

Mobile Connect for macOS 5.0

User Guide

SONICWALL®

Contents

Introduction to Mobile Connect	4
How Mobile Connect Works	4
New Features in Mobile Connect 5.0	5
Supported Platforms	6
Apple Product Support	6
SonicWall Appliance Support	6
Required Network Information	7
Installing and Connecting	9
Installing Mobile Connect	9
Creating and Saving Connections	10
Creating Firewall or SMA 100 Series Connections	10
Creating SMA 1000 Series Connections	13
Connecting to the Mobile Connect Server	14
Configuring Client Certificates	16
Configuring Client Certificates with SMA 1000 Series	16
Configuring Client Certificates with SMA 100 Series	17
Enabling Connect on Demand	18
Enabling Connect on Demand with SMA 1000 Series	18
Enabling Connect on Demand to SMA 100 Series	19
Preferences and URL Control	21
Preferences Overview	21
Additional SMA 1000 Series Options	22
Using Apple Configurator 2 with Mobile Connect	23
URL Control Syntax and Parameters	26
Using the addprofile Command	27
Using the connect Command	28
Using the disconnect Command	29
Using the callbackurl Command Parameter	29
Monitoring, Logs, and Troubleshooting	32
Monitoring Mobile Connect	32
Using Mobile Connect Help and Log Options	34
Troubleshooting Mobile Connect	34

SonicWall Support	36
About This Document	37

Introduction to Mobile Connect

SonicWall Mobile Connect for macOS is an application for Mac systems running macOS 14.x (Sonoma), macOS 13.x (Ventura), macOS 12.x (Monterey), and macOS 11.x (Big Sur), that enables secure, mobile connections to private networks protected by SonicWall security appliances.

Topics:

- [How Mobile Connect Works](#)
- [New Features in Mobile Connect 5.0](#)
- [Supported Platforms](#)

How Mobile Connect Works

Modern business practices increasingly require that users be able to access any network resource (files, internal websites, etc.), anytime, anywhere. At the same time, ensuring the security of these resources is a constant struggle. While most users are aware that they must take care to protect computers from network security risks, this security awareness does not always extend to Mac devices like the MacBook Air and MacBook Pro. And yet, Macs are increasingly subject to security attacks. Furthermore, remote Mac users can often use insecure, untrusted, public WiFi hotspots to connect to the Internet. It is therefore a challenge to provide secure, mobile access while still guarding against the inherent security risks faced by mobile users.

The SonicWall Mobile Connect for macOS app provides secure, mobile access to sensitive network resources. Mobile Connect establishes a Secure Socket Layer Virtual Private Network (SSL VPN) connection to private networks that are protected by SonicWall security appliances. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

Perquisite:

- Ensure that the Firewall or SMA 100 series being used by Mobile Connect is connected to the network.

To get started with SonicWall Mobile Connect:

1. Install SonicWall Mobile Connect from the Mac App Store.
2. Configure network information like server name, username, password, and so on.

3. Initiate a connection to the network.

Mobile Connect establishes a SSL VPN tunnel to the SonicWall security appliance.

You can now access resources on the private network. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

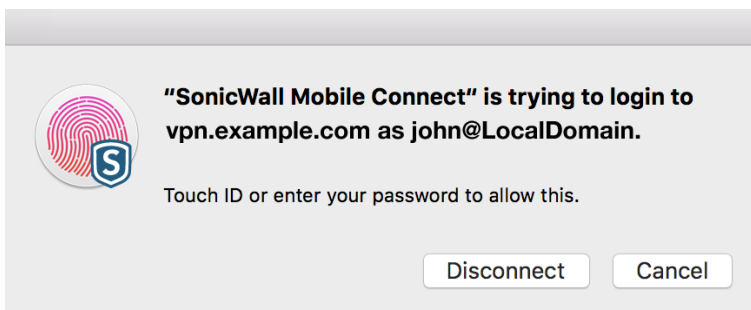
New Features in Mobile Connect 5.0

The following enhancements are included in the Mobile Connect 5.0 release.

- **macOS High Sierra Compatibility** - Mobile Connect is fully optimized for the latest release of macOS High Sierra.
- **Network Extension Support** - Mobile Connect now leverages Apple's current VPN framework, called Network Extension, to allow for more reliable VPN connectivity on macOS devices. After upgrading to the 5.0 version, Mobile Connect may need to be re-provisioned, including updating VPN connection configurations and certificates (if applicable).
- **Touch Bar Support** - On supported MacBook Pros, the Touch Bar at the top of the Mac keyboard adapts to what you're doing and gives you intuitive shortcuts and app controls when you need them. Mobile Connect now supports Touch Bar for all supported Mac devices.



- **Touch ID Support** - Touch ID may be used as a seamless alternative to username and password authentication if allowed by the VPN server. Requires compatible server with configured Touch ID policy, as well as a Mac with a configured Touch ID sensor.



- **Global HA Support** - Mobile Connect contains updates for the global high availability and disaster recovery capabilities for VPN connections to SMA1000 series servers running 12.4.1 or newer firmware.
- **SAML Authentication** - Latest Mobile Connect support SAML authentication with SMA100 and SMA1000 as well, enabling Mobile Connect to authenticate against third-party SAML IdP servers.

Supported Platforms

The following sections describe the supported platforms and network information for Mobile Connect:

- [Apple Product Support](#)
- [SonicWall Appliance Support](#)
- [Required Network Information](#)

Apple Product Support

SonicWall Mobile Connect 5.0 for macOS is supported on all Mac models running the following macOS versions:

- macOS 10.x (Catalina)
- macOS 11.x (Big Sur)
- macOS 12.x (Monterey)
- macOS 13.x (Ventura)
- macOS 14.x (Sonoma)

The following Mac models are supported:

- MacBook (Early 2015 or newer)
- MacBook Air (Mid 2012 or newer)
- MacBook Pro (Mid 2012 or newer)
- Mac mini (Late 2012 or newer)
- iMac (Late 2012 or newer)
- iMac Pro (2017)
- Mac Pro (Late 2013 or newer)

For information about supported models for earlier versions of macOS, refer to <https://www.apple.com/>.

SonicWall Appliance Support

SonicWall Mobile Connect for macOS is an app for Macs running macOS 14.x (Sonoma), macOS 13.x (Ventura), macOS 12.x (Monterey), and macOS 11.x (Big Sur), that enables secure, mobile connections to private networks protected by SonicWall security appliance:

- SonicWall Gen7 TZ firewalls running SonicOS 7.
- SonicWall firewall appliances running SonicOS 6.5.4.9 or higher

- Secure Mobile Access (SMA) 100 Series appliances running SMA 10.2 or higher
- Secure Mobile Access (SMA) 1000 Series appliances running SMA 12.4.1 or higher

SonicWall Mobile Connect connects to all SMA 1000, SMA 100 and SonicWall firewalls that support either SonicWall VPN Connections (SMA 1000) or NetExtender connections (SMA 100 and Firewalls).

Required Network Information

To use Mobile Connect, you need the following information from your network administrator or IT Support:

- **Server name or address** - This is either the IP address or URL of the SSL VPN server to which you are connecting. The SSL VPN server can be any supported SonicWall appliance. See [SonicWall Appliance Support](#).
- **Username and password** - Typically, you are required to enter your username and password, although some connections might not require this.
- **Domain name** - The domain name of the SSL VPN server. Mobile Connect might be able to automatically determine this when it first contacts the server, or there could be multiple domains that can be selected.

DNS Domain Settings on Appliances


Before Mobile Connect users are able to access the private network, the network administrator must configure the DNS Domain on the SonicWall appliance. When the Mobile Connect user accesses a URL on the private network, the configured DNS domain is used to resolve the hostname lookup. For public domains that do not match the configured DNS domain, the DNS server for the WiFi, Ethernet, or cellular network is used.

① **NOTE:** The Mobile Connect user does not need to perform any configuration tasks related to DNS. The following information is for SonicWall network administrators.

The DNS Domain configuration process varies, depending on the type of SonicWall appliance being used:

- **SonicWall firewall appliances** - On the **SSL VPN > Client Settings**, enter the DNS domain name in the **DNS Domain** field.
- **SonicWall SMA100 Series** - The DNS domain can be configured either globally, at the group level, or at the individual user level:
 - **Global level** - On the **Network > DNS**, enter the DNS domain name in the **DNS Domain** field.
 - **Group level** - On the **Users > Local Groups**, click the edit icon for the group. Click on the **NX Settings** tab and enter the DNS domain in the **DNS Domain** field.
 - **User level** - On the **Users > Local Users**, click the edit icon for the user.
 - Click on the **NX Settings** tab and enter the DNS domain in the **DNS Domain** field.
- **SonicWall SMA1000 Series** - The DNS domain can be configured either globally or for specific IP address pools:
 - **Global level** - From the main navigation menu in the Appliance Management Console (AMC), click **Network Settings**. In the Name resolution area, click **Edit**. The Configure Name Resolution page

appears. Enter the DNS domain name in the **Search domains** field.

- **IP address pool level** - From the main navigation menu in the AMC, click **Services**. Under Access services, in the Network tunnel service area, click **Configure**. The Configure Network Tunnel Service page appears.
 1. Click the name of the IP address pool you want to edit.
The Configure IP Address Pool page appears.
 2. In the **Advanced**, click the  arrow icon.
 3. Select **Customize default settings** and enter the DNS domain name in the **Search domains** field.

Installing and Connecting

This section describes how to install Mobile Connect on your device and how to configure and initiate a VPN connection using Mobile Connect.

Topics:

- [Installing Mobile Connect](#)
- [Creating and Saving Connections](#)
- [Connecting to the Mobile Connect Server](#)
- [Configuring Client Certificates](#)
- [Enabling Connect on Demand](#)

Installing Mobile Connect

SonicWall Mobile Connect is installed through the Mac App Store.

To download and install the Mobile Connect app:

1. On your Mac, click on the App Store icon.



2. In the **Search** field, type `SonicWall Mobile Connect`, and press **Return**.
3. In the search results, select **SonicWall Mobile Connect**.
4. Click **Free** and then **Install**. The app installs on your Mac. When installation is complete, the SonicWall Mobile Connect icon appears in your **Applications** folder and in Launchpad.



① **NOTE:** If you encounter an error when attempting to download SonicWall Mobile Connect, see the Mac App Store Support web site, where you can find troubleshooting procedures and instructions on how to report the issue to Apple Support if necessary: <http://www.apple.com/support/mac/app-store/>

Creating and Saving Connections

The process of creating a Mobile Connect connection is slightly different depending on the type of SonicWall appliance to which you are connecting.

- [Creating Firewall or SMA 100 Series Connections](#)
- [Creating SMA 1000 Series Connections](#)

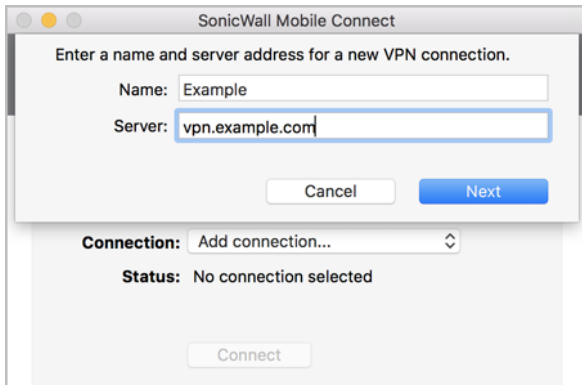
Creating Firewall or SMA 100 Series Connections

To create and save a new connection to a SonicWall network security appliance and SMA100 Series:

1. The first time you launch Mobile Connect, you must add a VPN connection before you can connect.
2. Select **Add connection** from the **Connection** list.



3. In the **Name** field on the popup dialog, type in a descriptive name for the connection.
4. In the **Server** field, type in the hostname or IP address of the server (firewall or SMA 100 Series).



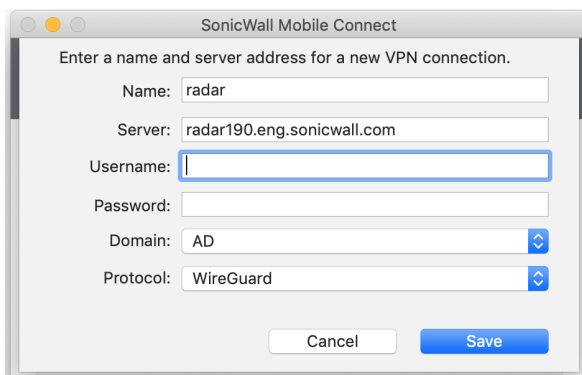
5. Click **Next**.

Mobile Connect attempts to contact the SonicWall appliance.

If the attempt fails, a warning message displays, asking if you want to save the connection. Verify that the server address or URL is spelled correctly, and then click **Save**.

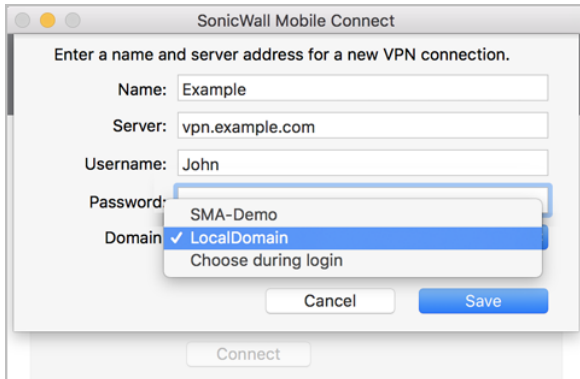


6. If Mobile Connect successfully contacts the server, you are prompted to enter your username and password, unless the server does not require this information.
7. Type your credentials into the **Username** and **Password** fields.

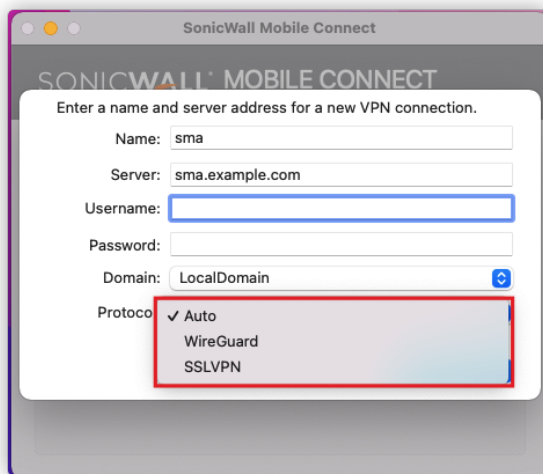


NOTE: If the previous screenshot does not match what is displayed on your device, you are connecting to a SonicWall SMA 1000 Series. See [Creating SMA 1000 Series Connections](#).

8. The **Domain** field is auto-populated with the default domain from the server. To select a different domain, click **Domain** to display a drop-down menu of the available options and then select the correct domain.



9. The **Protocol** field is auto-populated with the default VPN from the server. To select a different VPN, click **Protocol** to display a drop-down menu of the available options and then select the required VPN.
- **Auto**: Selecting **Auto** connects the VPN according to the preference setting of the appliance.
 - **WireGuard**: Selecting **WireGuard** connects to **WireGuard**.
 - **SSLVPN**: Selecting **SSLVPN** connects to **SSLVPN**.



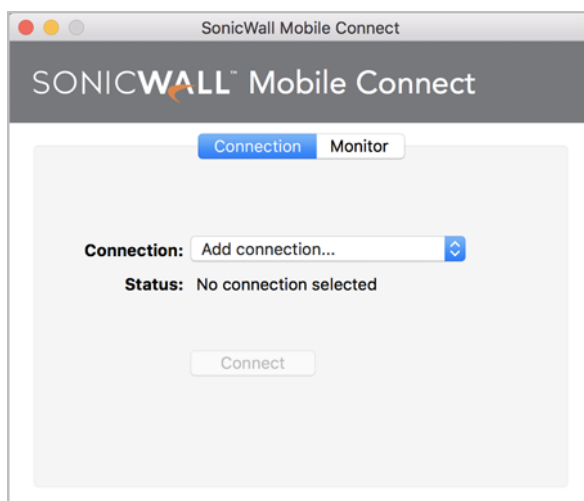
① **NOTE:** The **Protocol** selection is not displayed when you are connected to a SonicWall SMA 1000 Series.

10. Click **Save** to create the new connection.

Creating SMA 1000 Series Connections

To create and save a new connection to a SonicWall SMA 1000 Series:

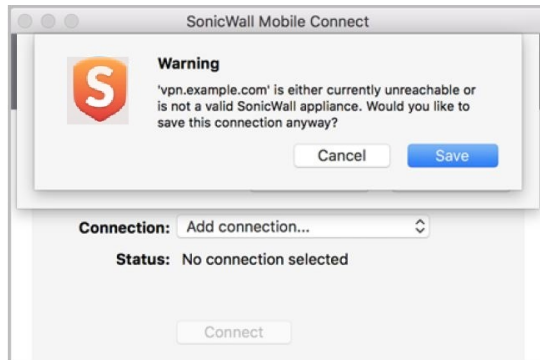
1. The first time you launch Mobile Connect, you must add a VPN connection before you can connect.
2. Select **Add connection** from the **Connection** list.



3. In the **Name** field on the popup dialog, type in a descriptive name for the connection.
4. In the **Server** field, type in the hostname or IP address of the server (SMA 1000 Series).



5. Click **Next**. Mobile Connect attempts to contact the SonicWall appliance.
 - If Mobile Connect contacts the appliance successfully, the server connection is added to the list of saved connections.
 - If the attempt fails, a warning message displays, asking if you want to save the connection. Verify that the server address or URL is spelled correctly, and then click **Save**.

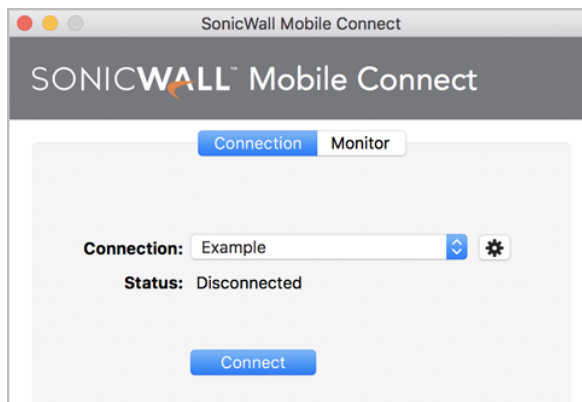


- Clicking **Save** adds the server connection to the list of saved connections.

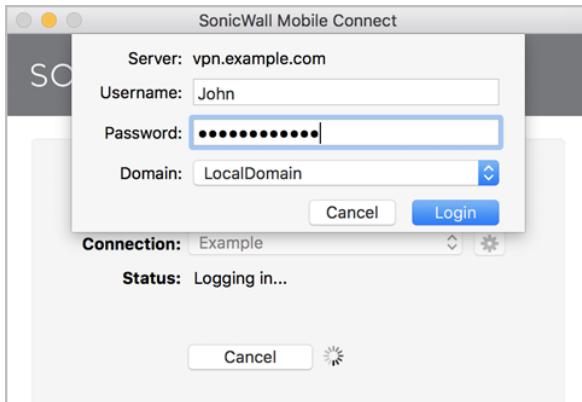
Connecting to the Mobile Connect Server

To establish a Mobile Connect session:

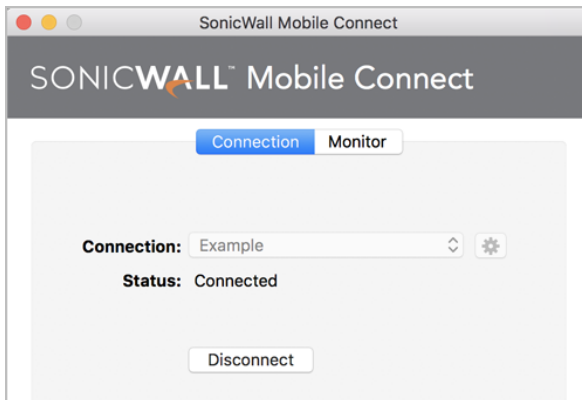
1. In the **Connection** list, select the connection that you want to initiate.



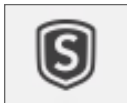
2. Click **Connect**.
3. Type your credentials into the **Username** and **Password** fields, if prompted (depending on whether the appliance you are connecting to allows for saving usernames and passwords), and then click **Login**.



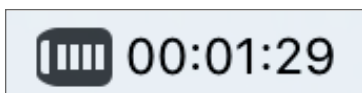
4. When the connection is successfully established, the **Status** row changes to **Connected** and the **Connect** button changes to **Disconnect**.



After connecting, you can access your Intranet network with other apps. The Mobile Connect menu bar icon indicates the connected state.



The native Mac system **VPN Status** in the menu bar can also be displayed from the **System Preferences** app under **Network**. The **VPN Status** icon changes to the connected state, and the connection time can be shown.



If the VPN connection is interrupted, the menu bar icons change to indicate that you are no longer connected or that Mobile Connect is reconnecting the VPN, and you are no longer able to access the Intranet network. This can happen if your device connection transitions from one WiFi network to another WiFi network or to another network type.

If the VPN disconnects, return to SonicWall Mobile Connect to reestablish the connection. Optionally, you can enable the **Automatic Reconnect** option in the Mobile Connect app **Preferences** to have Mobile Connect automatically attempt to reestablish interrupted connections.

Configuring Client Certificates

Client certificate support is only available for connections to SMA 1000 Series and SMA 100 Series.

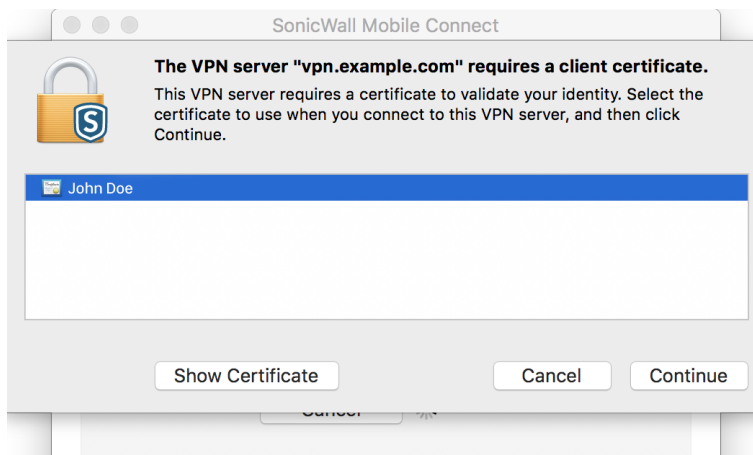
- [Configuring Client Certificates with SMA 1000 Series](#)
- [Configuring Client Certificates with SMA 100 Series](#)

Configuring Client Certificates with SMA 1000 Series

If a client certificate is required during authentication, you are automatically prompted to select a client certificate that is present in your keychain in macOS.

To configure the client certificate on your Mac:


1. Initiate a connection to the SMA 1000 Series. You are prompted to choose the certificate.

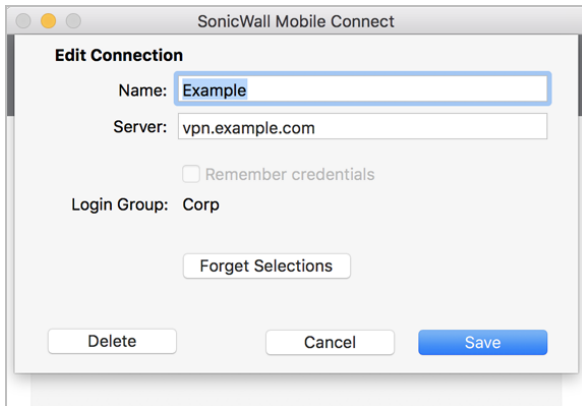


2. Select the client certificate from the list of certificates and then click **Continue**.

If you successfully authenticate with a client certificate, the VPN connection profile is automatically updated to use the client certificate for each subsequent connection attempt.

To reset the client certificate selection when disconnected:

1. In the **Connections** list, select the connection and click the **Edit** icon  to edit it.
2. Click the **Forget Selections** button.



① **NOTE:** If no client certificates are installed, an error message is shown indicating that no matching client certificates are present on your device. The Keychain Access app (in Applications/Utilities) can be used to view client certificates.

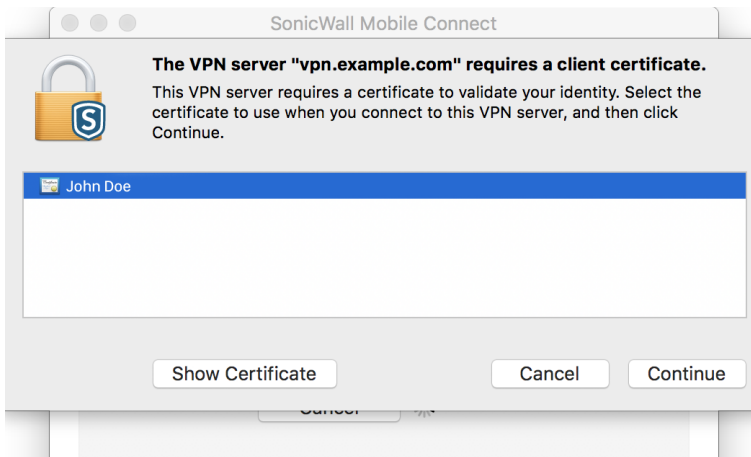
3. Click the **My Certificates** category to easily see available client certificates.

Configuring Client Certificates with SMA 100 Series

If a client certificate is required during authentication, you are automatically prompted to select a client certificate that is present in your keychain in macOS. Single factor client certificate authentication is supported for connections to SonicWall SMA 100 Series.


To configure the client certificate on your Mac:

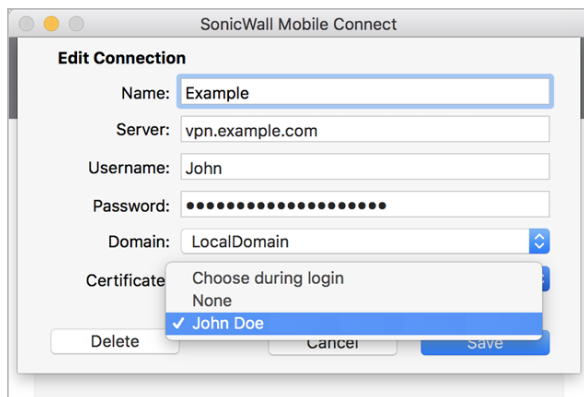
1. Initiate a connection to the SMA 100 Series. You are prompted to choose the certificate.



2. Select the client certificate from the list of certificates and then click **Continue**. By default, the client certificate is set to **Choose during login** for a VPN connection.


To modify the client certificate setting when disconnected:

1. In the **Connections** list, select the connection and click the **Edit** icon  to edit it.
2. In the **Certificate** field, select the appropriate client certificate option and then click **Save**.



Enabling Connect on Demand

The Connect on Demand feature provided by Mobile Connect provides the ability to automatically establish a VPN connection when you attempt to access a domain on the private network. To support Connect on Demand, a VPN connection should not request any user interaction. This provides a seamless VPN connectivity experience without the need to manually launch Mobile Connect.

 | **NOTE:** Connect on Demand is only available for connections to SMA 1000 Series and SMA 100 Series.

See the following:

- [Enabling Connect on Demand with SMA 1000 Series](#)
- [Enabling Connect on Demand to SMA 100 Series](#)

Enabling Connect on Demand with SMA 1000 Series

A VPN configuration on the SMA 1000 Series must meet the following requirements to support Connect on Demand:

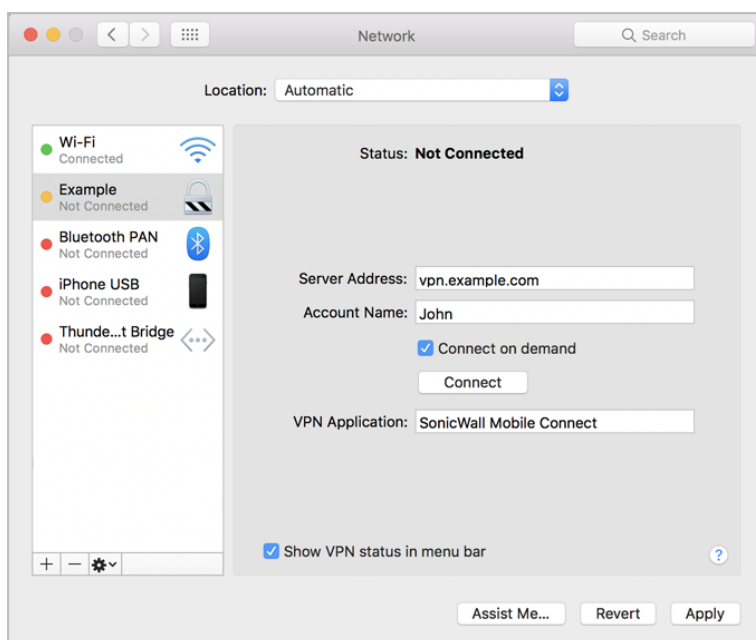
- The VPN tunnel must not be configured for **Redirect-All** mode.
- The realm must be configured to use client certificates for authentication. Chained authentication (where a second authentication server is used) does not support Connect on Demand.
- The valid client certificate for the realm must be present.
- The user must successfully connect to the appliance at least once.
- There must be no user interaction required for the user to connect.

If the Mobile Connect app is not running and user interaction is required for the VPN connection attempt to succeed, Connect on Demand might fail to connect. Scenarios where user interaction might be required include the following:

- User authentication by entering a username and password is required.
- Two-factor authentication is enabled, requiring a one-time password or token.
- The VPN server's SSL certificate is untrusted, requiring acceptance of an SSL certificate warning.
- Personal Device Authorization is enabled on the server and the device has not been authorized, requiring acceptance of a personal device authorization policy.

To enable Connect on Demand to an SMA 1000 Series:

1. On your Mac, open **Network Settings** in **System Preferences**.
2. Select the VPN connection from the list of network connections.
3. Select the **Connect on demand** checkbox to enable the feature.



4. Click **Apply**.

Enabling Connect on Demand to SMA 100 Series

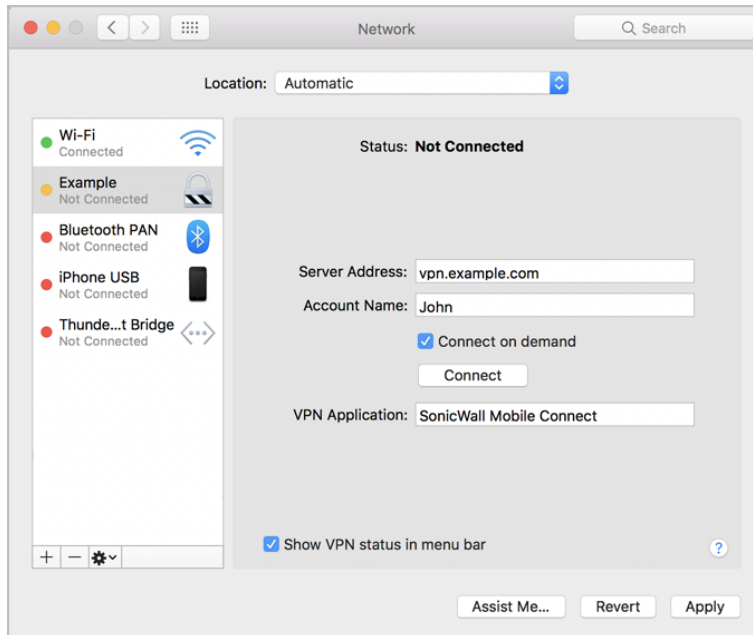
To support Connect on Demand, a VPN configuration on the SMA 100 Series must meet the following requirements:

- The user's effective client certificate enforcement policy, configured at the domain or user level, must be enabled to use client certificates for authentication.

- The user's effective user name and password caching policy, configured at the global, group, or user level, must be set to **Allow saving of username and password**, or the user's domain must be a **Digital Certificate** domain.
- The valid client certificate for the user must be present on the Mac.
- The VPN connection profile must have the user name and password configured, and the appropriate client certificate must be selected.
- ① **NOTE:** If no client certificates are installed, an error message is shown indicating that no matching client certificates are present on your device. The Keychain Access app (in Applications/Utilities) can be used to view client certificates.
- Click the **My Certificates** category to view available client certificates.

To enable Connect on Demand to an SMA 100 Series:

1. On your Mac, open **Network Settings** in **System Preferences**.
2. Select the VPN connection from the list of network connections.
3. Select the **Connect on demand** checkbox to enable the feature.



4. Click **Apply**.

Preferences and URL Control

This section describes the configurable elements that are accessed from the Preferences screen in Mobile Connect, including connection settings and URL control.

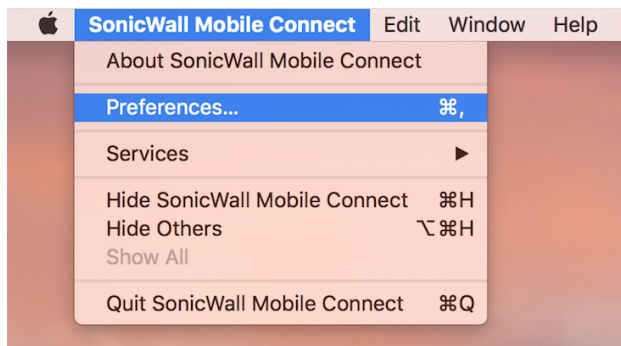
Topics:

- [Preferences Overview](#)
- [Additional SMA 1000 Series Options](#)
- [Using Apple Configurator 2 with Mobile Connect](#)
- [URL Control Syntax and Parameters](#)

Preferences Overview

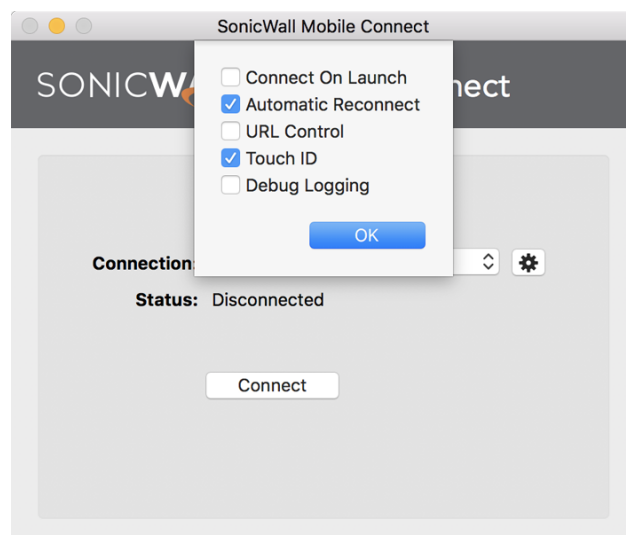
SonicWall Mobile Connect allows you to set several preferences for connection and logging options. The Preferences screen is available under the SonicWall Mobile Connect menu.

SonicWall Mobile Connect Menu



Clicking **Preferences** displays the configurable settings.

preferences settings



The following options are controlled from the **Preferences**:

- **Connect on Launch** - Sets Mobile Connect to automatically initiate a connection to the last-used profile when the application is launched.
- **Automatic Reconnect** - Sets Mobile Connect to automatically attempt to reconnect if the connection is lost. The SSL VPN connection can be disrupted when your device's connection transitions to a different network type (for example, from WiFi to Ethernet). This setting lets applications rely on a sustained VPN connection. There is no limit on the amount of time it takes to reconnect.
- **URL Control** - Allows other mobile applications to pass action requests using special URLs to Mobile Connect. These action requests can create VPN connection entries and connect or disconnect VPN connections. For example, another application can launch Mobile Connect, access internal resources as needed, and then disconnect by using the `mobileconnect://` or `sonicwallmobileconnect://` URL scheme. Additional information about URL Control is provided in [URL Control Syntax and Parameters](#).
- **Touch ID** - Set Mobile Connect to prompt for Touch ID during username/password authentication. Requires connection to servers that have a configured Touch ID policy.
- **Debug Logging** - Enables full debug log messages of Mobile Connect activity. Leave this section disabled unless instructed to enable it by SonicWall Support staff.

Additional SMA 1000 Series Options

Two additional options can be modified for connections to SonicWall SMA 1000 Series.

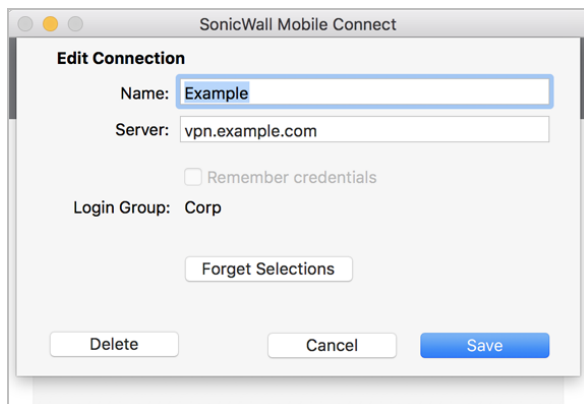
To view these options:

1. Navigate to the Connection screen.
2. Select an SMA 1000 Series connection from the **Connections** list.

3. Click the **Edit** icon next to the selected connection.



The Edit Connection screen displays.



The following options can be configured:

- **Remember Credentials** - Enables saving of user authentication credentials for the VPN connection. This is disabled by default and can be controlled by the SonicWall SMA 1000 Series server configuration.
- **Forget Selections** - Mobile Connect remembers the Login Group that you specified when configuring the connection. To change to a different Login Group, click **Forget Selections**. The next time you connect to the server, you are prompted to select a new Login Group.

NOTE: If these options are not displayed, then you are connecting to either a SonicWall firewall or SMA 100 Series.

Using Apple Configurator 2 with Mobile Connect

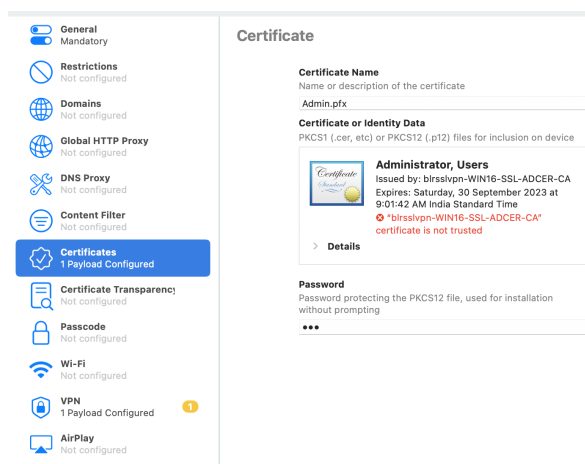
Apple Configurator 2 enables administrators to configure Mobile Connect profiles for their users' macOS devices. Information about downloading Apple Configurator 2 is available here [Mac App Store-Apple Configurator](#).

For more information, refer to:

- Apple Configurator 2 user guide- <https://support.apple.com/en-in/guide/apple-configurator-mac/welcome/mac>
- About mobile device management profiles- <https://support.apple.com/en-in/guide/deployment/depc0aadd3fe/1/web/1.0>

To Configure a Mobile Connect Profile Using Apple Configurator 2:

1. Download, install, and launch Apple Configurator 2.
2. In Apple Configurator 2, choose **File > New Profile**.
A new configuration profile document window appears.
3. In the **General**, fill in the mandatory fields.
4. If the user authentication type is certificate, go to the **Certificates** page, and do the following:



- a. Enter a **Certificate Name**.
 - b. Browse and select the **Certificate or Identity Data**.
 - c. Enter a **Password** to open the protected certificate without prompting to enter the password.
5. Go to **VPN** and click **Configure** the following settings:

- General**
Mandatory
- Restrictions**
Not configured
- Domains**
Not configured
- Global HTTP Proxy**
Not configured
- DNS Proxy**
Not configured
- Content Filter**
Not configured
- Certificates**
Not configured
- Certificate Transparency**
Not configured
- Passcode**
Not configured
- Wi-Fi**
Not configured
- VPN**
1 Payload Configured 1
- AirPlay**
Not configured
- AirPlay Security**
Not configured
- AirPrint**
Not configured
- Calendar**
Not configured
- Subscribed Calendars**
Not configured
- Contacts**
Not configured
- Exchange ActiveSync**
Not configured
- Google Account**
Not configured
- LDAP**
Not configured

VPN

Connection Name
Display name of the connection (displayed on the device)

Connection Type
Type of connection enabled by this policy

Server
Host name or IP address for server

Account
User account for authenticating the connection

Login Group or Domain
Login Group or Domain for authenticating the connection

User Authentication
Authentication type for connection
 Send all traffic through VPN

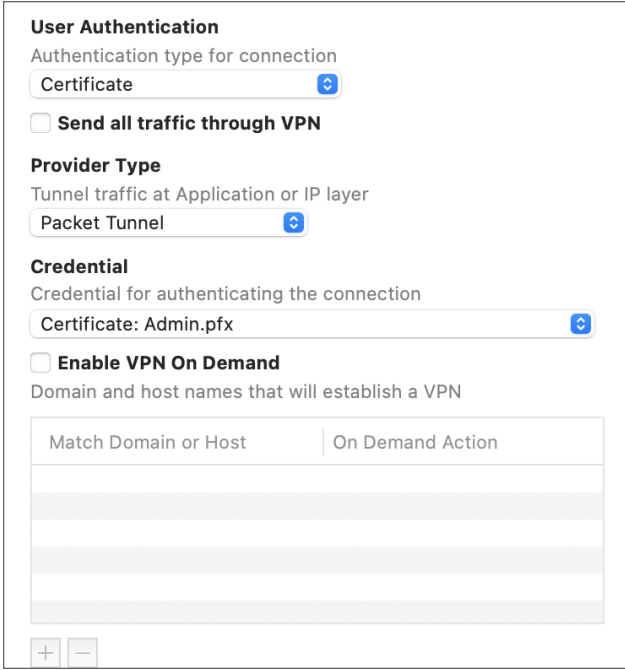
Provider Type
Tunnel traffic at Application or IP layer

Password
Password for authenticating the connection

Proxy Setup
Configures proxies to be used with this VPN connection

Disconnect on Idle
Disconnect after given time idle

Settings	Description
Connection Name	Enter a name for the connection. For example, <code>connect2</code>
Connection Type	Select SonicWall Mobile Connect from the drop-down menu.
Server	Enter the hostname or IP address for the SonicWall appliance. For example, <code>connect2.sonicwall.com</code>
Account	Enter the username for the account if required.
Login Group or Domain	Enter the group name or domain name for authenticating the connection

Settings	Description
User Authentication	<ul style="list-style-type: none"> If you select Password, in the Password field, enter the password for the user account. If you select Certificate, in the Credential select the uploaded certificate.
	
Provider Type	Select the Packet Tunnel from the drop-down menu.
Proxy Setup	Leave the with default value or set any custom value from the drop-down menu.
Disconnect on Idle	Leave the with default value or set any custom value from the drop-down menu.

- Download the configuration file (`.mobileconfig`) to deploy.

URL Control Syntax and Parameters

This section provides the full set of URL parameters for the URL Control feature. URL Control currently supports the `addprofile`, `connect`, and `disconnect` commands. Callback URLs are also supported.

Topics:

- Using the `addprofile` Command
- Using the `connect` Command
- Using the `disconnect` Command
- Using the `callbackurl` Command Parameter

Using the addprofile Command

The `addprofile` command requires either the name or server parameter, and accommodates both. All other parameters are optional. When the URL is opened in Mobile Connect, all of the parameters included in the URL are saved in the connection entry associated with that name and server.

Syntax for addprofile:

```
mobileconnect://addprofile[/]?name=ConnectionName&server=ServerAddress  
[&Parameter1=Value&Parameter2=Value...]
```

addprofile command parameters

Command parameter	Description
name	The unique name of the VPN connection entry that is created and appears in the Mobile Connect Connections list. Mobile Connect accepts the name only if it is unique. Letters are case sensitive.
server	The domain name or IP address of the SonicWall appliance to which you wish to connect. For example: <code>vpn.example.com</code>
username	Optional: The username used in the VPN connection.
password	Optional: The password used in the VPN connection.
realm	Optional: The realm used in the VPN connection profile. Applies to SMA 1000 Series connections only.
domain	Optional: The domain used in the VPN connection profile. Applies to SMA 100 Series and Firewall connections only.
sessionid	Optional: The session ID or Team ID used for authentication.
connect	Optional: If presented and the value is non-null, the connection is initiated if the profile was successfully added.
callbackurl	Optional: The callback URL to be opened by Mobile Connect after the <code>addprofile</code> command has been processed. See Using the callbackurl Command Parameter for full details of the callback URL syntax and options.

Examples of the addprofile command:

```
mobileconnect://addprofile/?name=Example&server=vpn.example.com  
sonicwallmobileconnect://addprofile/?name=Example&server=vpn.example.com  
mobileconnect://addprofile?name=Example%20&server=vpn.example.com  
mobileconnect://addprofile?name=vpn.example.com  
mobileconnect://addprofile?server=vpn2.example.com  
mobileconnect://addprofile?name=SMA%20Connection&server=sslvpn.example.com  
&username=test&password=password&domain=LocalDomain&connect=1
```

```
mobileconnect://addprofile?name=EX%20Connection&server=workplace.example.com
&username=test&password=password&realm=Corp&connect=1
```

- ① **NOTE:** All appropriate characters in values of parameters used in URLs are required to be URL encoded. For instance, to match a space, enter %20.

Using the connect Command

The connect command is used to easily establish VPN connections. Connection information can be embedded in the URLs and they can be provided to users for easy setup and configuration. In addition, a callback URL can be provided that Mobile Connect opens after the connection attempt is completed, making it possible for other applications to initiate VPN connections in a seamless manner.

Syntax for connect:

```
mobileconnect://connect[/?[name=ConnectionName|server=ServerAddress]
[&Parameter1=Value&Parameter2=Value...]
```

Command parameter	Description
name	The unique name of the VPN connection entry that is created and appear in the Mobile Connect Connections list. Mobile Connect accepts the name only if it is unique. Letters are case sensitive.
server	The domain name or IP address of the SonicWallappliance in which you wish to connect. For example: <code>vpn.example.com</code>
username	Optional: The username used in the VPN connection.
password	Optional: The password used in the VPN connection.
realm	Optional: The realm used in the VPN connection profile. Applies to SMA 1000 Series connections only.
domain	Optional: The domain used in the VPN connection profile. Applies to SMA 100 Series and Firewall connections only.
sessionid	Optional: The session ID or Team ID used for authentication.
connect	Optional: If presented and the value is non-null, the connection is initiated if the profile was successfully added.
callbackurl	Optional: The callback URL is opened by Mobile Connect after the <code>connect</code> command has been processed. See Using the callbackurl Command Parameter for full details of callbackurl syntax and options.

Examples of the connect command:

```
mobileconnect://connect/?name=Example
sonicwallmobileconnect://connect/?name=Example
mobileconnect://connect?name=Example
mobileconnect://connect?server=vpn.example.com
```

```
mobileconnect://connect?name=Example%20&server=vpn.example.com

mobileconnect://connect?name=SMA%20Connection&server=sslvpn.example.com
&username=test&password=password&domain=LocalDomain

mobileconnect://connect?name=EX%20Connection&server=workplace.example.com
&username=test&password=password&realm=Corp
```

Using the disconnect Command

The `disconnect` command is used to disconnect an active connection. In addition, a callback URL can be provided that Mobile Connect opens after the connection is disconnected that makes it possible to return to the calling application. If there is no active VPN connection, the `disconnect` command is ignored.

Syntax for disconnect:

```
mobileconnect://disconnect[/]

mobileconnect://disconnect[/]?[callbackurl=CallBackURL]
```

disconnect command parameters

Command parameter	Description
<code>callbackurl</code>	Optional: The URL defined for <code>callbackurl</code> is opened by Mobile Connect after the <code>disconnect</code> command has been processed. See Using the callbackurl Command Parameter for full details of <code>callbackurl</code> syntax and options.

Examples of the disconnect command:

```
mobileconnect://disconnect

mobileconnect://disconnect/

sonicwallmobileconnect://disconnect

mobileconnect://disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24

sonicwallmobileconnect://disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
```

Using the callbackurl Command Parameter

`callbackurl` is an optional query string argument for each of the `connect/disconnect/addprofile` commands. If a callback URL is included in a command, then that URL will be launched by Mobile Connect once the command has been completed. While invoking Mobile Connect using a URL, a third-party application can use the `callbackurl` parameter to include a URL to be launched by Mobile Connect after it completes the requested action.

The `callbackurl` value can contain special tokens that are evaluated and dynamically replaced by Mobile Connect to provide additional status and connection information back to the app that is opened by the callback URL. Tokens are evaluated in place, in the same order in which the tokens were specified.

To ensure that it functions properly, the base `callbackurl` URL value format should be RFC 1808 compliant and should be able to be launched independently of Mobile Connect. For example, it should launch through a web page.

URL syntax for a callbackurl:

```
<scheme>://<net_loc>/<path>;<params>?<query>#<fragment>
```

NOTE: The URL value of `callbackurl` must be properly URL encoded to ensure that Mobile Connect can process the callback URL correctly. All appropriate characters in values of parameters used in URLs are required to be URL encoded. For instance, to match a space, enter `%20`.

Any number of dynamic tokens from the Dynamic tokens supported by `callbackurl` table can be specified in the `<query>` element of the URL. These can be used by administrators when configuring the callback URLs on a web site or in an email to their users, such as to auto-configure a VPN profile. The dynamic tokens are useful because they allow Mobile Connect to provide information to the website or app that is being launched when the callback URL is opened.

Dynamic Tokens Supported By Callbackurl

Dynamic token	Description
<code>\$ERROR_CODE\$</code>	The numerical value of the error from the failed connection attempt.
<code>\$ERROR_MESSAGE\$</code>	The string value of the error message from the failed connection attempt.
<code>\$LOGIN_GROUP\$</code>	The string value of the authentication login group or realm. Applies to SMA 1000 Series connections only.
<code>\$COMMUNITY\$</code>	The string value of authentication community. Applies to SMA 1000 Series connections only.
<code>\$ZONE\$</code>	The string value of EPC (End Point Control) zone. Applies to SMA 1000 Series connections only.
<code>\$TUNNEL_IP\$</code>	The string value of the Mobile Connect IPv4 client address.
<code>\$TUNNEL_MODE\$</code>	One of <code>split</code> , <code>split-nonlocal</code> , <code>redirectall</code> , or <code>redirectall-nonlocal</code> , depending on the tunnel mode. Applies to SonicWall SMA 1000 Series connections only.
<code>\$ESP_ENABLED\$</code>	One of yes or no, depending on if ESP (Encapsulating Security Payload) is enabled. Applies to SonicWall SMA 1000 Series connections only. ESP is a protocol used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

Examples of the callbackurl command:

Callback URL (1):

```
customapp://host?status=$STATUS&login_group=$LOGIN_GROUP&error_code= $ERROR_CODE$
```

Corresponding full URL with URL encoded callbackurl value:

```
mobileconnect://connect?sessionid=<teamid>&callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%26error_code%3D%24 ERROR_CODE%24
```

Callback URL (2):

```
myapp://callback?status=$STATUS&login_group=$LOGIN_GROUP&error_code= $ERROR_CODE$
```

Corresponding full URL with URL encoded callbackurl value:

```
mobileconnect://connect?sessionid=<teamid>&callbackurl=myapp%3A%2F%2Fcallback%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%26error_code%3D%24 ERROR_CODE%24
```

Callback URL (3):

```
http://server/example%20file.html
```

Corresponding full URL with URL encoded callbackurl value:

```
mobileconnect://connect?callbackurl=http%3A%2F%2Fserver%2Fexample%20file.html
```

Monitoring, Logs, and Troubleshooting

This section discusses the Mobile Connect Monitor screen, Help options including logging, and provides troubleshooting tips.

Topics:

- [Monitoring Mobile Connect](#)
- [Using Mobile Connect Help and Log Options](#)
- [Troubleshooting Mobile Connect](#)

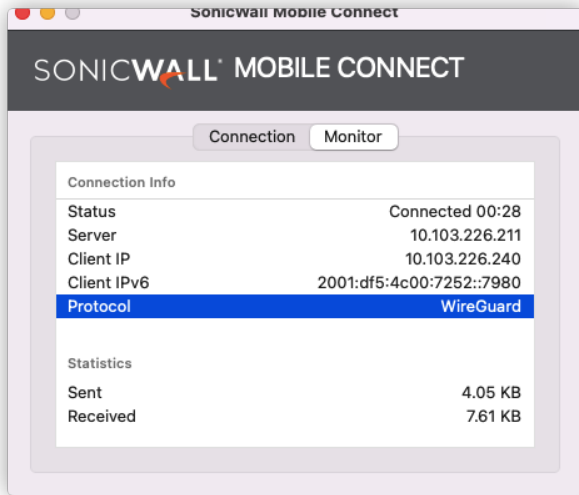
Monitoring Mobile Connect

The Monitor screen displays additional details about the connection, statistics on traffic transmitted, DNS information, and routes that have been installed.

The compression ratio is shown when connected to a SonicWall SMA 100 Series with compression enabled. Traffic over the VPN tunnel is compressed using the LZ4 algorithm.

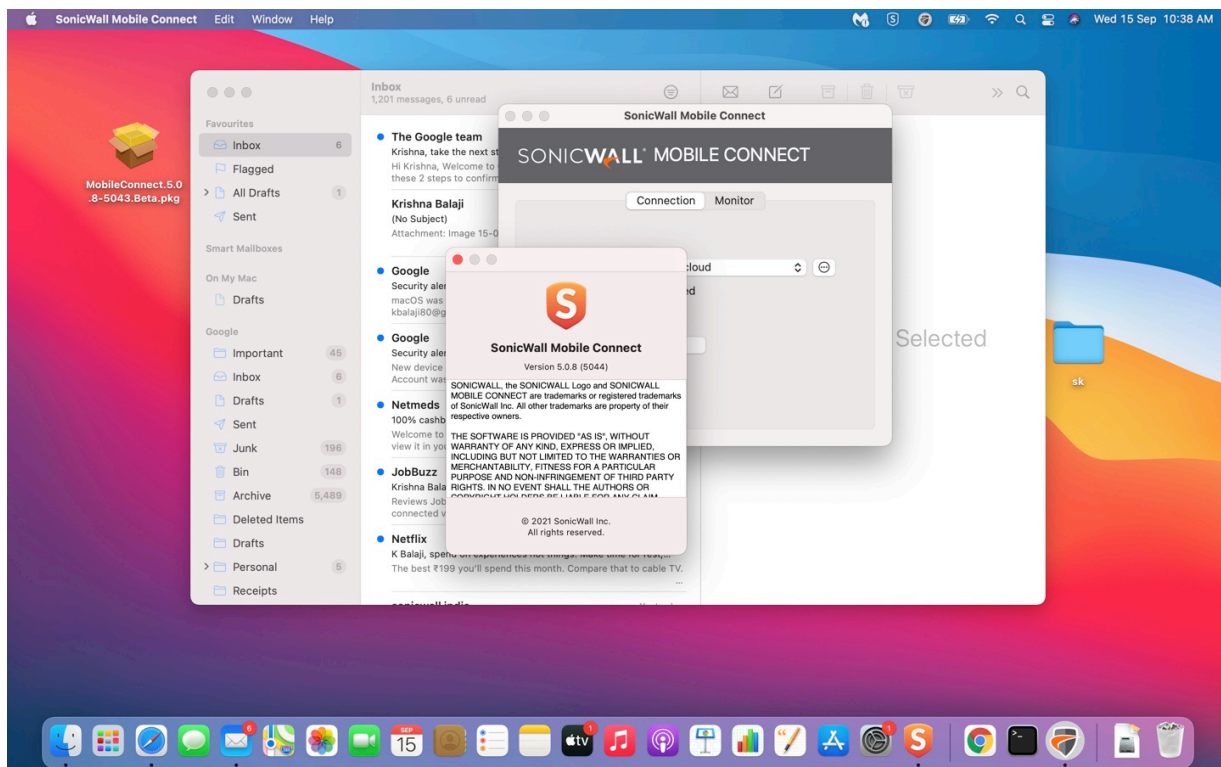
- ① **NOTE:** Displaying the protocol information in **Monitor** when connected to different appliances:
- When connected to SonicWall SMA100 Series, you will see **Auto** or **WireGuard** or **SSLVPN** in the **Protocol** information.
 - When connected to UTM appliances, you will see the **Protocol** information but, **WireGuard** is not supported.
 - When you are connected to SonicWall SMA 1000 Series, you will not see the **Protocol** information.

Monitor Screen



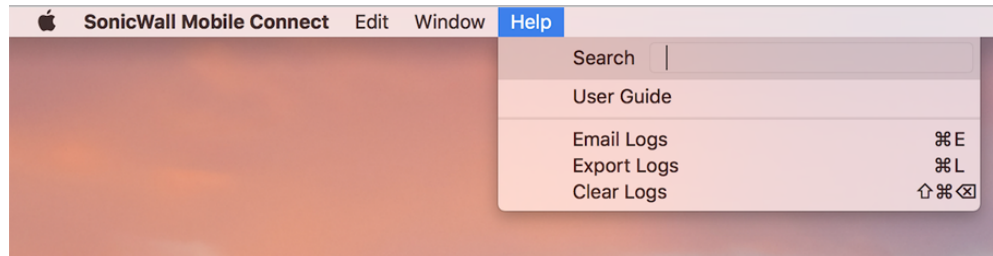
The **About** screen of Mobile Connect displays the version number and legal text.

About Screen



Using Mobile Connect Help and Log Options

The Help menu provides support information that includes a User Guide and log handling options.



The Help menu provides the following support information:

- **User Guide** - Displays the SonicWall Mobile Connect User Guide in the default web browser application (for example, Safari).
- **Email Logs** - Creates an email to send the Mobile Connect log files to SonicWall Support staff. The email is opened in the default mail application (for example, Mail).
- **Export Logs** - Opens a Finder window to a temporary folder containing a copy of the Mobile Connect log files.
- **Clear Logs** - Deletes all log files that have been saved on the device.

① **NOTE:** The Mobile Connect Preferences screen provides the **Debug Logging** option for turning on full debug log messages of Mobile Connect activity. For more information, see [Preferences Overview](#).

Troubleshooting Mobile Connect

This section describes some troubleshooting you can try if you are unable to connect to the SonicWall server.

If you are unable to connect to the SonicWall server, perform the following steps to troubleshoot the connection:

1. Double check that you have entered the server name properly in the connection configuration.
2. Go to the Safari browser on your Mac and attempt to navigate to the SMA 100 Series web portal.
3. If you are unable to load the web portal, the problem is with the SonicWall appliance. Contact your network administrator if the problem persists.
4. If the web portal loads successfully on the browser and you still cannot establish a Mobile Connect connection, notify SonicWall Support, as follows:
 - a. Under **Preferences**, enable the **Debug Logging** option.
 - b. Attempt a connection to the server again to ensure that full debugging messages are logged for the attempt.

- c. Then, under the **Help** menu, click **Email Logs**. An email will launch in your mail client with the Mobile Connect log attached. Address the email to **Support@sonicwall.com**. Add any additional comments to the email and click **Send**. SonicWall Support staff will contact you after reviewing your case.

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. 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 and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- 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

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

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

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

Mobile Connect for macOS User Guide

Updated - October 2023

Software Version - 5.0

232-004060-00 Rev D

Copyright © 2023 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