



# Secure Mobile Access 12.4

## Connect Tunnel User Guide

SONICWALL<sup>®</sup>

# Contents

<b>Introduction to Connect Tunnel</b>	<b>4</b>
About Connect Tunnel	4
Guide Conventions	4
Resources Available from Connect Tunnel	5
Downloading and Installing Connect Tunnel	5
 <b>Connect Tunnel Client for Windows</b>	 <b>11</b>
Launching VPN Connection	11
Launching VPN Connection using Network Logon	13
Launching VPN Connection using Always-ON VPN (AoV)	16
Always-On VPN	16
Enabling Always-On VPN (AoV) on Connect Tunnel	17
Launching a VPN connection	17
Launching VPN Connection using Device VPN	18
Device VPN	18
Enabling Device VPN on Connect Tunnel	18
Launching a VPN connection	18
Using Connect Tunnel	19
Viewing Connect Tunnel Status	19
Logging into Connect Tunnel	21
Choosing a Login Group	25
Processing Server Certificates	27
Disconnecting from Connect Tunnel	28
Customizing Connect Tunnel	29
Viewing Current Settings	29
Connecting to a Different VPN	29
Configuring Split Tunnel Mode	30
Configuring a Device VPN connection	31
Updating the Connect Tunnel Application	37
Provisioning of Connect Tunnel using SCCM or Intune	39
Creating a Default Profile	39
Configuration of Device VPN	40
Support for using default browser for SAML Authentication	41
Troubleshooting Connect Tunnel	42
Unable to Connect	42
Troubleshooting ESP	42
Unable to Access Resources or the Internet	44

Using Logs .....	45
Installation Fails .....	47
EPC Zone Classification doesn't work as intended .....	47
OpswatWrapper Init Error .....	48
<b>Connect Tunnel Client for macOS and Linux .....</b>	<b>49</b>
System Requirements for MacOS .....	49
System Requirements for Linux .....	49
Starting Connect Tunnel .....	50
Connect Tunnel on macOS .....	50
Connect Tunnel on Linux .....	52
Specifying a Login Group .....	52
Connecting to a Different VPN .....	53
Quitting Connect Tunnel .....	53
Managing Configurations .....	53
Viewing Connect Tunnel Settings .....	54
Deleting a Configuration .....	55
Creating a New Configuration .....	57
Selecting the Advanced Button .....	58
Advanced Options .....	60
Credential Caching/Secure Network Detection .....	61
Processing Server Certificates .....	62
Configuring Proxy Server Settings (Linux Only) .....	62
Troubleshooting .....	63
Unable to Connect VPN .....	64
Troubleshooting ESP .....	64
Unable to Access Resources or the Internet .....	64
Unable to Access Resources on Linux .....	65
<b>SonicWall Support .....</b>	<b>66</b>
About This Document .....	67

# Introduction to Connect Tunnel

## Topics:

- [About Connect Tunnel](#)
- [Guide Conventions](#)
- [Resources Available from Connect Tunnel](#)
- [Downloading and Installing Connect Tunnel](#)

## About Connect Tunnel

SonicWall Secure Mobile Access Connect Tunnel with Smart Tunneling is a client component of the Secure Mobile Access Virtual private network (VPN) solution, which enables secure, authorized access to Web based and client/server applications, and file shares. The Connect Tunnel client enables you to connect to network resources that are protected by the SonicWall SMA 1000 Series appliances. It is supported for use with Windows, macOS, and Linux.

The *Secure Mobile Access (SMA) Connect Tunnel User Guide* provides information for both the Administrator and the User.

❶ **NOTE:** The Legacy Connect Tunnel and Connect Tunnel Service (CTS) are deprecated from 12.4.1 onwards.

## Guide Conventions

Convention	Use
<b>Bold</b>	Highlights dialog, window, screen names, parameter names, icons, and buttons.
Code	Is used for file names and text or values you are being instructed to type into the interface.
<i>Italic</i>	Indicates the name of a technical manual. It also indicates emphasis on certain words in a sentence, and sometimes indicates the first instance of a significant term or concept.



# Resources Available from Connect Tunnel

Connect Tunnel allows you to securely access the following types of resources:

## RESOURCE TYPES

Resource type	Description
Client/server resources	Client/server applications, thin client applications, and terminal services, such as Microsoft Outlook, Citrix, and Windows Terminal Services.
Web sites and applications	Web content and Web-based applications that can be accessed through a browser, such as Microsoft Outlook Web Access, Domino Web Access, and general Web sites (such as intranets).
Windows network shares	Shared Windows folders and files through Windows Network Neighborhood, and mapped drives.

## Downloading and Installing Connect Tunnel

Connect Tunnel client is available to both administrators and end-users. The administrator can download it from Appliance Management Console (AMC), whereas an end-user can download it from WorkPlace and SonicWall website. The installation requires administrator privileges on the client machine.


### Topics:

- [Procedure to download and install Connect Tunnel from AMC](#)
- [Procedure to download and install Connect Tunnel from WorkPlace](#)
- [Procedure to download and install Connect Tunnel from SonicWall Website](#)

### ***Procedure to download and install Connect Tunnel from AMC:***

1. Log into the AMC on your SonicWall SMA 1000 Series appliance.
2. In the left pane, select **User Access > Agent Configuration > Access Agents > Client Installation**

**Packages.> The Client Installation Packages** page displays.

 / User Access / Agent Configuration / Client Installation Packages

Download the access agents to distribute to your end users. The installation package will be configured with the necessary information to connect to the appliance.

---

### CONNECT TUNNEL CLIENT

Click on one of the following links to download the Connect Tunnel client package for an operating system. See Help for information on the command line options to configure and extract the file.

Windows	<div>x64 (.exe) ▼</div>	<a href="#">Download</a>	Current version: 12.4.3.214
Mac	MacOS Big Sur (11.x) and later	<a href="#">Download</a>	Current version: 12.43.00214
Linux	<div>x64 ▼</div>	<a href="#">Download</a>	Current version: 12.43.00214

---

### SECURE ENDPOINT MANAGER

Click the following links to download the Secure Endpoint Manager client package for an operating system.

Windows	<div>x86 and x64 (.ex ▼</div>	<a href="#">Download</a>	Current version: 12.4.3.214
Mac	MacOS Big Sur (11.x) and later	<a href="#">Download</a>	Current version: 12.43.00214

1. **For Windows:** In the **Connect Tunnel Client** group, click the drop-down next to **Windows** option and select the installation package based on your operating system. Connect Tunnel for Windows is supported on platforms such as x86, x64, and ARM processor.

The available options are:

- x64 (.exe)
- x64 (.msi)
- x86 (.exe)
- x86 (.msi)
- ARM (.exe)
- ARM (.msi)

### CONNECT TUNNEL CLIENT

Click on one of the following links to download the Connect Tunnel client package for an operating system. See Help for information on the command line options to configure and extract the file.

Windows	<div>x64 (.exe) ▼<div>x64 (.exe) x64 (.msi) x86 (.exe) x86 (.msi) ARM (.exe) ARM (.msi)</div></div>	<a href="#">Download</a>	Current version: 12.4.3.214
Mac	MacOS Big Sur (11.x) and later	<a href="#">Download</a>	Current version: 12.4.3.214
Linux		<a href="#">Download</a>	Current version: 12.4.3.214

**NOTE:** Connect Tunnel and WorkPlace automatically detects and reports processor architecture (x84, x64, and ARM64) to the server. The server then tracks the architecture type in the user session state and installs or updates the platforms automatically.

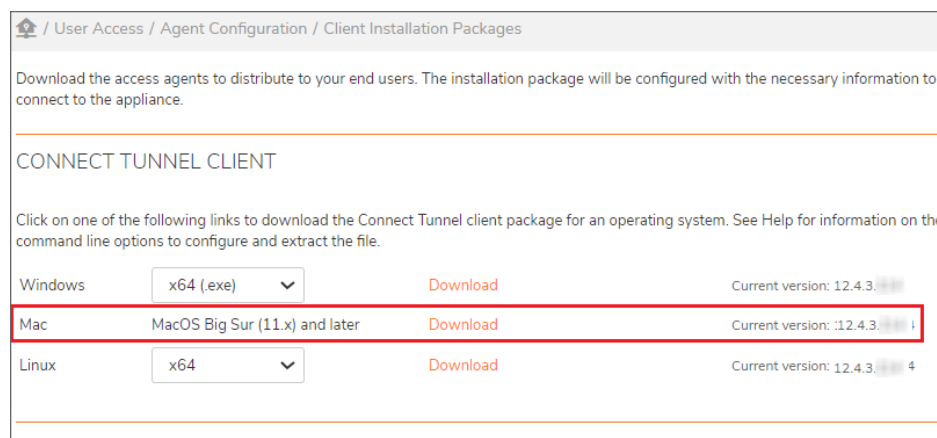
2. Click **Download**.

The install package is downloaded to your machine.

OR

**For Mac:** In the **Connect Tunnel Client** group, click **Download** next to **Mac** option.

① | **NOTE:** **Connect Tunnel Client** is built as universal application which can be run on both Intel and Apple Silicon Mac computers.

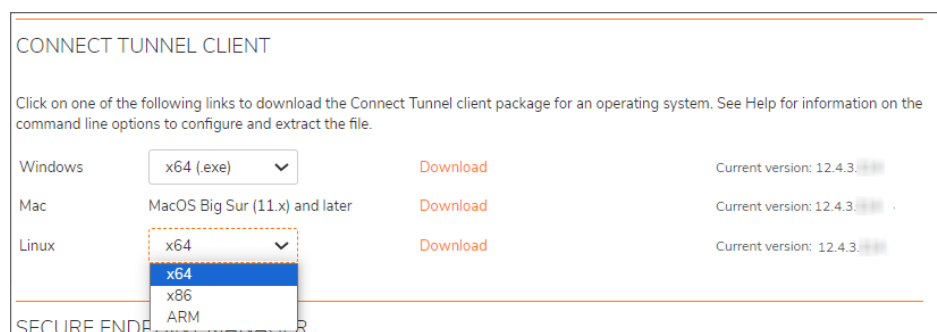


OR

**For Linux:** In the **Connect Tunnel Client** group, click the drop-down next to **Linux** option and select the installation package based on your operating system.

The available options are:

- x64
- x86
- ARM

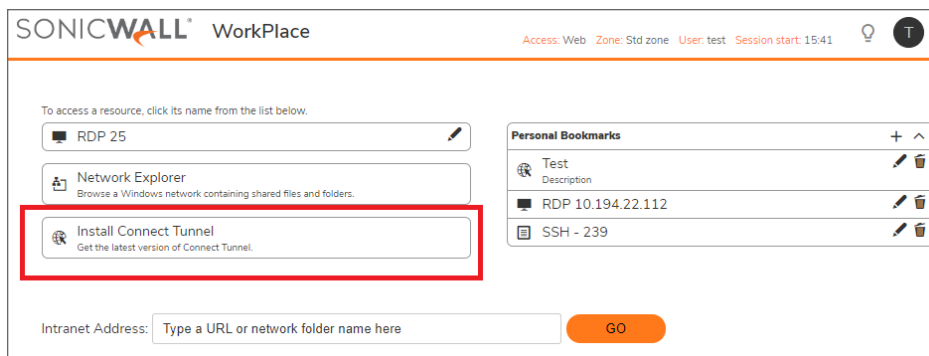


① | **NOTE:** For configuration details of macOS and Linux, see [Connect Tunnel Client for macOS and Linux](#)

3. Open the downloaded file and click **Agree** to agree to the terms, then click **Install**.

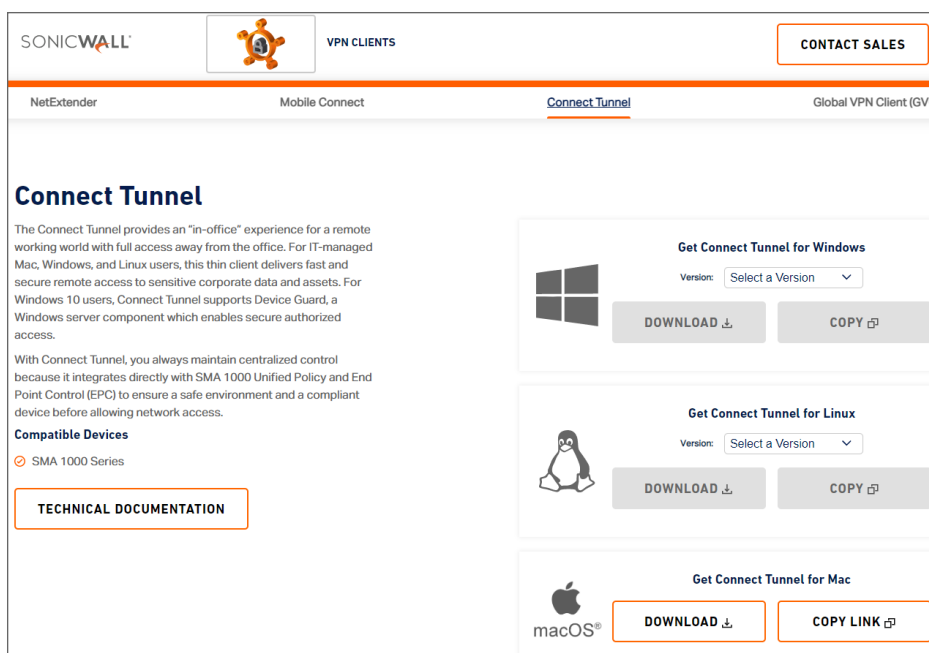
### Procedure to download and install Connect Tunnel from WorkPlace:

1. Log into your **WorkPlace**.
2. Click on the **Install Connect Tunnel** shortcut resource to download or to install.



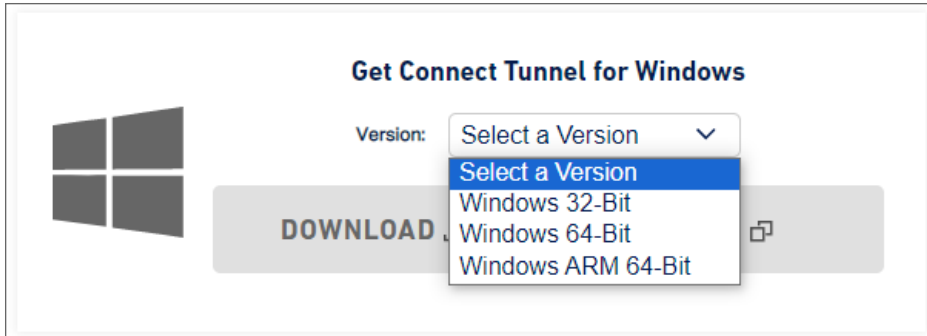
### Procedure to download and install Connect Tunnel from SonicWall Website:

1. Navigate to SonicWall.com > Products > All Products A-Z > Global VPN Client (or) Open [SonicWall Website](#).
2. Select the **Connect Tunnel** tab.



3. **For Windows:** In the **Get Connect Tunnel for Windows**, click the drop-down next to **Version** option and select a version based on your operating system.  
The available options for Windows are:

- Windows 32-Bit
- Windows 64-Bit
- Windows ARM 64-Bit

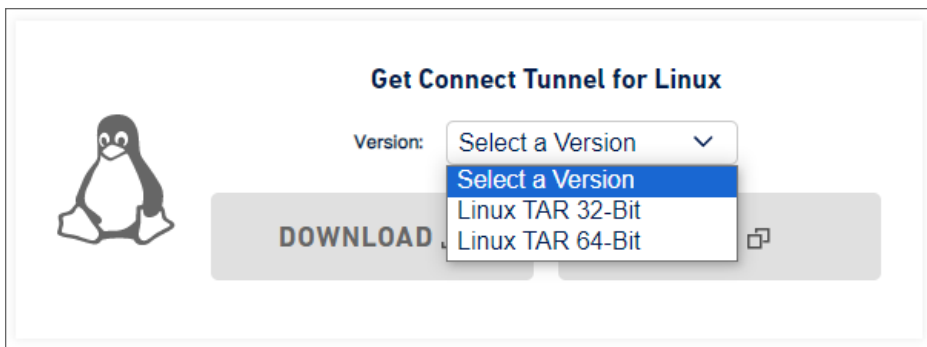


Click **Download** or Copy. The install package is downloaded to your machine

4. **For Linux:** In the **Get Connect Tunnel for Linux**, click the drop-down next to **Version** option and select a version based on your operating system.

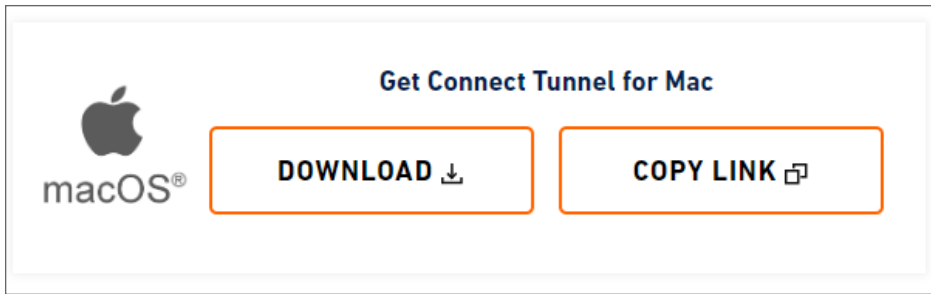
The available options for Linux are:

- Linux TAR 32-Bit
- Linux TAR 64-Bit
- Linux TAR ARM 64-Bit



Click **Download** or Copy. The install package is downloaded to your machine

5. **For Mac:** In the **Get Connect Tunnel for Mac**, click **Download** or **Copy Link** to install package is downloaded to your machine



6. Click **Download** or Copy The install package is downloaded to your machine
7. Open the downloaded file and click **Agree** to agree to the terms, then click **Install**.

# Connect Tunnel Client for Windows

## Topics:

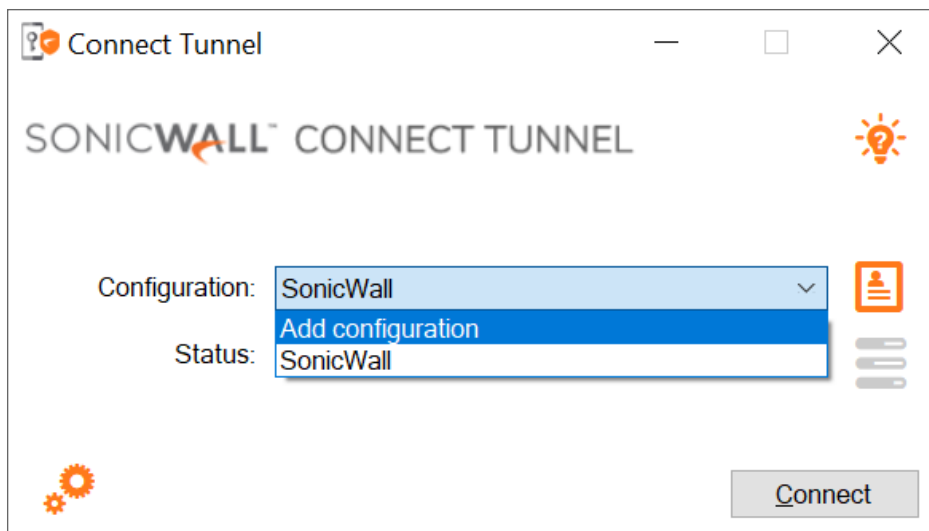
- [Launching VPN Connection](#)
- [Launching VPN Connection using Network Logon](#)
- [Launching VPN Connection using Always-ON VPN \(AoV\)](#)
- [Launching VPN Connection using Device VPN](#)
- [Using Connect Tunnel](#)
- [Customizing Connect Tunnel](#)
- [Provisioning of Connect Tunnel using SCCM or Intune](#)
- [Troubleshooting Connect Tunnel](#)

## Launching VPN Connection

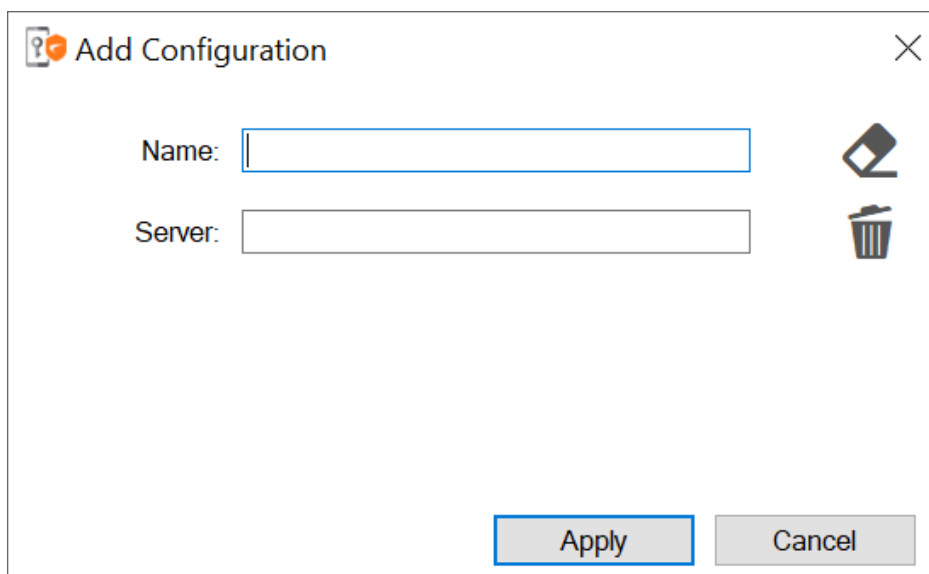
This section provides information on adding a connection profile and connecting to VPN.

### *To launch a VPN connection:*

1. After installation, open the **Connect Tunnel** application using desktop shortcut or from Start menu.
2. The initial login screen appears, click on the drop-down list, then click on **Add configuration**.

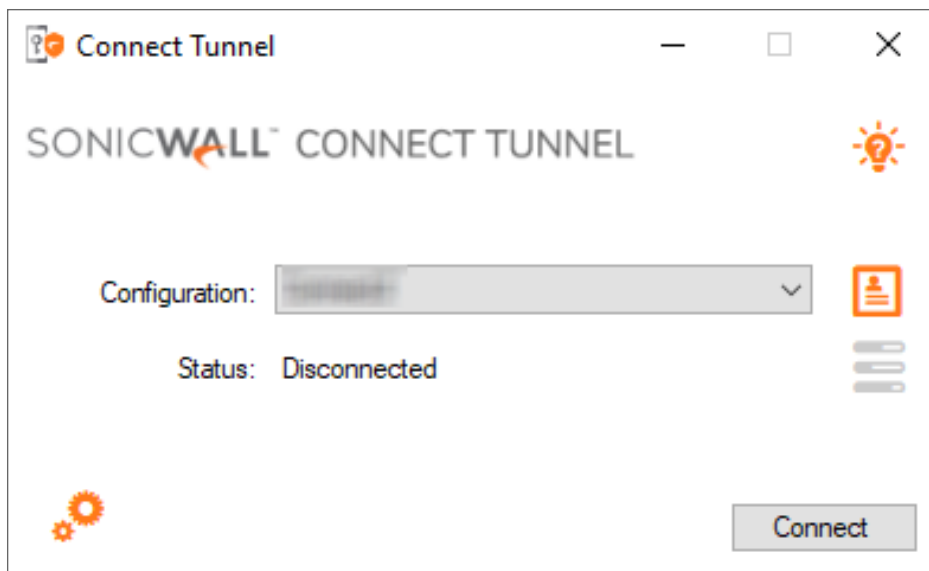


3. Enter a name in the **Name** field. In the **Server** field, enter the IP address of the VPN.  
 ⓘ | **NOTE:** **Server** field can be either a URL or an IP address.



4. Click **Apply** to complete the process.
5. Select the confirmed configuration from the drop-down configuration list and click **Connect**.





It may take a few seconds and several screen changes for initialization and for the VPN to connect.

## Launching VPN Connection using Network Logon

Users always log in to their Windows accounts before connecting a VPN tunnel. But in a typical scenario, a VPN tunnel is required to allow the user to log in for the first time or after a password reset. Network Logon is a feature that allows users to establish a VPN tunnel before they can log on to their Windows accounts. Network Logon is built using the Windows credential provider framework and is enabled by your administrator. Network Logon requires an EPC configuration to evaluate the device without a user context.

This section provides information on connecting to the VPN tunnel using Network logon before log on to Windows accounts.

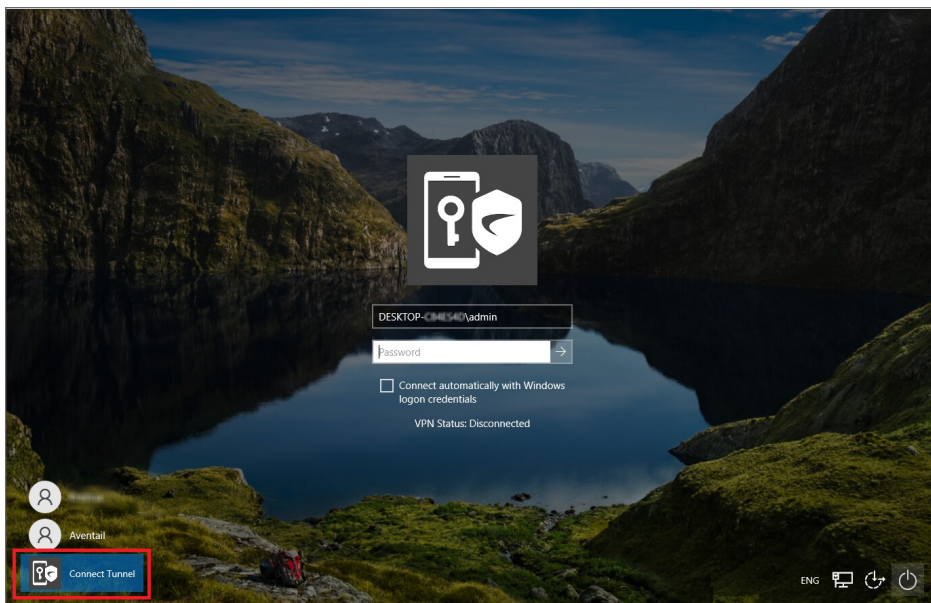
### Perquisites:

- Connect Tunnel must be installed and enabled for Network Logon.
- ① **NOTE:** Network Logon is disabled by default and can be enabled by passing "NetworkLogon=1, 2 or 3" parameter to Connect Tunnel setup.

### *To launch a VPN connection using Network Logon:*

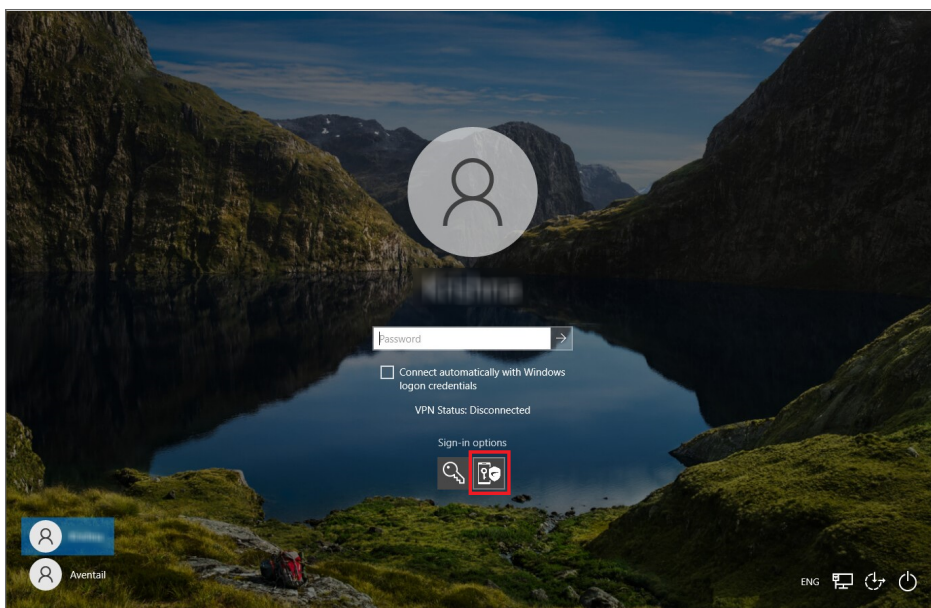
Based on your administrator configuration, the Connect Tunnel icon is displayed either on the bottom left corner or accessible via Sign-in options.

1. Select the **Connect Tunnel** icon on the bottom left corner.



(or)

Select the **Connect Tunnel** icon from the **Sign-in options**.

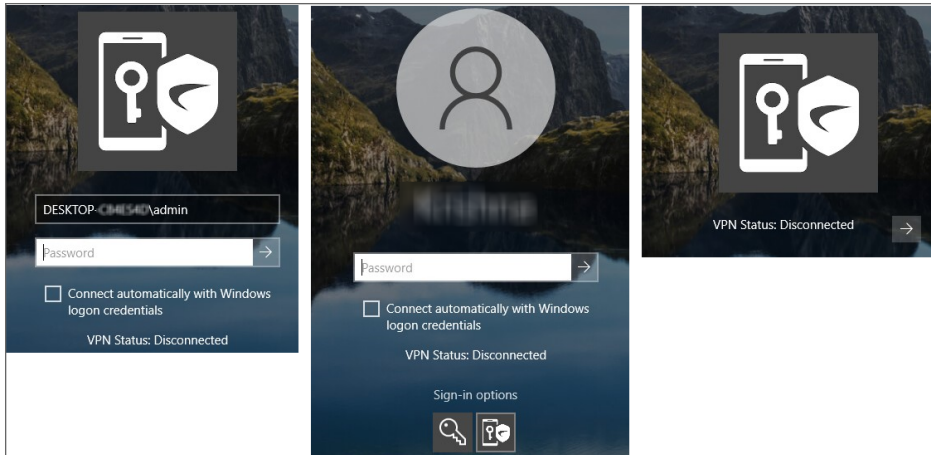


① **NOTE:** Windows logon screen displays fields and status. VPN connection status displays either **Device VPN Connected** or **Connected** or **Disconnected**.

2. Provide the credentials for Windows logon if required.

Select the **Connect automatically with Windows logon credentials** checkbox to connect the VPN with Windows logon credentials and submit.

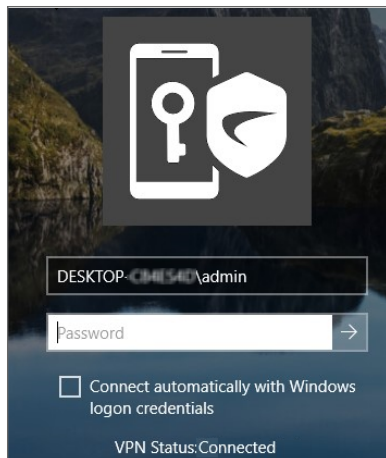
- ① | **NOTE:** Windows logon and VPN credentials must be same. If the credentials are not same, VPN authentication fails and a warning message appears to enter the correct credentials.



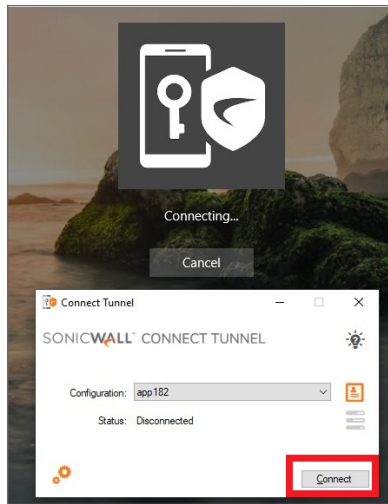
3. Submit your login credentials.

① | **NOTE:**

- If Device VPN or User VPN is already connected, connection status displays either **Device VPN Connected** or **Connected**, then Windows logon proceeds immediately.



- If VPN is not connected, **Connect Tunnel** initial login screen appears. If you do not have configuration, then create a configuration and click **Connect** to start the login process. For more information, see [Launching VPN Connection](#).



- VPN and Windows login have a timeout of 120 seconds. The VPN connection gets aborted if the VPN connection does not succeed within 120 seconds.
4. During VPN login process, provide the credentials as requested to establish the VPN connection.
    - ① | **NOTE:**
      - PKI authentication requires a client certificate in the machine store.
      - SAML authentication is not supported.
  5. After VPN is connected, then Windows login proceeds.
    - ① | **NOTE:** If your administrator has configured the credential provider to launch VPN only, then after establishing the VPN connection, choose your preferred account to login to the Windows session.

## Launching VPN Connection using Always-ON VPN (AoV)

This section provides information on connecting to the VPN tunnel using Always-On VPN (AoV).

### Topics:

- [Always-On VPN](#)
- [Enabling Always-On VPN \(AoV\) on Connect Tunnel](#)
- [Launching a VPN connection](#)

## Always-On VPN

AoV enforces that a VPN connection is always active during the Windows user session whenever the device has a network connection to the Internet.

# Enabling Always-On VPN (AoV) on Connect Tunnel

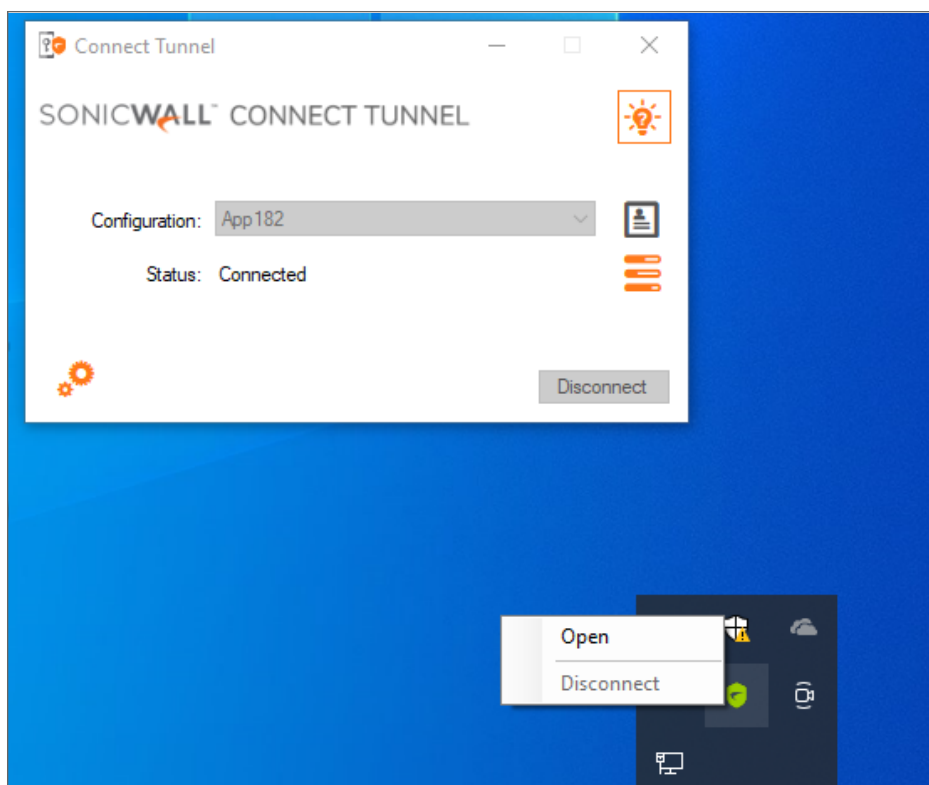
AoV is enabled by administrator in the SMA appliance. On subsequent connection of Connect Tunnel to the SMA appliance, this AoV policy is pushed to the client and gets enabled in the Connect Tunnel.

## Launching a VPN connection

After the user logs on to Windows user session, a VPN connection is automatically established between the user's device and the appliance. Also, VPN connection is triggered to reconnect automatically after a network change or system hibernation.

Based on the administrator configuration in the SMA appliance, the AoV feature may differ in the Connect Tunnel as below:

1. The profile is locked from modification and the disconnect option is disabled by default unless the administrator allows user to disconnect the Connect Tunnel in the AoV configuration.



2. Network access is allowed by default when VPN is not connected unless the admin restricts the network access in the AoV configuration.

For more information about the AoV configuration, refer to the section *Configuring Always-On VPN (AoV)* in the *SMA 1000 Administration Guide*.

# Launching VPN Connection using Device VPN

This section provides information on connecting to the VPN tunnel using Device VPN.

## Topics:

- [Device VPN](#)
- [Enabling Device VPN on Connect Tunnel](#)
- [Launching a VPN connection](#)

## Device VPN

Device VPN provides VPN access to a device on boot. VPN access is expected to be always available and limited to critical common resources that provide basic network access, logon, remote management, and remediation services (for devices lacking capability). For example, DNS, PDC, Windows Update and other critical services. The Device VPN session is non-interactive and establishes a VPN connection in background.

## Enabling Device VPN on Connect Tunnel

Device VPN is enabled by administrator in the SMA appliance. On subsequent connection of Connect Tunnel to the SMA appliance, this Device VPN policy is pushed to the client and gets enabled in the Connect Tunnel.

## Launching a VPN connection

A Device VPN is automatically established between the user's device and the appliance on system boot. After the user logs on to Windows user session, a User VPN is established based on the user's credentials.

A user must disconnect from User VPN to login to another user realm or to disable Device VPN altogether.

Based on the administrator configuration in the SMA appliance, the Device VPN and User VPN feature may differ in the Connect Tunnel as below:

1. The disconnect option is enabled by default to allow user to disconnect from User VPN, unless the administrator disables the disconnect option in the Device VPN configuration.
2. Network access is allowed by default when VPN is not connected unless the admin restricts the network access in the Device VPN configuration.
3. An User VPN is automatically established on user logon irrespective of whether device is in secure network or not. An administrator can disable this in the Device VPN configuration so that a User VPN is only established when in non-secure network.

For more information about the Configuration a Device VPN connection on Connect Tunnel refer to the section [Configuring a Device VPN connection](#).

For more information about the Device VPN and Device VPN endpoint enrollment, refer to the sections Device VPN and Device VPN endpoint enrollment in the *SMA 1000 Administration Guide*.

# Using Connect Tunnel

## Topics:

- [Viewing Connect Tunnel Status](#)
- [Logging into Connect Tunnel](#)
- [Choosing a Login Group](#)
- [Processing Server Certificates](#)
- [Disconnecting from Connect Tunnel](#)

## Viewing Connect Tunnel Status

To find out if Connect Tunnel is already installed and connected to the VPN, the user can check if an icon appears on the desktop or the task bar, or if the program is on the program list. If the program does not appear, contact the administrator, who can then reconfigure it appropriately. Hovering over the icon displays the connection status.

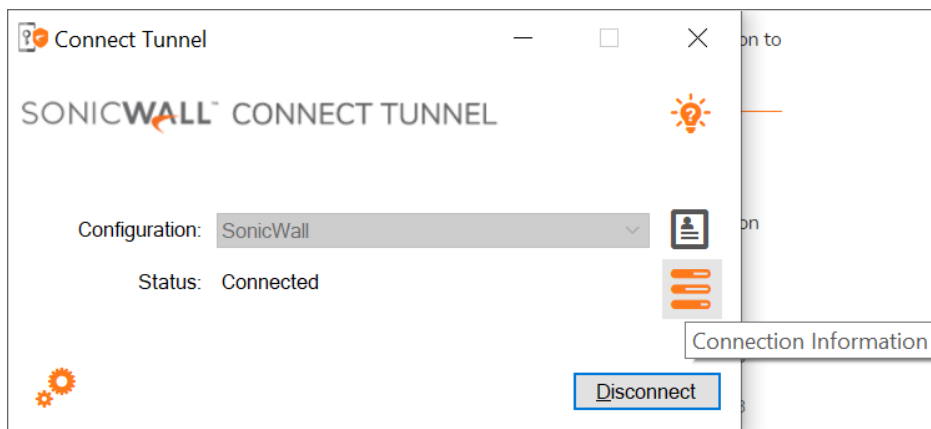


Connect Tunnel icon in the task bar notification area indicates the connection status:

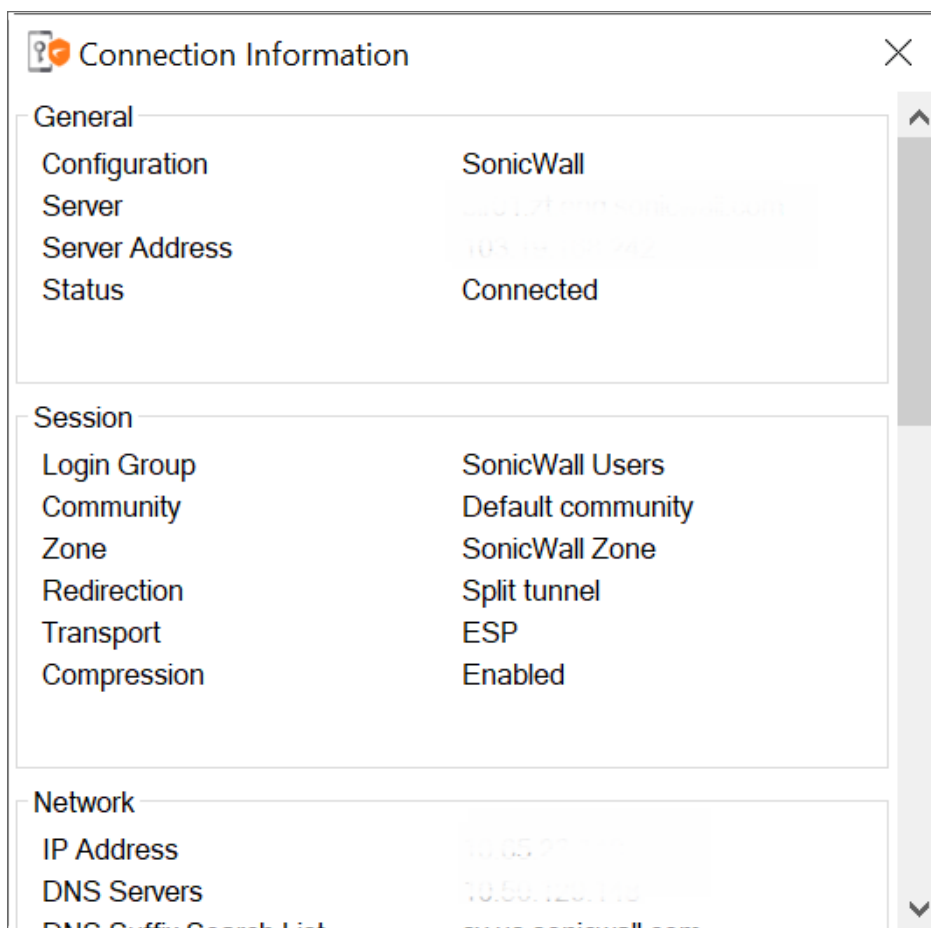
Icon Color	Description
Orange	VPN connection is not established or temporary network interruption
Green	VPN connection is established
Blue	VPN connection in secure network
Yellow icon	VPN connection is established as Device VPN

To view all the connection information, click on **Connection Information** on the **Main Window**.





The screen below shows the information given.





# Logging into Connect Tunnel

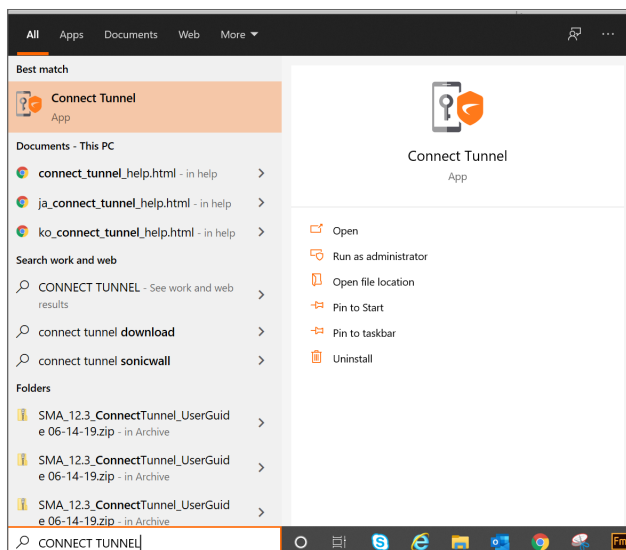
To access network resources through Connect Tunnel, users must first verify their identity. This ensures that only authorized users can access protected network resources. The credentials used to verify your identity typically consist of a user name and password (or pass code).

Depending on the resources, you may also need to enter a one-time password given to you by your administrator and/or accept an **Acceptable Use Policy**.

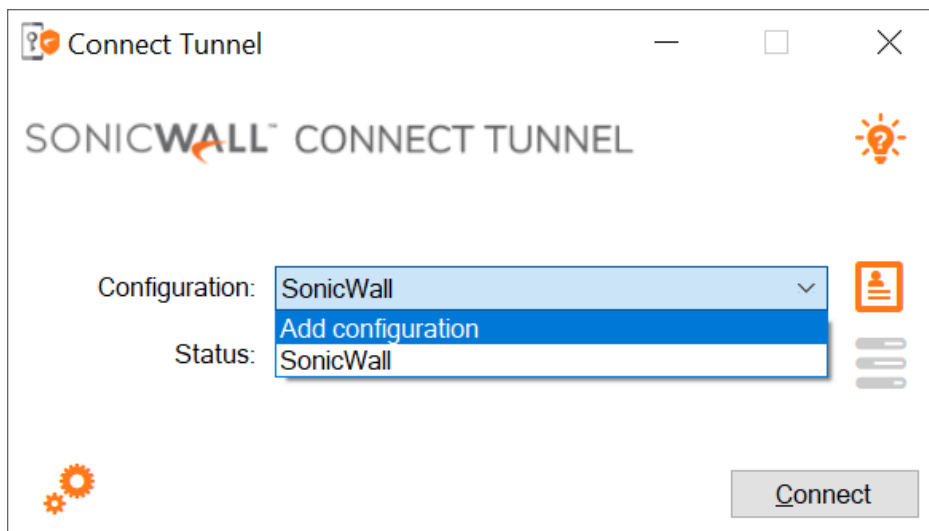
During Login, a prompt may appear indicating that an upgrade is ready. For instructions on upgrading, see [Updating the Connect Tunnel Application](#).

## **To log into Connect Tunnel:**

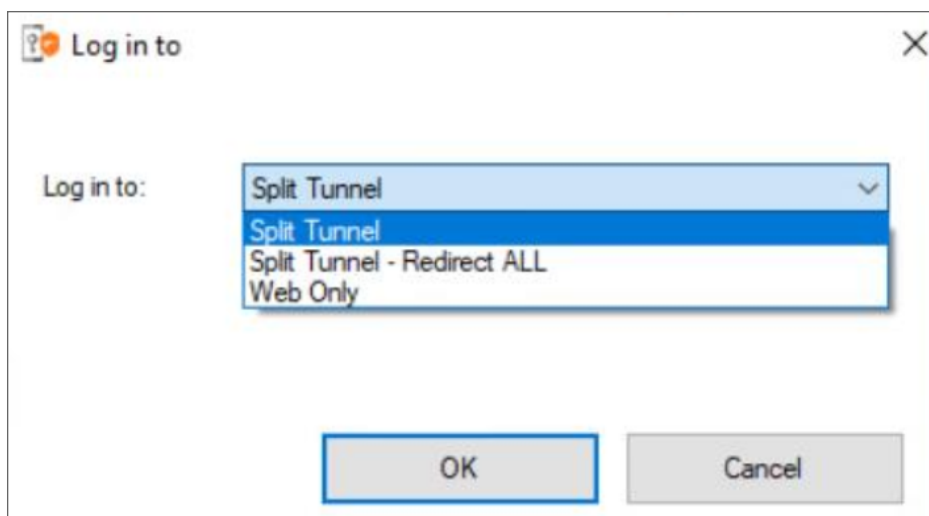
1. Click the Windows **Start** button.
2. Click **All Programs** > search for **Connect Tunnel**.



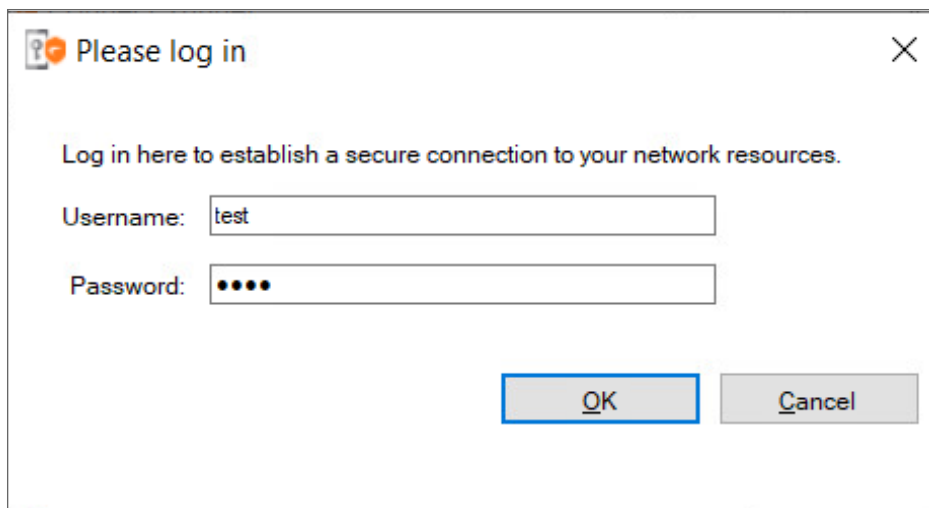
3. Click on **Connect Tunnel** application or **Open**.
4. The initial login screen appears. Enter your VPN configuration choice and click **Connect** to start the login process.



5. The next screen gives a drop down list to choose between login groups/realms to log into. Select a login groups/realm, then click **OK**.

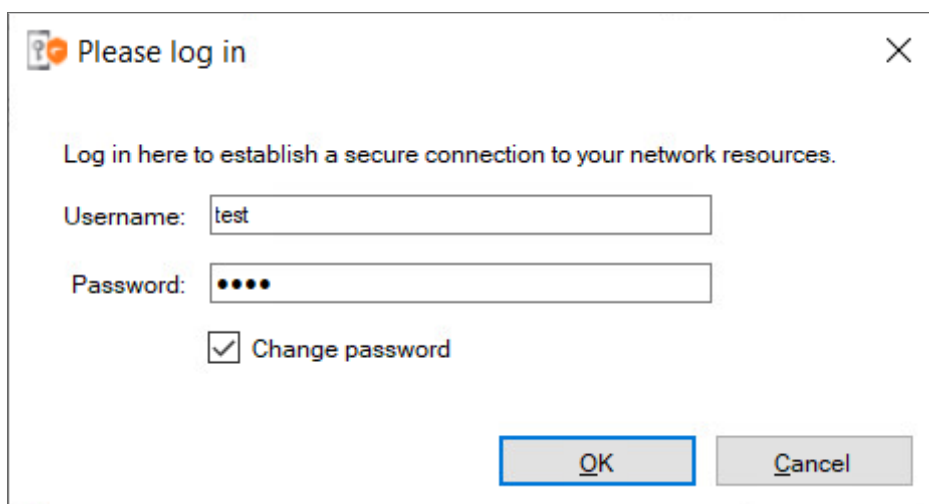


6. Enter your authentication credentials.  
Depending on how your administrator has configured Connect Tunnel, you may see a combination of these prompts.  
The screen below are examples:

A Windows-style dialog box titled "Please log in" with a close button (X) in the top right corner. The dialog contains the text "Log in here to establish a secure connection to your network resources." Below this text are two input fields: "Username:" with the text "test" entered, and "Password:" with four black dots representing a masked password. At the bottom right of the dialog are two buttons: "OK" (highlighted with a blue border) and "Cancel".

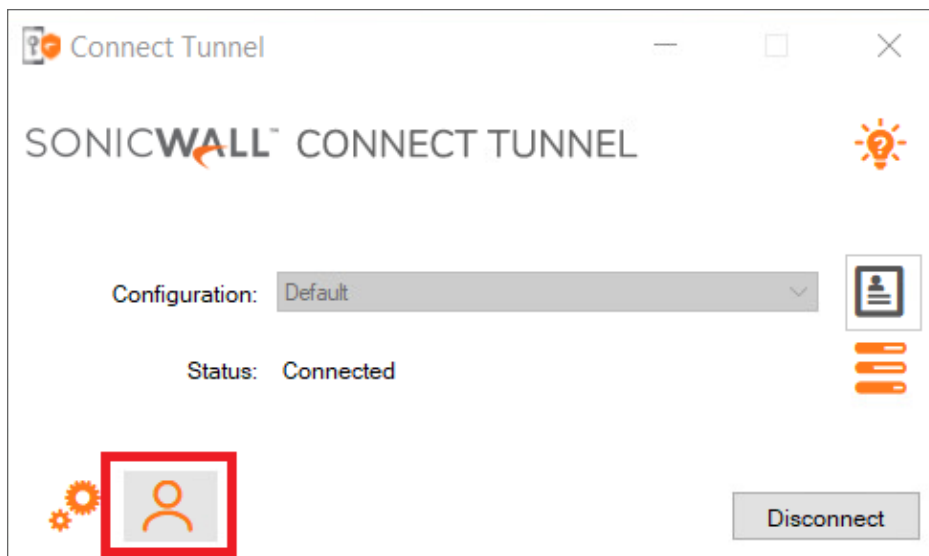
- Type your username in the **Username** field.
- In the **Password** or **Passcode** field, type your password or passcode. (Passwords may be case-sensitive. Make sure the Caps Lock or Num Lock keys are not enabled.)
- Enter a one-time password if one was sent to you by your administrator and click **OK**.

If your administrator has configured Connect Tunnel with the enabled change password option, you can view the **Change Password** checkbox.

A Windows-style dialog box titled "Please log in" with a close button (X) in the top right corner. The dialog contains the text "Log in here to establish a secure connection to your network resources." Below this text are two input fields: "Username:" with the text "test" entered, and "Password:" with four black dots representing a masked password. Below the password field is a checkbox labeled "Change password" which is checked. At the bottom right of the dialog are two buttons: "OK" (highlighted with a blue border) and "Cancel".

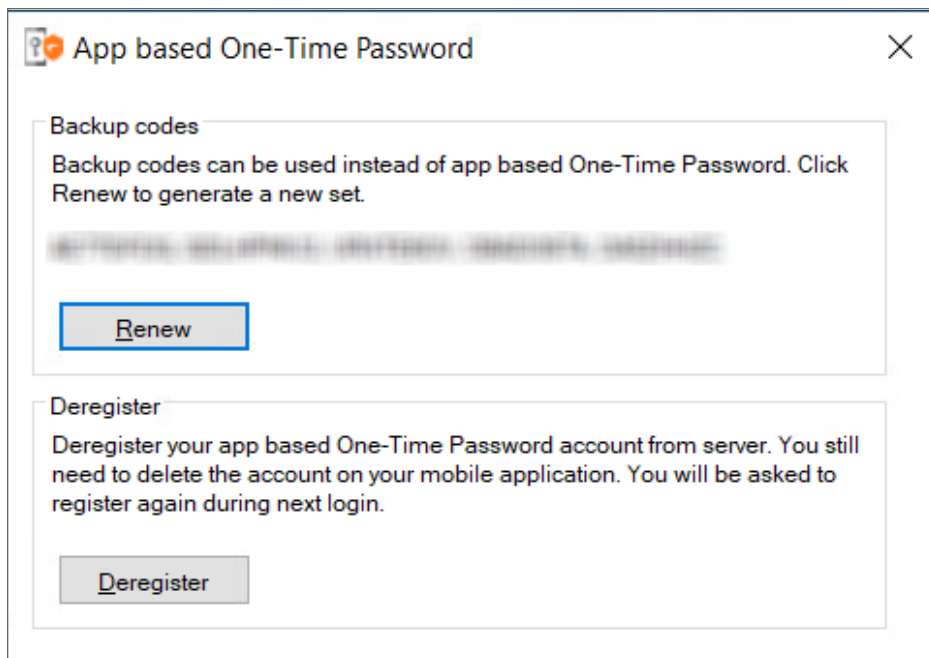
- Select the **Change Password** check box to reset the password and click **OK**.

If your administrator has configured Connect Tunnel with the enabled settings for Time-based One-time Passwords (TOTP), you can view the app-based one-time password icon as below.



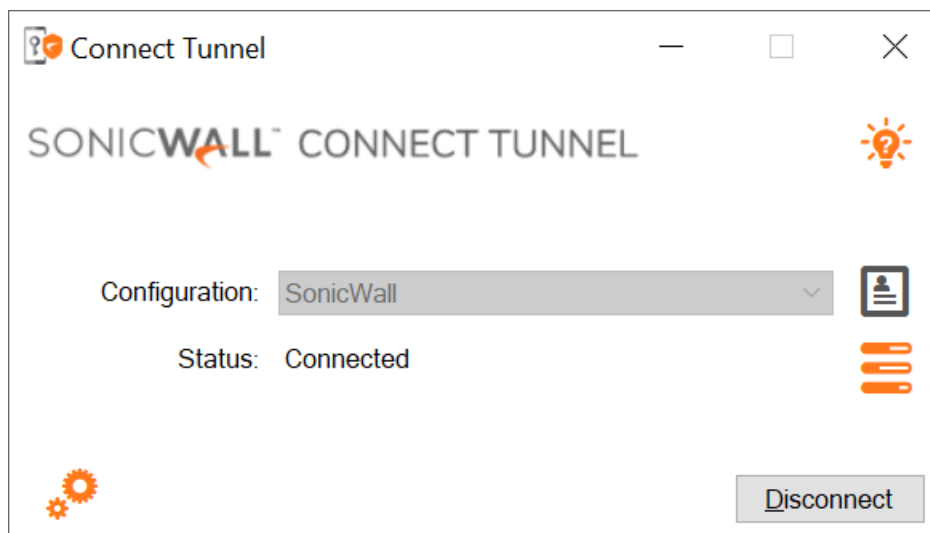
If your administrator has configured settings for Time-based One-time Passwords (TOTP) by enabling allowing user to deregister account and to use back-up codes options in the AMC, you can view both Renew backup codes and Deregister buttons.

① **NOTE:** Based on the enabled option, you can view the particular section and button in the Connet Tunnel.



- Click **Renew** button to generate a new set of back-up codes.
- Click **Deregister** button to remove your app-based one-time password (TOTP) account from server. You will be asked to register again during next login.

- If a client certificate is required for authentication, the **Certificate** list displays the ones on your device that match the certificate authority (CA) used by the authentication server. Often there is only one listed.
  - If an Acceptable Use Policy is displayed, click **Accept** to accept it.
7. If your login is successful, the following screen appears to show that you are connected to the VPN.



**NOTE:** The Status “Device VPN connected” is displayed when you have selected the Device VPN enabled realm.

The Connect Tunnel icon appears in the task bar notification area, indicating that Connect Tunnel is running and connected to the VPN.

Your login may not be exactly the same as that shown above. Your administrator might send you login instructions that allow you to connect to a specific network.

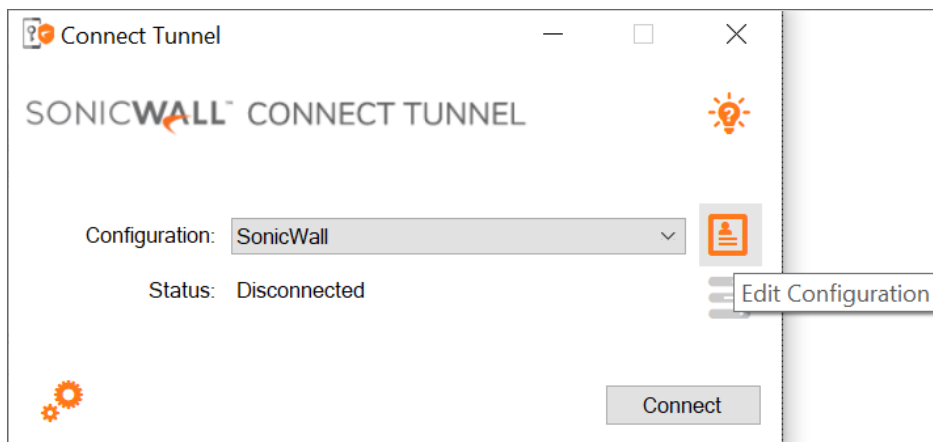
## Choosing a Login Group

Connect Tunnel allows you to choose the group or location you want to log into. This might be different at different times. (For example, you might sometimes login to the Sales group and at other times the Marketing group.) You may need to provide different authentication credentials for each login group.

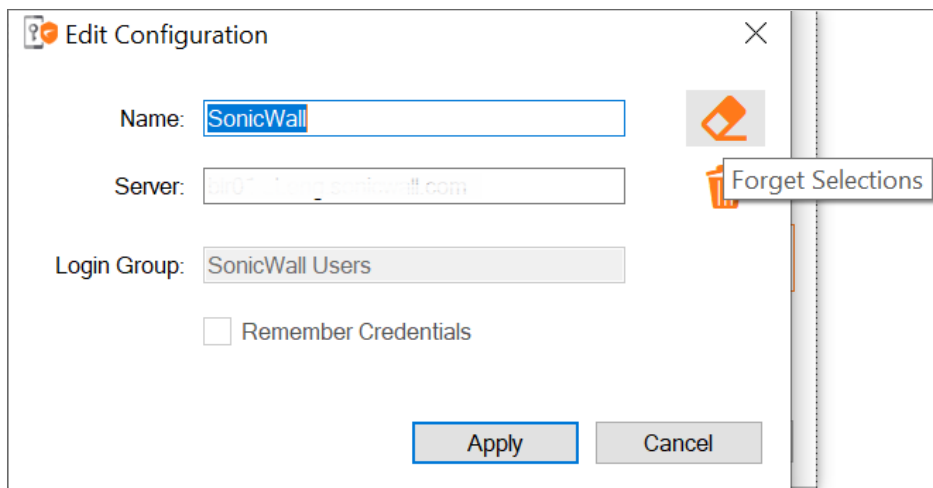
You must specify a login group each time you initiate a connection to your VPN. This option is available only when Connect Tunnel is off-line (that is, when it is not connected to your VPN). You do not need administrator privileges to change a host name or login group.

### *To specify the login group:*

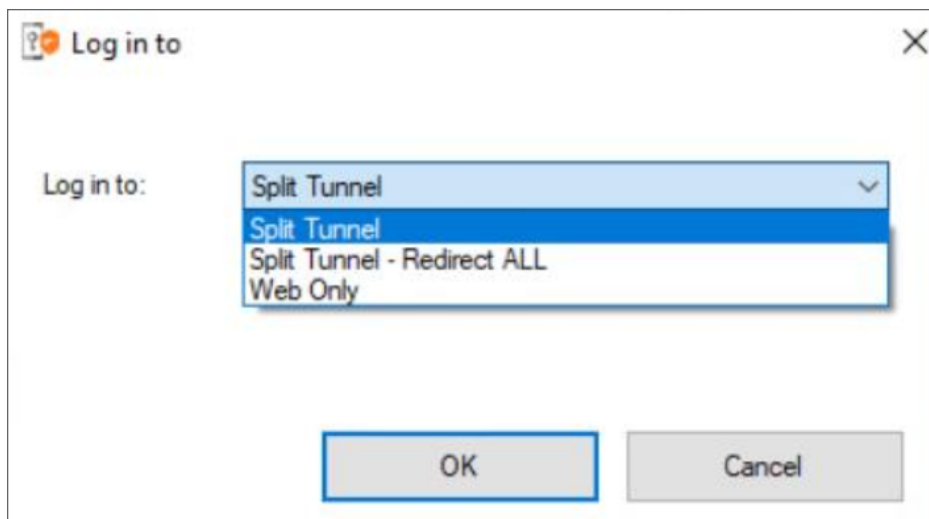
1. Launch **Connect Tunnel**.
2. Click on the **Edit Configuration** icon next to the **Configuration** drop-down list.



3. Click on the **Forget Selections** icon next to the **Name** field, then click **Apply**.



4. Click **Apply**.
5. Select or type the name of the login group you want to log into.



Depending on how your administrator has configured Connect Tunnel, some login groups may not appear in the list. However, you can still log into a “hidden” login group, if you are authorized to do so, by typing its name.

6. Click **OK**.

## Processing Server Certificates

Some VPN configurations require that you accept a server certificate before you can gain access to a protected network resource. A server certificate is a digital signature that verifies a server’s identity.

If you access a network resource that uses a server certificate, Connect Tunnel may display the certificate. Connect Tunnel displays a certificate warning only if the VPN appliance certificate is not from a trusted source. You must then verify that the server certificate is from a trusted source before accepting it. Otherwise, the login process continues without any prompt.

- ① **NOTE:** During the login process, Connect Tunnel processes or warns only for certificates from the VPN, not from resources. Applications, such as supported browsers are used to access resources, should handle any certificates that are associated with resources.

Because anyone can issue a certificate, you should accept certificates only from trusted sources, as the information you receive from others may be invalid. You do not need Administrator privileges to process server certificates. If you have any concerns about whether to accept a certificate or not, check with your administrator.

### ***To process a server certificate:***

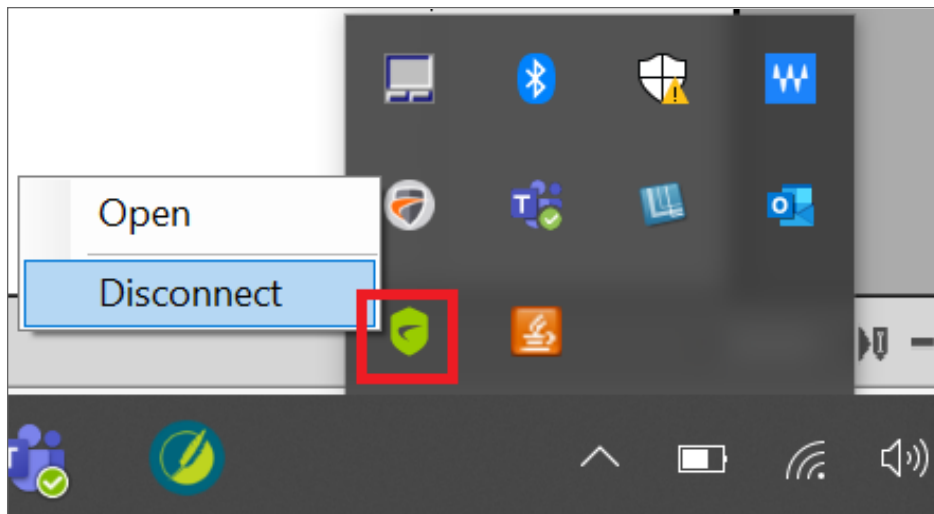
1. When a trusted certificate appears, verify that the certificate is associated with the correct server.
2. Accept or reject the certificate:
  - If you click **Reject**, your connection is not established.
  - If you click **Accept**, the certificate is accepted as valid, and the login process continues.
3. Accept a license agreement or Acceptable Use Policy, if required.

# Disconnecting from Connect Tunnel

Leaving Connect Tunnel ends your VPN session and disconnects you from the remote network.

## ***To disconnect from Connect Tunnel:***

1. In the task bar notification area, right-click the **Connect Tunnel** icon.
2. Click **Disconnect**.





# Customizing Connect Tunnel

This section describes how to view and customize the Connect Tunnel client settings. Connect Tunnel must be off-line to change program settings.

## Topics:

- [Viewing Current Settings](#)
- [Connecting to a Different VPN](#)
- [Configuring Split Tunnel Mode](#)
- [Configuring a Device VPN connection](#)
- [Updating the Connect Tunnel Application](#)

## Viewing Current Settings

Connect Tunnel must be off-line to view current settings.

### *To view current Connect Tunnel settings:*

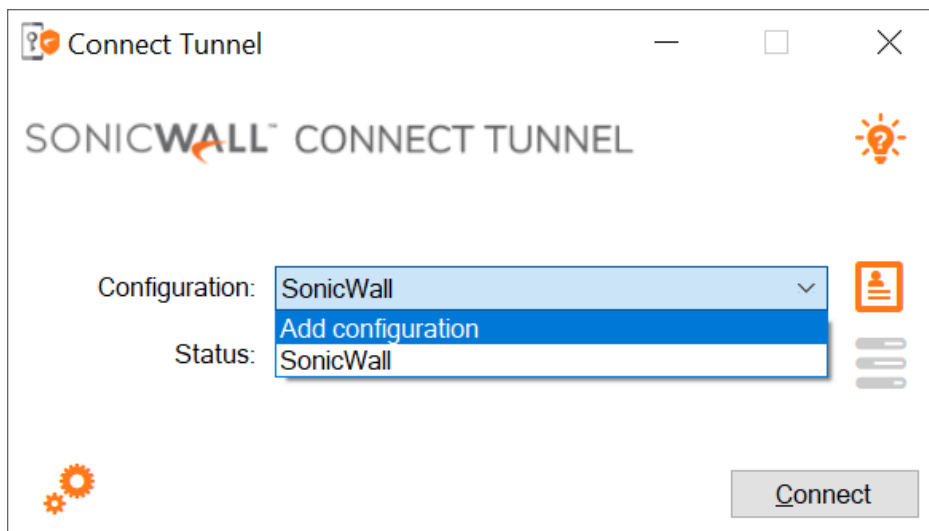
1. On the Connect Tunnel login dialog box, select the configuration from the drop-down **Configuration** list.
2. Click **Edit Profile** next to the list to view previously made configuration settings for the chosen **Configuration**.

## Connecting to a Different VPN

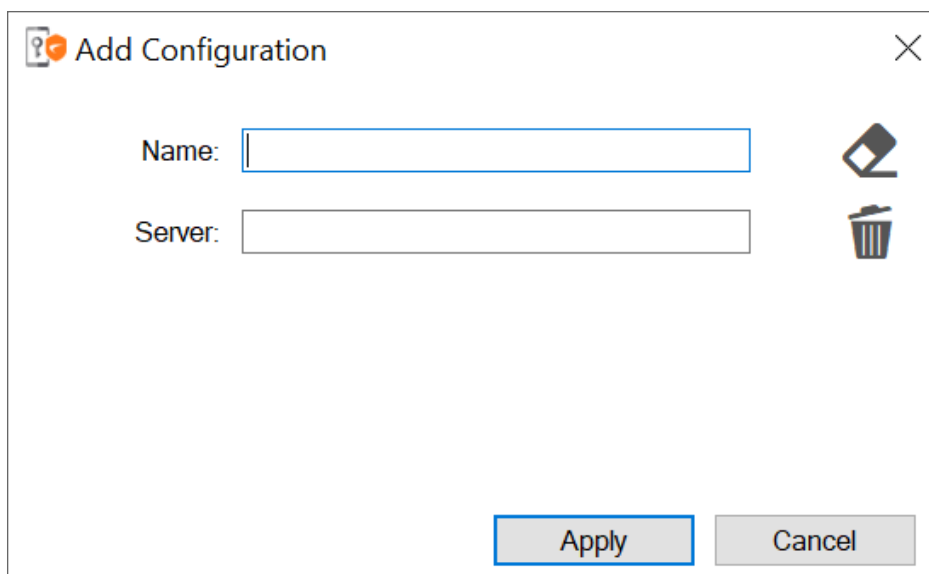
Connect Tunnel must be off-line to change the connection to a different VPN.

### *To specify the host name or IP address of a different VPN:*

1. In the Connect Tunnel login dialog box, click the drop-down list to choose a different VPN.
2. On the screen below, click **Add configuration**.

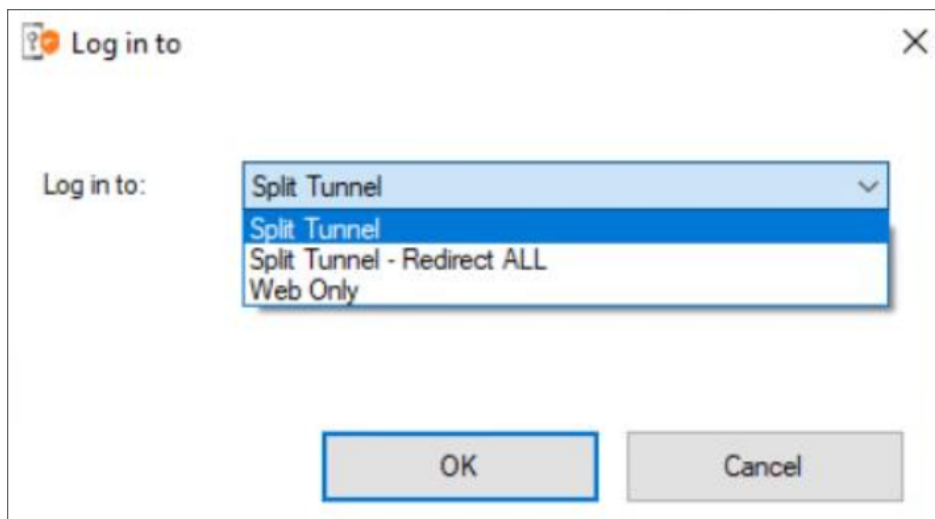


3. Enter a name in the **Name** field. In the **Server** field, enter the IP address of the VPN you want to connect to. Click **Apply** to complete the process.



## Configuring Split Tunnel Mode

When requests for resources or Internet access are received from clients by the appliance, they can be handled a few different ways. The administrator makes this configuration choice in the Appliance Management Console (AMC).



- In **split tunnel** mode, only traffic destined for resources that have been specified in AMC is redirected to the appliance. All other traffic is routed as normal. In other words, the administrator sets up a list of resources that are kept secure because they are accessible only through the appliance, but you have open access to anything not spelled out in the resource list (for example, other Internet sites).
- In **redirect all** mode, which is the more secure (and restrictive) approach, all traffic is redirected through the appliance. You are not allowed to access anything that is not in the list of allowed resources.
- The administrator can opt to give you access to local printers and file shares, regardless of the tunnel mode.

If you are having trouble accessing resources, your administrator may instruct you to make a change in the Advanced settings. Network Preference option allows users to choose local/remote network preference in any tunnel mode (Split tunnel or Re-direct all).

Administrators can allow users to add custom exclusions in **No VPN for** field.

① | **NOTE:** IP range is not supported in **No VPN for** section.

If you need to make a configuration change, it must be done while Connect Tunnel is disconnected.

## Configuring a Device VPN connection

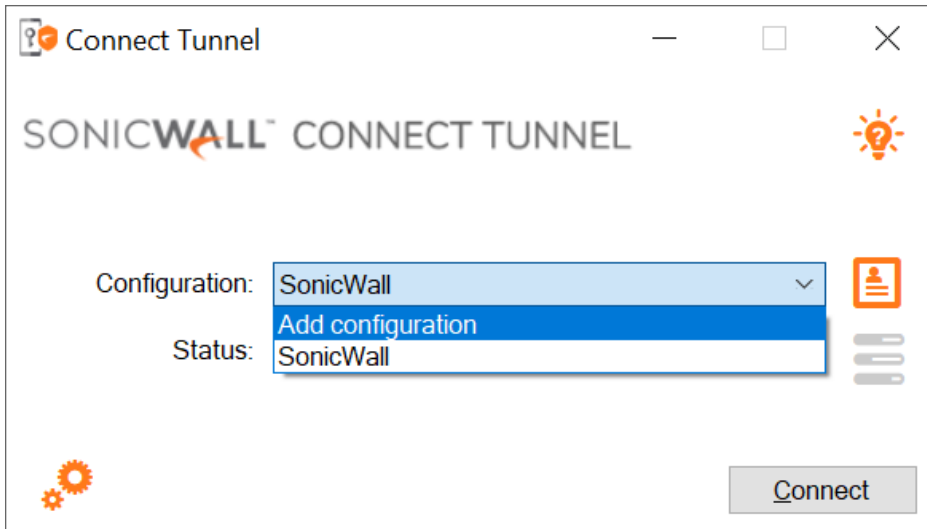
① | **NOTE:** Connect Tunnel client supports the Device VPN endpoint enrollment feature which is available from 12.4.2 onwards.

① | **NOTE:** Connect Tunnel must be off-line to change the connection to a Device VPN for the first time configuration.

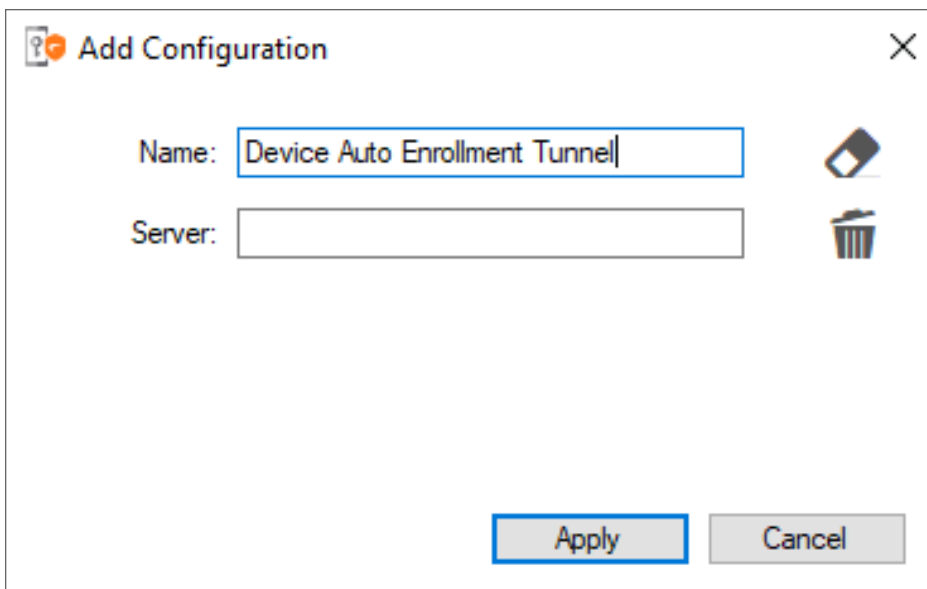
### **To establish a Device VPN connection:**

1. Open **Connect Tunnel** application.
2. In the **Connect Tunnel** login dialog box, click the drop-down list to choose a different VPN.

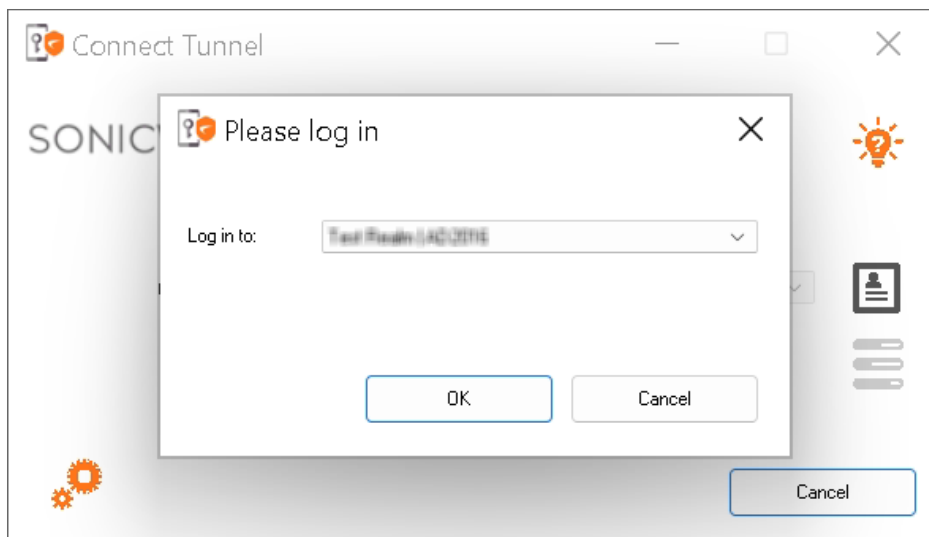
3. On the screen below, click **Add configuration** to add new configuration.



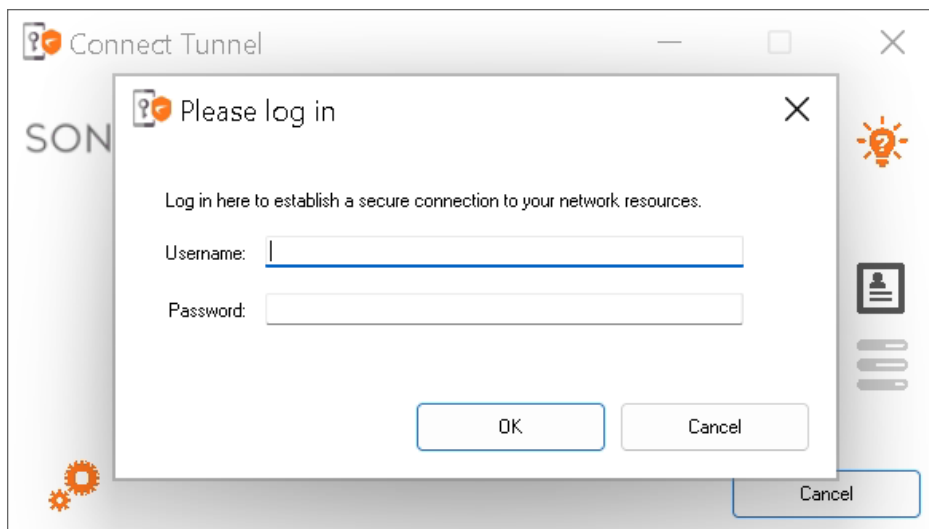
4. Enter a name in the **Name** field. In the **Server** field, enter the IP address of the VPN you want to connect.



5. Click **Apply** to complete the process.
6. The next screen gives a drop down list to choose an enabled realm which is provisioned for Device VPN connection. Select the realm, then click **OK**.

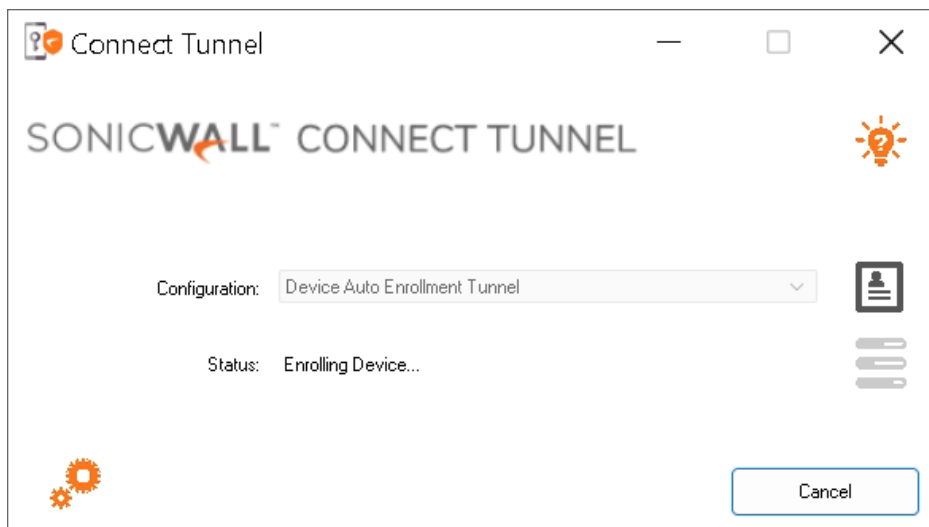


7. Enter your authentication credentials. Depending on how your administrator has configured Connect Tunnel, you may see a combination of these prompts. Click **OK** to login. The screen below is an example:

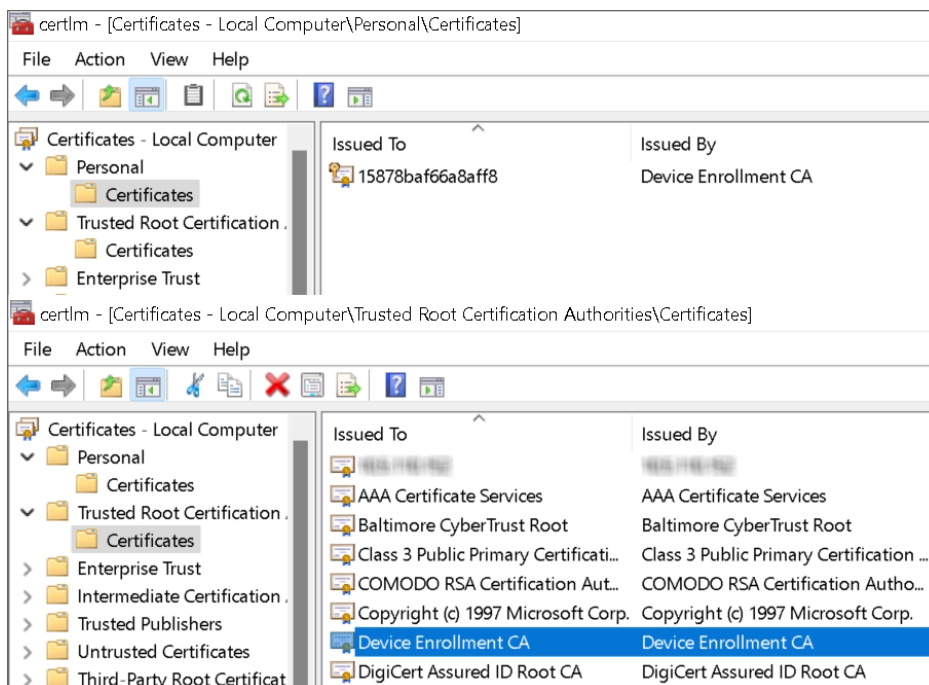


- Type your username in the **Username** field.
- In the **Password** or **Passcode** field, type your password or passcode. (Passwords may be case-sensitive. Make sure the Caps Lock or Num Lock keys are not enabled.)
- Enter a one-time password if one was sent to you by your administrator.

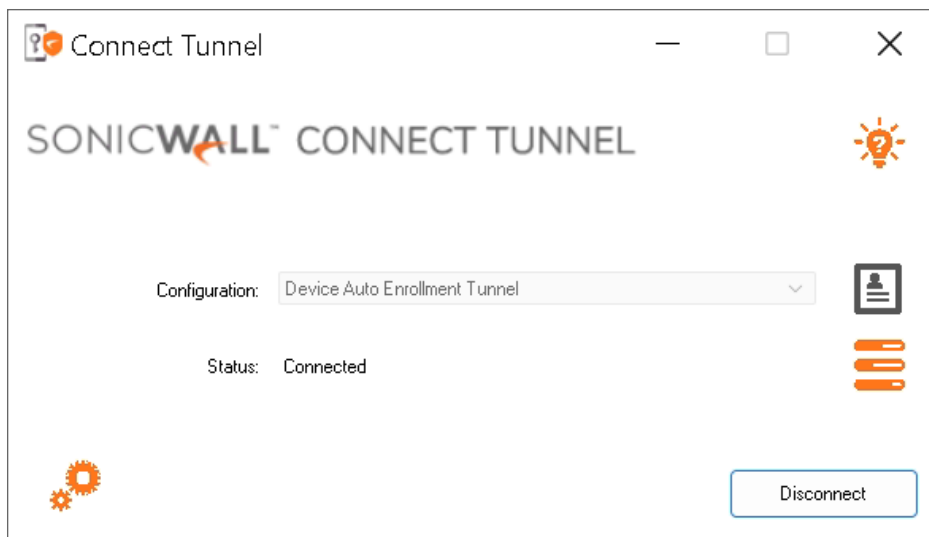
The Connect Tunnel client performs endpoint enrollment.



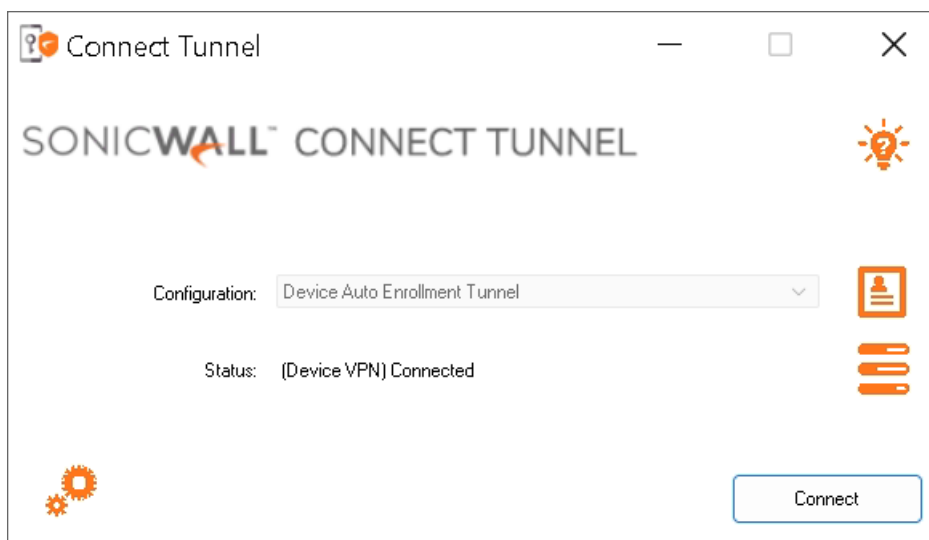
The Connect Tunnel client installs CA certificate under Local Computer\Trusted Root certification store and device certificate under Local Computer\Personal store.



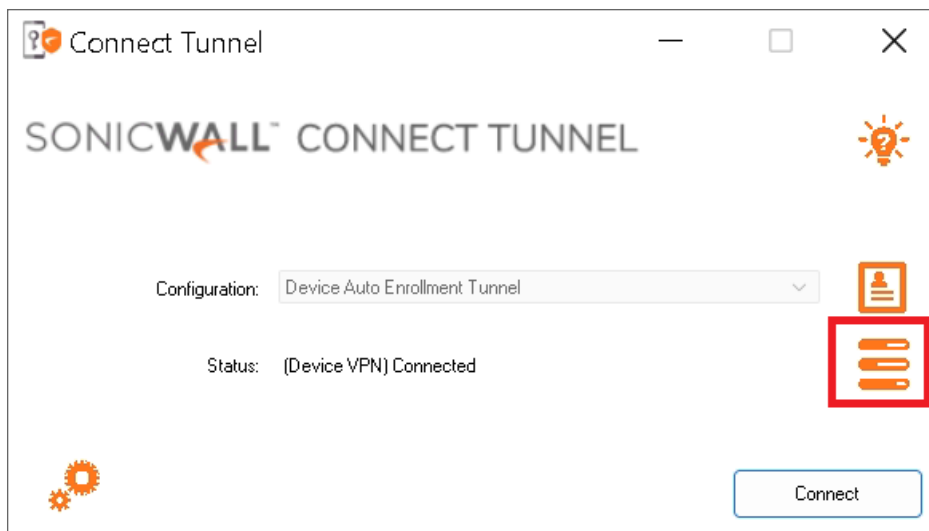
If your login is successful, the following screen appears to show that you are connected to the User VPN connection and displays status **Connected**.



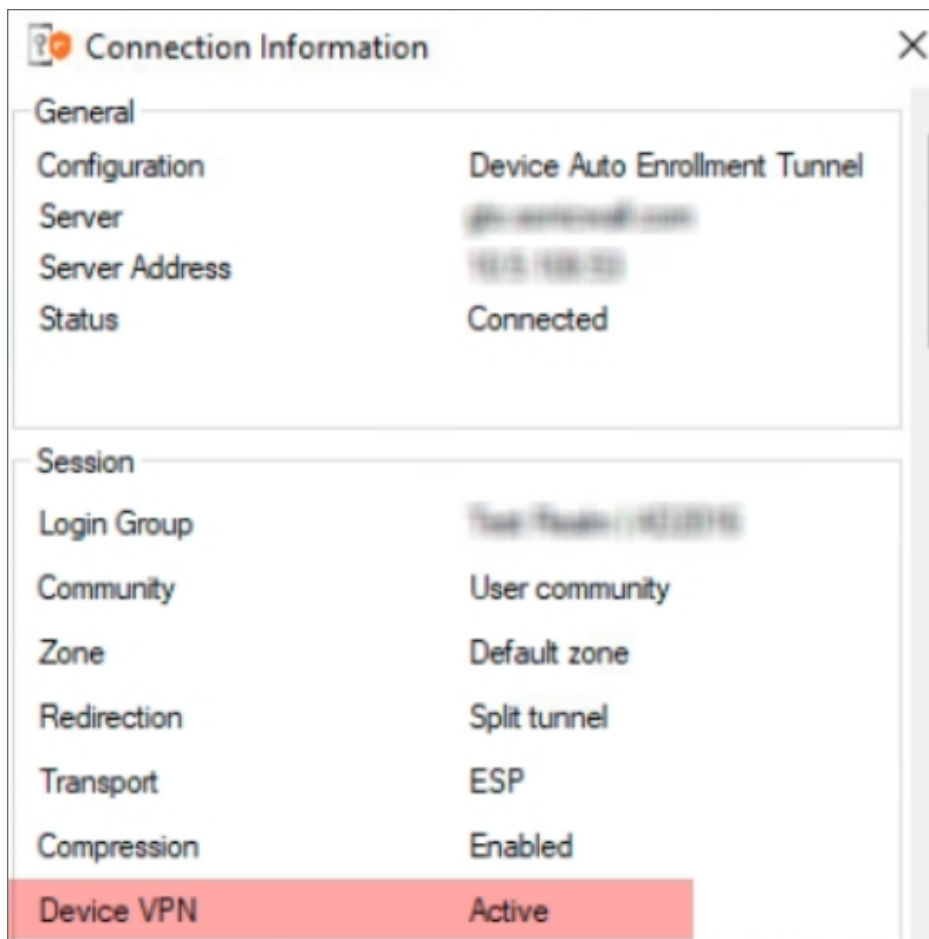
8. Click **Disconnect**, User VPN connection will fallback to Device VPN connection and displays status **(Device VPN) Connected**.



9. Click **Connect**, to connect back to User VPN and follow the Step 7.
10. Click **Connection Information** on the Main Window to view all the connection information.



The screen shows the connection information to verify the details of session.





The issued device certificate is renewed automatically by Connect Tunnel client before the expiry of the certificate. Re-enrollment triggers when the certificate validity is less than 15 days.

① **NOTE:** By default, the enrolled device certificate is valid for 90 days (unless changed by your administrator). This certificate is renewed automatically when the validity is less than 15 days before the expiry.

The **Connect Tunnel** icon appears in the task bar notification area, indicating that Connect Tunnel is running and connected to the VPN.

Your login may not be exactly the same as that shown above. Your administrator might send you login instructions that allow you to connect to a specific network.

## Updating the Connect Tunnel Application

Connect Tunnel can be updated either automatically or manually. Your administrator controls the auto-update based on the policy settings. End-users can manually update the client anytime after receiving the new installer.

### Topics:

- [Auto Update](#)
- [Manual Update](#)

## Auto Update

The network administrator may issue software updates when a new version of the Connect Tunnel software becomes available or when your network requirements change. Your administrator determines whether and when to make software updates available.

If your administrator has enabled the Connect Tunnel software update, an alert appears during the login process whenever an Connect Tunnel update is ready to download.

After updating the Connect Tunnel, do the following steps for the auto-update:

- During login, if the **Connect Tunnel Software Update** dialog box appears to indicate that a software update is available, the available options depend on how your administrator has configured software updating:
  - Click **Yes or OK** to download and install the software update immediately. If you select this option, the software updates and installs automatically, then the login process continues.
  - Click **No** to postpone the software update and continue logging in. If you select this option, Connect Tunnel prompts you again (once per day) until you download and install the update by clicking **Yes or OK**. Depending on how your administrator has configured Connect Tunnel, this option may be unavailable.
  - Click **Cancel** to cancel the software update and the login process.

## Manual Update

To perform a manual update, Connect Tunnel installer can be downloaded from the workplace portal, the [SonicWall.com](https:// SonicWall.com) portal or from the administrator.

# Provisioning of Connect Tunnel using SCCM or Intune

This section provides information on how to provision Connect Tunnel using SCCM or Intune.

## Creating a Default Profile

Connect Tunnel setup executable accepts few command line parameters to initialize the default connection profile during setup.

Command	Description
Name	Name of the VPN profile
VpnServer	Host name or IP address of the appliance
Realm	Realm name (only user VPN realm, Device VPN realm is not recommended)

### Example configuration:

```
MCTSetup.exe Name=Vpnname VpnServer=vpn.example.com Realm="Split Tunnel"
```

The above configuration process accepts additional parameters for either silent or non-interactive installation.

Parameter	Description
/s	Silent installation without any UI display
/passive	Non-interactive installation with minimal UI display
/log logfile	Installer logs can be redirected to logfile instead of default location %temp%
RemoveLegacy	Uninstalls legacy Connect Tunnel when installing the Modern Connect Tunnel.  Pass a value <i>true</i> or <i>yes</i> to uninstall legacy CT.

### Example:

```
MCTSetup.exe /passive Name=Vpnname VpnServer=vpn.example.com  
Realm="Split Tunnel" RemoveLegacy=yes
```

❗ **NOTE:** If *RemoveLegacy* parameter is not specified and if the installer is running in interactive mode, then setup will prompt user to uninstall Legacy Connect Tunnel.

### Example configuration:

```
MCTSetup.exe /passive Name=Vpnname VpnServer=vpn.example.com Realm="Split Tunnel"
```

❗ **NOTE:** The configuration set up does not accept any *INI* file for configuration other than the parameters mentioned above.

- ① | **NOTE:** When the parameters are passed for default profile, it does not create the profile during installation but only on first launch. The parameters are kept in registry for initialization while launching the application.

## Configuration of Device VPN

- ① | **NOTE:** The Legacy Connect Tunnel and Connect Tunnel Service (CTS) is deprecated from 12.4.1 onwards, if you still wish to use CTS in 12.4.2, SMA recommends to use the Device VPN which is similar to Connect Tunnel Service.

The setup accepts additional parameters to allow configuration of Device VPN. *VpnServer* parameter mentioned above is a prerequisite for configuration.

Parameter	Description
DeviceVpn	Pass value 1 to enable Device VPN
EnableVpnOnlyNetwork	Pass value 1 to restrict network access to VPN only network
	①   <b>NOTE:</b> This is effective only when the parameter <i>DeviceVpn</i> is enabled.
DisableUserVpn	Pass value 1 to disable User VPN and run only Device VPN to get similar functionality like Connect Tunnel Service (Legacy).
	①   <b>NOTE:</b> This is effective only when the parameter <i>DeviceVpn</i> is enabled.
	①   <b>NOTE:</b> This disables the <b>Connect</b> button and user will not have any control to launch User VPN.

### Example configuration:

*MCTSetup.exe Name=Vpnname VpnServer=vpn.example.com DeviceVpn=1*

*MCTSetup.exe Name=Vpnname VpnServer=vpn.example.com DeviceVpn=1 DisableUserVpn=1*

## Support for Always-On VPN

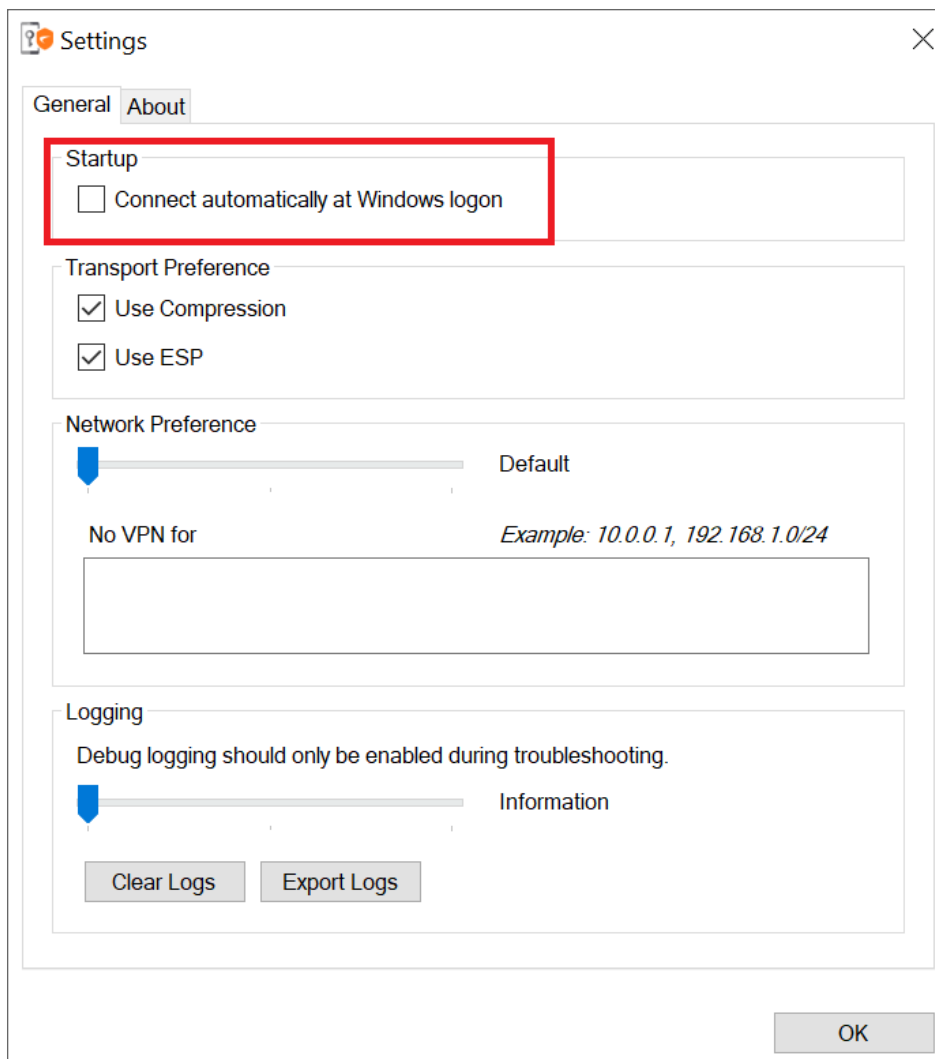
Connect Tunnel client supports limited features of Always-On VPN from Legacy CT client. To achieve an alternative and better functionality uses a combination of Device VPN, Auto Launch, and Network Logon modes.

The Device VPN can be restricted to block all internet traffic except for the tunnel interface with the switch *EnableVpnOnlyNetwork*.

## Support for Auto Launch at Windows Logon

Connect Tunnel client supports auto-launch at Windows logon and is useful when **Device VPN** or **Always On VPN** are not configured but users want automatically connect to VPN.

This setting can be enabled from **Advanced Settings > General** tab or by passing "AutoConnect=1" parameter to Connect Tunnel setup. By default, this setting is disabled.



## Support for using default browser for SAML Authentication

Connect Tunnel Client uses an embedded browser by default for SAML authentication. If you prefer to use the default browser, you can use it by creating a registry key as given below to override the default behavior.

[HKEY\_CURRENT\_USER\Software\SonicWall\SonicWall Secure Mobile Access]

"DefaultBrowser"=dword:00000001

# Troubleshooting Connect Tunnel

This section describes how to troubleshoot common Connect Tunnel client problems. If you are having trouble connecting to your VPN, or accessing local or remote network resources, check if your problem is addressed by the following. If the problem persists, contact your system administrator.

## Topics:

- [Unable to Connect](#)
- [Troubleshooting ESP](#)
- [Unable to Access Resources or the Internet](#)
- [Using Logs](#)
- [Installation Fails](#)
- [EPC Zone Classification doesn't work as intended](#)
- [OpSwatWrapper Init Error](#)

## Unable to Connect

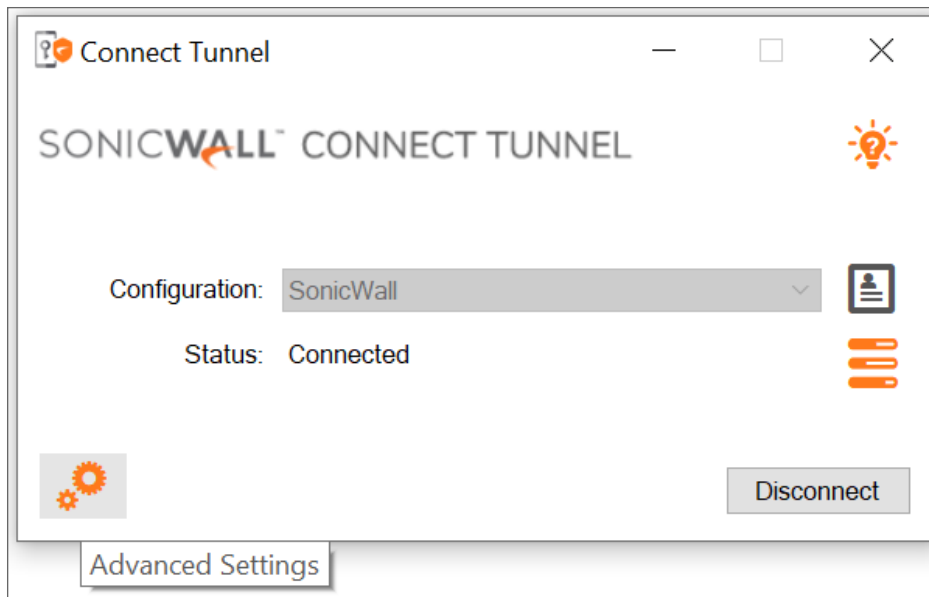
Here are a few items to check if you are having trouble connecting to your VPN:

- Make sure that Connect Tunnel is running and actively connected to the network. For more information, see [Viewing Connect Tunnel Status](#).
- Verify in the **Connect Tunnel Properties** dialog box that you are initiating a connection to the correct host name or IP address. For more information, see [Connecting to a Different VPN](#).
- Verify in the **Connect Tunnel Properties** dialog box that you are initiating a connection to the correct login group. For more information, see [Choosing a Login Group](#).
- If you use a personal firewall, you may need to reconfigure the firewall before you can access the VPN. To do this, configure the firewall to allow `SnwlConnect.exe` traffic to access the Internet, and add the VPN's host name or IP address as a trusted host or zone.
- Authentication may require that you have a particular client certificate on your device. If you make changes to the certificates installed on your computer between logon attempts, update the list presented during login by clicking **Refresh**.

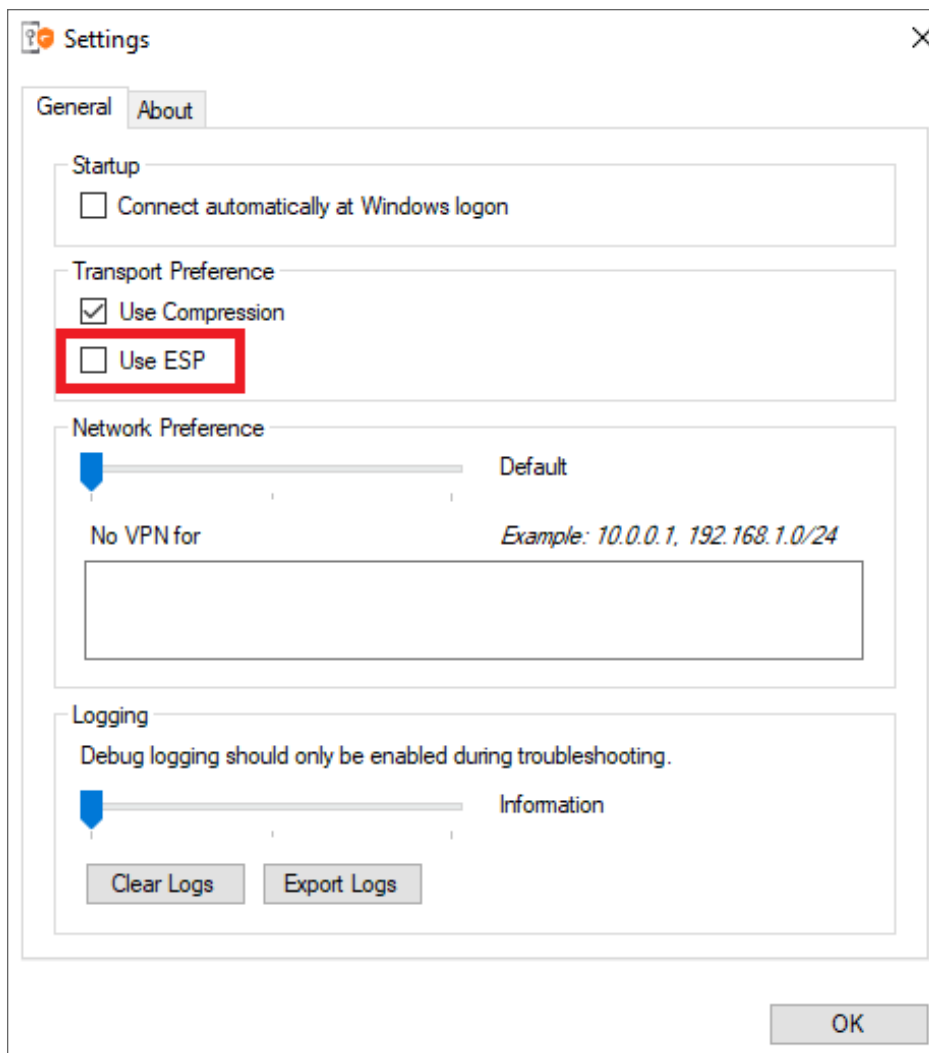
## Troubleshooting ESP

This section describes how to troubleshoot ESP. On the ESP-enabled Connect Tunnel session, if the user faces network-related issues. The following instructions show how to troubleshoot any ISP-related issue with UDP traffic.

1. Launch **Connect Tunnel**.  
Click on **Advanced Settings**.



2. Click the **General** tab.
3. Under **Transport Preference** section, deselect the check box **Use ESP** to disable it.



4. Click **OK**.

## Unable to Access Resources or the Internet

Your device may have been classified into the wrong security zone:

- Your administrator may ask you to confirm the security zone into which you have been classified. If security zones have been configured, click on the **Connection Information** icon on the Connect Tunnel screen.

When requests for resources or Internet access are received from clients by the appliance, they can be handled in several different ways. Your administrator makes this configuration choice in AMC:

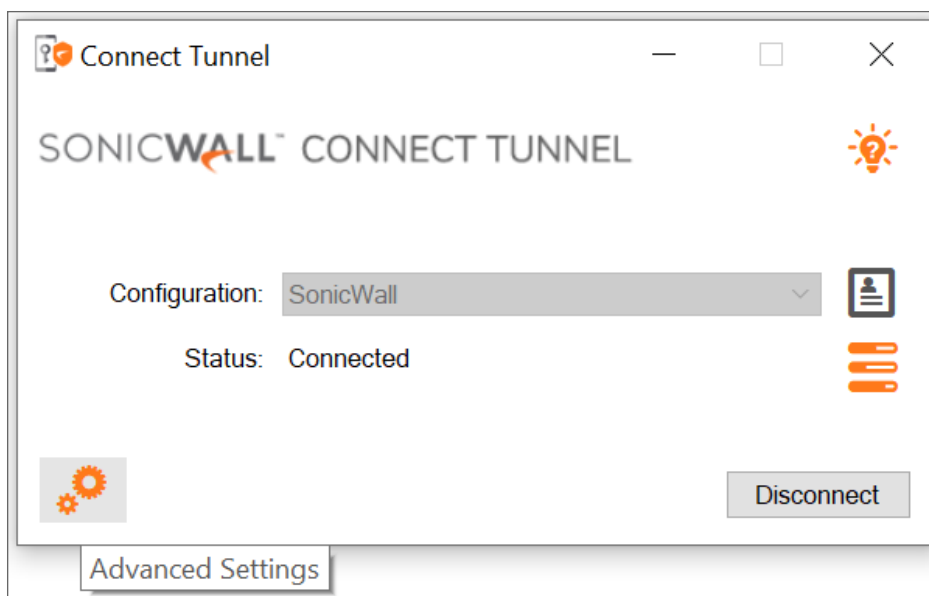


- In **split tunnel** mode, only traffic destined for resources that have been specified in AMC is redirected to the appliance, and all other traffic is routed as normal. In other words, your administrator sets up a list of resources that are kept secure because they are accessible only through the appliance, but you have open access to anything that is not spelled out in the resource list (for example, other Internet sites).
- In **redirect all** mode, which is the more secure (and restrictive) approach, all traffic is redirected through the appliance, you are not allowed to access anything that is not in the list of allowed resources.
- Your administrator can opt to give you access to local printers and file shares, regardless of the tunnel mode.

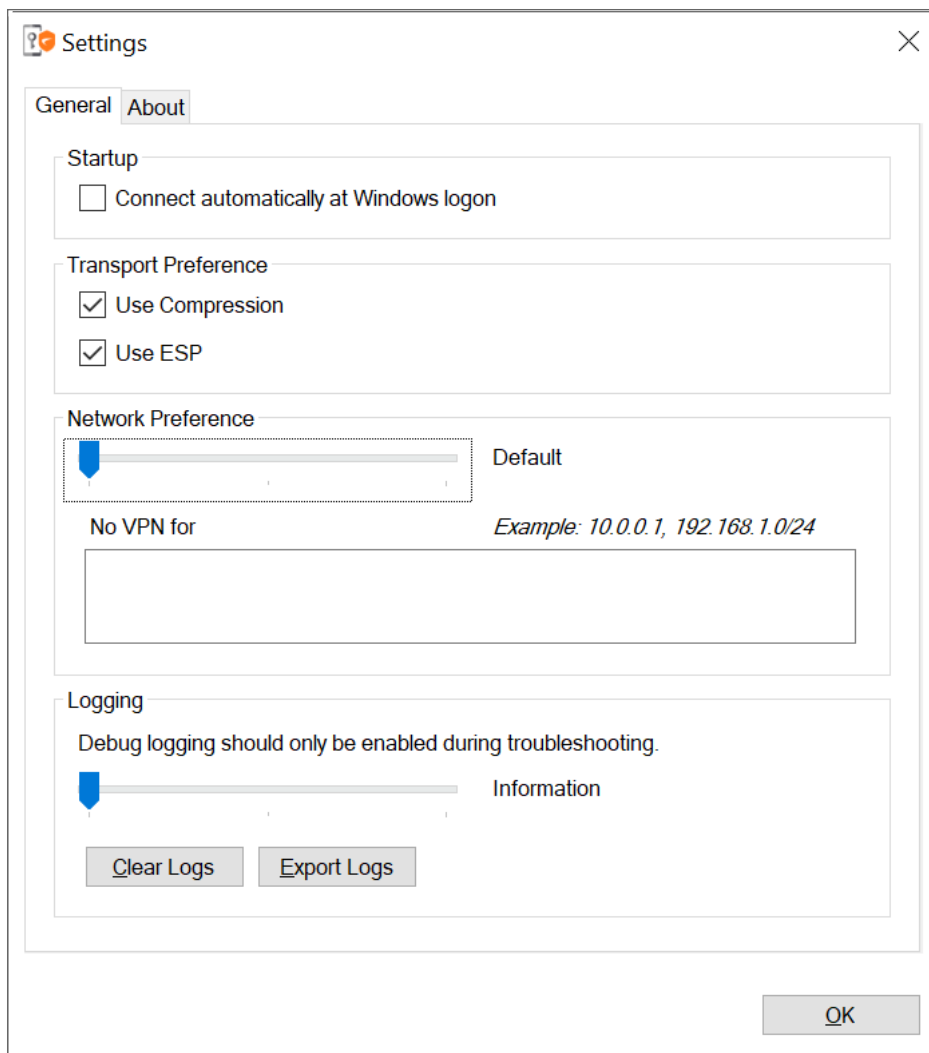
## Using Logs

The following instructions show how to respond to an administrator request to print debug logs, reproduce a problem, or download logs for any reason.

1. To enable logging, click on **Advanced Settings**.



2. Click the **General** tab.
3. Clear the existing logs by clicking **Clear Logs**.
4. Set **Logging** levels to **Information / Debug enabling / Packet Capture**.
5. Click **OK**, and let the log run for the specified time. Logs are named according to the formula:  
ConnectTunnel-YYYYMMDD\_at\_HHMMSS.ZIP.



6. When you want to export a log, navigate to the Connect Tunnel **Advanced Settings** tab.
7. Click **Export Logs**.
8. Click **OK**.

# Installation Fails

When the installation fails with the following error:

*Service "SonicWall Secure Mobile Access" (SnwlVpn) failed to start. Verify that you have sufficient privileges to start system services.*

The error is occurred due to corrupted MS Visual C++ 2015-2019 runtime on the windows machine.

## **To repair MS Visual C++ runtime:**

1. Uninstall MS Visual C++ 2015-2019 runtime (both x86 and x64).
2. Install the latest runtime from <https://support.microsoft.com/en-us/topic/the-latest-supported-visual-c-downloads-2647da03-1eea-4433-9aff-95f26a218cc0>.
3. Restart the computer.

# EPC Zone Classification doesn't work as intended

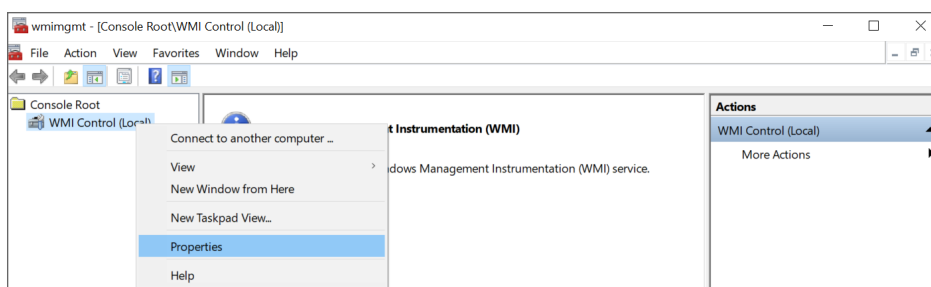
Open the *SnwlConnect.log* and see for below log:

*Connect Tunnel has identified an issue on your machine and may not work properly. Please fix the issue before connecting to VPN.*

The error is occurred due to corrupted WMI on the Windows machine.

## **To repair WMI:**

1. Press **Windows Start** key and search for **Run** application.
2. In the **Run** dialog, type *wmicmgmt.msc* and then click **OK**.
3. In the **wmicmgmt** screen, right-click WMI Control (Local) and click **Properties**.



If Win32\_Process shows as invalid class, then follow the below steps to repair WMI:

- a. Open Command Prompt.
- b. Run the command *net stop winmgmt*.
- c. Open Windows Explorer and navigate to "C:\Windows\System32\wbem\" folder and then rename "Repository" folder to "RepositoryOLD"

- d. Restart the computer.
- e. Open Command Prompt and run the command *net stop winmgmt*.
- f. Run the command *winmgmt /resetRepository*.
- g. Restart the computer.

## OpswatWrapper Init Error

When you get the below error:

*OpswatManager - OpswatWrapper Init Error<80040154>*

This indicates that SonicWall OPSWAT wrapper distributed with advanced EPC updates are not installed properly.

### ***To install the updates:***

1. Uninstall **SonicWall SMA Secure Endpoint Manager** and **SonicWall SMA OPSWAT End Point Control** applications.
2. Log in to WorkPlace and install **SMA Secure Endpoint Manager**.
3. Check the zone classification for WorkPlace session.
4. Log in using Connect Tunnel and load OPSWAT wrapper.
5. Ensure the OPSWAT wrapper is loaded appropriately.

# Connect Tunnel Client for macOS and Linux

## Topics:

- [System Requirements for MacOS](#)
- [System Requirements for Linux](#)
- [Starting Connect Tunnel](#)
- [Managing Configurations](#)
- [Processing Server Certificates](#)
- [Configuring Proxy Server Settings \(Linux Only\)](#)
- [Troubleshooting](#)

## System Requirements for MacOS

This new client application doesn't require JVM (Java Virtual Machine) and is intended for use on Apple Macs based on Intel or Apple Silicon.

① | **NOTE:** New Client application is supported only with Big sur (11.x) and later.

If you want the Legacy Client, you can also switch to Legacy (Java-based) Client application. For more information, see [Connect Tunnel on macOS](#).

① | **NOTE:** This Legacy Client application requires JVM (Java Virtual Machine) and is intended for use on Apple Macs based on Intel or Apple Silicon.

## System Requirements for Linux

This client application requires JVM (Java Virtual Machine) version 11 or later and is intended for use on 64-bit, 86-bit, and ARM Linux.

# Starting Connect Tunnel

To access network resources through Connect Tunnel, your identity must first be verified. This ensures that only authorized users can access protected network resources. The credentials used to verify your identity typically consist of a username and password or passcode.


## Topics:


- [Connect Tunnel on macOS](#)
- [Connect Tunnel on Linux](#)
- [Specifying a Login Group](#)
- [Connecting to a Different VPN](#)
- [Quitting Connect Tunnel](#)

## Connect Tunnel on macOS

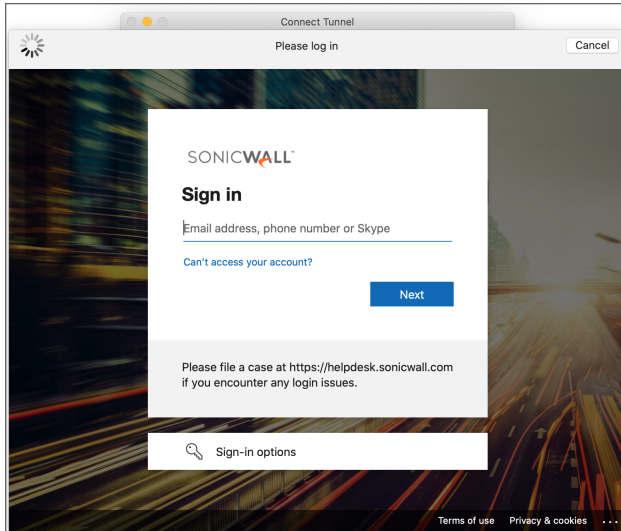
### *To start Connect Tunnel on macOS:*

1. In the Finder, double-click **Applications**, and then double-click the **Connect Tunnel** icon.  
The **Connect Tunnel** login dialog appears.
2. In the **Configuration** list, select a VPN configuration and click **Connect**.  
If there are no saved configurations, you must create one; see [Editing Connect Tunnel Settings](#) for more information.
3. If you access a network resource that uses a self-signed or invalid server certificate, Connect Tunnel will display the certificate. Verify that the server certificate is from a trusted source before accepting it.  

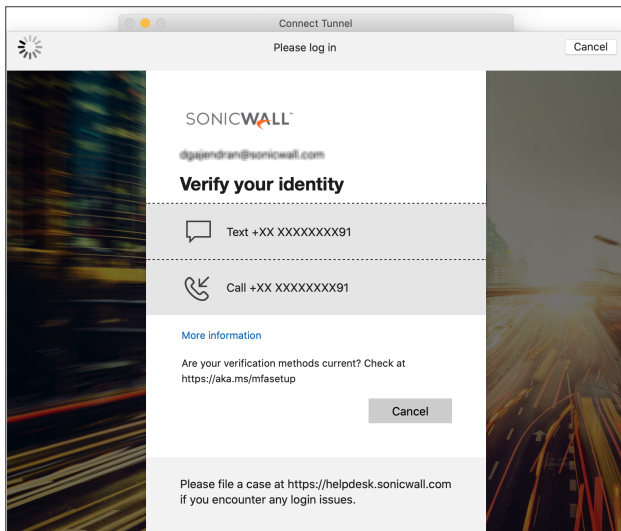
 **NOTE:** As anyone can issue a certificate, you should accept certificates only from trusted sources as the information you receive may be invalid. If you have any concerns about whether or not to accept a certificate, check with your administrator.
4. In the **Login Group** selection, choose your Login Group and then click **OK**.
5. In the **Username** field, type your username.
6. In the **Password** or **Passcode** field, type your password or passcode. (Passwords may be case-sensitive: make sure the Caps Lock and Num Lock keys are not enabled)  
The SAML Authentication login dialog appears.  

 **NOTE:** Connect Tunnel uses embedded browser for SAML Authentication.

7. Enter the appropriate account you want to sign in and click **Next**.



8. The login screen prompts you for different verification options based on sign in options such as Multi-Factor Authentication (MFA) or Single sign-on (SSO).
9. Choose the verification option and verify your identity. You are signed into the **Connect Tunnel**.



10. Click **OK**.

A message in the login dialog indicates the status of the VPN connection.

- ① | **TIP:** In the **Connect Tunnel** login dialog, you can initiate a connection to a list.
- ① | **TIP:** From the **Applications** directory, you can drag the **Connect Tunnel** icon to the dock for easier access.

# Connect Tunnel on Linux

## *To start Connect Tunnel on the Linux platform:*

1. After Connect Tunnel is installed, you can run `startctui` from any location.  
OR  
You can also start **Connect Tunnel** by double-clicking the Connect Tunnel icon in the desktop.  
The **Connect Tunnel** login dialog appears.
  2. In the **Configuration** list, select a VPN configuration and click **Connect**. If there are no saved configurations, you must create one; see [Creating a New Configuration](#) for more information.
  3. If you access a network resource that uses self-signed or invalid server certificate, Connect Tunnel will display the certificate. Verify that the server certificate is from a trusted source before accepting it. Because anyone can issue a certificate, you should accept certificates only from trusted sources. Otherwise, the information you receive may be invalid. If you have any concerns about whether to accept a certificate, check with your administrator.
  4. In the **Login Group** selection, choose your Login Group and click **OK**.
  5. In the **Username** field, type your username.
  6. In the **Password** or **Passcode** field, type your password or passcode. (Passwords may be case-sensitive: make sure the Caps Lock and Num Lock keys are not enabled.)
  7. Click **OK**.  
A message in the login dialog indicates the status of the VPN connection.
- ❶ | **TIP:** In the Connect Tunnel login dialog, you can initiate a connection to a different VPN or login group by choosing a different configuration from the **Configuration** list.

## Specifying a Login Group

Connect Tunnel enables you to log in to different login groups; for example, you can alternate between logging in to the Sales and Marketing groups. You may need to provide different authentication credentials for each login group.

You must specify a login group each time you initiate a connection to your VPN. This option is available only when Connect Tunnel is offline; that is, when not connected to your VPN.

### *To specify the login group:*

1. In the **Connect Tunnel** login dialog box, choose a **Configuration** and click **Edit**.
2. In the **Edit Configuration** dialog, click **Forget Selection** and choose **Save**.
3. Choose the saved **Configuration** and click **Connect**.
4. Select the new Login Group and click **OK**.



## Connecting to a Different VPN

To specify a different VPN to connect to, Connect Tunnel must be offline (that is, not connected to your VPN - **Status: Disconnected**).

*To specify the host name or IP address of the VPN:*

1. In the Connect Tunnel login dialog box, click **Add Configuration**.
2. Enter a name for the configuration in the **Name** field.
3. In the **Server** field, type the host name or the IP address of the VPN you want to connect to.
4. Click **OK**.

The login dialog is displayed.

## Quitting Connect Tunnel

To end your VPN session and disconnect from the remote network, click **Disconnect** in the **Connect Tunnel** login dialog.

## Managing Configurations

To simplify the login process, you can set up one or more VPN configurations. If, for example, you sometimes connect to a different login group or a different VPN, you can save these settings under different names.

### Topics:

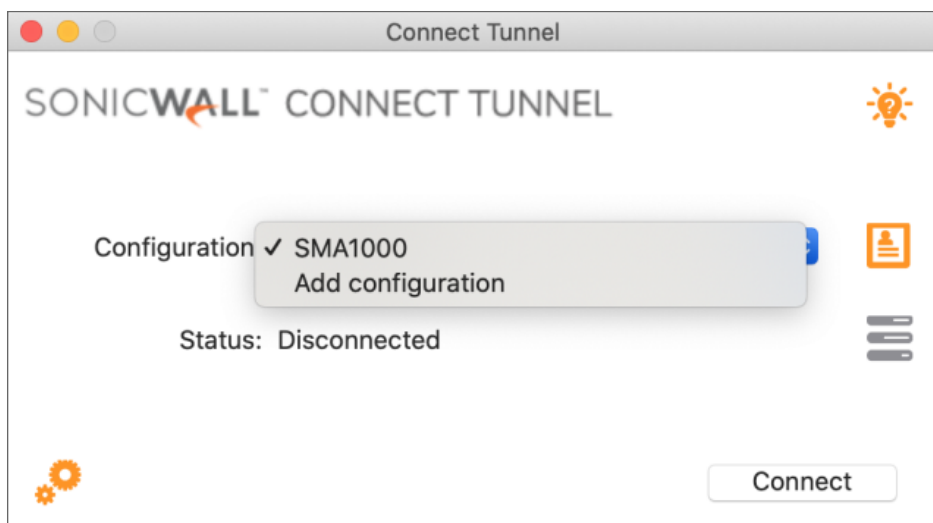
- [Viewing Connect Tunnel Settings](#)
- [Editing Connect Tunnel Settings](#)
- [Deleting a Configuration](#)
- [Creating a New Configuration](#)
- [Selecting the Advanced Button](#)
- [Advanced Options](#)
- [Credential Caching/Secure Network Detection](#)

# Viewing Connect Tunnel Settings

① | **NOTE:** Connect Tunnel must be offline; that is, not connected to your VPN (**Status: Disconnected**).

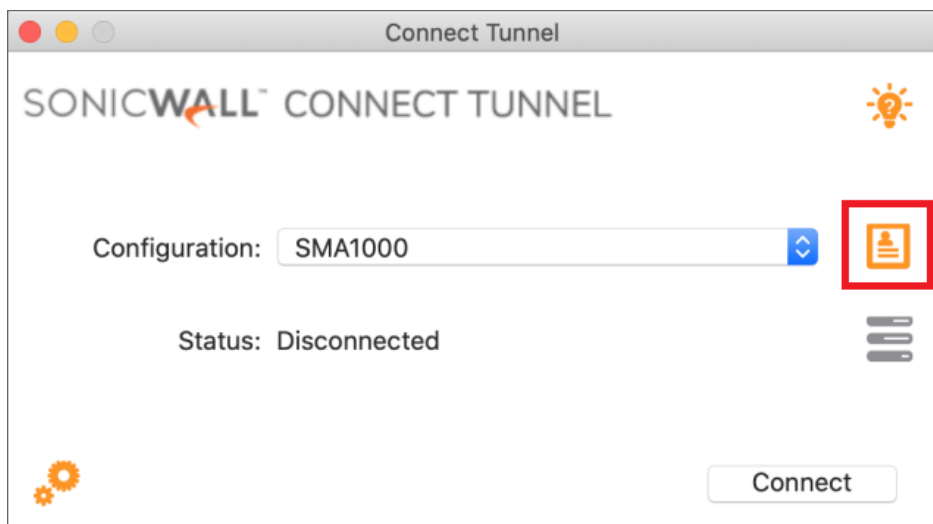
## To view your settings:

1. In the **Connect Tunnel** login dialog, select the configuration from the **Configuration** list.



2. Click **Edit**.

From here you can view your previously made configuration settings after selecting the desired configuration.

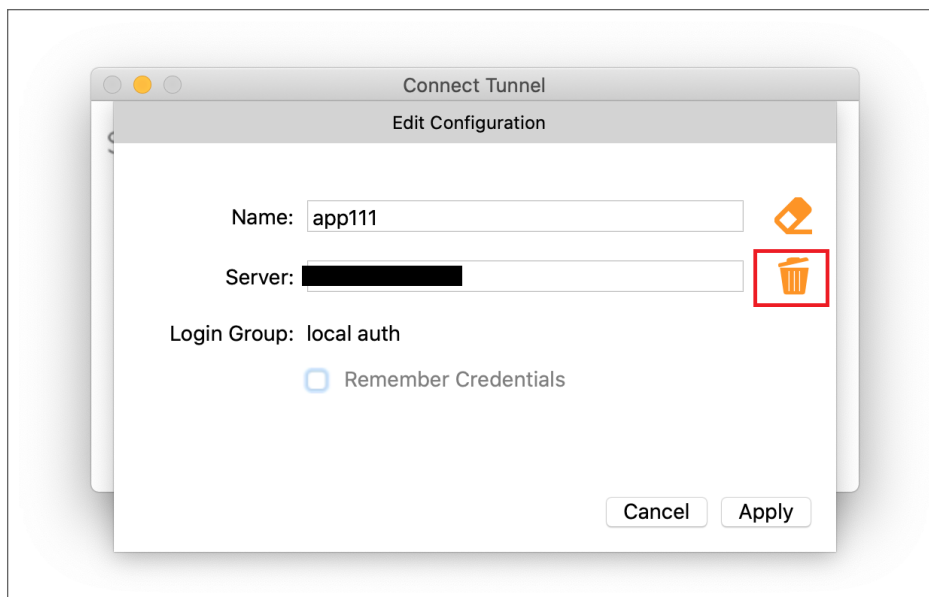


## Deleting a Configuration

① | **NOTE:** Connect Tunnel must be offline; that is, not connected to your VPN (**Status: Disconnected**).

*To delete a configuration:*

1. In the **Connect Tunnel** login dialog, select the configuration from the **Configuration** list and click **Edit**.
2. Click **Delete**.

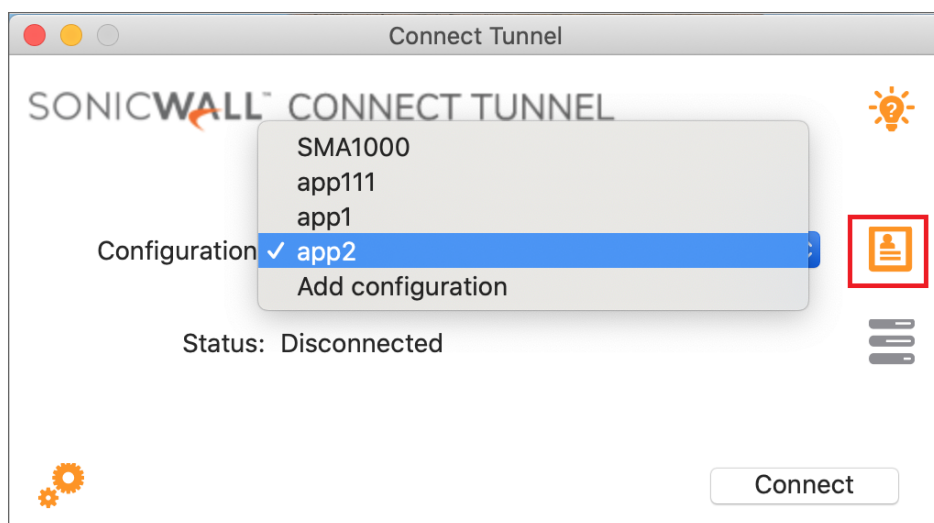


## Editing Connect Tunnel Settings

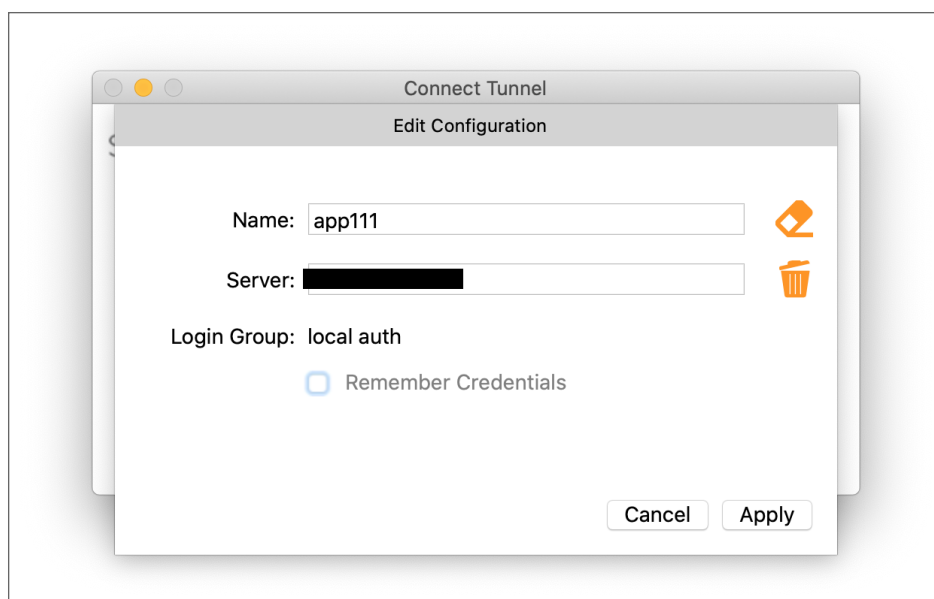
① | **NOTE:** Connect Tunnel must be offline; that is, not connected to your VPN (**Status: Disconnected**).

**To edit your settings:**

1. In the **Connect Tunnel** login dialog, select the configuration from the **Configuration** drop-down menu.



2. Click **Edit** to edit the configuration.  
The **Edit Configuration** dialog appears.



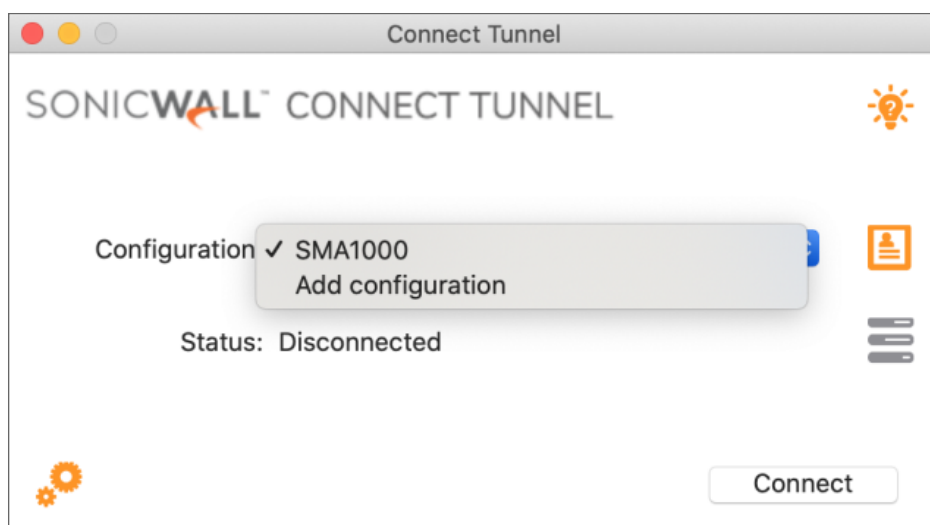
3. Make edits to the **Name** or **Server** field as necessary.
4. Click **Apply** to save your changes.

# Creating a New Configuration

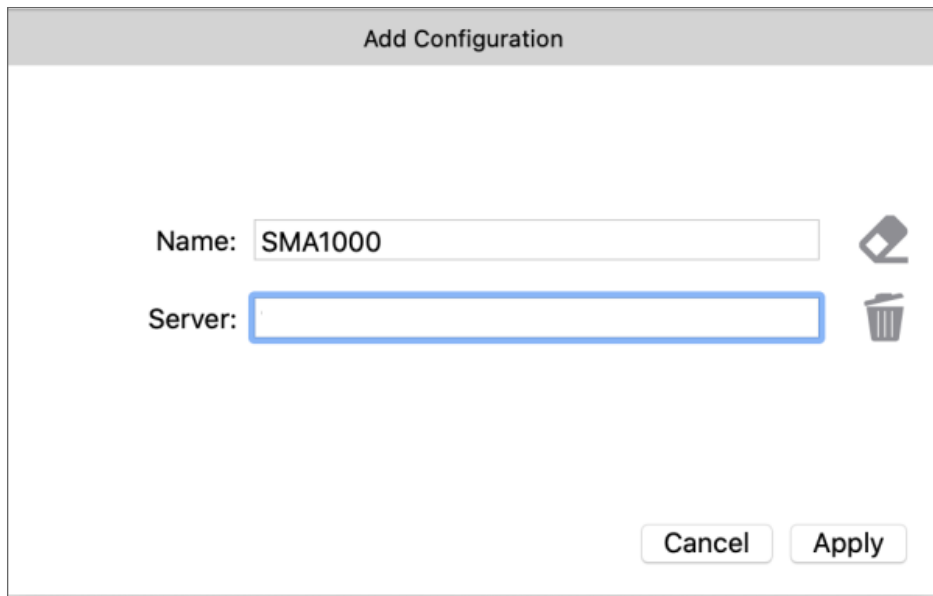
① | **NOTE:** Connect Tunnel must be offline; that is, not connected to your VPN (**Status: Disconnected**).

*To create a new configuration:*

1. In the **Connect Tunnel** login dialog, select **Add Configuration** from the **Configuration** list.



2. Assign a name to the new configuration (for example, *Connect from home*).  
This is the name that you will see in the **Configuration** list when you log in, so specify one that best describes its function.
3. In the **Server** field, enter the host name or IP address for the VPN.

A dialog box titled "Add Configuration" with a light gray header. It contains two text input fields. The first field is labeled "Name:" and contains the text "SMA1000". To its right is a small icon of a document with a checkmark. The second field is labeled "Server:" and is currently empty, with a blue border around it. To its right is a small trash can icon. At the bottom right of the dialog are two buttons: "Cancel" and "Apply".

Add Configuration

Name: SMA1000

Server:

Cancel Apply

4. Click **Apply** to save your changes.

## Selecting the Advanced Button

① | **NOTE:** Connect Tunnel must be offline; that is, not connected to your VPN (**Status: Disconnected**).

These tabs appear upon clicking **Advanced**: General, Certificate Manager, Proxy, and About.

## GENERAL

The screenshot shows a 'General' settings window with two tabs: 'General' (selected) and 'About'. The window is divided into three main sections: 'Transport Preference', 'Network Preference', and 'Logging'. In the 'Transport Preference' section, both 'Use Compression' and 'Use ESP' are checked. The 'Network Preference' section features a shield icon on a slider set to 'Default', a text field for 'No VPN for' with an example '10.0.0.1, 192.168.1.0/24', and an empty text area below. The 'Logging' section includes a note about debug logging, a shield icon on a slider set to 'Information', and 'Clear Logs' and 'Export Logs' buttons. An 'OK' button is located at the bottom right.

**General** About

**Transport Preference**

☒ Use Compression

☒ Use ESP

**Network Preference**

Default

No VPN for Example: 10.0.0.1, 192.168.1.0/24

**Logging**

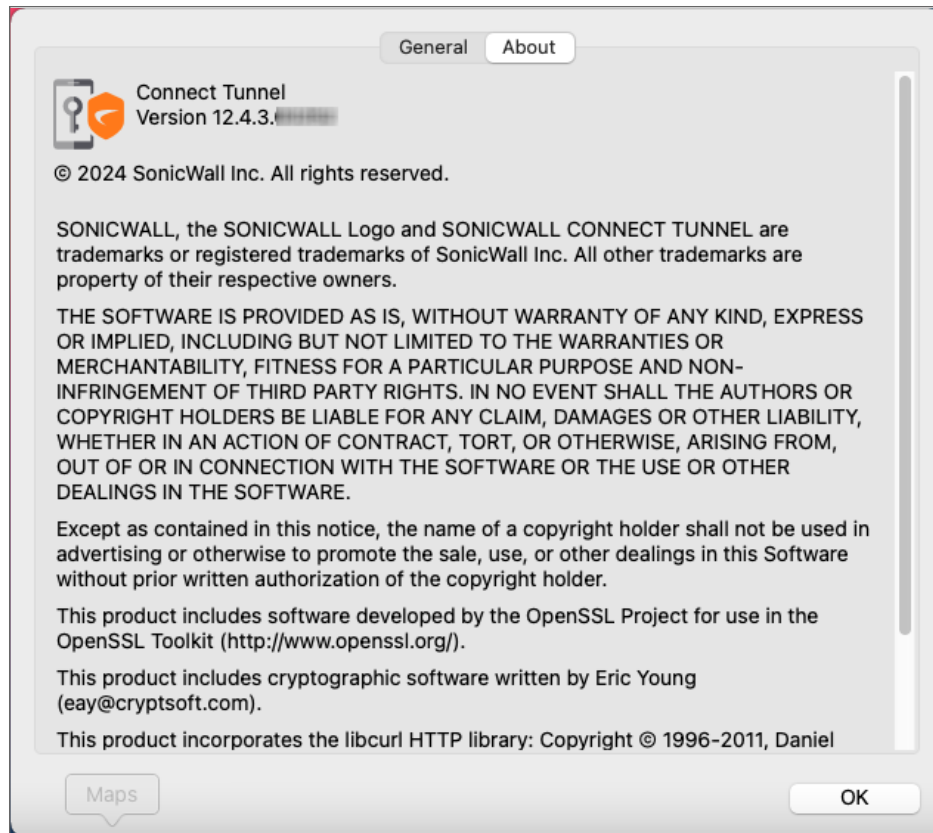
Debug logging should only be enabled during troubleshooting.

Information

Clear Logs Export Logs

OK

## ABOUT



## Advanced Options

When requests for resources or Internet access are received from clients by the appliance, they can be handled a few different ways. Your administrator makes this configuration choice in Appliance Management Console (AMC).

- In **split tunnel** mode, only traffic destined for resources that have been specified in AMC is redirected to the appliance. All other traffic is routed as normal.  
In other words, your administrator sets up a list of resources that are kept secure because they are accessible only through the appliance, but you have open access to anything not spelled out in the resource list (for example, other Internet sites).
- In **redirect all** mode, which is the more secure (and restrictive) approach, all traffic is redirected through the appliance. You are not allowed to access anything that is not in the list of allowed resources.
- Your administrator can opt to give you access to local printers and file shares, regardless of the tunnel mode.

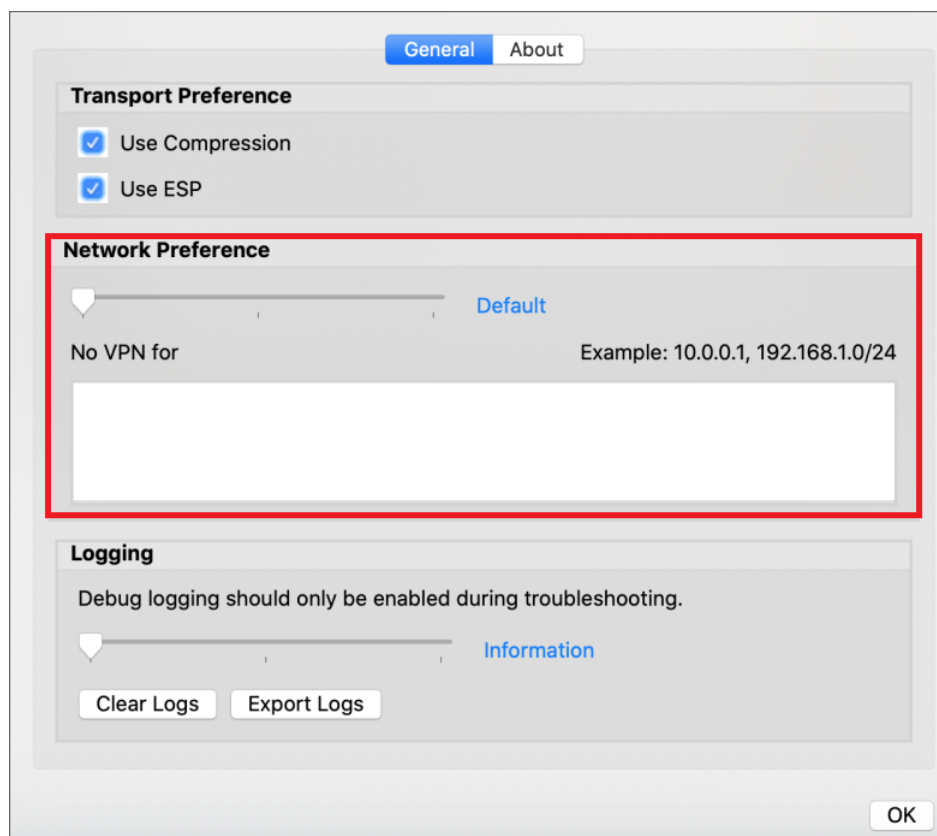


If you are having trouble accessing resources, your administrator may instruct you to make a change in the **Advanced** settings. Network Preference option allows users to choose local/remote network preference in any tunnel mode (Split tunnel or Re-direct all).

Administrators can allow users to add custom exclusions in **No VPN for** field.

① | **NOTE:** IP range is not supported in **No VPN for** section.

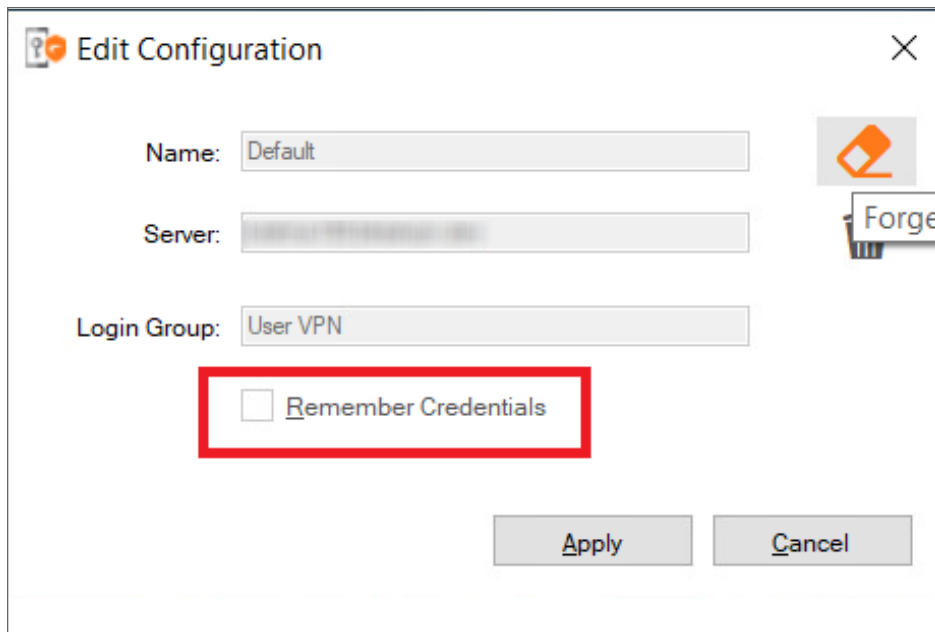
If you need to make a configuration change, it must be done while Connect Tunnel is disconnected.



For example, let's say you have a host resource—a Web server—with an address of `192.168.230.1`. You are on a business trip and the printer you want to use is on a local network at a conference center and uses that same address. You are using a realm that is configured for split tunnel mode, and your administrator has opted to give you access to local printers and file shares. To enable you to print at the conference center, your administrator may instruct you to open the **Advanced** settings, click **Prefer local network resource access**, and then click **Update**.

## Credential Caching/Secure Network Detection

If your administrator has allowed the Credential Caching policy, you can enable or disable it via the **Remember Credential** checkbox on the **Connect Tunnel Options** dialog. If enabled (checked) on Linux, the policy works while Connect Tunnel is running. In macOS, the information is stored in the keychain and persists across reboots.



If Secure Network Detection is enabled, Connect Tunnel is put into one of three states when connecting to an appliance for the first time:

- **Connected:** The machine is not in a secure location and requires a VPN connection to access resources.
- **Idle:** The machine is in a secure network and does not need the VPN connection to access resources.
- **Disconnect/Error:** The connection is dropped and disconnected due to external network events (for example, network change, dropped wifi signal).

## Processing Server Certificates

Some VPN configurations require that you accept a server certificate before you can gain access to a protected network resource. A server certificate is essentially a digital signature that verifies the server identity.

If you access a network resource that uses a server certificate, Connect Tunnel may display the certificate. Verify that the server certificate is from a trusted source before accepting it.

- ① **NOTE:** As anyone can issue a certificate, you should accept certificates only from trusted sources as the information you receive may be invalid. If you have any concerns about whether or not to accept a certificate, check with your administrator.

## Configuring Proxy Server Settings (Linux Only)

For Linux users, some network resources may require traffic to pass through an Internet proxy server, which provides access from your local network to the Internet. Your administrator determines whether a proxy server is

required, but you may occasionally be required to specify settings for it.

In many cases, Connect Tunnel can automatically detect your Internet proxy server settings. However, if the settings cannot be automatically detected, you must manually specify them.

This section describes how to specify outbound proxy server settings. This option is available only when Connect Tunnel is offline (that is, when not connected to your VPN), and only in the Linux version of the program.

### ***To configure outbound proxy server settings (Linux):***

1. In the **Connect Tunnel** login dialog, click **Advanced**.
2. Click the **Proxy** tab.
3. Click one of the following options:
  - a. **Direct Connection to the Internet:** Enables a direct connection to the Internet, with no outbound proxy server redirection.
  - b. **Automatically detect proxy settings:** Configures the client to detect and use the outbound proxy server settings as defined on your remote network.
  - c. **Manual proxy configuration:** Enables you to manually specify proxy server settings. In the **SSL** field, type the host name or IP address of the Internet proxy server. In the **Port** field, type the number of the port on which the server is listening. Select the **Use the same proxy server for all protocols** to use the specified **SSL** server for all traffic, or specify different proxy servers and their port numbers for HTTP, FTP, or SOCKS traffic. Optionally, in the **No proxy for** field, you can specify host names or IP addresses that you do not want redirected through a proxy server.
  - d. **Automatic proxy configuration URL:** Configures the client to retrieve a proxy auto-configuration (.pac) file that specifies proxy-server settings. In the field, type the URL of the server that hosts the .pac file.
4. Click **OK**.

The login dialog appears.

## Troubleshooting

This section describes how to troubleshoot basic Connect Tunnel client problems. If you are having trouble connecting to your VPN, or accessing local or remote network resources, see if your problem is addressed by the following. If the problem persists, contact your system administrator.

### **Topics:**

- Unable to use new Connect Tunnel client on MacOS
- [Unable to Connect VPN](#)
- [Troubleshooting ESP](#)
- [Unable to Access Resources or the Internet](#)
- [Unable to Access Resources on Linux](#)

# Unable to Connect VPN

Here are a few items to check if you are having trouble connecting to your VPN:

- Make sure that Connect Tunnel is running and actively connected to the network. For more information, see [Viewing Connect Tunnel Status](#)
- Verify in the **Connect Tunnel Properties** dialog that you are initiating a connection to the correct host name or IP address. For more information, see [Starting Connect Tunnel](#).
- Verify in the **Connect Tunnel Properties** dialog that you are initiating a connection to the correct login group. For more information, see [Viewing Connect Tunnel Status](#).
- If you use a personal firewall, you may need to configure it before you can access your VPN. To do this, configure the firewall to enable traffic to the VPN host name or IP address over port 443.

## Troubleshooting ESP

This section describes how to troubleshoot ESP. On the ESP-enabled Connect Tunnel session, if the user faces network-related issues. The following instructions show how to troubleshoot any ISP-related issue with UDP traffic.

1. Launch **Connect Tunnel**.  
Click on **Advanced Settings**.
2. Click the **General** tab.
3. Under **Transport Preference** section, deselect the check box **Use ESP** to disable it.
4. Click **OK**.

## Unable to Access Resources or the Internet

- Your device may have been classified into the wrong security zone.
- Your administrator may ask you to confirm the security zone into which you have been classified. If security zones have been configured, you can view your current zone by pausing on the Connect Tunnel icon in the taskbar notification area with your cursor.
- When requests for resources or Internet access are received from clients by the appliance, they can be handled a few different ways. Your administrator makes this configuration choice in AMC.
- In split tunnel mode, only traffic destined for resources that have been specified in AMC is redirected to the appliance, and all other traffic is routed as normal. In other words, your administrator sets up a list of resources that are kept secure because they are accessible only through the appliance, but you have open access to anything not spelled out in the resource list (for example, other Internet sites).
- In redirect all mode, which is the more secure (and restrictive) approach, all traffic is redirected through the appliance: you are not allowed to access anything that is not in the list of allowed resources.

- Your administrator can opt to give you access to local printers and file shares, regardless of the tunnel mode.

If you are having trouble accessing resources, your administrator may instruct you to make a change in the **Connect Tunnel Properties** dialog, on the **Advanced** tab. Network Preference option allows users to choose local/remote network preference in any tunnel mode (Split tunnel or Re-direct all). Administrators can allow users to add custom exclusions in **No VPN for** field.

① | **NOTE:** IP range is not supported in **No VPN for** section.

If you need to make a configuration change, it must be done while Connect Tunnel is disconnected.

For example, you have a host resource—a Web server—with an address of 192.168.230.1. You are on a business trip and the printer you want to use is on a local network at a conference center and uses that same address. You are using a realm that is configured for split tunnel mode, and your administrator has opted to give you access to local printers and file shares. To enable you to print at the conference center, your administrator may instruct you to open the **Connect Tunnel Properties** dialog, click the **Advanced** tab, and then click **Prefer local network resource access** for your session.

## Unable to Access Resources on Linux

*If you are unable to access resources on Linux:*

1. Disconnect the Connect Tunnel session on Linux and check the interfaces.
2. If "tun0" is found even after Connect Tunnel is disconnected, then run the below command:  

```
sudo ip link delete tun0
```
3. Restart the computer.

# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The [Support Portal](#) provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The [Support Portal](#) enables you to:

- View [Knowledge Base articles](#) and [Technical Documentation](#)
- View and participate in the [Community Forum](#) discussions
- View [Video Tutorials](#)
- Access [MySonicWall](#)
- Learn about [SonicWall Professional Services](#)
- Review [SonicWall Support services and warranty information](#)
- Register at [SonicWall University](#) for training and certification

# About This Document

Secure Mobile Access Connect Tunnel User Guide  
Updated - August 2024  
Software Version - 12.4  
232-005700-00 Rev D

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

## Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request  
Attn: Jennifer Anderson  
1033 McCarthy Blvd  
Milpitas, CA 95035