

# SonicWall® Secure Mobile Access

## 12.1 Connect Tunnel

User Guide

SONICWALL®

# Contents

<b>Introduction</b> .....	<b>4</b>
About Connect Tunnel .....	4
Organization of This Guide .....	4
Guide Conventions .....	5
<b>Connect Tunnel Service</b> .....	<b>6</b>
About Connect Tunnel Service .....	6
Installing Connect Tunnel Service .....	6
Importing the Client Certificate .....	8
Using Windows Services to run CTS .....	9
Using a Command or Script to run CTS .....	9
Troubleshooting .....	10
<b>Connect Tunnel Client for Windows</b> .....	<b>11</b>
About Connect Tunnel .....	11
Resources Available from Connect Tunnel .....	11
How to Tell if Connect Tunnel is Running .....	12
Running the Connect Tunnel Client .....	12
Downloading Connect Tunnel .....	13
Starting Connect Tunnel .....	13
Specifying a Login Group .....	16
Processing Server Certificates .....	18
Quitting Connect Tunnel .....	18
Configuring Connect Tunnel Settings .....	18
Viewing Current Connect Tunnel Settings .....	19
Configuring General Settings .....	19
Connecting to a Different VPN .....	20
Configuring Connections .....	20
Configuring a Default Connection .....	21
Establishing an Initial Network Connection .....	22
Updating the Connect Tunnel Software .....	23
Troubleshooting .....	23
Unable to Connect .....	23
Unable to Access Resources or the Internet .....	24
Working with Logs .....	24
<b>Connect Tunnel Client for Mac/Linux</b> .....	<b>26</b>
About Connect Tunnel .....	26
Starting Connect Tunnel .....	26
Connect Tunnel on MacOS .....	27
Connect Tunnel on Linux .....	27
Specifying a Login Group .....	28
Connecting to a Different VPN .....	28
Quitting Connect Tunnel .....	28

Managing Configurations .....	29
Viewing Connect Tunnel Settings .....	29
Editing Connect Tunnel Settings .....	30
Deleting a Configuration .....	30
Creating a New Configuration .....	31
Selecting the Advanced Button .....	31
Advanced Options .....	33
Credential Caching/Secure Network Detection .....	34
Processing Server Certificates .....	34
Configuring Proxy Server Settings (Linux Only) .....	35
Troubleshooting .....	35
Unable to Connect .....	36
Unable to Access Resources or the Internet .....	36
<b>SonicWall Support .....</b>	<b>37</b>
About This Document .....	38

# Introduction

- [About Connect Tunnel](#)
- [Connect Tunnel Service](#)
- [Connect Tunnel Client for Windows](#)
- [Connect Tunnel Client for Mac/Linux](#)
- [SonicWall Support](#)

## About Connect Tunnel

The *Secure Mobile Access (SMA) 12.1 Connect Tunnel User Guide* provides information on installing and using the Connect Tunnel Service and Connect Tunnel clients. A section on troubleshooting is also included.

 **NOTE:** SMA 12.1 provides the Central Management Service (CMS) with Global Traffic Optimization (GTO). To use this feature, you must upgrade to Connect Tunnel 12.1.

### Topics

- [Organization of This Guide](#)
- [Guide Conventions](#)

## Organization of This Guide

<b>Chapter 1 Introduction</b>	This chapter provides a summary of the chapters in this guide as well as a description of the conventions used.
<b>Chapter 2 Connect Tunnel Service</b>	This chapter provides instructions on installing and using Windows to run Connect Tunnel Service (CTS) as well as using a command line or script to run CTS.
<b>Chapter 3 Connect Tunnel Client for Windows</b>	This chapter provides instructions on downloading, installing, configuring, and operating the Secure Mobile Access (SMA) Connect Tunnel Client for Windows.
<b>Chapter 4 Connect Tunnel Client for Mac/Linux</b>	This chapter provides instructions on downloading, installing, configuring, and operating the SMA Connect Tunnel (CT) client for Mac and Linux.
<b>SonicWall Support</b>	This chapter provides SonicWall Support contact information.

# Guide Conventions

Convention	Use
<b>Bold</b>	Highlights dialog, window, screen names, parameter names, and icons and buttons.
Code	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. Also indicates emphasis on certain words in a sentence. Sometimes indicates the first instance of a significant term or concept.

# Connect Tunnel Service

- [About Connect Tunnel Service](#)
- [Installing Connect Tunnel Service](#)
- [Importing the Client Certificate](#)
- [Using Windows Services to run CTS](#)
- [Using a Command or Script to run CTS](#)
- [Troubleshooting](#)

## About Connect Tunnel Service

The Connect Tunnel Service client is a Windows server component of the SonicWall Secure Mobile Access (SMA 1000) solution that enables secure, authorized access to Web-based and client/server applications and Windows file shares.

In a server environment, you can install and configure an add-on component—CTS—so that the VPN connection starts automatically without user intervention: no user login is required and no user interface or icons are displayed.

For example, you may want to synchronize data between a remote system in the field and a file server secured behind the VPN at corporate headquarters. On the remote system—running the Windows Server platform—CTS is configured to run at a specific time, connect to the corporate file server, and synchronize its database with the master database at headquarters.

CTS is supported on Windows Server 2008 R2 and above.

## Installing Connect Tunnel Service

Using Connect Tunnel Service involves installing both Connect Tunnel (CT) and Connect Tunnel Service (CTS).

### *To install and configure Connect Tunnel Service:*

- 1 Log into the Appliance Management Console (AMC) on your SonicWall SMA 1000 Series appliance.
- 2 Navigate to the **Agent Configuration > Download** page.
- 3 Under **Client Installation Packages**, download the 32-bit or 64-bit installation packages for both Connect Tunnel and Connect Tunnel Service.
- 4 Install Connect Tunnel first (`ngsetup_<xx>.exe` or `ngsetup64_<xx>.exe`). A shortcut named **SonicWall VPN Connection** is created on the desktop.

- 5 Install Connect Tunnel Service (ctsssetup\_<xx>.exe or ctsssetup64\_<xx>.exe). A shortcut named **SonicWall VPN Service Options** is created on the desktop.



- 6 On the desktop, double-click the **SonicWall VPN Service Options** shortcut. Alternatively, double-click **SonicWall VPN Service Options** in the Control Panel. The **SonicWall VPN Service Properties** dialog appears.



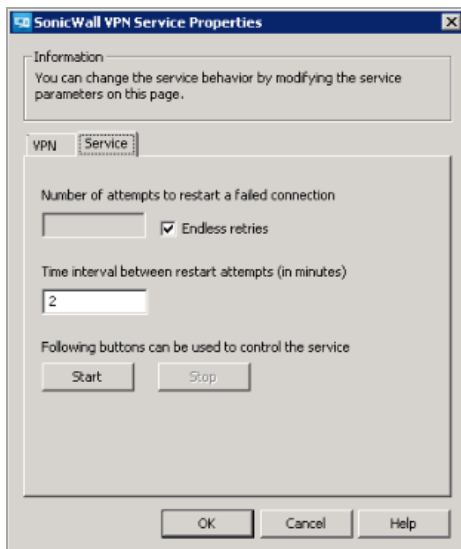
- 7 On the **VPN** tab, configure these settings:

<b>VPN Connection Name</b>	Type the name of the SonicWall Connect Client connection object exactly as it appears in the Windows <b>Network Connections</b> window ( <b>Start   Connect To   Show All Connections</b> ). By default, this is <b>SonicWall VPN Connection</b> .
<b>Hostname or IP address</b>	Type the host name or IP address of the SonicWall SMA 1000 Series appliance.
<b>Login group</b>	Type the name of the realm used by users in this login group.
<b>Username and Password</b>	Type the credentials for a user in this <b>Login group</b> . You must enter a username and password or a certificate CN. In some cases of chained authentication, both a username and certificate are required.
<b>Certificate CN</b>	A certificate's common name (CN) identifies its owner. Specify the CN for the certificate associated with this realm.

8 On the **Service** tab, configure the following settings:

<b>Number of attempts to restart a failed connection</b>	Specify how many times to attempt restarting if an initial connection attempt fails.
<b>Endless Retries</b>	Select this check box to continuously keep trying to connect until connected successfully.
<b>Time interval between restart attempts</b>	Specify the amount of time (in minutes) to wait between restart attempts.

9 Click the **Start** button. The **Start** and **Stop** buttons are used to control the service.



10 To verify that Connect Tunnel started, open the **SonicWall VPN Connection** shortcut on the desktop. You should see the established connection.

Alternatively, you can issue the `ipconfig` command on the command line to verify that you have a virtual IP address for the SonicWall VPN Connection.

## Importing the Client Certificate

The certificate specified for CTS must be located in the **Local Computer** certificate store of the user's device; certificates in a user's store are not available to the service. The Microsoft Management Console (MMC) is a tool for managing administrative tools, including snap-ins and extension snap-ins.

### *To import a certificate into the user's Local Computer store:*

- 1 To open the Microsoft Management Console, click the Windows start button and type `mmc` in the text field.
- 2 Press **Enter**.
- 3 In the **File** menu, choose the option for adding a snap-in.
- 4 To add a standalone snap-in, select **Certificates**, and then click the **Add >** button. Snap-ins can manage certificates for different accounts.
- 5 Select **Computer account**.
- 6 Click **Next**.



7 Select **Local computer**.

8 Click **Finish**.

You should now see **Certificates (Local Computer)** in the list of selected snap-ins. The certificate must now be copied to a certificate store.

9 In the Microsoft Management Console, right-click **Personal > Certificates** in the left navigation pane, and then select **All Tasks > Import**.

10 Specify the certificate file you want to import, along with its password.

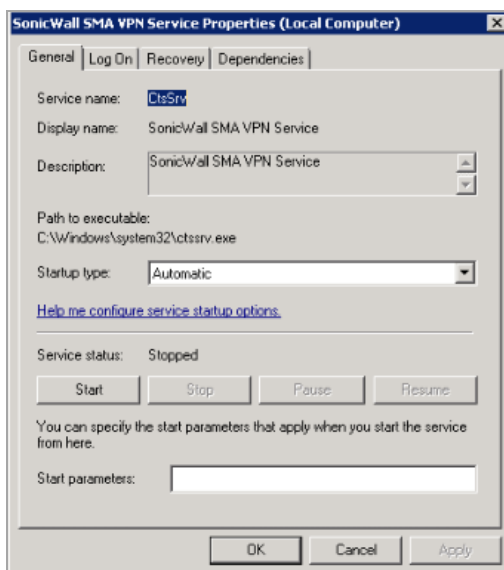
11 Place the certificate in your **Personal** store.

## Using Windows Services to run CTS

You can use Windows Services to manage CTS on a local or remote computer.

### *How to use Windows Services to configure and run CTS:*

- 1 On the Windows Server platform running Connect Tunnel Service, run Windows Services.
- 2 Open the SonicWall VPN Service Properties dialog (**Control Panel > Administrative Tools > Services > SonicWall SMA VPN Service**).



3 Use these settings to control the service (start, stop, pause, resume, or disable), set up recovery actions in case of service failure, or disable the service for a particular hardware profile.

4 Click **OK**.

## Using a Command or Script to run CTS

You can use the Windows `sc.exe` utility to communicate with Service Controller (`services.exe`) from the command prompt or in a batch file. This enables you to automate the startup and shutdown of the SonicWall VPN service.

In an environment where you want users to be able to start the VPN connection by clicking on a shortcut (and without being aware of the credentials), you could also create a shortcut on the desktop that launches a command or batch file. For example:

To start and stop Connect Tunnel Service on a remote computer use the following commands:

```
sc \\SERVERNAME start ctssrv  
sc \\SERVERNAME stop ctssrv
```

To start or stop the Connect Tunnel Service from the command line or a third-party application, invoke these commands:

```
%windir%\system32\sc.exe start ctssrv  
%windir%\system32\sc.exe stop ctssrv
```

## Troubleshooting

Use the Windows Event Viewer (**Control Panel > Administrative Tools > Event Viewer > Application**, where the **Source** is CTS) to view any information, warning, or error messages related to running Connect Tunnel Service.

For more detailed messages, look in the service log; the default location is:  
ALLUSERSPROFILE%\Application Data\SonicWall.

**i** | **NOTE:** If your environment includes an outbound HTTP proxy for access to the Internet, you must use one that does not require authentication; otherwise, you will see the following error message in the log file for CTS (ctssrv.log): Direct internet access is not available.

**i** | **NOTE:** You must also configure CTS to run under a Windows user account with administrative privileges.

# Connect Tunnel Client for Windows

- [About Connect Tunnel](#)
- [Running the Connect Tunnel Client](#)
- [Quitting Connect Tunnel](#)
- [Configuring Connect Tunnel Settings](#)
- [Updating the Connect Tunnel Software](#)
- [Troubleshooting](#)

## About Connect Tunnel

The Connect Tunnel client is a Windows client component of the Connect Tunnel (SMA) solution, which enables secure, authorized access to Web-based client/server applications and Windows file shares.

The Connect Tunnel client enables you to connect to network resources that are protected by the SonicWall SMA 1000 Series appliances.

Connect Tunnel is supported on Windows 7 and above and Windows 10 Anniversary Update and above. Windows Vista is not supported.

## Resources Available from Connect Tunnel

Connect Tunnel enables 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.

# How to Tell if Connect Tunnel is Running

When Connect Tunnel is running and connected to the VPN, an icon may appear in the taskbar notification area. If you pause on the icon with your cursor, connection status information will appear:



You can configure Connect Tunnel to not display this during active connections: for more information, see [Configuring Connect Tunnel Settings](#).

You can also verify the state of the Connect Tunnel VPN connection in the Windows **Network Connections** window.

## Viewing Connection Status Information

### *To view connection status information:*

- 1 On the **Start** menu, click **Control Panel**. Continue with the following steps, depending on your operating system. To display all available wireless, wired, dial-up, and VPN connections:
  - a Click **Network and Internet**.
  - b Click **Network and Sharing Center**.
  - c Click the **Connect to a network** link.
- 2 On the **View** menu, click **Details**.
- 3 In the **Dial-up** section, view connection status information for the Connect Tunnel connection.

**(i)** **NOTE:** Your administrator may have customized the name of this application.)

If Connect Tunnel experiences a temporary network interruption, a **red circle** with an **X** appears on the Connect Tunnel icon in the taskbar notification area. If the network connection is reestablished, the red circle with the X disappears, and the Connect Tunnel icon returns to its normal state.

## Running the Connect Tunnel Client

### Topics:

- [Downloading Connect Tunnel](#)
- [Starting Connect Tunnel](#)
- [Specifying a Login Group](#)
- [Processing Server Certificates](#)

# Downloading Connect Tunnel

Connect Tunnel can be downloaded from the WorkPlace menu. You must have administrator privileges to install the software.

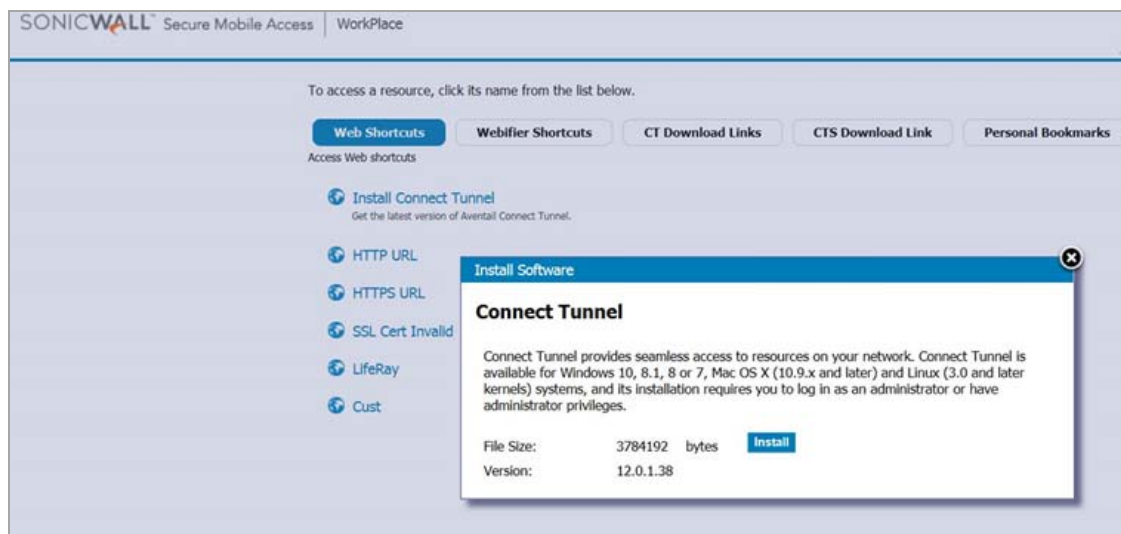
## To download Connect Tunnel:

- 1 Log in to WorkPlace.

Depending on your configuration, you might be issued a one-time password by your administrator, that allows you to download Connect Tunnel.



- 2 Enter the password that was sent to you. The Workplace application appears and allows you to download the software.
- 3 In WorkPlace, click the entry for **Install Connect Tunnel**.



- 4 Click **Install**. When the installation is complete, log out of Workplace.

# Starting Connect Tunnel

To access network resources through Connect Tunnel, you must first verify your identity. 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).

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

**To start Connect Tunnel:**

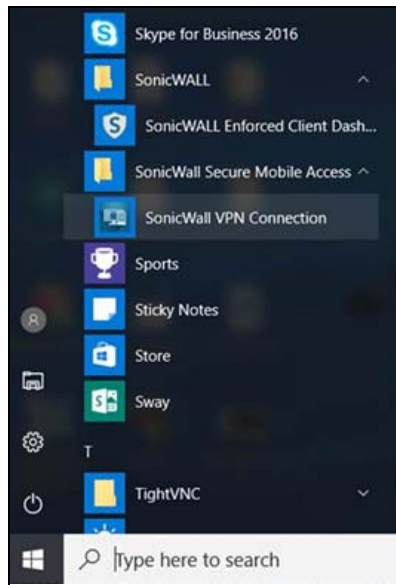
1 For:

- Windows 7, click on **Start > All Programs > SonicWall Secure Mobile Access > SonicWall VPN Connection**.



- For Windows 8.x and above:
  - 1) Click the **Start** button, then select either:
    - ① **NOTE:** Your administrator may have customized the name of this application.

- **All Programs > SonicWall VPN Connection**, point to **Connections**, select the Connect Tunnel connection you want to use.



- **Network > SonicWall VPN Connection**.



- 2) Click the **Connect** button.

- 2 You will see an initial login screen.



- 3 Enter your authentication credentials. Depending on how your administrator has configured Connect Tunnel, you may see a combination of these prompts:
  - 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 that was sent to you by your administrator.
  - 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 will be only one listed.
- 4 If an Acceptable Use Policy is displayed, click **Accept** to accept it.
- 5 Click **Connect**.

The Connect Tunnel icon appears in the taskbar 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 could send you a login that allows you to connect to a specific network.

**NOTE:** In the Connect Tunnel login dialog, you can click **Properties** to display the **Connect Tunnel Properties** dialog, where you can initiate a different connection or change program preferences. For more information, see [Configuring Connect Tunnel Settings](#).

## Specifying a Login Group

Connect Tunnel enables you to log in to different groups if necessary (for example, if you alternate between logging in to the Sales group and 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 offline (that is, when not connected to your VPN). You do not need administrative privileges to change a host name or login group.

### *To specify the login group:*

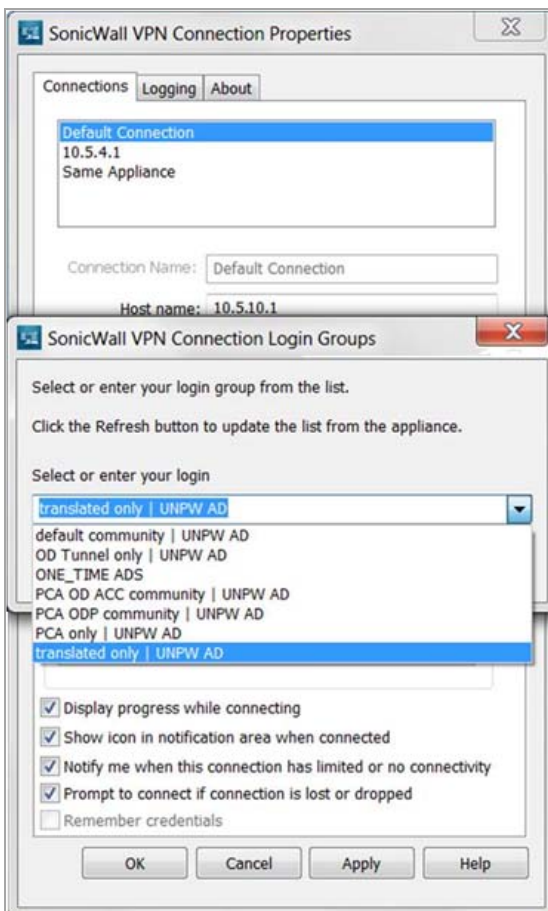
- 1 In the **Secure Mobile Access VPN Connection** login dialog, click **Properties**.



- To the right of the **Login group** field, click **Change**.



The **Secure Mobile Access VPN Connection Login Groups** dialog appears and displays the current list of login groups.



- 3 In the **Select or enter your login group** field, select or type the name of the login group you want to log in to.

If the correct login group does not appear in the list, click **Refresh** to update the list of available login groups.

Depending on how your administrator configured Connect Tunnel, some login groups may not appear in the list; however, you can still log in to a “hidden” login group (if you are authorized to do so) by typing its name in the **Select or enter your login group**.

- 4 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 essentially 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 will display 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 will continue without any prompt.

**i** **NOTE:** Connect Tunnel will process/warn only certificates of the VPN during the login process but not from resources. Applications, such as Internet Explorer, 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 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 will continue.

Similarly, you may be asked to accept a license agreement or Acceptable Use Policy.

## Quitting Connect Tunnel

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

### *To quit Connect Tunnel:*

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

## Configuring Connect Tunnel Settings

This section describes how to view and configure the Connect Tunnel client settings. You must have administrator privileges on your computer to change any of these settings.

## Topics:

- [Viewing Current Connect Tunnel Settings](#)
- [Configuring General Settings](#)
- [Connecting to a Different VPN](#)
- [Configuring Connections](#)
- [Configuring a Default Connection](#)
- [Establishing an Initial Network Connection](#)

# Viewing Current Connect Tunnel Settings


## *To view current Connect Tunnel settings:*

- 1 On the **Start** menu, click **Control Panel**. Continue with the following steps depending on your operating system. To display all available wireless, wired, dial-up, and VPN connections:
  - a Click **Network and Internet**.
  - b Click **Network and Sharing Center**.
  - c Click the **Connect to a network** link.
- 2 In the **Dial-up** section, right-click the name of the Connect Tunnel connection (your administrator may have customized the name of this application), and then click **Properties**. The **Connect Tunnel Properties** dialog appears.
- 3 Review the information on the **Connection** and **About** tabs:
  - Click the **Connections** tab to view the current connection settings.
  - Click the **About** tab to view basic information about the application.
  - Click **File Info** on the **About** tab for more detailed information.

# Configuring General Settings

This section describes how to configure general settings for Connect Tunnel.

## *To configure general Connect Tunnel settings:*

- 1 On the **Start** menu, click **Control Panel**. Continue with the following steps depending on your operating system. To display all available wireless, wired, dial-up, and VPN connections:
  - a Click **Network and Internet**.
  - b Click **Network and Sharing Center**.
  - c Click the **Connect to a network** link.
- 2 In the **Dial-up** section, right-click the name of the Connect Tunnel connection.  
 **NOTE:** Your administrator may have customized the name of this application).
- 3 Click **Properties**. The Connect Tunnel **Properties** dialog appears.
- 4 Click the **Connections** tab, and configure the Connection settings as necessary. To display:


- A status bar during the connection process, select the **Display progress while connecting** checkbox.
- The Connect Tunnel icon in the taskbar notification area during active connections, select the **Show icon in notification area when connected** checkbox.
- A notification if the network connection is experiencing limited or no connectivity, select the **Notify me when this connection has limited or no connectivity** checkbox.
- A prompt to establish a new connection if network connectivity is lost, select the **Prompt to connect if connection is lost or dropped** checkbox.

5 Click **OK**.

## Connecting to a Different VPN

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

- 1 On the **Start** menu, click **Control Panel**. Continue with the following steps depending on your operating system. To display all available wireless, wired, dial-up, and VPN connections:
  - a Click **Network and Internet**.
  - b Click **Network and Sharing Center**.
  - c Click the **Connect to a network** link.
- 2 In the **Dial-up** section, right-click the name of the Connect Tunnel connection.
 

 **NOTE:** Your administrator may have customized the name of this application).
- 3 Click **Properties**. The Connect Tunnel **Properties** dialog appears.
- 4 Click the **Connections** tab, and then, in the **Host name or IP address of the VPN** field, type the host name or the IP address of the VPN you want to connect to.
- 5 Click **OK**.

## Configuring Connections

Clicking the **Properties** button on the login menu takes you to the **Connections** tab, which contains the list of connections and their associated properties, along with operations for modifying, adding, and deleting connections.

The **Connections** tab list shows all of the connections configured for the client machine. Selecting one item from the list populates all data fields under the **Properties** section for both the **Connection** and **Logging** tabs.

**Default Connection** is a connection you can use to modify and/or connect to an appliance to pull down the administrator-defined list of connections.

The **Properties** section is hidden for AMC Administrator defined connections, visible for **Default Connection**.

The **Connections** tab contains general parameters for the selected connection.

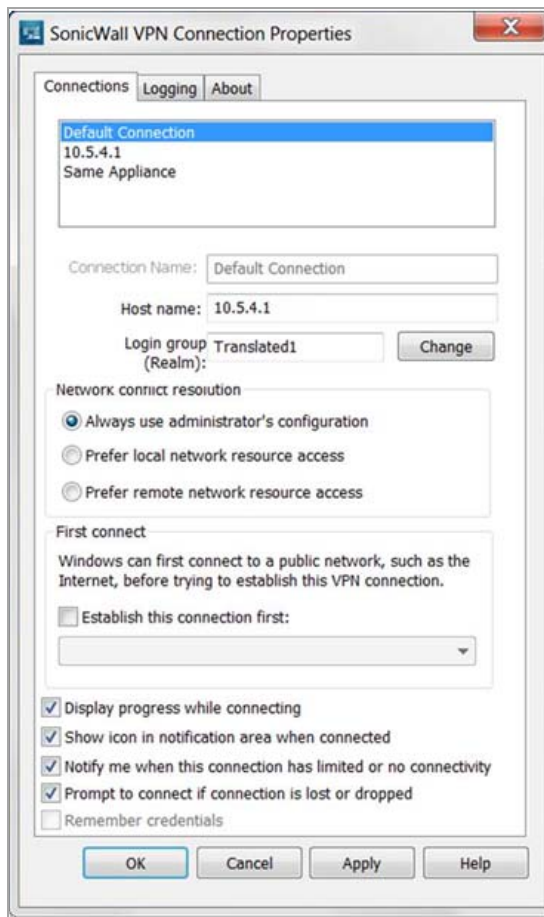
**Connection Name** shows a user-friendly name for the connection, used in the connection display list. It is disabled for **Default Connection**.

# Configuring a Default Connection

The login for your Connect Tunnel may have the option for default connections. In this case, **Default Connection** is available in the **Connections** list.



If **Default Connection** is selected, clicking the **Properties** button brings up the **Connections Properties** dialog.



The **Connections** tab displays information about the Host name and Login group (Realm). If you wish to change login groups, clicking **Change** will allow you to choose from a list of your current login groups. If no other groups are available, click **Cancel** to return to the **Connection** dialog.

The **Network Conflict Resolution** section allows you to choose what type of network conflict resolution should be performed. If Network Conflict Resolution is administrator controlled by community settings, this section is not available.

The **First Connect** section allows you to establish an Internet connection prior to establishing a VPN connection. This is most often used when establishing connections by running dialup over VPN. To use this option, select the Establish this connection from check box and then select from the drop-down list of connections.

**Display progress while connecting** is an option that controls whether or not to display the logon sequence messages while the connection is being established. This includes, but is not limited to: Authentication, EPC Checks and VPN Establishment.

**Show icon in notification area** is an option that lets you specify whether or not the Secure Mobile Access VPN Connection icon (Knight head) is displayed in the Windows system tray.

**Notify me when this connection has limited or no connectivity** is an option that lets you see messages about possible connection problems (slowness, packet loss, etc.) that may be incurred while Connect Tunnel is running.

**Prompt to connect if connection is lost or dropped** is an option that controls whether or not the **Secure Mobile Access VPN Connection** login dialog pops back up if the connection is dropped or lost for any reason.


When finished making your choices, click **OK**. Connect Tunnel saves the current configuration and closes the **Connection Properties** dialog.

## Establishing an Initial Network Connection

In some cases, you may need to establish a network connection before you can connect to the VPN; this is usually necessary only if you use a dial-up connection to connect to the Internet.

This section describes how to configure a connection that must be established before you connect to the VPN.

### *To configure a first connection:*

- 1 On the **Start** menu, click **Control Panel**. Continue with the following steps depending on your operating system. To display all available wireless, wired, dial-up, and VPN connections:
  - a Click **Network and Internet**.
  - b Click **Network and Sharing Center**.
  - c Click the **Connect to a network** link.
- 2 In the **Dial-up** section, right-click the name of the Connect Tunnel connection.  
 **NOTE:** Your administrator may have customized the name of this application).
- 3 Click **Properties**. The Connect Tunnel **Properties** dialog appears.
- 4 Click the **Connections** tab and then, under **First connect**, select the **Establish this connection first** checkbox.
- 5 From the list, select the connection that must be established first, and then click **OK**.

# Updating the Connect Tunnel Software

Your 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 to make software updates available to you, and when.

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

## *To download and install a software update:*

- During login, if the **Connect Tunnel Software Update** dialog appears and indicates that a software update is available, the available options depend on how your administrator has configured software updating:
  - Click **Update** to immediately download and install the software update. If you select this option, the software update will be installed, and then the login process will continue.
  - Click **Remind Me Later** to postpone the software update and continue logging in. If you select this option, Connect Tunnel will reprompt you (once per day) until you download and install the update by clicking **Update**. 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.

## 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 Connect](#)
- [Unable to Access Resources or the Internet](#)
- [Working with Logs](#)

## 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 [How to Tell if Connect Tunnel is Running](#).
- 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 [Connecting to a Different VPN](#).
- Verify in the **Connect Tunnel Properties** dialog that you are initiating a connection to the correct login group. For more information, see [Specifying a Login Group](#).
- If you use a personal firewall, you may need to configure the firewall before you can access your VPN. To do this, configure the firewall to allow `ngvpnmgr.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**.

# 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 that's 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 Secure Mobile Access VPN Connection **Properties** dialog, on the **Connections** tab. The **Network conflict resolution** options are available only when your administrator has configured you for split tunnel mode. If you need to make a configuration change, it must be done while the 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 it 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 Secure Mobile Access VPN Connection **Properties** dialog, click the **Connections** tab, and then click **Prefer local network resource access** for your session.

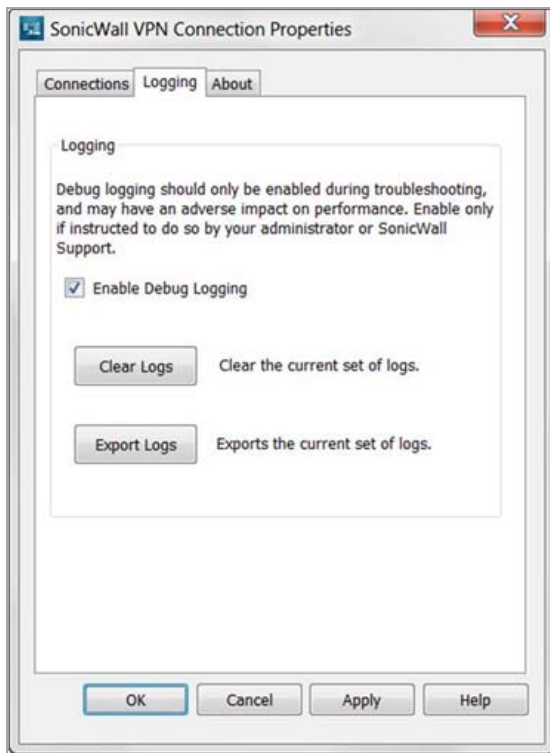
## Working with Logs

You may need to respond to an administrator request to enable debug logs, to reproduce a problem, or download logs for another reason.

- 1 To enable logging, click the **Properties** button.



- 2 Click on the **Logging** tab.



- 3 Clear the existing log by clicking **Clear Logs**, then click **Apply**.
- 4 Select the checkbox for **Enable Debug Logging** and click **OK**. Let the log run for the specified time. The log will be named according to the formula:  
`ngutil-YYYYMMDD_at_HHMMSS.txt`
- 5 When you want to export the log, return to the **Settings** tab, click **Export Logs**, and then click **OK**.

# Connect Tunnel Client for Mac/Linux

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

## 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. This section describes Connect Tunnel for the MacOS and Linux operating systems and consists of the following sections:

With Connect Tunnel, you can connect to network resources that are protected by the Secure Mobile Access VPN and access the following types of resources:

- **Client/server resources:** Client/server applications, thin client applications, and terminal services.
- **Web sites and applications:** Web content and Web-based applications that can be accessed through a browser.
- **Network shares:** Shared folders and files, and mapped drives.

Connect Tunnel on MacOS and Linux platforms supports IPv6, which is preferred if both IPv4 and IPv6 are available.

## System Requirements

This client application requires JVM (Java Virtual Machine) and is intended for use on 32-bit and 64-bit Linux computers and Apple Macintosh-based PPC/IA-32 and PPC/IA-64 computers.

## 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.  
**i** | **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.)
- 7 Click **OK**. A message in the login dialog indicates the status of the VPN connection.  
**i** | **TIP:** In the Connect Tunnel login dialog, you can initiate a connection to a list.  
**i** | **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. 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.
- i** | **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 appears.

## How to Tell if Connect Tunnel is Running

When Connect Tunnel is running and connected to the VPN, a connection status dialog appears. This dialog contains basic connection information, including the name of the configuration you are currently using and the host name or IP address of the VPN you are connected to. You can minimize this dialog' on Linux systems, however, closing this dialog will end your network connection and close Connect Tunnel.

# 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:

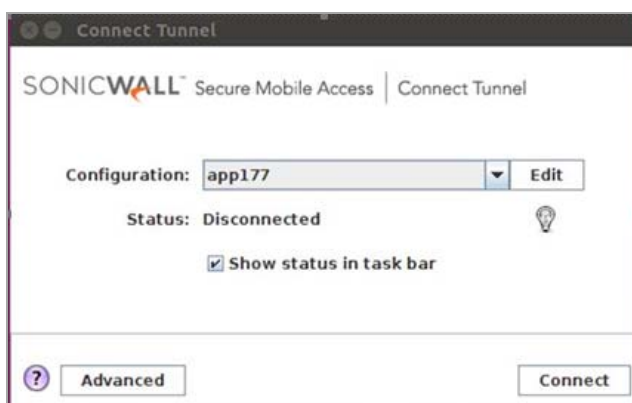
- [Viewing Connect Tunnel Settings](#)
- [Editing Connect Tunnel Settings](#)
- [Deleting a Configuration](#)
- [Creating a New Configuration](#)
- [Selecting the Advanced Button](#)
- [Advanced Options](#)
- [Credential Caching/Secure Network Detection](#)

## Viewing Connect Tunnel Settings

 **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.

# Editing Connect Tunnel Settings

**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 **Save** to save your changes.

# Deleting a Configuration

**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** to delete the configuration.

# Creating a New Configuration

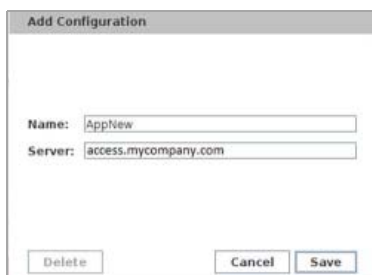
**NOTE:** Connect Tunnel must be offline; that is, not connected to your VPN (**Status: Disconnected**).

*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.
- 4 Click **Save** to save your changes.

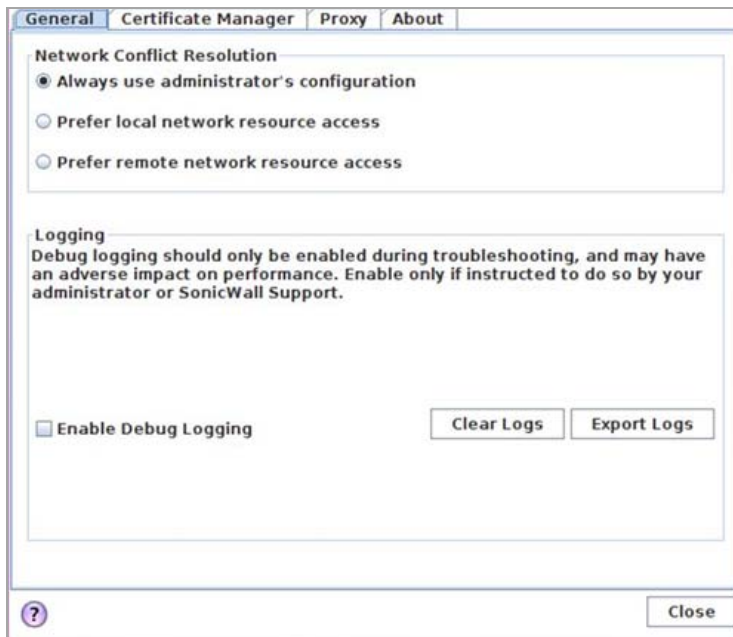


# Selecting the Advanced Button

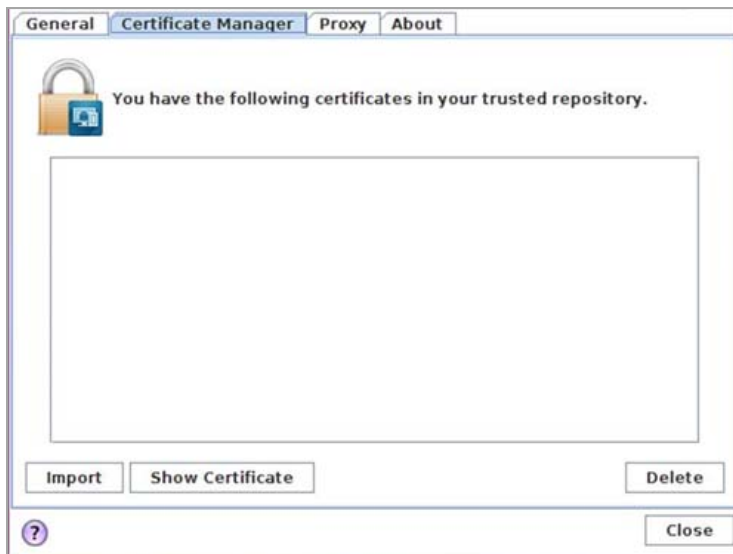
**NOTE:** Connect Tunnel must be offline; that is, not connected to your VPN (**Status: Disconnected**).

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

## General



## Certificate Manager





## Proxy

Type	Proxy address to use	Port
SSL:	<input type="text"/>	<input type="text"/>
HTTP:	<input type="text"/>	<input type="text"/>
FTP:	<input type="text"/>	<input type="text"/>
SOCKS:	<input type="text"/>	<input type="text"/>

Example: verisign.com, 192.168.1.0/24

## About

Connect Tunnel  
Version 12.0.1.022  
© 2017 SonicWall Inc. All rights reserved.

SONICWALL, the SONICWALL Logo and SONICWALL CONNECT TUNNEL are trademarks or registered trademarks of SonicWall Inc. All other trademarks are property of their respective owners.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT, OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use, or other dealings in this Software without prior written authorization of the copyright holder.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)

## 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. The **Network conflict resolution** options are available only when your administrator has configured you for split tunnel mode for this particular VPN configuration. 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. However, on the 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.

**i** **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 Connect](#)
- [Unable to Access Resources or the Internet](#)

# 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 [How to Tell if Connect Tunnel is Running](#).
- 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 [How to Tell if Connect Tunnel is Running](#).
- 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.

# 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. The **Network conflict resolution** options are available only when your administrator has configured you for split tunnel mode. If you need to make a configuration change, it must be done while the 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.

# SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

# About This Document

## Legend



**WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.



**CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



**IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Connect Tunnel User Guide  
Updated - November 2017  
Software Version - 12.1  
232-004069-00 Rev A

## Copyright © 2017 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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. SonicWall Inc. 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/en-us/legal/license-agreements>. Select the language based on your geographic location to see the EUPA that applies to your region.

## Open Source Code

SonicWall 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 US 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request  
SonicWall Inc. Attn: Jennifer Anderson  
5455 Great America Parkway  
Santa Clara, CA 95054