set to TCP 8013.

4. Click *OK*.
5. Go to *Policy & Objects* > *Firewall Policy*. Click *Create New*.
6. Input the following values:

Field	Value/configuration
Name	WANtoEMS-Telemetry
Incoming Interface	port3
Outgoing Interface	port2
Source	All
Destination	Telemetry-VIP
Schedule	Always
Service	HTTPS, Telemetry
Action	ACCEPT
Log Allow Traffic	Enabled, All Sessions

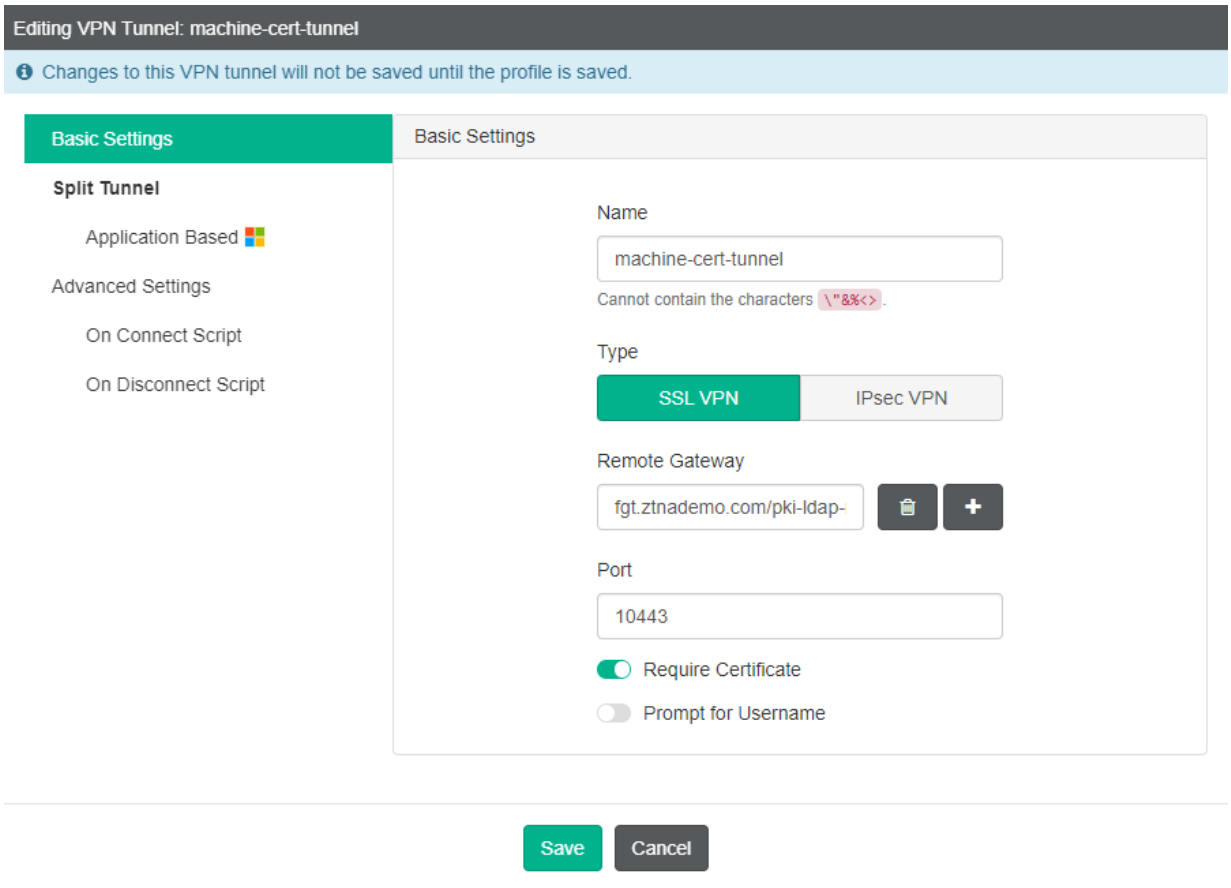
7. Click *OK* to save.

Configuring and applying a Remote Access profile

To configure a Remote Access profile on EMS:

1. In EMS, go to *Endpoint Profiles* > *Remote Access*. Click *+Add* to create a new profile.
2. For *Name*, enter Machine-VPN
3. In *Advanced* view, under *General*, enable *Show VPN before Logon*.
4. Under *SSL VPN*, enable *Enable Invalid Server Certificate Warning*.
5. Create the VPN tunnel:
   a. Under *VPN Tunnels*, click *+Add Tunnel*.
   b. In the VPN tunnel wizard, do the following:
   c. Select the *VPN Type Manual*, then click *Next*.
   d. Under *Basic Settings*, set the following values:

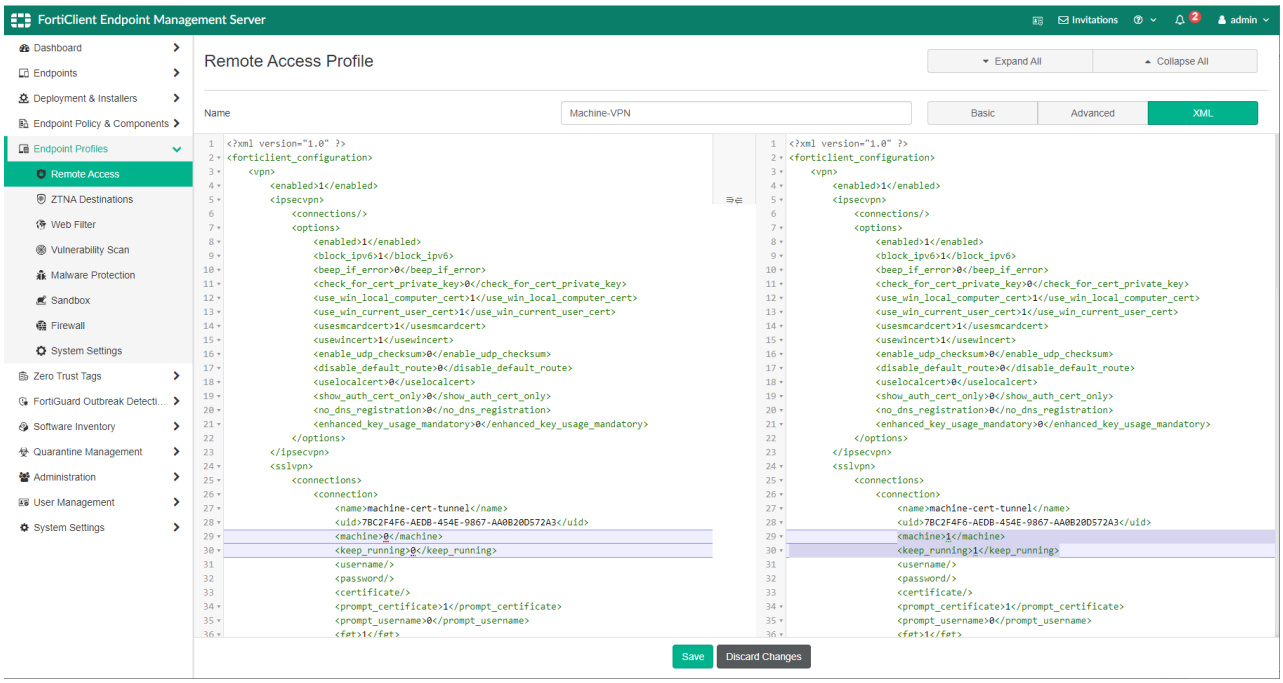
Field	Value/configuration
Name	machine-cert-tunnel
Type	SSL VPN
Remote Gateway	fgt.ztnademo.com/pki-ldap-machine fgt.ztnademo.com resolves to 10.0.3.254. /pki-ldap-machine is the realm used for this VPN.
Port	10443
Require Certificate	Enable
Prompt for Username	Disable



e. Under *Advanced Settings*, enable *Allow Non-Administrators to Use Machine Certificates*.
f. Click *Save* to save the tunnel.

6. Click *Save* to save the Remote Access profile.
7. In XML view, click *Edit*.
8. Locate the machine-cert-tunnel connection. Under this connection, set the following settings:

```
<machine>1</machine>
<keep_running>1</keep_running>
```



9. Click *Save*.

To apply the Remote Access profile to an endpoint policy:

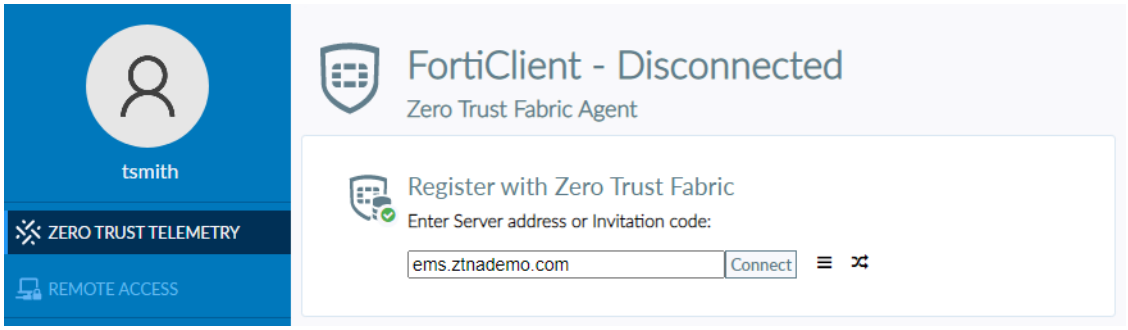
1. From *Endpoint Policy & Components* > *Manage Policies*, select the policy that is being applied to your endpoint, and click *Edit*.
2. Under *Profile*, change the VPN selection to Machine-VPN.
3. Click *Save*.

Verifying and troubleshooting

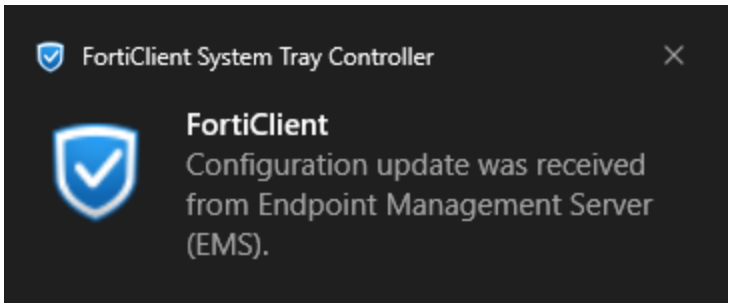
The remote endpoint, WIN10-01, is ready to connect to VPN before logon. The example assumes that the endpoint already has the latest FortiClient version installed. Ensure that the endpoint can register to EMS:

To verify FortiClient is registered and received the VPN tunnel settings:

1. In FortiClient, go to the *Zero Trust Telemetry* tab.
2. In the *Server address* field, enter ems.ztnademo.com. This resolves to the FortiGate external virtual IP address, 10.0.3.254.



3. Click *Connect*. Once connected, FortiClient receives a sync notification.

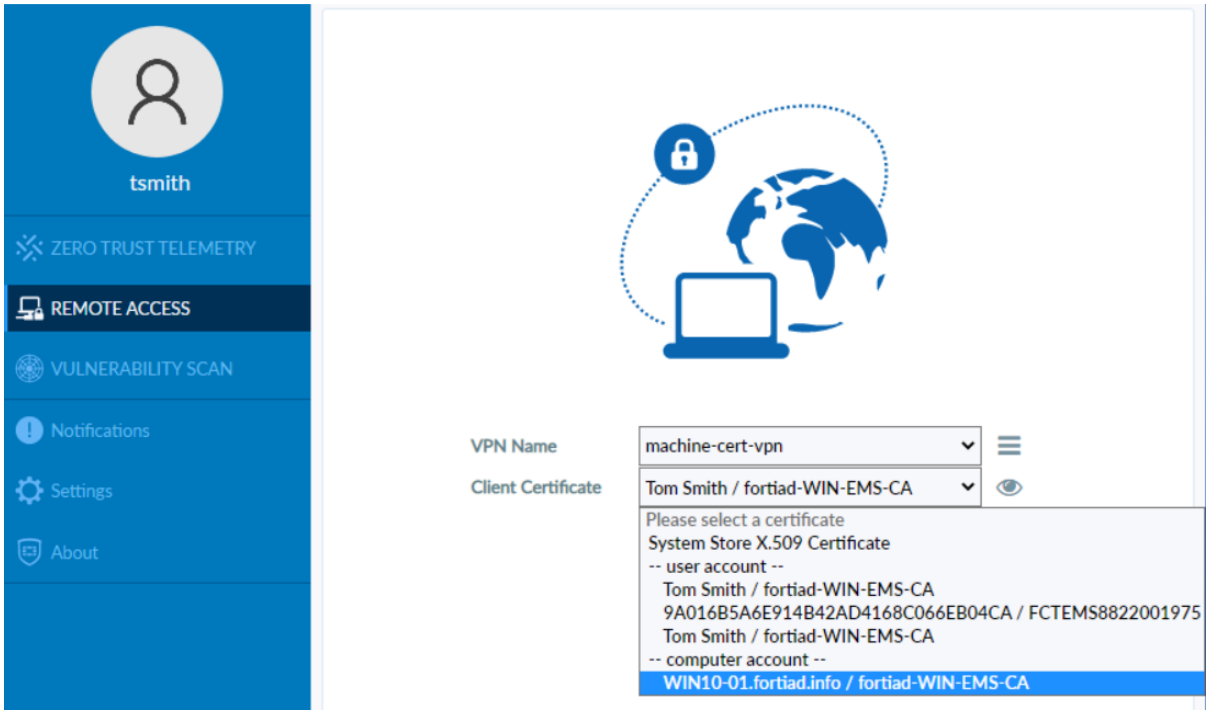


4. On the *Remote Access* tab, the machine-cert-vpn tunnel appears. Click the icon beside the VPN name to view the tunnel details. Verify it matches the EMS VPN tunnel settings configured.

To verify FortiClient can connect to the VPN:

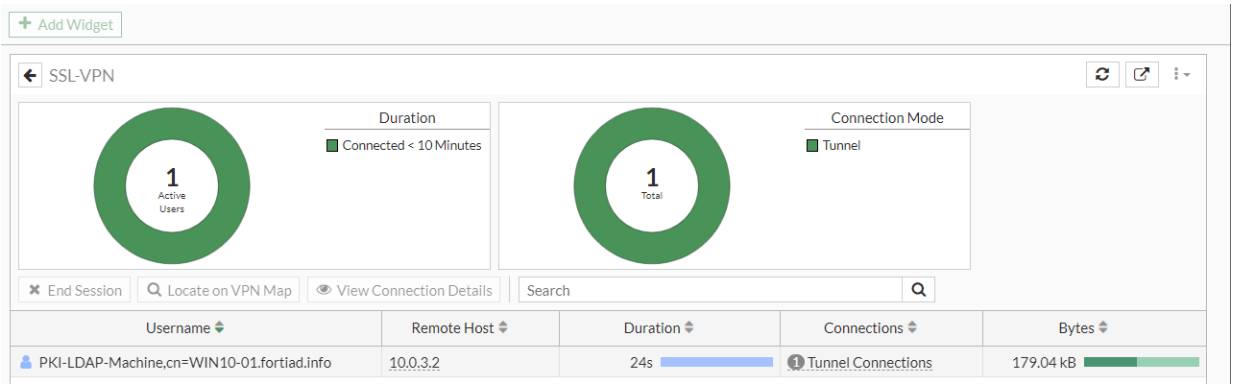
This step enables debug logs on the FortiGate to demonstrate the authentication that occurs during the connection.

1. In FortiOS, run the following commands:
```
diagnose debug enable
diagnose debug application fnbamd -1
```
2. In FortiClient on the *Remote Access* tab, select the machine-cert-vpn tunnel from the *VPN Name* dropdown list.
3. From the *Client Certificate* dropdown list, select the machine client certificate that was issued to this machine.



4. Click the eye icon beside the selected certificate. This certificate should match the computer/machine certificate in SSL VPN prelogon using AD machine certificate on page 141.
5. Click *Connect* to initiate the VPN connection. If the connection succeeds, a popup indicates the VPN is up.
6. From the FortiGate, go to the *Dashboard* > *Network* > *SSL-VPN* widget to see the new tunnel created. The tunnel username is identified by the common name found on the machine certificate assigned to the client. The user group

that was matched, PKI-LDAP-Machine, is also indicated.



To interpret the debug logs:

From the CLI console, you can interpret the debugs as follows:

```
diagnose debug enable
diagnose debug application fnbamd -1
Debug messages will be on for 30 minutes.
```

Verify the certificate chain by looking for the bolded output:

```
[500] fnbamd_cert_verify-Following cert chain depth 0
[573] fnbamd_cert_verify-Issuer found: FortiAD.Info (SSL_DPI opt 1)
[500] fnbamd_cert_verify-Following cert chain depth 1
```

Verify the certificate subject, if enabled:

```
[675] fnbamd_cert_check_group_list-checking group with name 'PKI-Machine-Group'
[490] __check_add_peer-check 'LDAP-fortiad-Machine'
[492] __check_add_peer-'LDAP-fortiad-Machine' is not a peer user.
[490] __check_add_peer-check 'PKI-LDAP-Machine'
[366] peer_subject_cn_check-Cert subject 'CN = WIN10-01.fortiad.info'
```

Obtain the UPN from the certificate subject alternate name (SAN) field. In this case, it is the DNS name:

```
[426] __cert_ldap_query-LDAP query, idx 0
[448] __cert_ldap_query-UPN = 'WIN10-01.fortiad.info'
```

Filter the LDAP query to perform a lookup on the UPN attribute in the fortiad.info directory:

```
[1718] fnbamd_ldap_init-search filter is: (&(userPrincipalName=WIN10-01.fortiad.info)(!
     (UserAccountControl:1.2.840.113556.1.4.803:=2)))
[1728] fnbamd_ldap_init-search base is: dc=fortiad,dc=info
```

Verify LDAP connection and user binding:

```
[1108] __ldap_connect-tcps_connect(10.88.0.1) is established.
[986] __ldap_rxtx-state 3(Admin Binding)
[363] __ldap_build_bind_req-Binding to 'fortiad\Administrator'
[1083] fnbamd_ldap_send-sending 43 bytes to 10.88.0.1
```

Beginning of DN search:

```
[1053] __ldap_rxtx-Change state to 'DN search'
[986] __ldap_rxtx-state 11(DN search)
[750] fnbamd_ldap_build_dn_search_req-base:'dc=fortiad,dc=info' filter:(&
     (userPrincipalName=WIN10-01.fortiad.info)(!
     (UserAccountControl:1.2.840.113556.1.4.803:=2)))
```

DN entry found for the desired filter:

```
[1226] __fnbamd_ldap_dn_entry-Get DN 'CN=WIN10-01,CN=Computers,DC=fortiad,DC=info'
```

Begin searching for the MemberOf attribute for the DN entry:

```
[649] fnbamd_ldap_build_attr_search_req-Adding attr 'memberOf'
[661] fnbamd_ldap_build_attr_search_req-base:'CN=WIN10-01,CN=Computers,DC=fortiad,DC=info'
     filter:cn=*
[1083] fnbamd_ldap_send-sending 119 bytes to 10.88.0.1
```

Found all groups including the primary group:

```
[522] __retrieve_group_values-Get the memberOf groups.
[532] __retrieve_group_values- attr='memberOf', found 1 values
[542] __retrieve_group_values-val[0]='CN=VPNComputers,CN=Users,DC=fortiad,DC=info'
[1127] __fnbamd_ldap_read-Read 8
…
[1053] __ldap_rxtx-Change state to 'Primary group query'
[986] __ldap_rxtx-state 13(Primary group query)
…
[472] __get_one_group-group: CN=Domain Computers,CN=Users,DC=fortiad,DC=info
[1127] __fnbamd_ldap_read-Read 8
```

Authentication is accepted, matching the FortiGate PKI-LDAP-Machine PKI peer:

```
[1431] __fnbamd_ldap_primary_grp_next-Auth accepted
…
[377] __cert_ldap_query_cb-LDAP ret=0, server='LDAP-fortiad-Machine', req_id=1534052817
[388] __cert_ldap_query_cb-Matched peer 'PKI-LDAP-Machine'
[755] __ldap_destroy-
[271] __cert_resume-req_id=1534052817
[99] __cert_chg_st- 'Status-Query' -> 'Done'
```

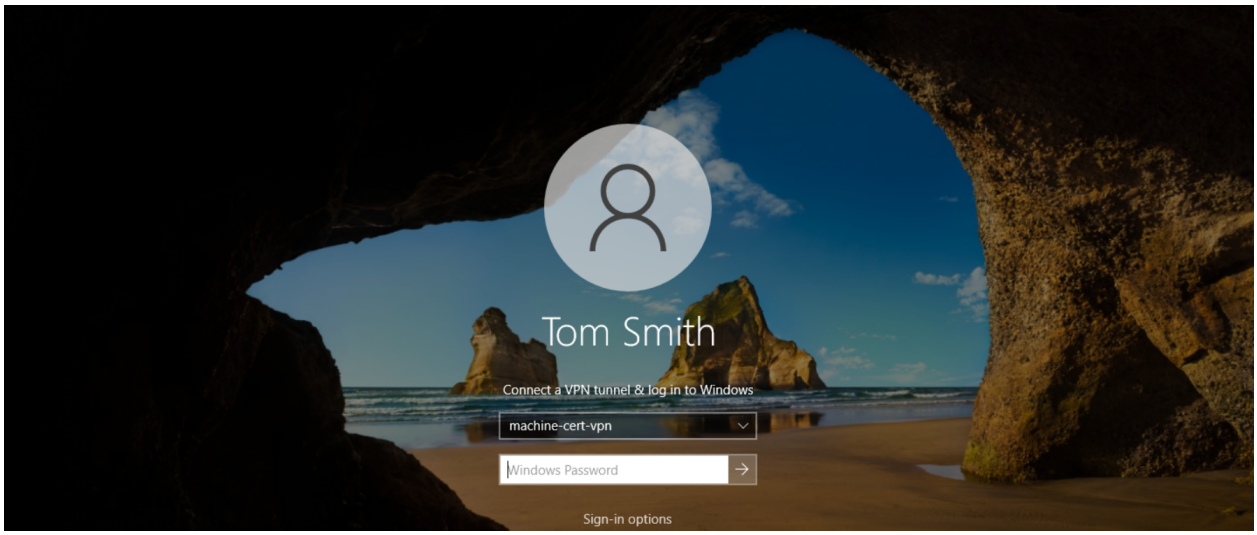
User group PKI-Machine-Group is matched:

```
[833] fnbamd_cert_check_matched_groups-checking group with name 'PKI-Machine-Group'
[121] fnbamd_ldap_dn_match-DN 'CN=VPNComputers,CN=Users,DC=fortiad,DC=info' is matched with
     'CN=VPNComputers,CN=Users,DC=fortiad,DC=info', idx=0.
[895] fnbamd_cert_check_matched_groups-matched
```

To verify FortiClient can connect to the tunnel during Windows logon:

The earlier test verified a user can connect to the VPN using the machine certificate. The following verifies that FortiClient can connect to the VPN during Windows logon.

1. Disconnect the current VPN connection by going to clicking *Disconnect* on the FortiClient *Remote Access* tab. A VPN down notification appears on the endpoint.
2. In FortiOS, verify the VPN is down in *Dashboard* > *Network* > *SSL-VPN* widget.
3. Sign out of the current Windows session to arrive at the Windows logon screen.
4. In the user sign-in page, the following prompt appears:



   If the prompt for VPN tunnel does not appear, click *Sign-in options* and select the FortiClient icon.
5. Enter the user password and sign in to Windows. Windows shows the progress and briefly shows a *Connecting to VPN (machine-cert-vpn)…* message. A message appears to indicate the VPN connection succeeded.
6. On the FortiGate, verify the connection is up.

Enabling automatic VPN prelogon in EMS

Following the previous example, this section configures additional settings to allow the VPN to automatically establish after Windows bootup and before the user signs in.

If you did not configure the previous settings, see Enabling VPN prelogon in EMS on page 151.

Configuring VPN to automatically connect before logon

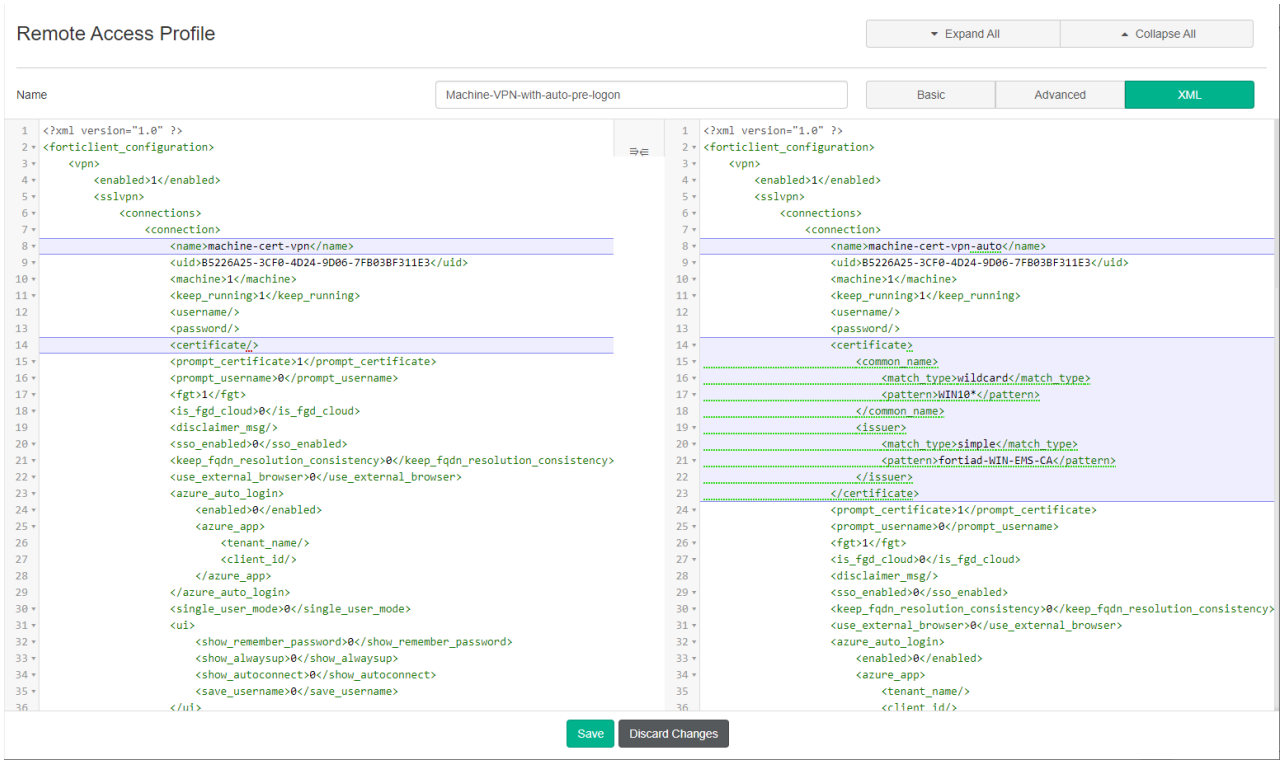
To configure VPN to automatically connect before logon:

1. In EMS, go to *Endpoint Profiles* > *Remote Access*.
2. Clone the Machine-VPN profile.
3. Name the new profile Machine-VPN-with-auto-pre-logon.
4. Click *Save*.
5. In XML view, click *Edit*.

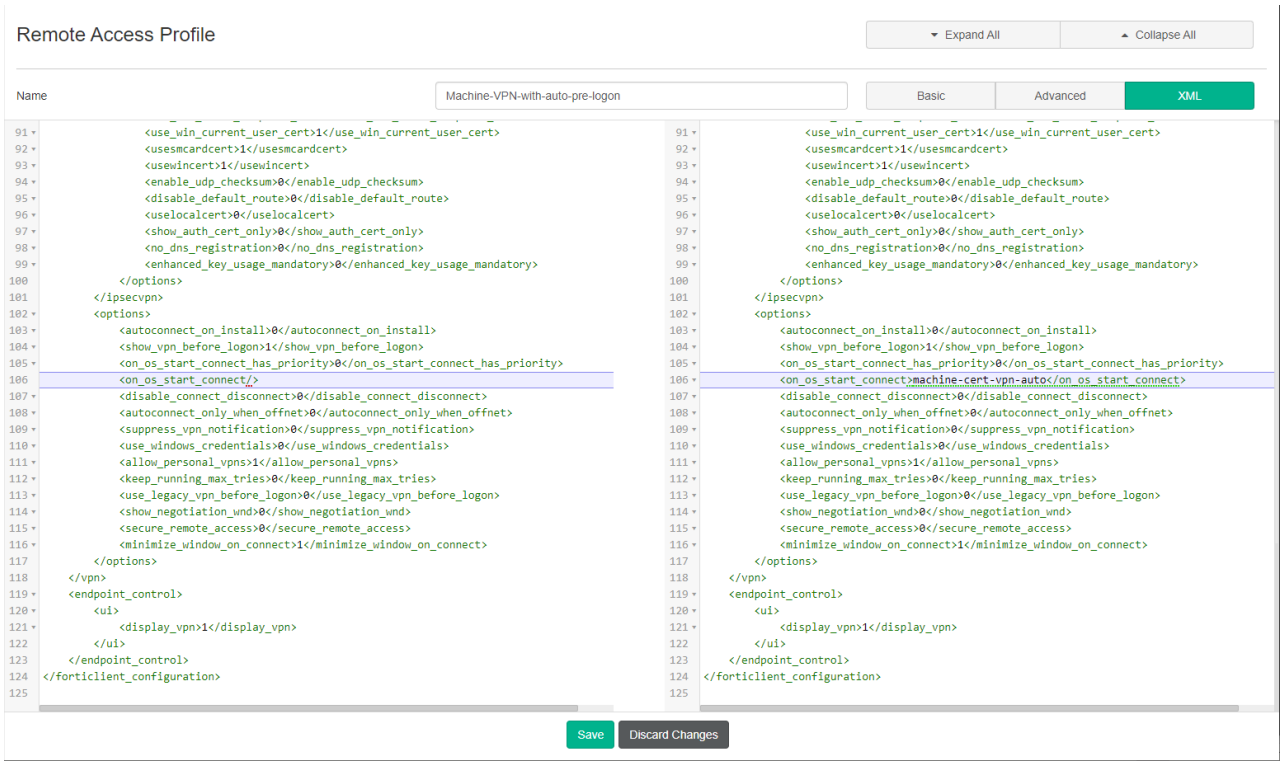
6. Locate the machine-cert-vpn connection.
7. Modify the name to machine-cert-vpn-auto.
8. Locate the `<certificate/>` element, and make the following modifications:

```
<certificate>
        <common_name>
                <match_type>wildcard</match_type>
                <pattern>WIN10*</pattern>
        </common_name>
        <issuer>
                <match_type>simple</match_type>
                <pattern>fortiad-WIN-EMS-CA</pattern>
        </issuer>
</certificate>
```

The `common_name` element uses wildcard matching to identify a machine certificate with CN matching WIN10*. The `issuer` element matches a machine certificate that the fortiad-WIN-EMS-CA certificate authority issued. Replace these with the appropriate patterns for your organization.



9. Under global VPN options, locate the `<on_os_start_connect/>` element and modify as follows:
`<on_os_start_connect>machine-cert-vpn-auto</on_os_start_connect>`



To apply the Remote Access profile to an endpoint policy:

1. From *Endpoint Policy & Components* > *Manage Policies*, select the policy that is being applied to your endpoint, and click *Edit*.
2. Under *Profile*, change the VPN selection to Machine-VPN-with-auto-pre-logon.
3. Click *Save*.

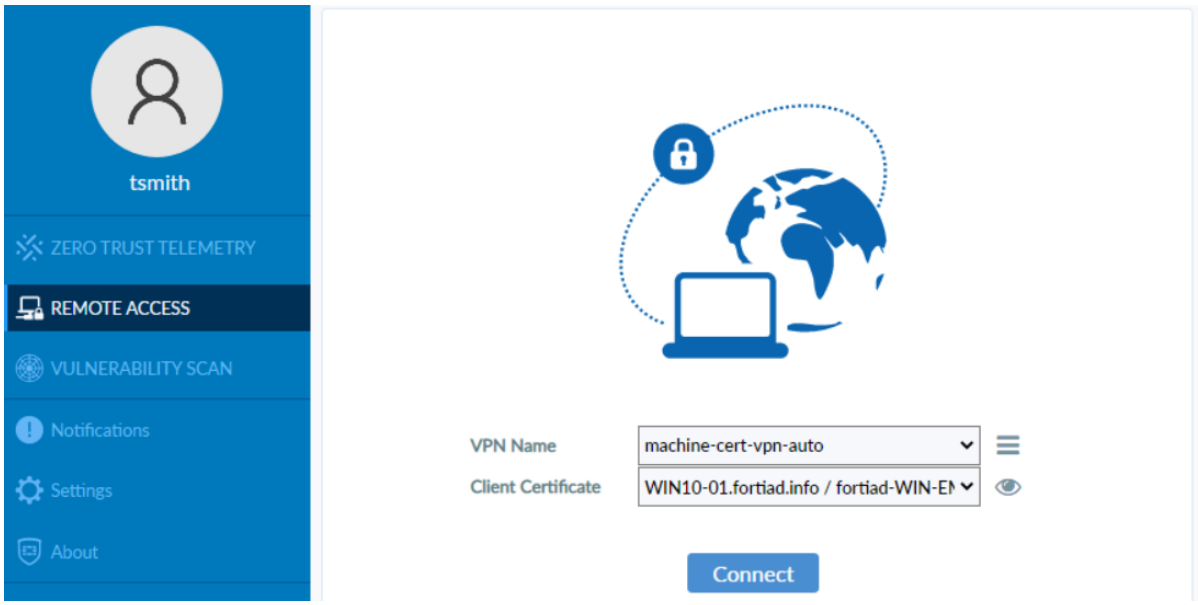
Verifying and troubleshooting

The remote endpoint, WIN10-01, is ready to connect to VPN before logon automatically. The example assumes the following:

- User has logged in to Windows.
- FortiClient is registered to EMS.
- FortiClient received the latest Remote Access profile update from EMS.
- VPN is not established.

To verify FortiClient received the VPN tunnel settings:

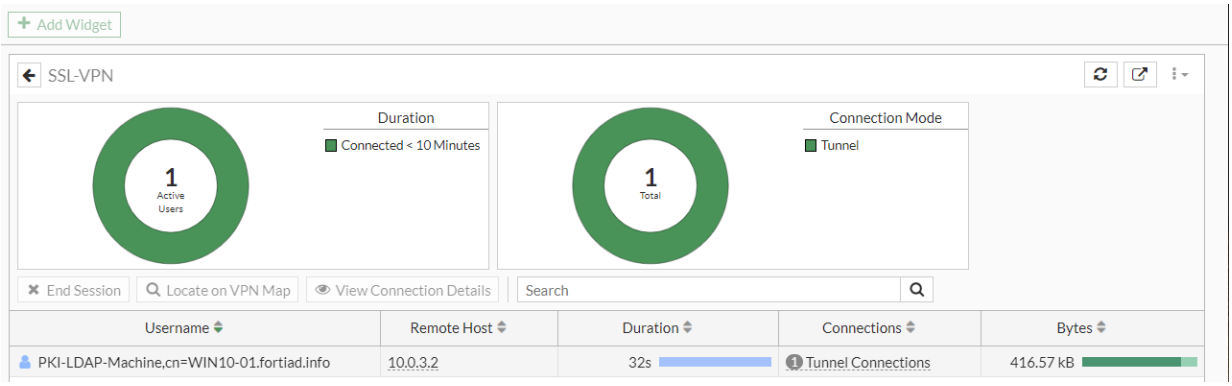
In FortiClient, go to the *Remote Access* tab. The machine-cert-vpn-auto tunnel appears. The client certificate of the matching certificate should be selected.



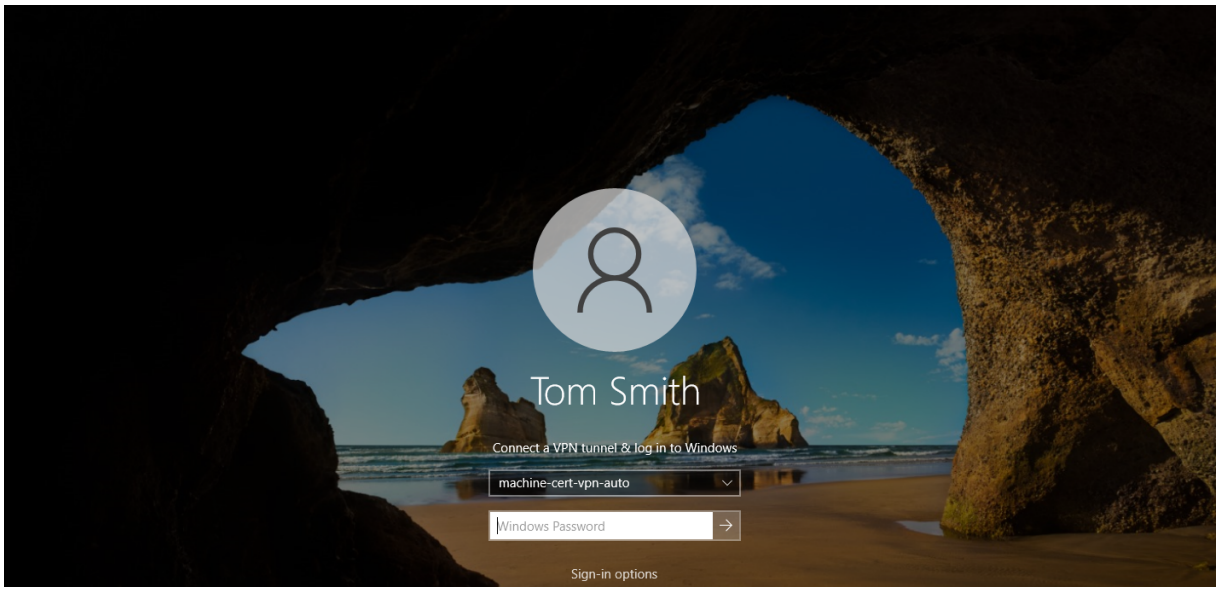
To verify FortiClient can connect to the VPN before logon:

This step restarts the Windows computer to demonstrate automatic VPN connection before user logon. It also optionally enables debug logs on the FortiGate to demonstrate the authentication that occurs during the connection.

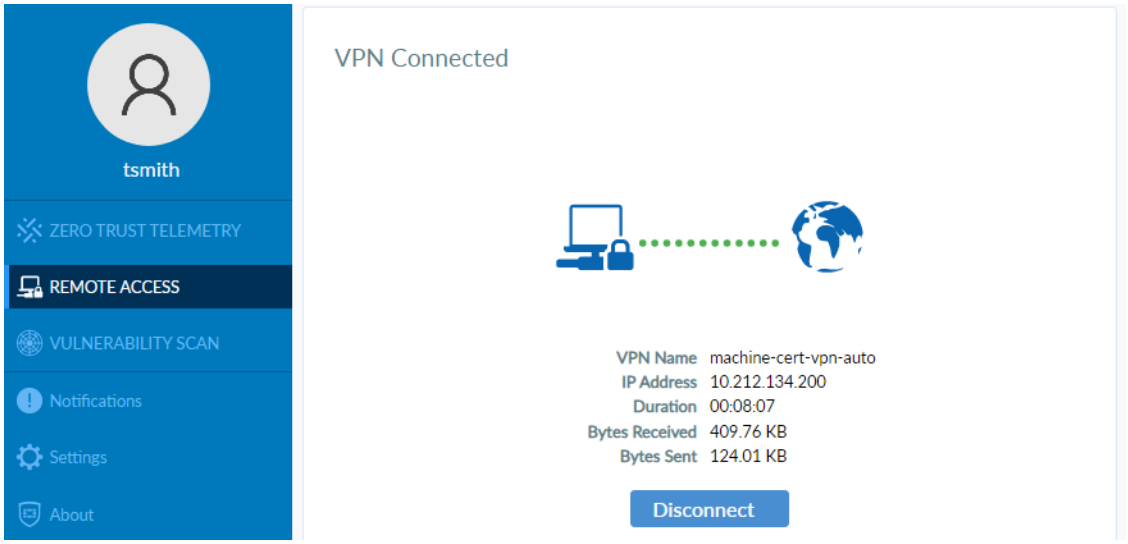
1. In FortiOS, run the following commands:
   ```
   diagnose debug enable
   diagnose debug application fnbamd -1
   ```
2. Restart the remote endpoint.
3. When Windows boots up and the signin screen appears, FortiOS receives the SSL VPN connection request, and the debugs appear in the CLI. Go to the *Dashboard* > *Network* > *SSL-VPN* widget to confirm the tunnel has been established.



4. On the Windows signin screen, log in with your user credentials. No additional VPN tunnel successful messages display.



5. In FortiClient on the *Remote Access* tab, confirm that the tunnel already established.



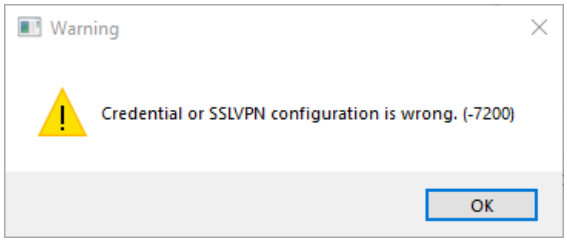
Troubleshooting the prelogon SSL VPN connection

A variety of problems may occur during the SSL VPN connection phase. These are a few scenarios and debugs that identify problems that may occur.

For reference, review To interpret the debug logs: on page 157 to see outputs of a successful connection and authentication.

No connection

When first trying to connect to the manual tunnel configuration, the tunnel does not come up and FortiClient returns the following error message at around 48% of connection progress:



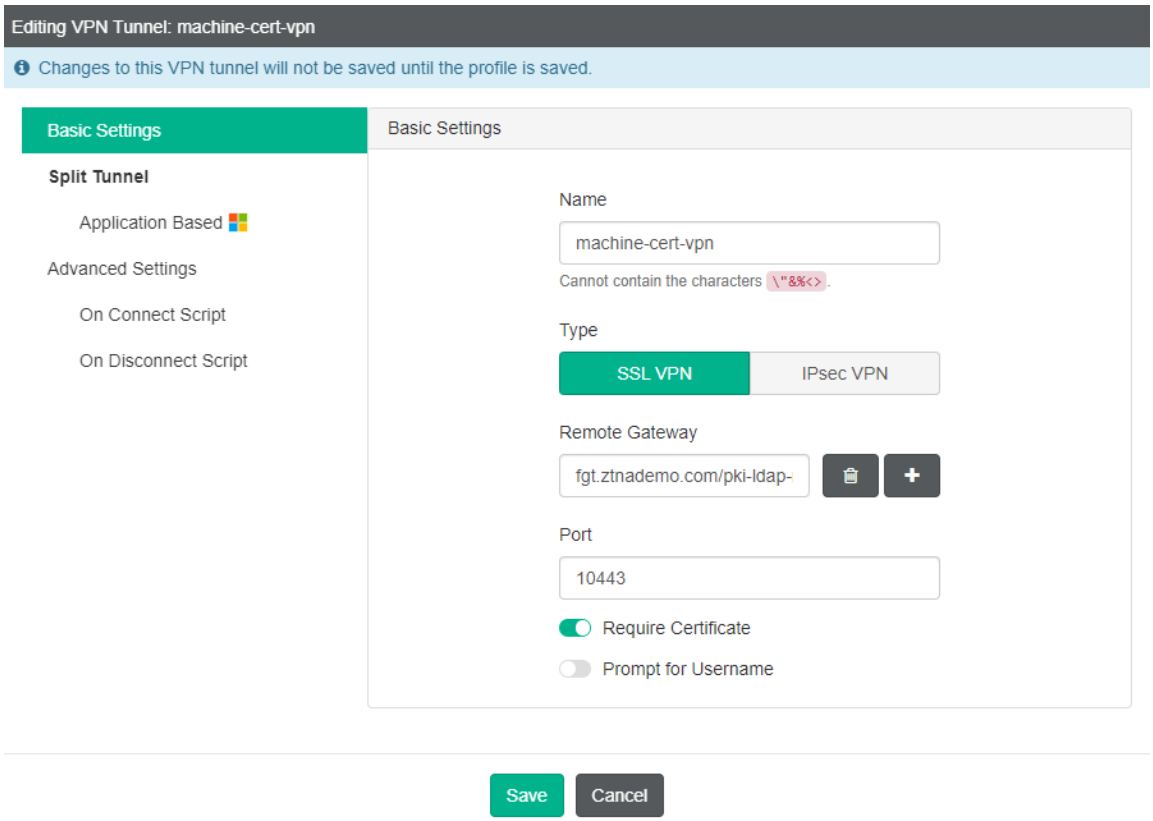
On the FortiGate, use the CLI to verify whether traffic has been initiated to the correct interface and port:

```
diagnose sniffer packet port3 'port 10443' 4 0 l
Using Original Sniffing Mode
interfaces=[port3]
filters=[port 10443]
```

No output indicates that the wrong address or port is used. Verify the remote gateway address, port, and realm to ensure you entered them properly.

VPN tunnel prompts for credentials

The VPN prelogon with machine certificate configuration does not rely on username and password to connect. On the Remote Access profile assigned to the endpoint policy, edit the tunnel settings. In *Basic Settings*, ensure that *Prompt for Username* is disabled.



Wrong certificate selected

Similar to the error in No connection on page 164, the connection progress stops at 48% and *Credential or SSLVPN configuration is wrong (-7200)* displays.

To troubleshoot authentication errors, enable fnbamd debugs on the FortiGate:

```
diagnose debug enable
diagnose debug application fnbamd -1
```

Reconnect to the VPN and observe the debugs. If a wrong certificate is selected, the following places may indicate as such:

```
[320] fnbamd_chain_build-Extend chain by system trust store. (no luck)
[352] fnbamd_chain_build-Extend chain by remote CA cache. (no luck)
```

When verifying the certificate, there is no certificate chain back to the certificate authority (CA). This indicates one of the following:

- CA certificate was not installed on the FortiGate.
- Wrong client certificate is being used to connect.

This output indicates that the certificate subject field identifies a user called Tom Smith. This indicates that a user certificate is likely being used rather than a machine certificate:

```
[366] peer_subject_cn_check-Cert subject 'DC = info, DC = fortiad, OU = Sales, CN = Tom
      Smith, emailAddress = tsmith@ztnademo.com'
```

FortiGate does not pick up UPN from certificate

The FortiGate looks at the certificate subject alternate name (SAN) field to identify the machine/computer name. If the wrong SAN attribute is used, the FortiGate returns an empty string in the following debug output:

```
[448] __cert_ldap_query-UPN = ''
```

Subsequently, the LDAP search filter is empty, and the LDAP lookup fails:

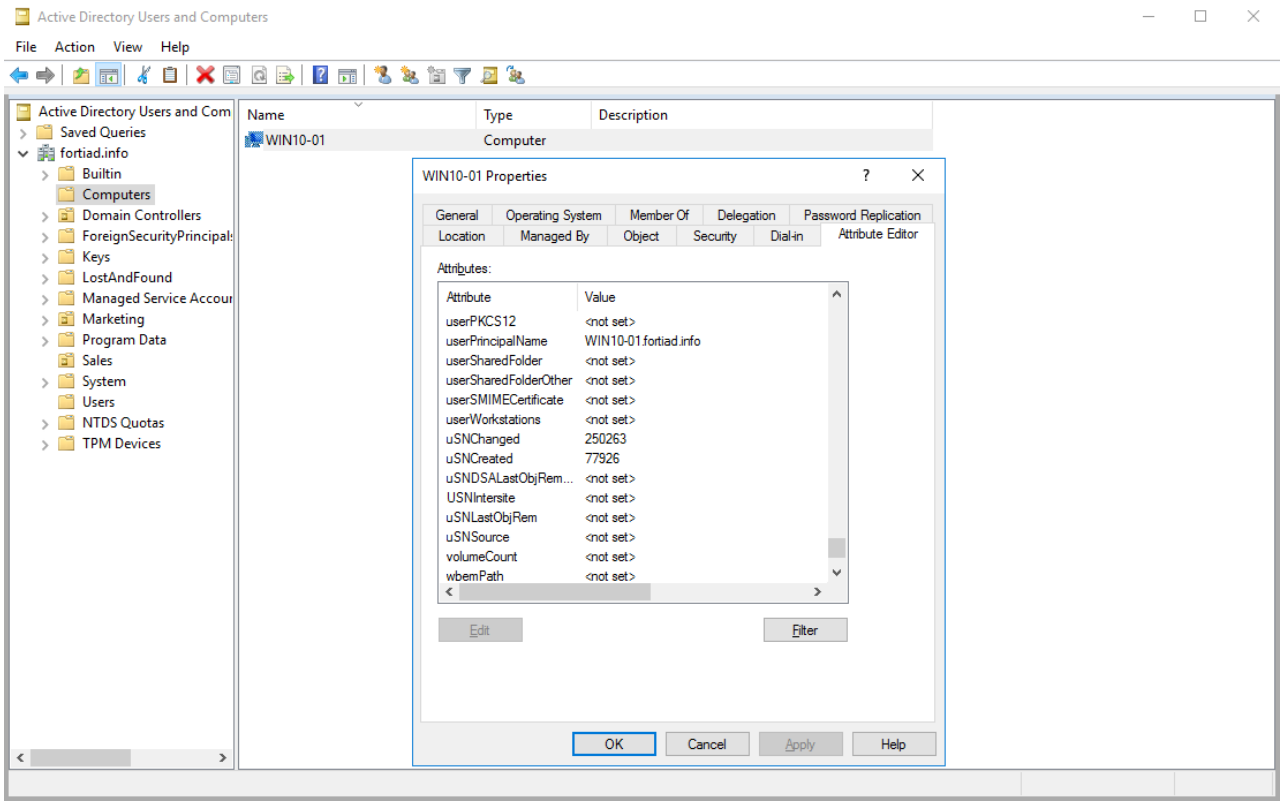
```
[1718] fnbamd_ldap_init-search filter is: (&(userPrincipalName=)(!
     (UserAccountControl:1.2.840.113556.1.4.803:=2)))
```

Review the correct setting to configure on the FortiGate (`set account-key-upn-san <option>`) and the SAN field to use on the certificate in FortiGate authentication configuration on page 147.

LDAP lookup fails to match computer

There can be many ways for LDAP lookup to fail. Following are some scenarios:

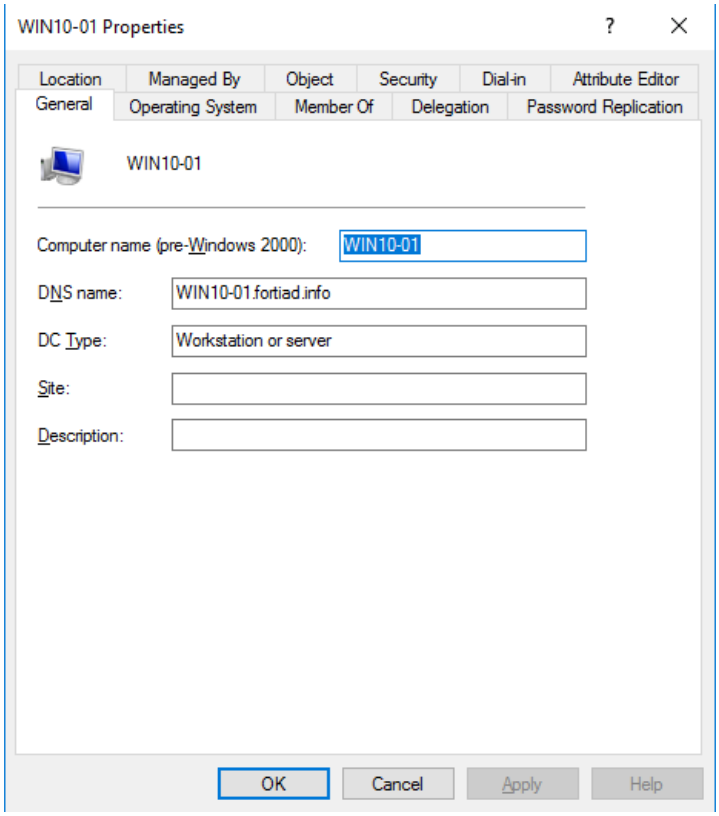
- LDAP looks up the wrong attribute: By default, LDAP queries using the filter `(&(userPrincipalName=%s)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))`. This looks up the UPN attribute of the computers within the LDAP directory.



  However, the matching may need to occur on a different attribute, such as the name of the computer. Therefore, ensure the filter is defined correctly to look for the proper attribute, and that the attribute on the computer on Active Directory is defined properly.
- The subject alternate name (SAN) field and the value of the attribute of the computer do not match completely. See as follows:

```
[448] __cert_ldap_query-UPN = 'WIN10-01.fortiad.info'
[1718] fnbamd_ldap_init-search filter is: (&(name=WIN10-01.fortiad.info)(!
     (UserAccountControl:1.2.840.113556.1.4.803:=2)))
```

In this example, the FortiGate retrieves the certificate DNS name, which is WIN10-01.fortiad.info. However, the computer name attribute of the computer is WIN10-01. So, this mismatch results in the computer not being matched during LDAP lookup.



Resolving the issue may require a new certificate. You can also configure a different filter on the FortiGate's `user.ldap.account-key-filter` setting to look up a different attribute.

FortiGate cannot match right group

Assuming that LDAP lookup found the computer on the LDAP directory:

```
[750] fnbamd_ldap_build_dn_search_req-base:'dc=fortiad,dc=info' filter:(&
     (userPrincipalName=WIN10-01.fortiad.info)(!
     (UserAccountControl:1.2.840.113556.1.4.803:=2)))
...
[1226] __fnbamd_ldap_dn_entry-Get DN 'CN=WIN10-01,CN=Computers,DC=fortiad,DC=info'
```

Next it searches for the groups that this computer belongs to:

```
[649] fnbamd_ldap_build_attr_search_req-Adding attr 'memberOf'
[661] fnbamd_ldap_build_attr_search_req-base:'CN=WIN10-01,CN=Computers,DC=fortiad,DC=info'
     filter:cn=*
```

Search returns multiple groups:

```
[532] __retrieve_group_values- attr='memberOf', found 1 values
[542] __retrieve_group_values-val[0]='CN=VPNComputers,CN=Users,DC=fortiad,DC=info'
...
```

```
[472] __get_one_group-group: CN=Domain Computers,CN=Users,DC=fortiad,DC=info
```

However, group matching fails:

```
[1074] fnbamd_cert_auth_copy_cert_status-Matched peer user 'PKI-LDAP-Machine'
[833] fnbamd_cert_check_matched_groups-checking group with name 'PKI-Machine-Group'
[903] fnbamd_cert_check_matched_groups-not matched
```

Verify `group-name` in the LDAP setting:

```
config user group
    edit "PKI-Machine-Group"
        set member "LDAP-fortiad-Machine" "PKI-LDAP-Machine"
        config match
            edit 1
                set server-name "LDAP-fortiad-Machine"
                set group-name "CN=VPNComputers,DC=fortiad,DC=info"
            next
        end
    next
end
```

Since `group-name` is missing `CN=Users`, group matching failed.

Windows started up but tunnel did not come up

If you confirmed that FortiClient received the Remote access profile updates from EMS and that you can establish the tunnel manually, verify the configuration by doing the following.

To verify the configuration:

1. Enable `diagnose debug application fnbamd -1` debugs on the FortiGate.
2. Restart the Windows computer.
3. If upon restart, no debugs appear, the device has not attempted VPN connection.
4. On EMS, edit the Remote Access profile currently assigned to the endpoint policy.
5. In XML view, verify under the global `<options>` settings that `<on_os_start_connect>` is configured and assigned the machine-cert-vpn-auto tunnel.

Change log

Date	Change description
2024-12-12	Initial release.

www.fortinet.com