User Guide

FortiClient Standalone 7.4.7

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

June 02, 2026
FortiClient Standalone 7.4.7 User Guide
04-747-1287839-20260602

TABLE OF CONTENTS

Change log **5**
Introduction **6**
FortiClient Standalone feature comparison 6
Getting started with FortiClient Standalone **7**
Provisioning preparation **9**
Installation requirements 9
Licensing 10
Required services and ports 10
Firmware images and tools 11
Microsoft Windows 11
macOS 12
Linux 12
Provisioning **13**
Manually installing FortiClient Standalone on computers 13
Microsoft Windows 13
macOS 14
Linux 16
Centralized FortiClient Standalone deployment using Microsoft AD servers 16
Deploying FortiClient Standalone with Microsoft AD 17
Uninstalling FortiClient Standalone with Microsoft AD 17
Logging into FortiClient Standalone 18
Uninstalling FortiClient Standalone 22
Remote Access **23**
Configuring an IPsec VPN connection 23
Connecting to VPN 26
Connecting VPN with FortiToken Mobile 27
Internal resource lookup with IPv6 enabled on NIC interface 28
VPN performance 28
Notifications **29**
Settings **30**
Logging 30
VPN options 31
Advanced options 32
FortiPAM agent client executable integrity check 33
FortiTray 38
Diagnostic Tool **39**
Appendix A - Processes **43**
FortiClient Standalone (Windows) processes 43
FortiClient Standalone (macOS) processes 44
Appendix B - CLI commands **45**
FortiClient Standalone (Windows) CLI commands 45

VPN 45
Configuration backup and restoration 47
FortiClient Standalone (macOS) CLI commands 47
FortiClient Standalone (Linux) CLI commands 47
Configuration backup and restoration 48

Change log

Date	Change description
2026-05-04	Initial release.
2026-06-02	Updated Licensing on page 10.

Introduction

FortiClient Standalone is a lightweight endpoint client that provides secure remote access and identity-based services without requiring FortiClient EMS. Unlike the full FortiClient solution, the Standalone version operates independently and uses FortiIdentity Cloud (FIC) for licensing, authentication, and user management. FortiClient Standalone supports the following core features:

- IPsec VPN (IKEv2 only)—Create a secure Virtual Private Network (VPN) using IPsec connection between your Windows, macOS, Linux device and the FortiGate. Your connection will be fully encrypted and all traffic will be sent over the secure tunnel.
- SSOMA (Single Sign-On Mobility Agent)
- PAM (Privileged Access Management integration)

The client uses a token-based licensing model and performs both online and offline license validation to ensure continuous operation.

- This document is written for FortiClient Standalone (Windows) 7.4.7. FortiClient Standalone macOS and Linux 7.4.7 do not support all features that this document describes. See FortiClient Standalone feature comparison on page 6 for more details.
- FortiClient Standalone supports limited basic features for IPsec VPN with limited TAC support (email only). For advanced VPN functionality and EPP capabilities with central management and full TAC support, use the FortiClient full version. See the FortiClient Administration Guide.

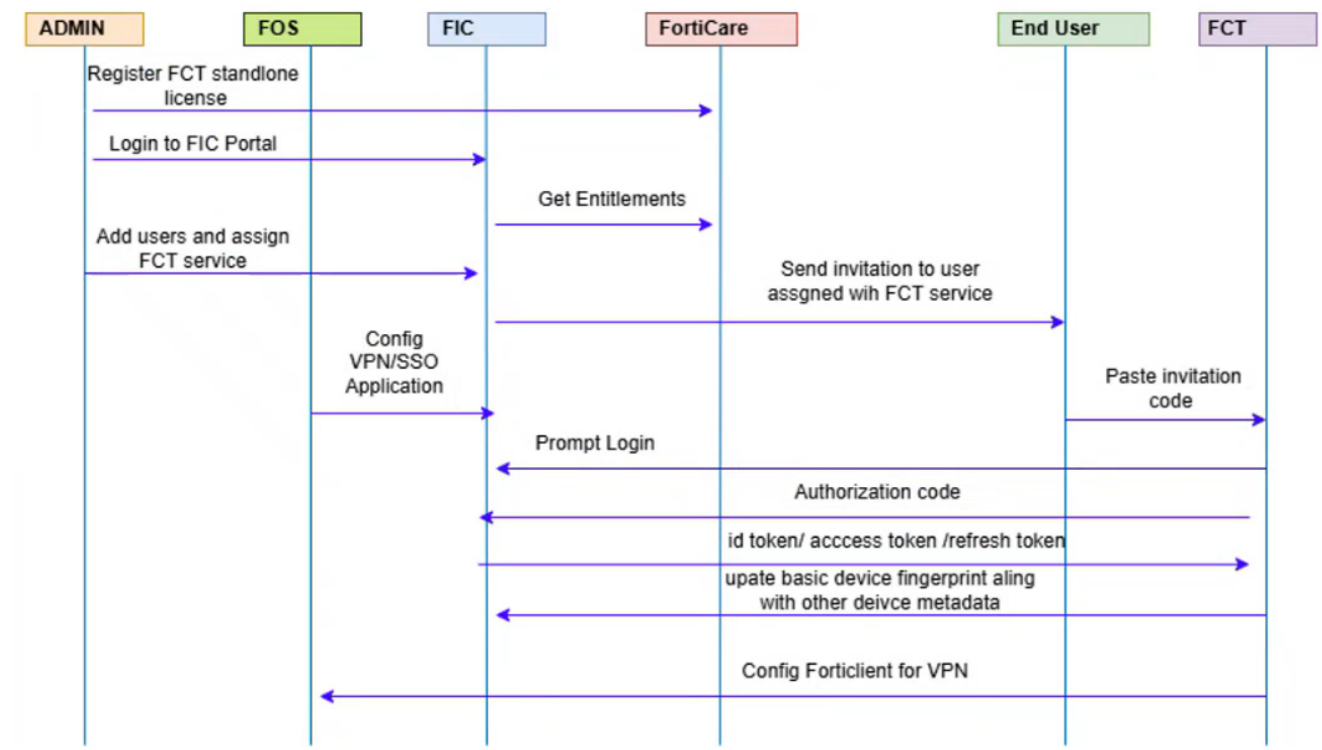
FortiClient Standalone feature comparison

The following chart provides FortiClient Standalone feature comparison for different operating systems:

Module	Windows	macOS	Linux
Remote Access	Yes	No support for IPv6.	No support for SmartCard authentication.
Single sign on mobility agent	Yes	Yes	No
Privileged access agent	Yes	No	No

Getting started with FortiClient Standalone

You must use FortiClient Standalone with FortiIdentity Cloud (FIC). FortiClient Standalone communicates with FIC for authentication, device registration, and license validation. The setup process is as follows. The FIC administrator completes some actions and the endpoint user completes others.



1. The administrator registers the FortiClient Standalone license on FortiCare. FIC will then sync with FortiCare and create an account. It will also retrieve entitlement details and push to FortiClient Standalone.
2. The administrator logs into the FIC portal and creates a FortiClient Standalone local user or connects to an external IDP. See Provisioning FIC for FortiClient integration.
3. The administrator gets an invitation code to be used as an identifier when an end user authenticates to service.
4. The endpoint user installs FortiClient Standalone (see Manually installing FortiClient Standalone on computers on page 13 or Centralized FortiClient Standalone deployment using Microsoft AD servers on page 16) and log into it using the invitation code to get license entitlement (see Logging into FortiClient Standalone on page 18). Re-authentication is required only if the password changes or the user is removed. FortiClient Standalone regularly syncs with FIC for entitlement updates.
5. Once licensed, the device is associated with the user account (three devices maximum for each account) and the user has access to all allowed features. For VPN, user can then create an IPsec VPN

tunnel and connect to their FortiGate. See VPN with FortiClient Standalone and FortiIdentity Cloud. Hosted VPN is currently unsupported.

Provisioning preparation

Before provisioning FortiClient Standalone, administrators and endpoint users should understand the installation requirements and FortiClient Standalone 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) • Windows 10 IoT Enterprise • Windows 11 IoT Enterprise	• Microsoft Windows-compatible computer with Intel processor or equivalent. • 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
• macOS Tahoe (version 26) • macOS Sequoia (version 15) • macOS Sonoma (version 14)	• Apple Mac computer with Intel processor or Apple silicon 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 • CentOS Stream 9	• Linux-compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512 MB RAM

OS support	Minimum system requirements
All supported with GNOME	• 600 MB free hard disk space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections

Licensing

The FortiClient Standalone license includes a basic FortiIdentity Cloud (FIC) license (limited to two user sources — one remote and one local, one FortiToken per user with no SMS quota), which remains valid until the FortiClient Standalone license expires. See Registering FortiClient Standalone license and the FortiClient Ordering Guide for details.

If you have an existing FIC instance to use with FortiClient Standalone, you must register the FortiClient Standalone license in the same FortiCare account where your FortiGate and FIC licenses are registered.

For further questions about the FortiClient Standalone license, contact your Fortinet sales representative.

Required services and ports

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

Communication	Usage	Protocol	Port	Incoming/outgoing	How to customize
Remote access - IPsec VPN	Establish VPN connection to the FortiGate	UDP	IKE 500 ESP (IP 50) NAT-T 4500	Outgoing	N/A
		TCP	443		

Communication	Usage	Protocol	Port	Incoming/outgoing	How to customize
FortiAuthenticator/FortiGate	Single sign on (SSO) mobility agent, FortiClient SSO	TCP	8001 (default)	Outgoing	GUI
FortiPAM	Use FortiPAM for privilege access management	TCP	9191	Outgoing	N/A

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_7.4.7.4917.F.zip`	Zip package containing miscellaneous tools, including VPN automation files.
`FortiClientStandaloneSetup_7.4.7.4917.F_x64.zip`	FortiClient Standalone installer (64-bit) and zip package.

The following tools and files are available in the `FortiClientTools_7.4.7.4917.F.zip` file:

File	Description
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstall, and reinstall 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 (32-bit).

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal. After logging in, click *Download* > *Firmware Image Checksum*, enter the image file name, including the extension, and select *Get Checksum Code*.

macOS

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

File	Description
`FortiClientStandaloneSetup_7.4.7.xxxx.F_macosx.dmg`	Standard installer for macOS.

Linux

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

File	Description
`forticlient_standalone_7.4.7.xxxx.F_amd64.deb`	Standard installer package for Ubuntu.
`forticlient_standalone_7.4.7.xxxx.F_x86_64.rpm`	Standard installer package for Red Hat and CentOS.
`forticlient_standalone_7.4.7.xxxx.F_arm64.deb`	Standard installer package for ARM based Ubuntu.
`forticlient_standalone_7.4.7.xxxx.F_aarch64.rpm`	Standard installer package for ARM based Red Hat and CentOS.

Provisioning

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

FortiClient Standalone prevents uninstallation only for non-administrator users.

Manually installing FortiClient Standalone on computers

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

Microsoft Windows

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

To check FortiClient Standalone'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 Standalone has system privileges.

To install FortiClient Standalone on Windows:

1. Double-click the FortiClient Standalone executable file. The *Setup Wizard* launches.
2. In the *Welcome to the FortiClient Standalone 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.

6. Click *Next*. The *Ready to install FortiClient Standalone* screen displays.
7. Click *Install* and then *Finish*. On a new installation, you do not need to reboot your system.
8. Double-click the desktop shortcut to launch FortiClient Standalone.

Alternatively, run the following command to install FortiClient Standalone from the CLI:

```
m>msiexec.exe /i "FortiClientStandalone.msi"
```

macOS

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

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

1. Install FortiClient Standalone on a macOS computer using the installer file. See To install FortiClient Standalone on a macOS computer: on page 14.
2. Activate system extensions. See To activate the extension: on page 14.
3. Enable notifications. See To enable notifications: on page 15.

FortiClient Standalone (macOS) requires the use of the 198.19.0.0/16 subnet. You cannot use this subnet for other uses in your environment.

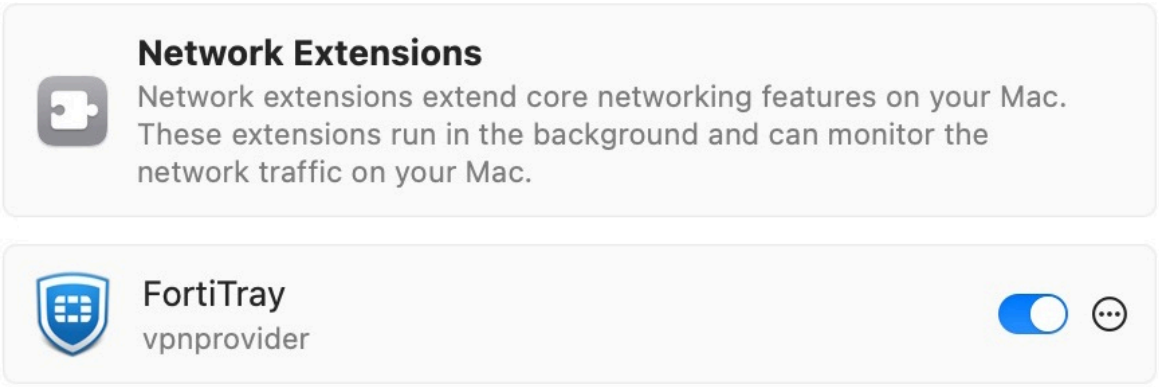
To install FortiClient Standalone on a macOS computer:

1. Double-click the `FortiClientStandaloneSetup_7.4.7.xxxx.F_macosx.dmg` installer file. The *FortiClient Standalone for macOS* dialog displays.
2. Double-click *Install*. The *Welcome to the FortiClient Standalone 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 Standalone has been saved to the *Applications* folder.
8. Double-click the FortiClient Standalone icon to launch the application. The application loads to your desktop.

To activate the extension:

After you perform an initial install of FortiClient Standalone, you must enable the *FortiTray* extension for VPN to work properly. The FortiClient Standalone team ID is AH4XFXJ7DK.

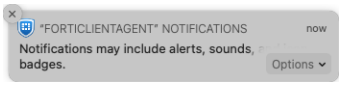
1. Ensure you have administrator credentials for the macOS machine.
2.
   - **(macOS Tahoe (version 26)** Go to *System Settings > General > Login Items & Extensions > By Category > Network Extensions*.
   - **(macOS Sequoia (version 15)** Go to *System Settings > General > Login Items & Extensions > Network Extensions*.
   - **(macOS Sonoma (version 14)** Click *Some system software requires your attention before it can be used*.
3. Toggle on the *FortiTray* extension for VPN to work properly.



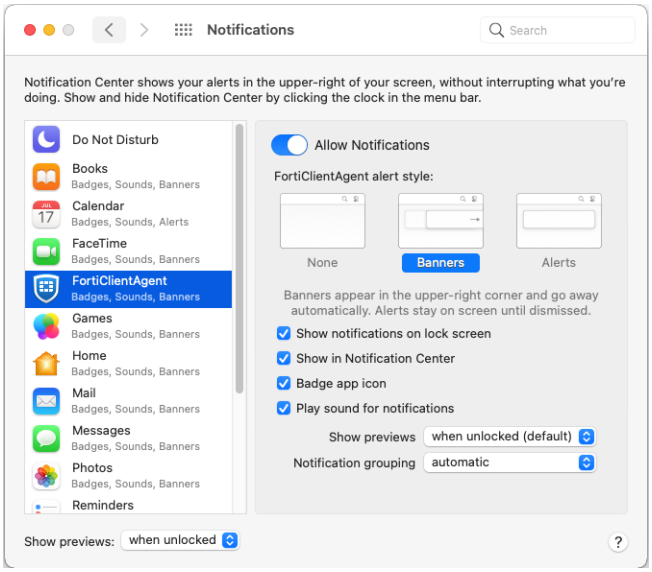
4. Click *Done*.

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.



Linux

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

Various CLI commands are available for FortiClient Standalone (Linux) 7.4.7. See FortiClient Standalone (Linux) CLI commands on page 47.

Installing FortiClient Standalone (Linux) requires root or sudo privileges. Once FortiClient Standalone (Linux) is installed, it has root/sudo privileges.

To install on Red Hat or CentOS:

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

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

To install on Ubuntu:

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

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

Centralized FortiClient Standalone deployment using Microsoft AD servers

You can centrally deploy FortiClient Standalone to multiple endpoints using Microsoft AD servers. While there are multiple ways to deploy FortiClient Standalone MSI packages to endpoints including using AD servers (see Firmware images and tools on page 11, 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 Standalone with Microsoft AD on page 17
- Uninstalling FortiClient Standalone with Microsoft AD on page 17

Deploying FortiClient Standalone with Microsoft AD

To deploy FortiClient Standalone 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 Standalone MSI installer file is distributed from.
4. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient Standalone 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 Standalone software to into the newly-created OU.
8. Create a group policy object (GPO), then create the FortiClient Standalone 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 Standalone 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 Standalone with Microsoft AD

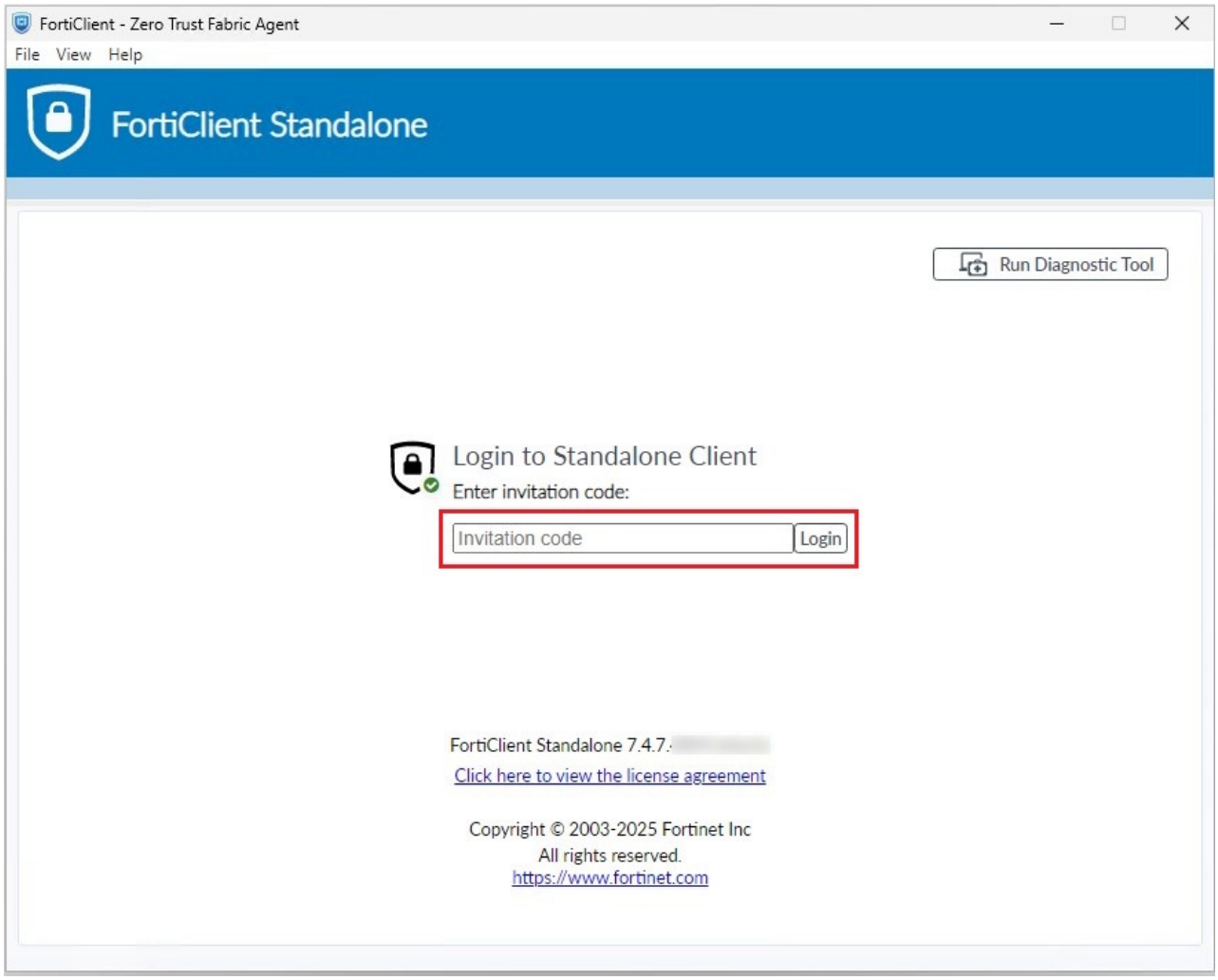
To uninstall FortiClient Standalone with Microsoft AD:

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 Standalone 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 Standalone.
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.

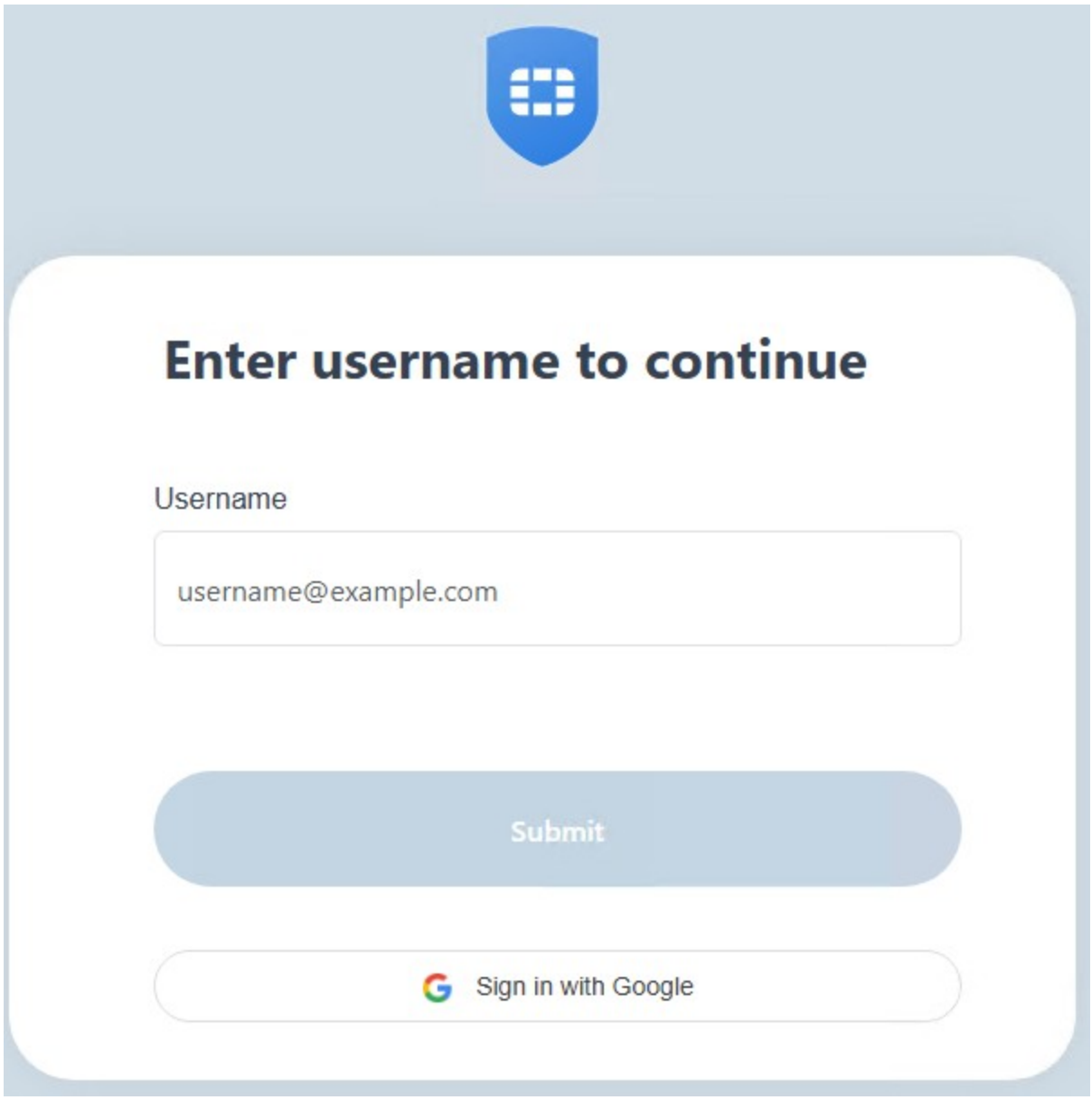
Logging into FortiClient Standalone

To log into FortiClient Standalone after installation:

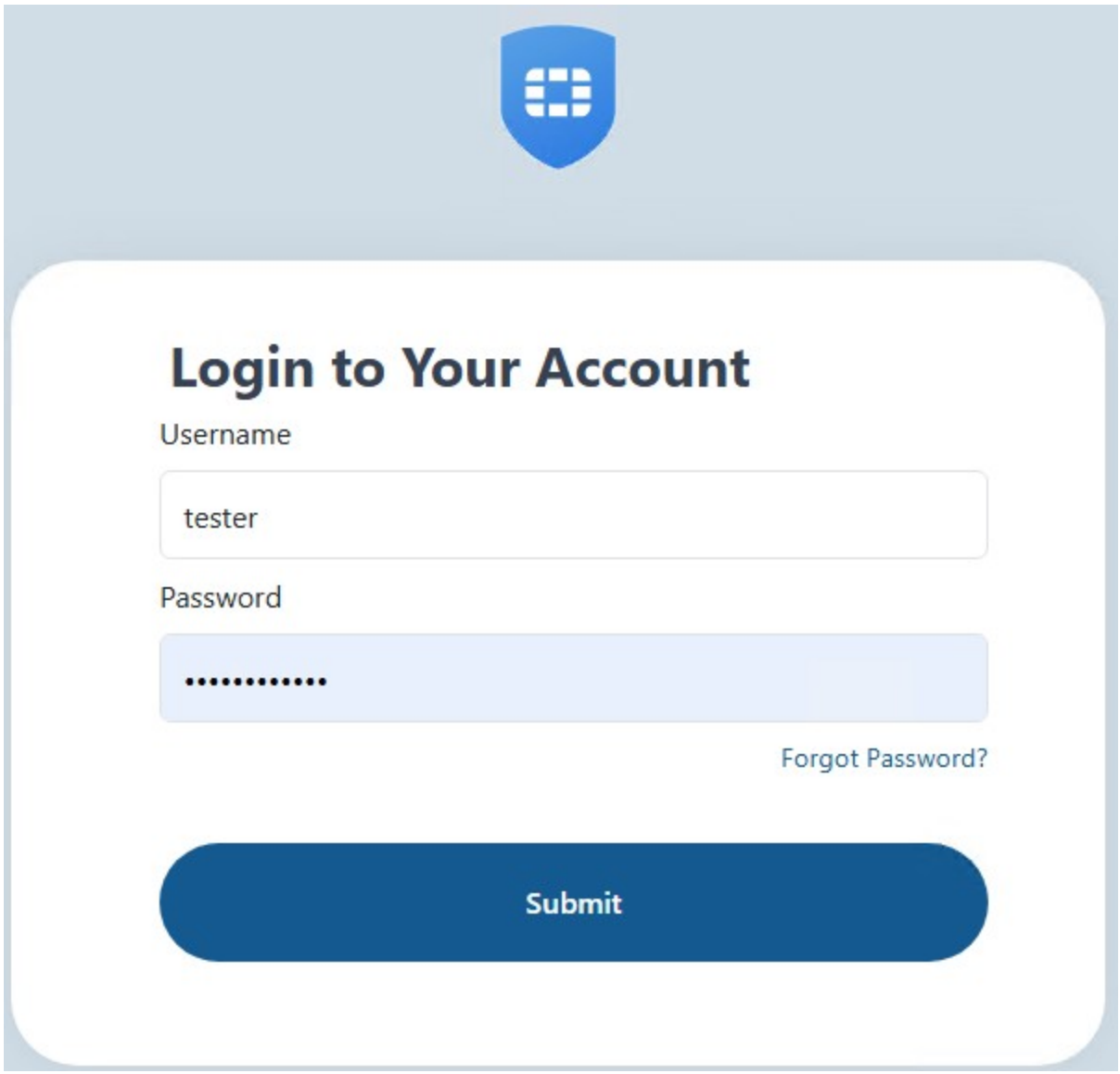
1. In the FortiClient Standalone GUI, enter the invitation code (that you received from the FortiIdentity Cloud administrator via email) and click *Login*.



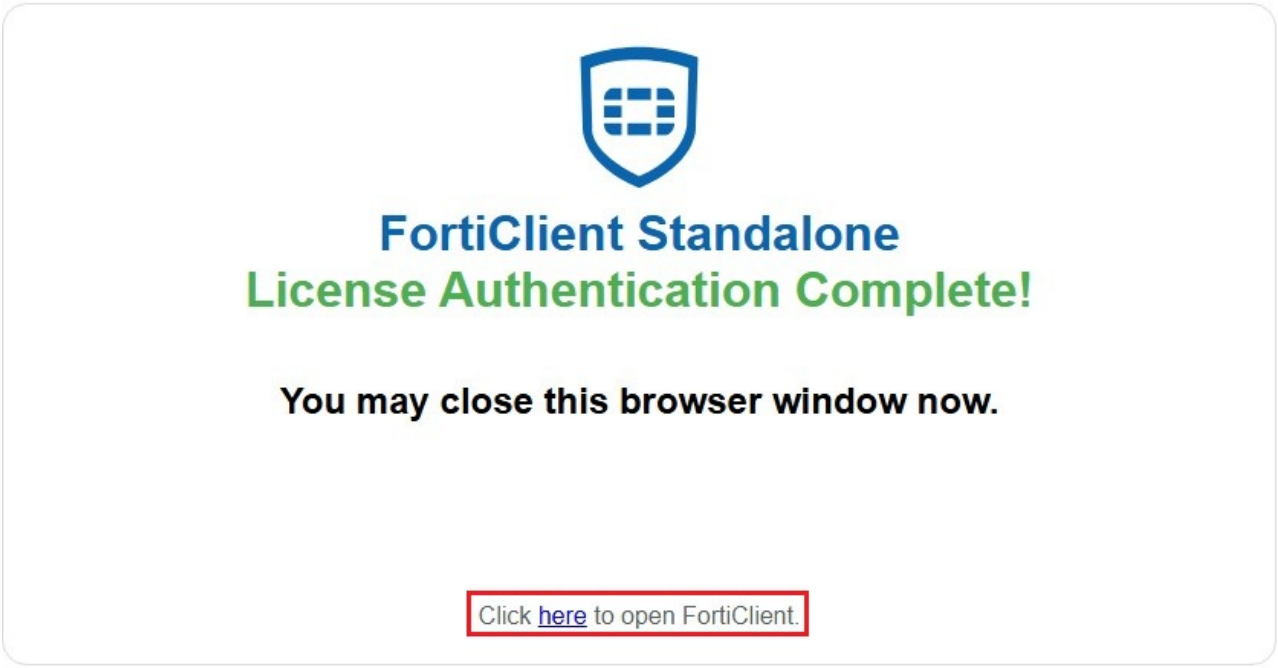
2. Enter the username as required and click *Submit*.



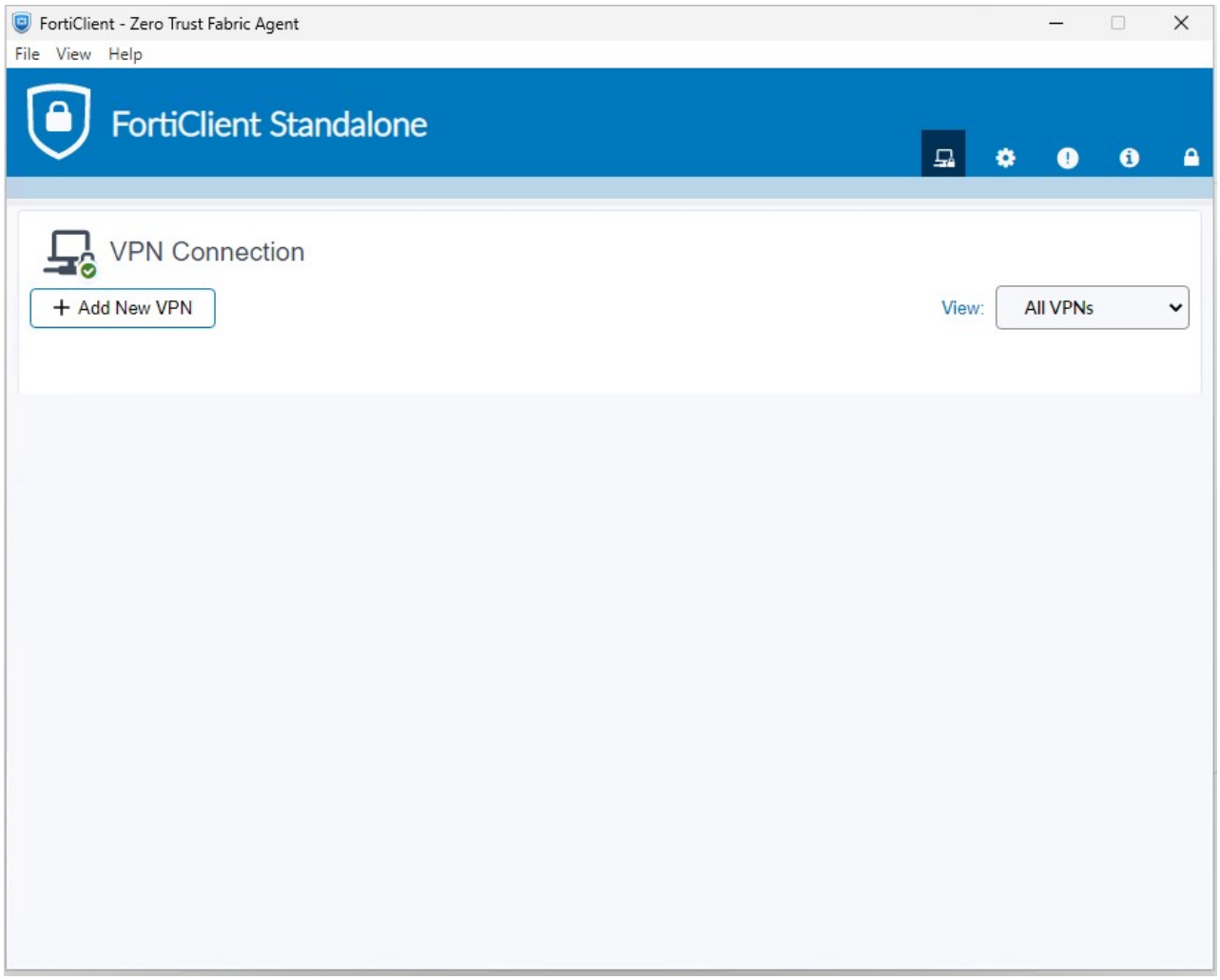
3. Enter the password and click *Submit*.



4. After successful authentication, close the page and click the link to open FortiClient Standalone.



You will then be redirected to the *Remote Access on page 23* page where you can start creating IPsec VPN tunnels.



Uninstalling FortiClient Standalone

To uninstall FortiClient Standalone:

1. In the Windows System Tray, right-click the FortiTray icon, then select *Shutdown FortiClient*.
2. Once FortiClient Standalone is shutdown, uninstall FortiClient Standalone using the Windows *Add/Remove Programs* application.

If the uninstallation does not work, try uninstalling FortiClient Standalone in Windows Safe mode by following this KB.

Remote Access

FortiClient Standalone supports IPsec VPN connections to your network for remote access. Endpoint users can configure new VPN connections using FortiClient Standalone.

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

Configuring an IPsec VPN connection

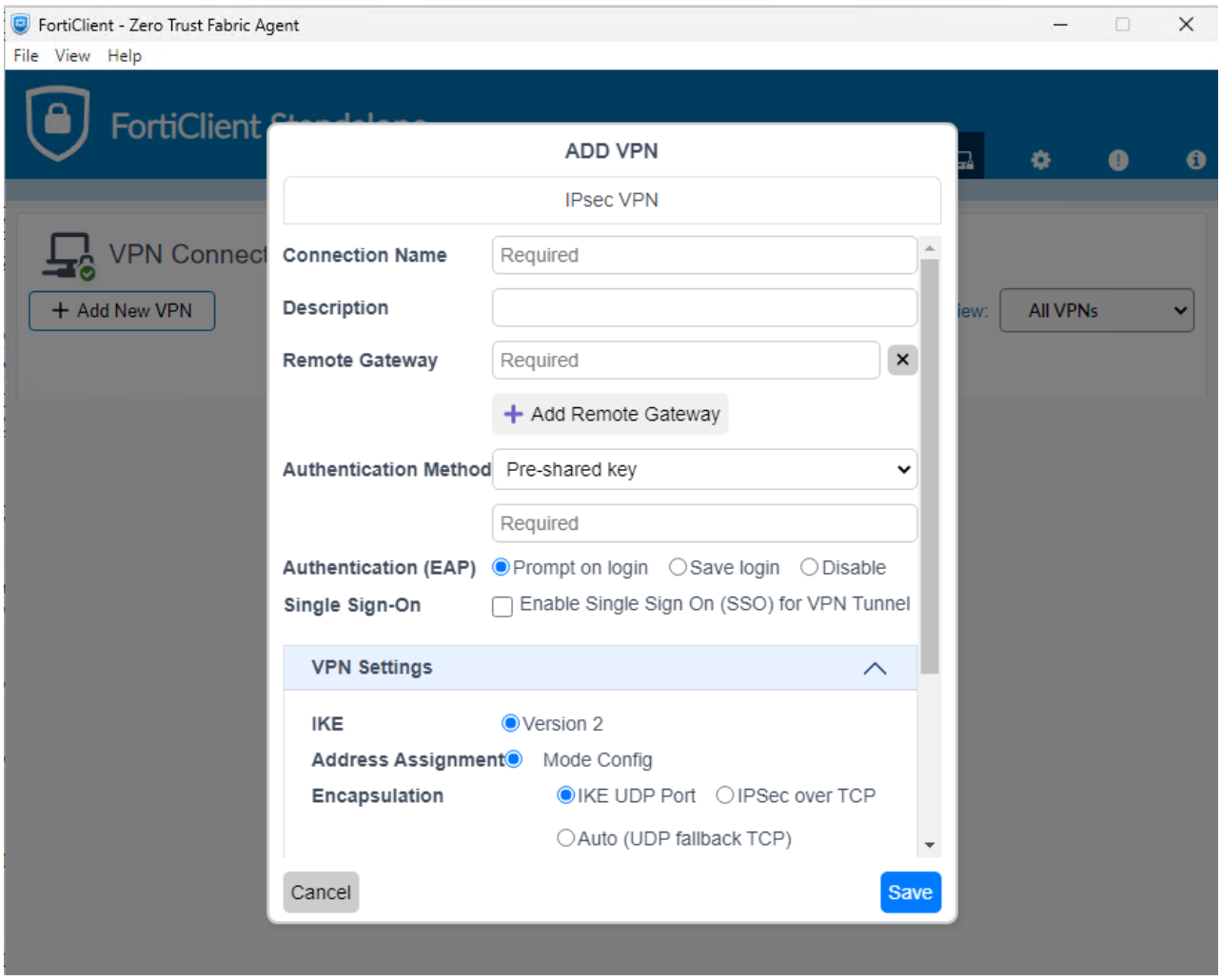
To configure an IPsec VPN connection:

1. Make sure you have created an IPsec VPN tunnel (for FortiClient Standalone) in FortiGate:
   - For FortiOS 8.0.0 or later, we recommend using the VPN wizard in the (FortiOS GUI) to create an IPsec VPN tunnel for FortiClient Standalone, which is convenient and efficient. See VPN with FortiClient Standalone and FortiIdentity Cloud in the *FortiOS Administration Guide*.
   - For FortiOS 7.6 or 7.4, use the CLI to create an IPsec VPN tunnel for FortiClient Standalone. See the *To configure IPsec VPN with FortiClient as the dialup client in the CLI:* section in the FortiClient as dialup client topic in the *FortiOS Administration Guide*.
2. On the *Remote Access* tab of the FortiClient Standalone GUI, click *Add New VPN*.
3. Configure the following settings:

Option	Description
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 (EAP)	Select *Prompt on login*, *Save login*, or *Disable*.
Single Sign On	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).

Option		Description
	SSO port	Enter the port number that FortiClient Standalone uses to communicate with the FortiGate, which acts as the SAML service provider.
	Use external browser for saml authentication	FortiClient Standalone can use a browser as an external user-agent to perform SAML authentication for VPN tunnel mode instead of the FortiClient Standalone embedded login window. If a user already authenticated using SAML in the default browser, they do not need to reauthenticate in the FortiClient Standalone built-in browser. Available if you enable *Enable Single Sign On (SSO) for VPN Tunnel*. See Using a browser as an external user-agent for SAML authentication in an SSL VPN connection. On FortiClient Standalone (macOS), if *Non-Secure site connections > Warn before connecting to a website over HTTP* is enabled in Safari and using an external browser for SAML authentication is configured, VPN connection may fail.
VPN Settings		
	IKE	Select *Version2*. IKEv1 is unsupported.
	Address Assignment	Only *Mode Config* is available for selection.
	Encapsulation	Configure one of the following for the encapsulation (or transport) mode: • *IKE UDP Port*: UDP encapsulation (transport) mode. This is the default and used for most VPN connections. Configure a custom port number if desired. • *IPsec over TCP*: TCP transport mode. This is recommended for use in restrictive networks. Configure a custom port number if desired. • *Auto*: FortiOS dynamically selects the transport mode.
	IKE UDP Port	Configure a custom port number if desired.
	IKE TCP Port	Configure a custom port number if desired.
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.

Option		Description
	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.
	Enable Local LAN	Enable local LAN when using a full tunnel. This setting does not apply to split tunnels.
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.



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

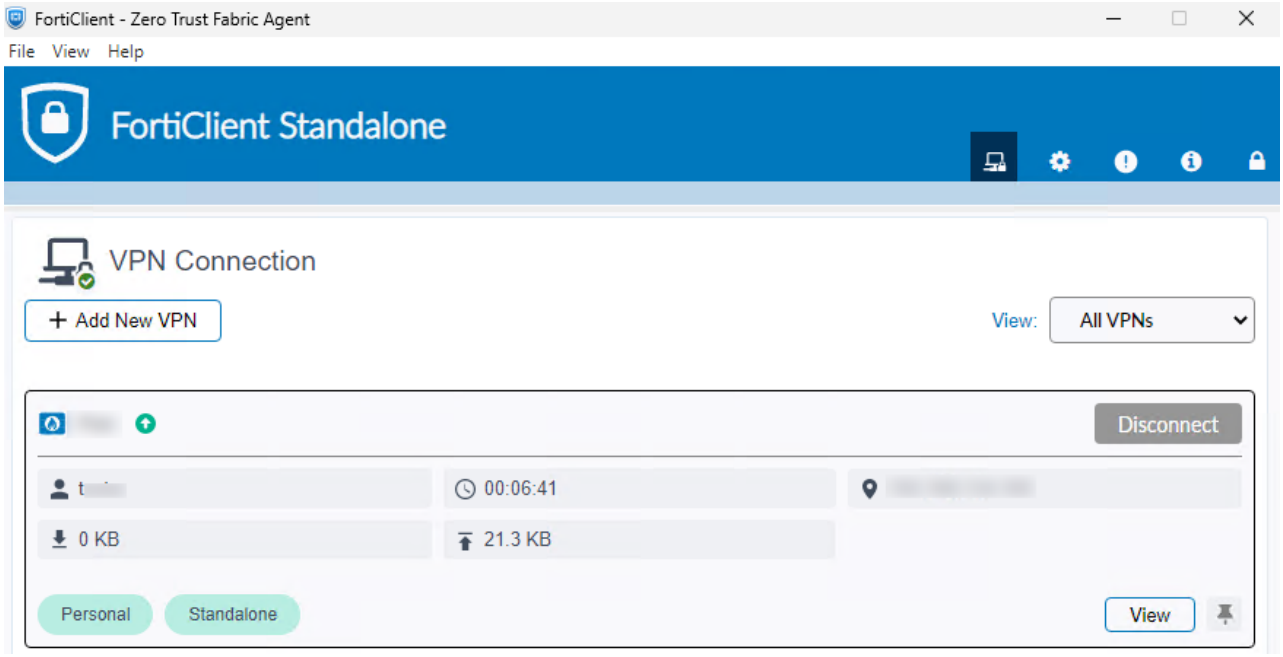
Connecting to VPN

You can connect VPN tunnels to FortiGate. Depending on the FortiClient Standalone 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.

To connect to VPN:

1. On the FortiClient Standalone GUI, click *Connect* for the desired VPN connection. Alternatively, you can right-click the FortiTray icon in the system tray and select a VPN configuration to connect to.



2. Enter your username and password.
3. If the tunnel requires a certificate, select a certificate. If the tunnel does not require a certificate, FortiClient Standalone hides the option. Your administrator may have configured FortiClient Standalone to automatically locate a certificate for you.
4. Click the *Connect* button.
   When connected, FortiClient Standalone 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.

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 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 Standalone 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.

3. 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.

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 disable ParallelAandAAAA capability as follows:

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

VPN performance

High latency can have a significant impact on a user's observed internet performance.

In general, physical distance (e.g. the speed of light) and third party internet service provider routing to the last-mile introduce most network latency between the user and VPN gateway.

To determine VPN performance, you can test the VPN gateway IP address or FQDN via `ping`, `traceroute`, or `mtr`.

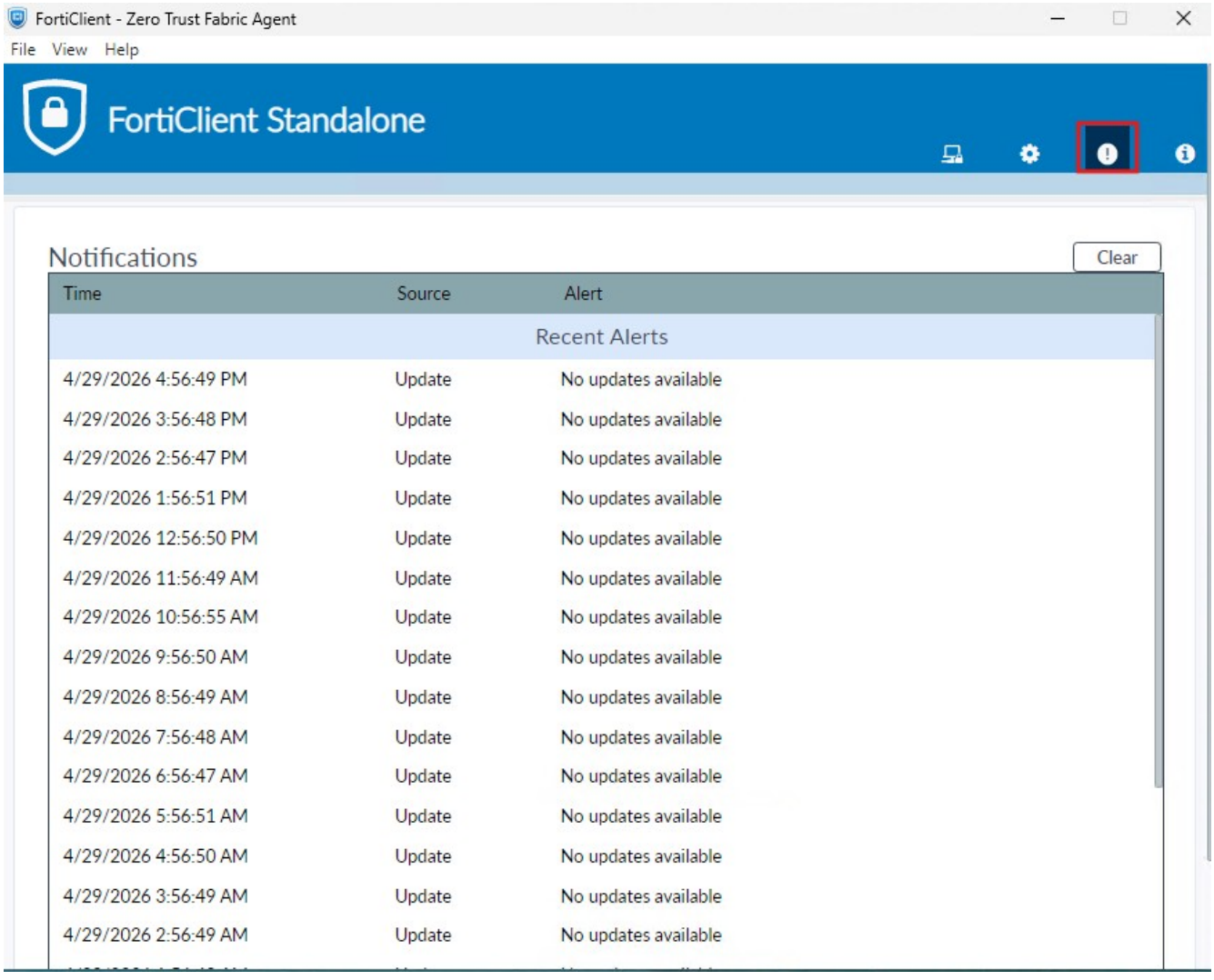
Keep these latency thresholds in mind when evaluating these selections:

Latency level	Impact to performance	Latency (milliseconds (ms))
Ideal	Best performance	< 20 ms
Acceptable	Slightly impacted	20-60 ms
High	Moderately impacted	60-100 ms
Extreme	Significantly impacted	> 100 ms

Notifications

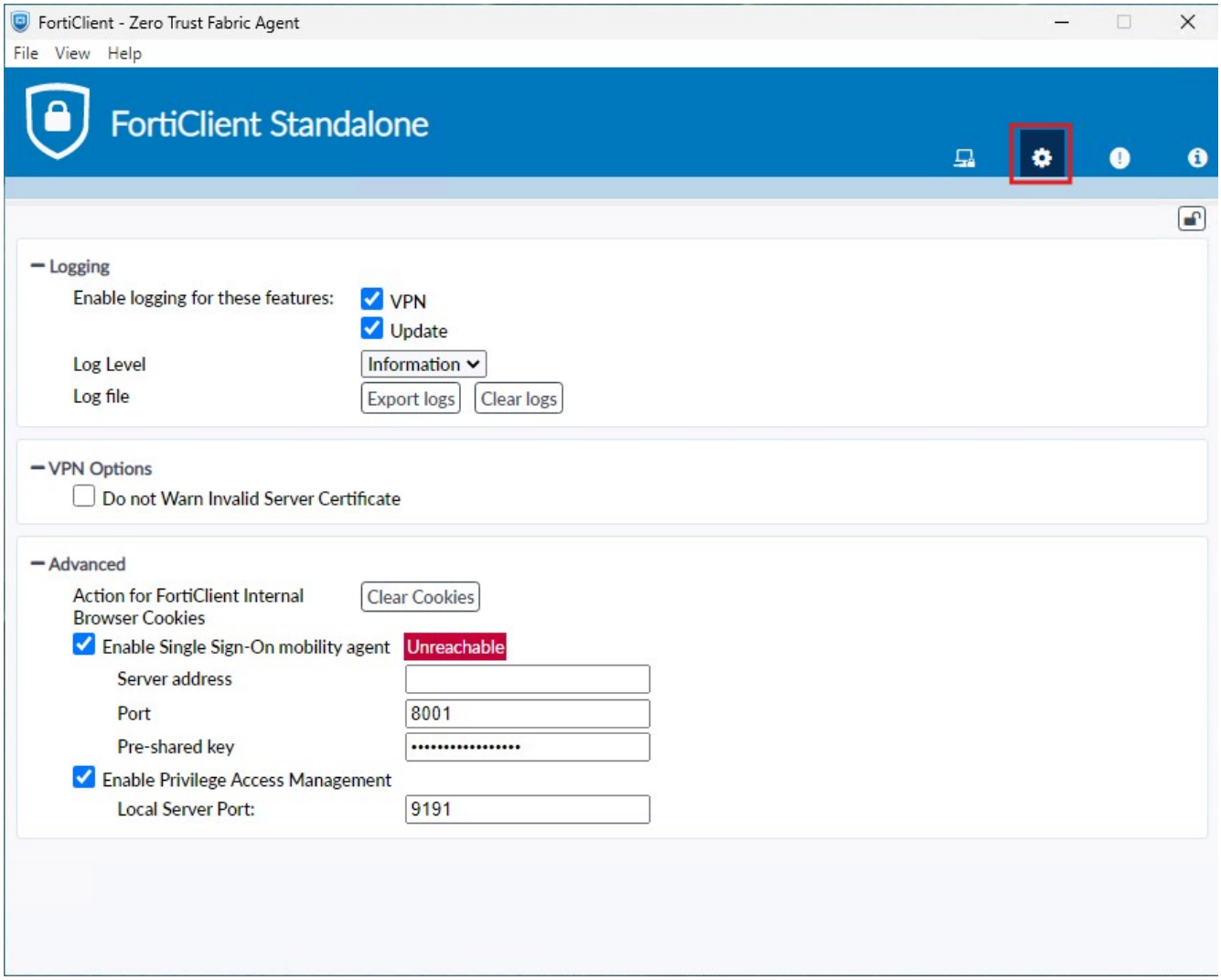
The *Notifications* tab in FortiClient Standaloneprovides real-time feedback about system status with event notifications for the following:

- Signature and engine updates
- Software upgrades
- License registration and status change
- VPN connection status (connecting, connected, disconnected)



Settings

This section describes the options on the *Settings* page. You must have administrator privileges for the machine to unlock the settings for configuration.



Logging

You can enable logging for VPN and update. You can also configure the log level for verbosity.

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*.

To delete the log file:

1. Go to *Settings*.
2. Expand the *Logging* section, and click *Clear logs*.

VPN options

You can configure whether to be warned if the server presents an invalid certificate. To do so, go to *Settings* and enable/disable the *Do not Warn Invalid Server Certificate* option in the *VPN Options* section.

Advanced options

To configure advanced options:

1. Go to *Settings*, configure the following settings in the *Advanced* section, and click *OK*:

Option	Description
Action for FortiClient Internal Browser Cookies	Click *Clear Cookies* to delete FortiClient internal browser cookies.
Enable Single Sign-On mobility agent	Enable FortiClient single sign on mobility agent (FSSOMA). A status displays beside this field: • *Disconnected* (gray): displays if FSSOMA is not configured. • *Unreachable* (red): displays if FSSOMA is configured but unable to connect to FortiAuthenticator due to a firewall block, incorrect IP address, port number, or improper resolution of the FortiAuthenticator FQDN. FortiClient also shows this status when the endpoint is logged in as a non-domain user. • *Connected* (green): displays if FSSOMA is configured, successfully connects to FortiAuthenticator, and the endpoint is logged in as a domain user.  The Entra ID JAMF Connector is required for FSSOMA to work on FortiClient Standalone (macOS).
Server address	FortiAuthenticator IP address or FQDN.
Port	Port that FortiClient Standalone uses to communicate with FortiAuthenticator.
Pre-shared key	Preshared key that FortiClient Standalone uses to authenticate to FortiAuthenticator.
Enable Privileged Access Management	Enable privileged 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.

FortiPAM agent client executable integrity check

FortiClient Standalone supports the FortiPAM integrity check feature that allows you to check wither the privileged 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 Standalone 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:

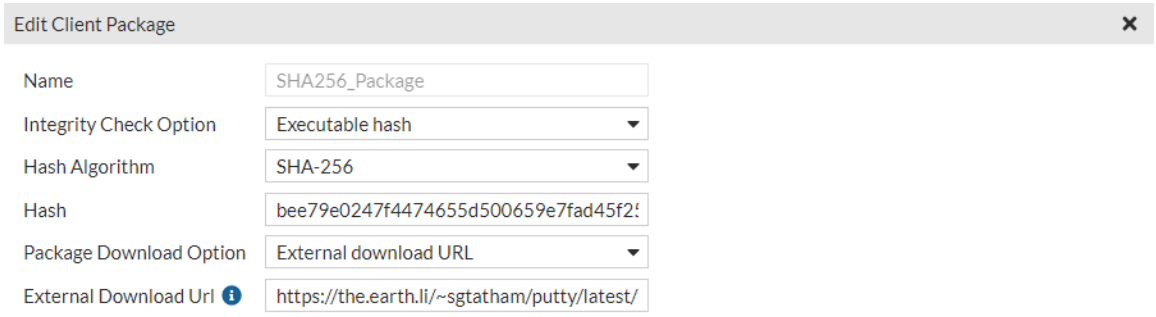
Package download option	Description
External Download URL	Enter launcher application's external download URL link.
Internal Download URL	Upload launcher application directly to the package.

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.



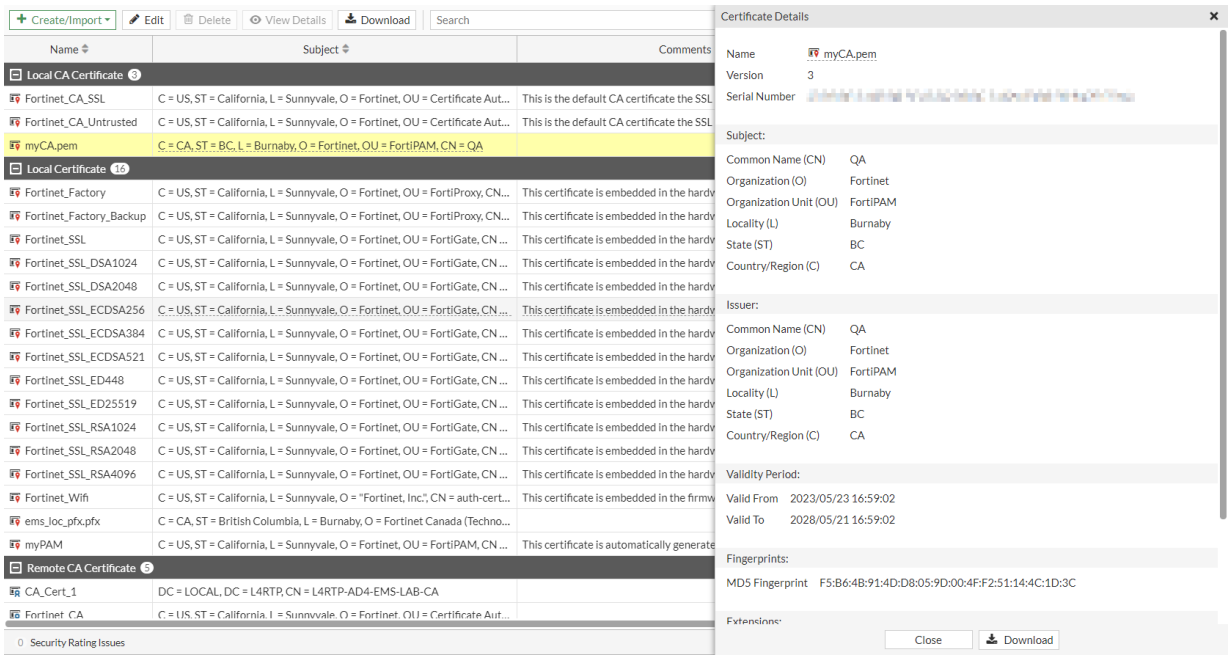
   f. Configure the PuTTy launcher:
      i. Go to *Secret Settings* > *Launchers* > *PuTTy*.
      ii. Enable *Client Software*.
      iii. From the dropdown list, select the desired client software package. Save.
   g. Configure the template:
      i. Go to *Secret Settings* > *Templates* > *FortiGate 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 Standalone(see Provisioning on page 13) with PAM enabled in *Settings* > *Advanced* (see Advanced options on page 32).
3. Log in to FortiPAM as a standard user from the endpoint.
4. Go to *Secrets* > *Secret List*.
5. Click *Launch Secret* to launch the PuTTy secret through the PuTTy application. The PuTTy session establishes.
6. 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*.

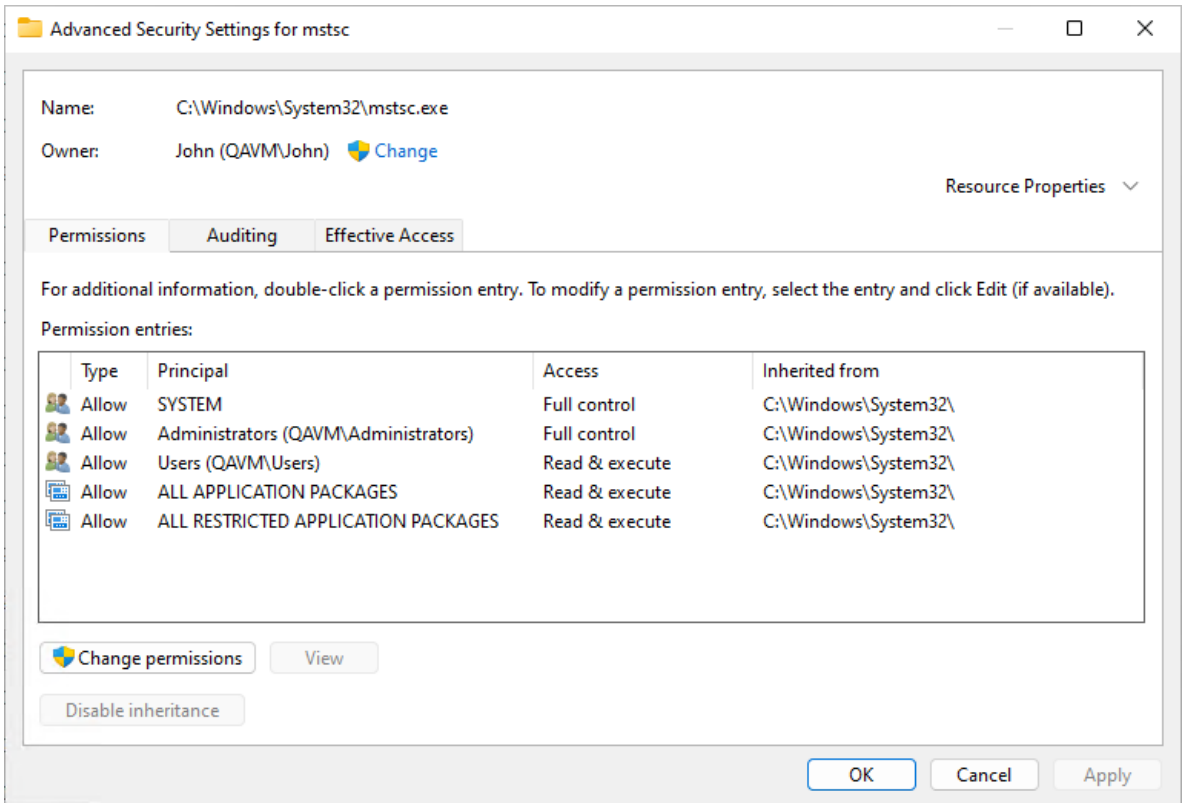
ii. Under *Launcher*, click *Create*.

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 Standalone(see Provisioning on page 13) with PAM enabled in *Settings > Advanced* (see Advanced options on page 32).
4. Log in to FortiPAM as a standard user from the endpoint.
5. Go to *Secrets > Secret List*.
6. 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.
7. 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 Standalone is running on your system, use the FortiTray icon in the Windows system tray for quick access to the following key FortiClient Standalone functions without opening the full GUI, even when FortiClient Standalone is closed.

- Default menu options:
  - Open FortiClient Standalone
  - View *About* tab in FortiClient Standalone
  - Shut down FortiClient Standalone
- Dynamic menu options, depending on configuration:
  - Connect to a configured IPsec VPN connection

Hover the cursor over the FortiTray icon to view the FortiClient Standalone version.

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 Standalone Diagnostic Tool from FortiClient Standalone. Go to *About*. It is available in both licensed and unlicensed states.

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

You can use the FortiClient Standalone Diagnostic Tool to generate a debug report, then provide the debug report to the FortiClient Standalone 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.

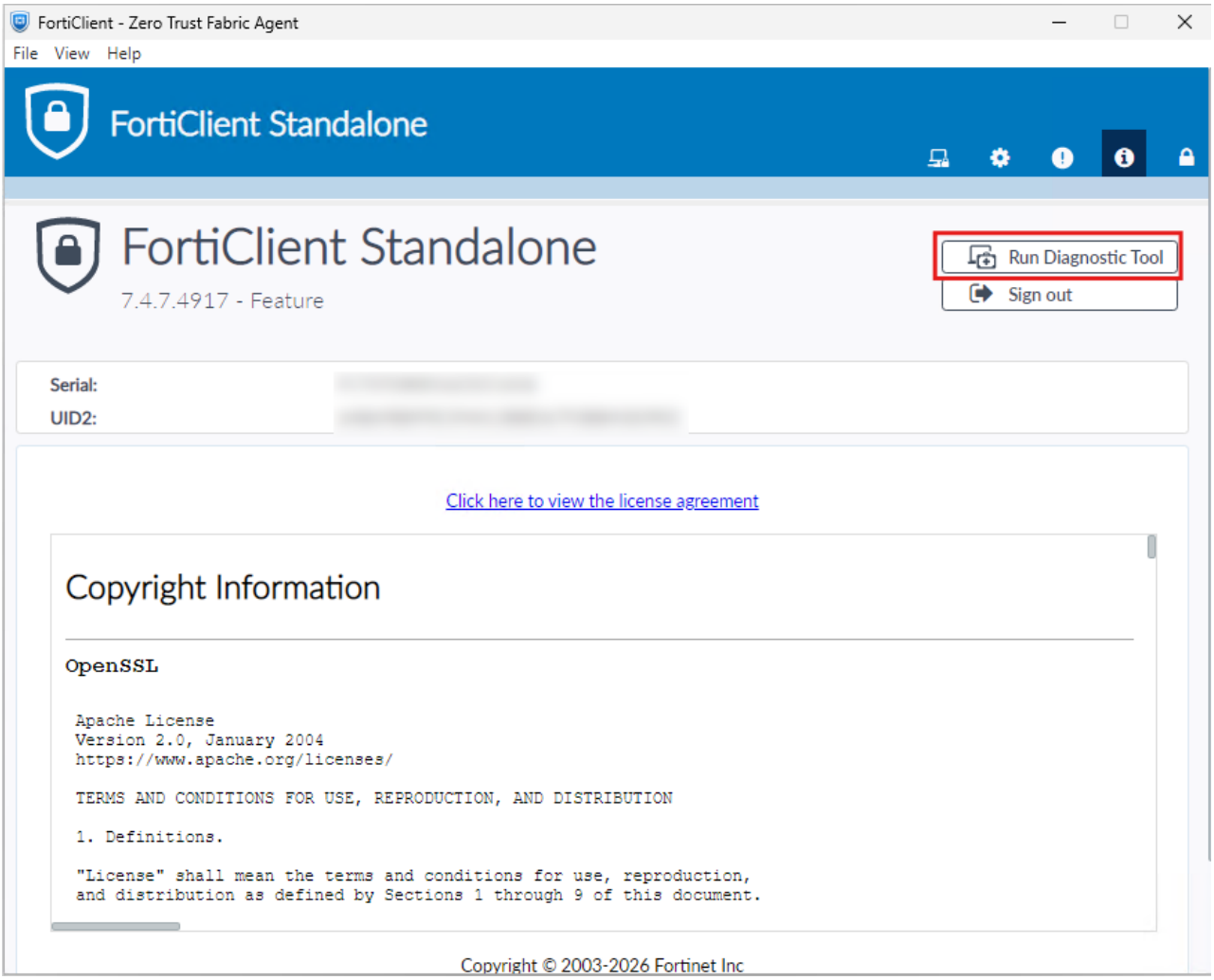
The FortiClient Standalone Diagnostic Tool does not record sensitive information. It contains information about the endpoint such as:

- Windows operating system version
- Windows software updates
- Names and versions of installed software
- Names and versions of installed drivers
- FortiClient Standalone configuration
- FortiClient Standalone system and application logs
- Licensing validation details
- Connectivity status with FortiCloud

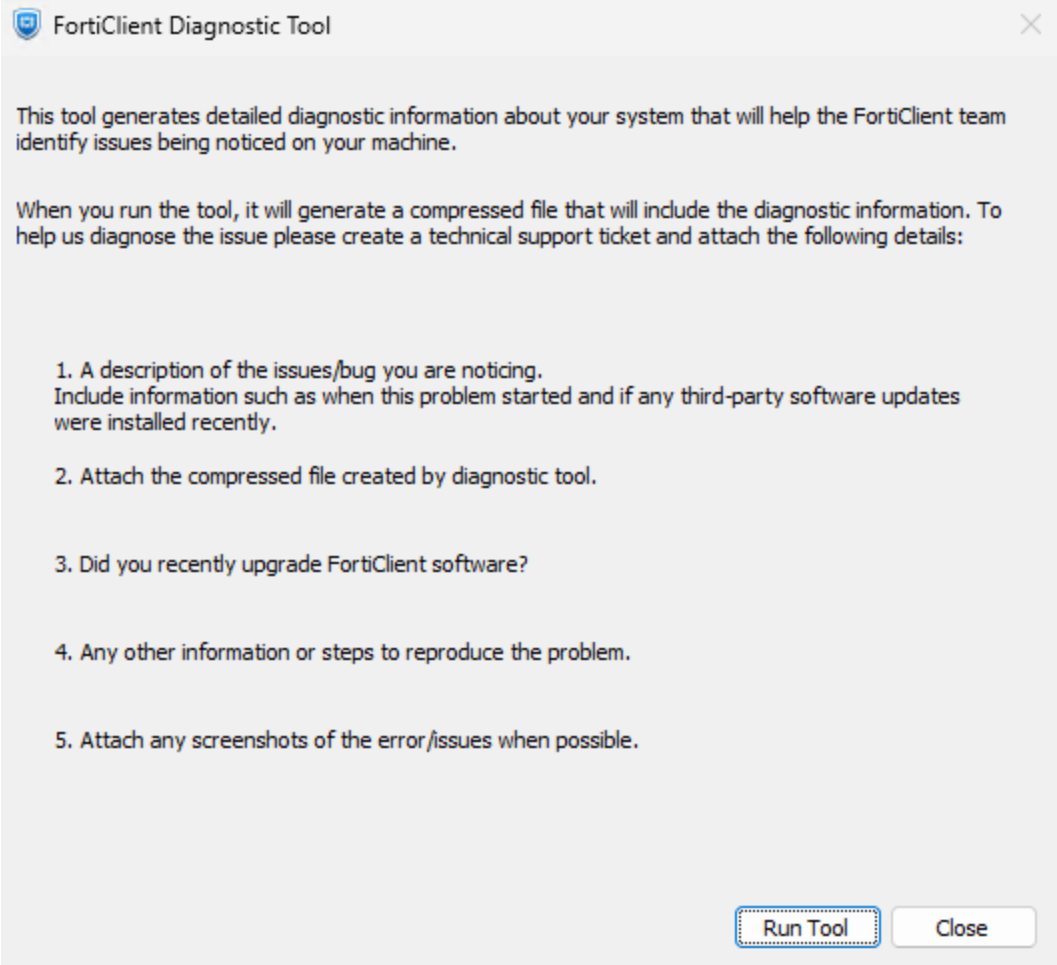
Before sending the package that the FortiClient Standalone Diagnostic Tool created to the FortiClient Standalone team, you can open and read the package.

To access the FortiClient Standalone Diagnostic Tool:

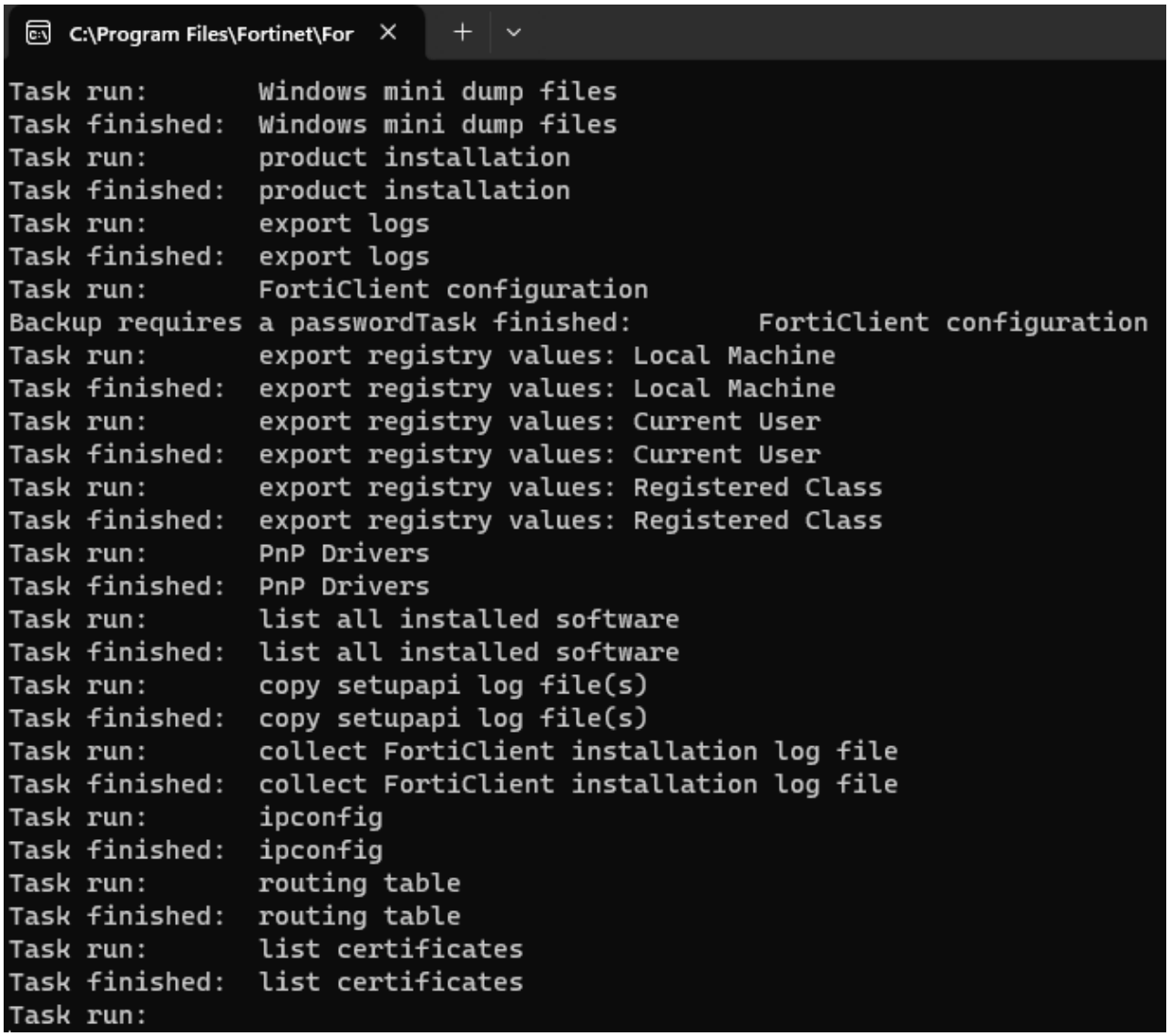
1. Go to the *About* tab.



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


FortiClient Diagnostic Tool
This tool generates detailed diagnostic information about your system that will help the FortiClient team identify issues being noticed on your machine.
When you run the tool, it will generate a compressed file that will include the diagnostic information. To help us diagnose the issue please create a technical support ticket and attach the following details:
1. A description of the issues/bug you are noticing.
Include information such as when this problem started and if any third-party software updates were installed recently.
2. Attach the compressed file created by diagnostic tool.
3. Did you recently upgrade FortiClient software?
4. Any other information or steps to reproduce the problem.
5. Attach any screenshots of the error/issues when possible.
Run Tool
Close

3. Click *Run Tool*. A window displays the provided status information.



4. (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 <user name>\AppData\Local\Temp\Diagnostic_Result*.
5. Click *Close*.

Appendix A - Processes

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

- FortiClient Standalone (Windows) processes on page 43
- FortiClient Standalone (macOS) processes on page 44

FortiClient Standalone (Windows) processes

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

Name	Description	Purpose
FortiClient.exe	FortiClient Standalone Console	FortiClient Standalone GUI
FCConfig2.exe	FortiClient Standalone Configuration Daemon	Configuration update
FCDBLog.exe	FortiClient Standalone Logging Daemon	Logging
FortiESNAC.exe	FortiClient Standalone Network Access Control	FortiClient Standalone Telemetry
FortiSettings.exe	FortiClient Standalone Settings Service	Used by FortiClient Standalone settings
FortiTray.exe	FortiClient Standalone System Tray Controller	FortiTray
FortiVPN.exe	FortiClient Standalone VPN Controller	Schedules, controls, and monitors VPN connections
fortivrs.exe	FortiClient Standalone Video Record Daemon	provides PAM functionality
scheduler.exe	FortiClient Standalone scheduler	Windows ensures FortiClient Standalone services are running when needed
FcVpnSched.exe	FortiClient Standalone VPN scheduler	Windows ensures FortiClient Standalone VPN services are running when needed
FSSOMA.exe	Single sign on mobility agent	User authentication

FortiClient Standalone (macOS) processes

FortiClient Standalone (macOS) uses the following processes:

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

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

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

Name	Purpose
fctservctl	FortiClient Standalone Service Controller
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 Standalone update tool
fctupgrade	FortiClient Standalone upgrade tool

FortiClient Standalone (macOS) also uses the `utun40` virtual interface (no traffic by default) to reduce overhead during service startup or reload and to prepare for future network-layer capabilities. This interface is active as long as FortiClient Standalone (macOS) is installed and running.

Appendix B - CLI commands

FortiClient Standalone (Windows) CLI commands

VPN

FortiClient Standalone supports the following CLI options with `FortiVPN.exe` for remote access to connect tunnels that are already configured via the FortiClient Standalone GUI. It does not support creating new tunnels.

```
C:\Program Files\Fortinet\FortiClient>fortivpn --cli

FortiClient VPN 7.4.7.XXXX

Usage:

Options:
FortiVPN.exe --cli --list
FortiVPN.exe --cli --listcertificates --tunnel <tunnelname>
FortiVPN.exe --cli --connect --tunnel <tunnelname> [--username <username>] [--password <password>]
                                                   [--computerstore-thumbprint|--userstore-
thumbprint|--smartcardstore-thumbprint <certificate thumbprint>]
                                                   [--savecredentials] [--keeprunning]
FortiVPN.exe --cli --status [--tunnel <tunnelname>]
FortiVPN.exe --cli --disconnect [--tunnel <tunnelname>]

================================================================================================
==============
FortiVPN.exe --cli --list
SSL:
 machine
 sslvpn test
IPSEC:
 ipsec test

================================================================================================
==============
FortiVPN.exe --cli --listcertificates --tunnel <tunnelname>

Lists the certificates than can be used by the specified tunnel <tunnelname>

fortivpn.exe --cli --listcertificates --tunnel test
User Store:
 thumbprint="16B7611982622CB83C14D706377A150E7D553A99" cn="employee" issuer="fortinet.com"
Computer Store:
 thumbprint="8940143F71AE2A3C9251F6C4322981EE16BACDB9" cn="device" issuer="fortinet.com"
```

```
================================================================================================
==============

FortiVPN.exe --cli --connect --tunnel <tunnelname> [--username <username>] [--password <password>]
                                                   [--computerstore-thumbprint|--userstore-
thumbprint|--smartcardstore-thumbprint <certificate thumbprint>]
                                                   [--savecredentials] [--keeprunning]

Connects the specified tunnel <tunnelname>
If the tunnel requires a certificate, the certificate can be specified by using ONE of:
  --computerstore-thumbprint
  --userstore-thumbprint
  --smartcardstore-thumbprint

e.g.
FortiVPN.exe --cli --connect --tunnel test --userstore-thumbprint
16B7611982622CB83C14D706377A150E7D553A99

Note:
username, password, computerstore-thumbprint, userstore-thumbprint, smartcardstore-thumbprint,
savecredentials and keeprunning are optional parameters
savecredentials and keeprunning have no effect if those options are disabled in the tunnel
configuration.

================================================================================================
==============

FortiVPN.exe --cli --status [--tunnel <tunnelname>]
Shows the status of the vpn.
tunnel is an optional parameter. If specified, only that tunnel will be checked.

FortiVPN.exe --cli --status
machine :: Disconnected
sslvpn test :: Connecting
ipsec :: Disconnected

FortiVPN.exe --cli --status
machine :: Disconnected
sslvpn test :: Connected
ipsec :: Disconnected

FortiVPN.exe --cli --status --tunnel "ipsec test"
ipsec test :: Disconnected

================================================================================================
==============

FortiVPN.exe --cli --disconnect [--tunnel <tunnelname>]

Disconnects the VPN
tunnel is an optional parameter. If specified, only that tunnel will targeted for disconnection.
If the tunnel is not currently connected, no action will be taken.
```

```
If tunnel is not specified, then any currently connected tunnel will be disconnected.
```

Configuration backup and restoration

FortiClient Standalone (Windows) 7.4.7 supports backing up and restoring an XML configuration file using the following commands:

- `FCConfig.exe -f <path to xml config file to import> -o export -p <password to decrypt config file, if any>`
- `FCConfig.exe -f <path to xml config file to import> -o import -p <password to decrypt config file, if any>`

For example:

```
cd "C:\Program Files\Fortinet\FortiClient"
FCConfig.exe -f c:\temp\Standalone_FCT.conf -o import -p 11111111
```

FortiClient Standalone (macOS) CLI commands

FortiClient Standalone (macOS) 7.4.7 supports backing up and restoring an XML configuration file using the following commands:

- `sudo /Library/Application\ Support/Fortinet/FortiClient/bin/fcconfig -f {filepath} -o import`
- `sudo /Library/Application\ Support/Fortinet/FortiClient/bin/fcconfig -f {filepath} -o export -p {password to decrypt config file, if any}`

FortiClient Standalone (Linux) CLI commands

The following summarizes the CLI commands available for FortiClient Standalone (Linux) 7.4.7:

VPN

You can access VPN features through the vpn CLI command. This command allows you 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.

FortiClient Standalone (Linux) does not support IPsec VPN IKEv2 with SAML authentication for CLI-triggered VPN connection.

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
   ```

Configuration backup and restoration

You can back up and restore an XML configuration file using the following commands:

- `forticlient log backup <path to config file>`
- `forticlient log restore <path to config file> -p <password to decrypt config file, if any>`

www.fortinet.com