

Mobile Connect for Android 5.0

User Guide

SONICWALL®

Contents

Introduction to Mobile Connect	4
How Mobile Connect Works	4
New Features in Mobile Connect 5.0	5
Additional Feature Information	5
Supported Platforms	7
Android Product Support	7
SonicWall Appliance Support	7
Required Network Information	8
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
Initiating a Connection	14
Connecting to a Firewall or SMA 100 Series	14
Connecting to an SMA 1000 Series	17
Configuring Client Certificates	23
Client Certificates with SMA 1000 Series	23
Client Certificates with SMA 100 Series	25
Using the Mobile Connect Widget	26
Installing and Using the Quick Settings Tile	27
Installing the Quick Settings Tile	27
Using the Quick Settings Tile	29
Using App Shortcuts	29
Settings, Bookmarks, and Files	30
Settings Overview	30
Settings Section	31
Support Section	33
Additional Settings for SMA 1000 Series	33
URL Control Syntax and Parameters	34
Using the addprofile Command	34
Using the connect Command	35
Using the disconnect Command	36
Using the callbackurl Command Parameter	37
Using Bookmarks	39

Showing and Filtering Bookmarks	39
Supported Bookmark Types	40
Using Files	43
File Types and Policies	45
Application Access Control	48
About Application Access Control	48
Logging in and Registering your Device	49
Controlling App Behavior	50
Viewing the App List after Connecting	51
About Learning Mode (Administrators Only)	52
Monitoring and Troubleshooting	53
Monitoring Mobile Connect	53
Troubleshooting Mobile Connect	56
Failed End Point Control Check	56
General Troubleshooting	57
SonicWall Support	59
About This Document	60

Introduction to Mobile Connect

SonicWall Mobile Connect for Android is an app that enables Android devices to establish secure, mobile connections to private networks protected by SonicWall security appliances.

① | **NOTE:** Use SonicWall Mobile Connect for Android instead of SonicWall Mobile Connect for Chrome OS.

Topics:

- [How Mobile Connect Works](#)
- [New Features in Mobile Connect 5.0](#)
- [Additional Feature Information](#)
- [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 mobile devices. And yet, mobile devices are increasingly subject to security attacks. Furthermore, mobile devices often use insecure, untrusted, public Wi-Fi hotspots to connect to the Internet. It is therefore a challenge to provide secure, mobile access while still guarding against the inherent security risks of using mobile devices.

The SonicWall Mobile Connect for Android 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.

To get started with SonicWall Mobile Connect:

1. Install SonicWall Mobile Connect from the Google Play Store or the Amazon Appstore.
2. Enter connection information (server name, username, password, etc.).
3. Initiate a connection to the network.
4. 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

This section describes the enhancements included in the Mobile Connect 5.0 release.

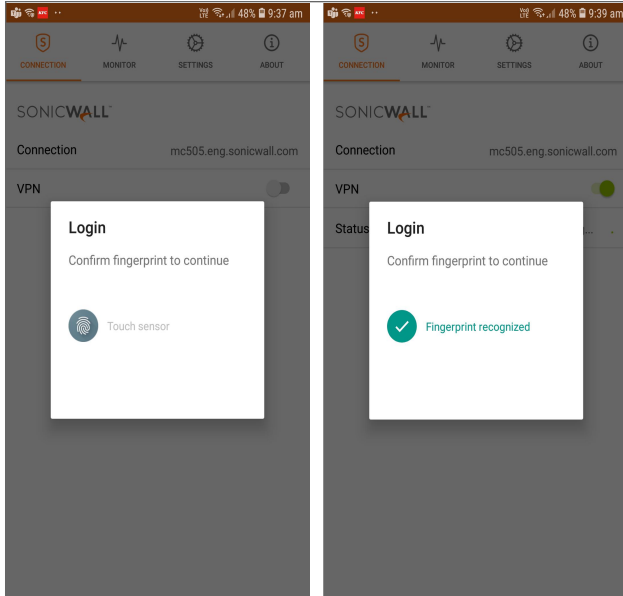
- **Android (12.0)** - Mobile Connect is supported in Android 12.x onwards for MC Android 5.0.
- **Secure Web Bookmarks** - Web bookmarks can now be launched within Mobile Connect instead of launching a third party browser, allowing for a seamless and more secure user experience. Secure Web Bookmarks also support Single Sign-On and require a connection to a VPN server with software that supports the secure web bookmark policy.
- **Additional HTML5 Bookmarks Support** - Mobile Connect now supports HTML5 Bookmarks for VPN connections to supported SMA 1000 Series Appliances.
- **Additional Fingerprint Authentication Support** - Mobile Connect now supports Fingerprint Authentication for VPN connections to supported SMA 1000 Series Appliances.
- **Capture ATP Integration** - Uploaded files can be scanned by the SonicWall Capture Advanced Threat Protection service. A SonicWall SMA 1000 Series Appliance with Capture ATP add-on is required.
- **SAML IdP authentication for SMA 1000** - Mobile Connect supports connecting to SMA 1000 Series Appliances configured with SAML 2.0 IdP.
- **File Browser Enhancements** - Additional folder operations (add, rename and delete) and file operations (upload, rename and delete) are now available.
- **SAML Authentication** - Latest Mobile Connect support SAML authentication with SMA 100 and SMA 1000 as well, enabling Mobile Connect to authenticate against third-party SAML IdP servers.

Additional Feature Information

SonicWall Mobile Connect for Android continues to support the following features:

- **Material Design** - Mobile Connect has been redesigned according to Android's material design guidelines, Google's comprehensive guide for visual, motion, and interactive design across platforms and devices that was broadly introduced in Android 5.0.
- **Fingerprint Authentication** - Android 6.0+ devices equipped with fingerprint scanners can use fingerprint authentication as a seamless alternative to username and password authentication if allowed by the VPN server. Requires a compatible server with configured Fingerprint Authentication policy.

logging in with fingerprint authentication



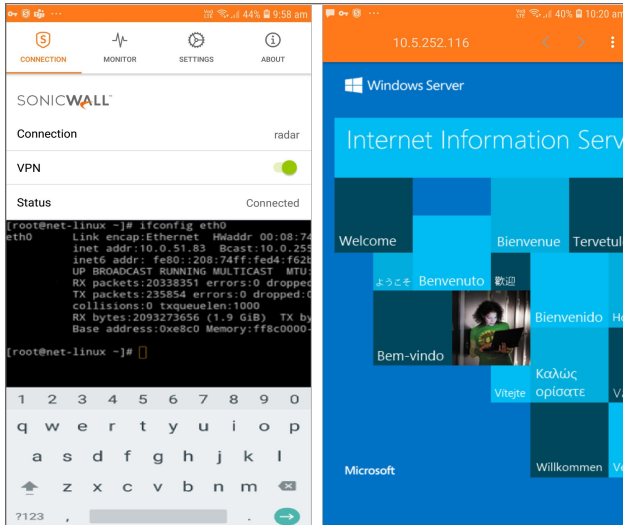
- **Files Enhancements** - Files Bookmarks support FTP and SFTP file server Bookmarks in addition to CIFS file Bookmarks.
- **HTML5 Bookmarks Enhancements** - Support for in-app access with single sign-on for HTML5 Bookmarks including RDP, VNC and SSH.

The following third party apps are supported:

- Dell vWorkspace
- JuiceSSH

HTML5 Bookmarks are displayed natively within Mobile Connect and provide a seamless and more secure user experience, including support for single sign-on.

HTML5 Bookmarks



Supported Platforms

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

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

Android Product Support

SonicWall Mobile Connect 5.0 for Android requires

- Android 12.x and 13.x
- Supported Chromebooks include those which support Android apps.

SonicWall Appliance Support

SonicWall Mobile Connect 5.0 for Android is a free app, but requires a concurrent license on one of the following SonicWall solutions to function properly:

- SonicWall firewall appliances including the TZ, NSa, NSA, and SuperMassive series running SonicOS 6.5.4.9 or higher. This includes SonicWall Gen7 TZ firewalls running SonicOS 7.
- Secure Mobile Access (SMA) 100 series appliances running 10.2 or higher.

① **NOTE:** With the VPN tunnel running in Tunnel All Mode, attempts to access resources belonging to the local subnet are not redirected to the SMA 100 series appliance. Instead, users can access the resources directly.

- Secure Mobile Access (SMA) 1000 series appliances running 12.4.2 or higher.

Required Network Information

To use Mobile Connect, the following information is needed 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.
- **Protocol** - You are required to select the type of protocol. However SonicWall Secure Mobile Access 1000 series do not support and display this information.

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. Additional features are also described.

Topics:

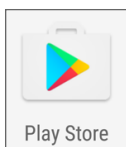
- [Installing Mobile Connect](#)
- [Creating and Saving Connections](#)
- [Initiating a Connection](#)
- [Configuring Client Certificates](#)
- [Using the Mobile Connect Widget](#)
- [Installing and Using the Quick Settings Tile](#)
- [Using App Shortcuts](#)

Installing Mobile Connect

SonicWall Mobile Connect is installed through the Google Play Store or the Amazon Appstore.

To download and install the Mobile Connect app:

1. On your Android device, tap the Google Play icon.



Or, type the following in the browser:

Google Play Store:

<https://play.google.com/store/apps/details?id=com.sonicwall.mobileconnect>

Amazon Appstore:

<https://www.amazon.com/gp/mas/dl/android?p=com.sonicwall.mobileconnect>

2. Go to the Search tab, type `SonicWall Mobile Connect`, and tap **Search**.

3. In the search results, select SonicWall Mobile Connect.
4. Tap the **Install** button under SonicWall Mobile Connect. The app will install on your device. When installation is complete, the SonicWall Mobile Connect icon will appear on your device



If you encounter an error when attempting to download SonicWall Mobile Connect, please go to the appropriate site for help:

Google Play Store Help - Follow troubleshooting procedures and instructions on how to report the issue using your Google account:

<http://support.google.com/googleplay/?hl=en>

Amazon Appstore Help - Follow troubleshooting procedures and instructions on how to report the issue using your Google account:

<http://www.amazon.com/gp/help/customer/display.html?nodeid=201111910>

Creating and Saving Connections

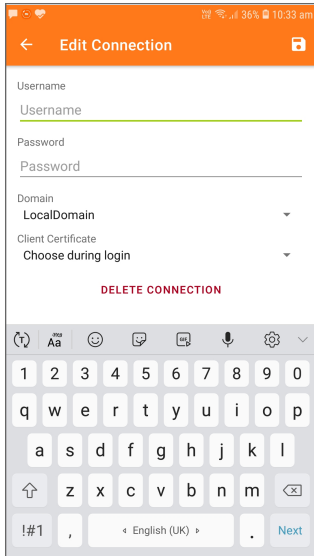
The process of creating a Mobile Connect connection is slightly different depending on the type of SonicWall appliance to which you are connecting.

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

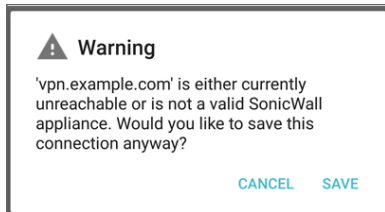
Creating Firewall or SMA 100 Series Connections

To create and save a new connection to a SonicWall network security appliance or SMA 100 Series:

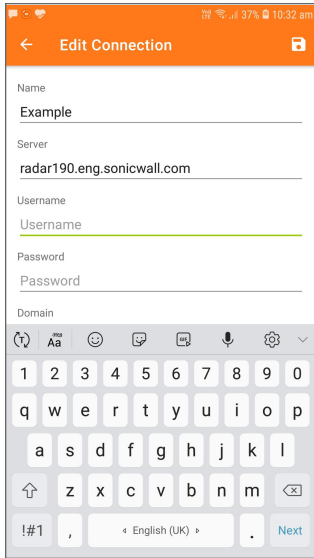
1. Launch SonicWall Mobile Connect. You will be presented with the screen to begin your first connection. Tap **Add connection**.



2. In the **Name** field, type in a descriptive name for the connection.
3. In the **Server** field, type in the URL or IP address of the server (appliance).
4. Tap **Next**, **Done**, **Finished**, or **Save** (depending on version used). 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 on the Connections screen.
 - 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 tap **Save**.

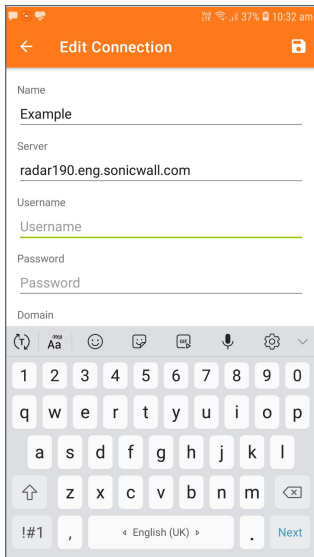


5. If Mobile Connect successfully contacts the server, you are prompted to enter your username and password, unless the server does not require this information. Type your credentials into the **Username** and **Password** fields.

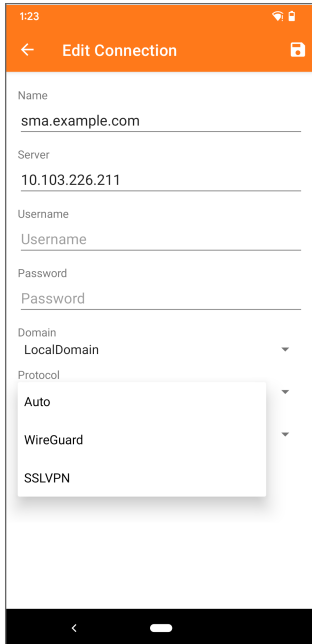


NOTE: If the previous screenshot does not match what is displayed on your device, you are connecting to a SonicWall SMA 1000 Series. See [Creating SMA 1000 Series Connections](#).

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



- 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**.

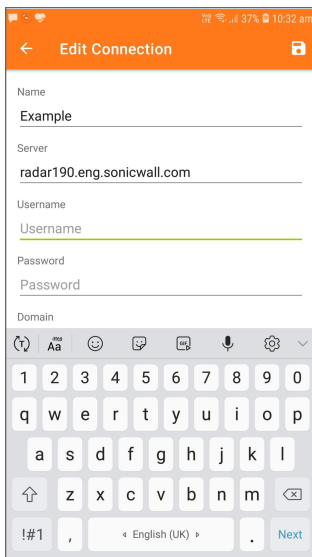


① | **NOTE:** The Protocol selection is not displayed when you are connected to a SonicWall SMA 1000 Series.

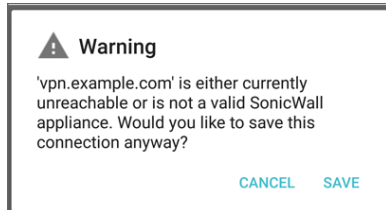
Creating SMA 1000 Series Connections

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

1. Launch SonicWall Mobile Connect. You will be presented with the screen to begin your first connection. Tap **Add connection**.



2. In the **Name** field, type in a descriptive name for the connection.
3. In the **Server** field, type in the URL or IP address of the server (appliance).
4. Tap **Next**, **Done**, **Finished**, or **Save** (depending on version used). 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 on the Connections screen.
 - 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 tap **Save**.



Clicking **Save** adds the server connection to the list of saved connections on the Connections screen.

Initiating a Connection

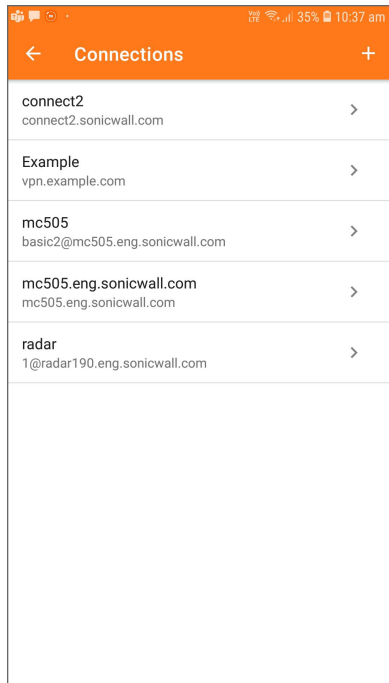
The process of connecting Mobile Connect to SonicWall appliances varies slightly depending on the types of appliances you are connecting.

- [Connecting to a Firewall or SMA 100 Series](#)
- [Connecting to an SMA 1000 Series](#)

Connecting to a Firewall or SMA 100 Series

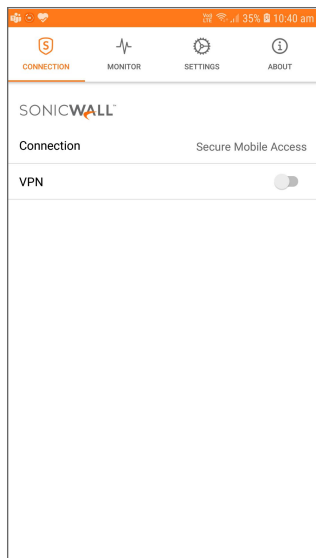
After you save a new connection, the Connections screen displays the list of all configured connections.

Connections Screen



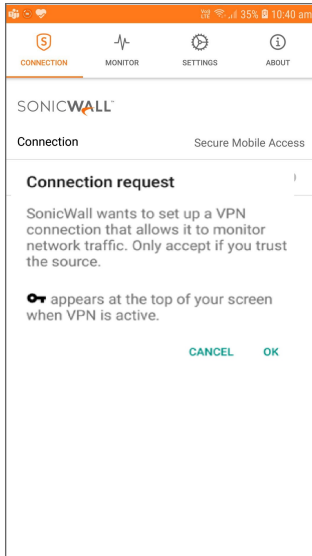
To initiate a Mobile Connect session:

1. In the list, tap the connection that you want to initiate. The Connection status page displays.

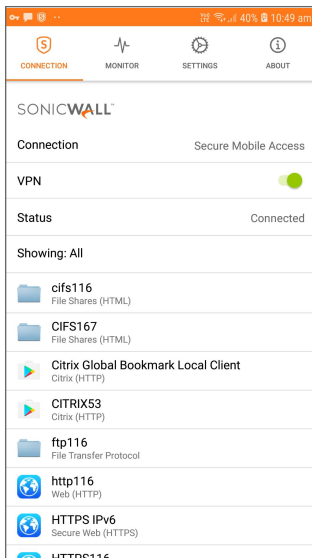


2. Tap the **VPN** on/off switch to turn on the VPN.

- The first time you initiate a connection a Connection Request message displays. Tap **OK** to continue.



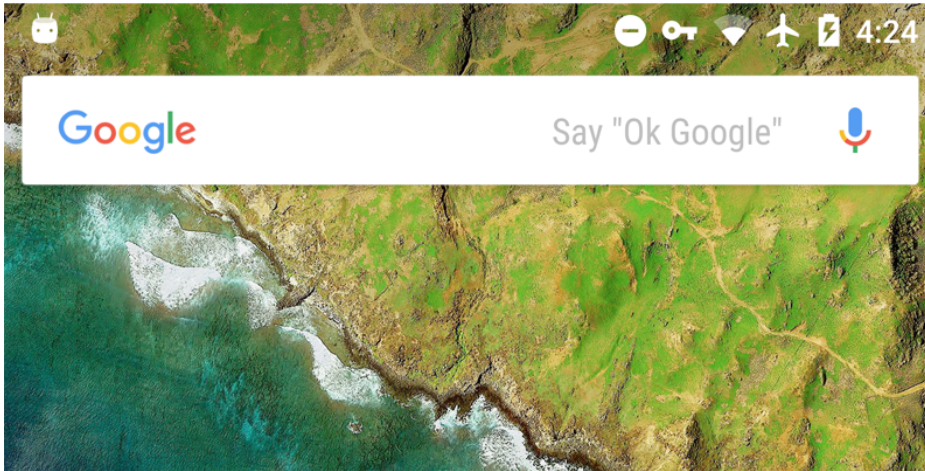
- When the connection is successfully established, the **Status** changes to **Connected** and the VPN switch remains in the ON position.



NOTE: If this sequence of events does not match what is displayed on your device, you are connecting to a SonicWall SMA 1000 Series. See [Connecting to an SMA 1000 Series](#).

Any bookmarks defined for the portal are displayed below the Status line, and allow you to navigate directly to the bookmark's destination. Bookmarks only appear after a VPN connection is established to a server that is running firmware that supports Mobile Connect bookmarks, and bookmarks have been defined for that user.

5. Press the **Home** button to return to your device's home screen. You can now navigate to other apps to access your Intranet network.



The status bar displays a VPN icon  to indicate that the session is still connected.

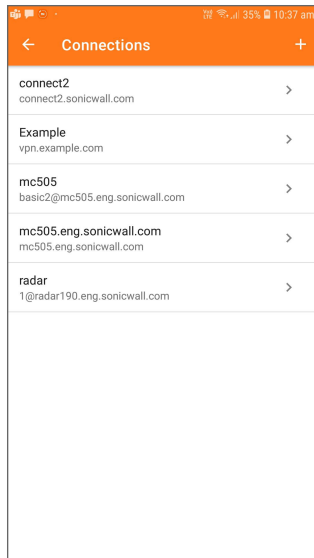
If the VPN connection is interrupted, the VPN icon will disappear and you will no longer be able to access the Intranet network. This can happen if your device's connection transitions to a different network connection (for example, from Wi-Fi to cellular).

Return to Mobile Connect to reestablish the connection. Optionally, you can configure the **Automatic Reconnect** option on the Settings screen to have Mobile Connect automatically attempt to reestablish interrupted connections.

Connecting to an SMA 1000 Series

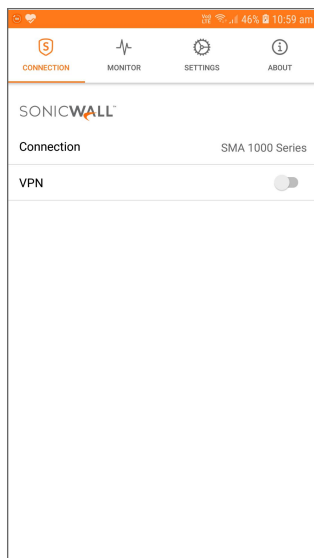
After you save a new SMA 1000 Series connection, the Connections screen displays the list of all configured connections. In the Connections screen image, the SMA connections are **Secure Mobile Access** and **SMA Virtual Appliance**.

Connections Screen

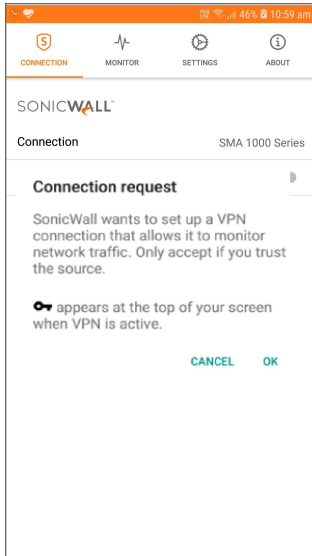


To initiate a Mobile Connect session:

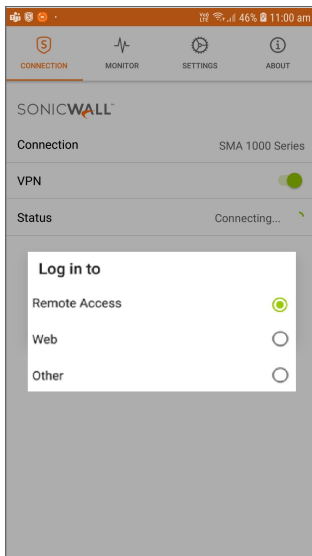
1. In the list, tap the connection that you want to initiate. The Connection status page displays.



2. Tap the **VPN** on/off switch to turn on the VPN.
3. The first time you initiate a connection, a Connection Request message displays. Tap **OK** to continue.

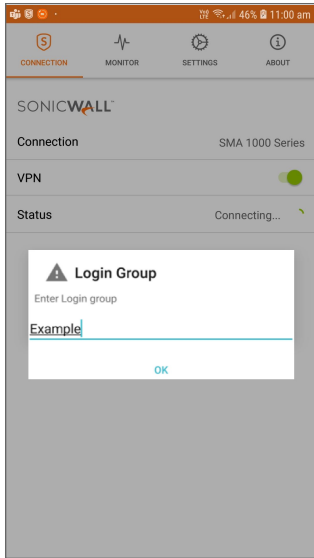


4. If Mobile Connect successfully contacts the server, you are prompted to select which Login Group on the appliance you want to connect to. If you do not know which Login Group to connect to, contact your network administrator.

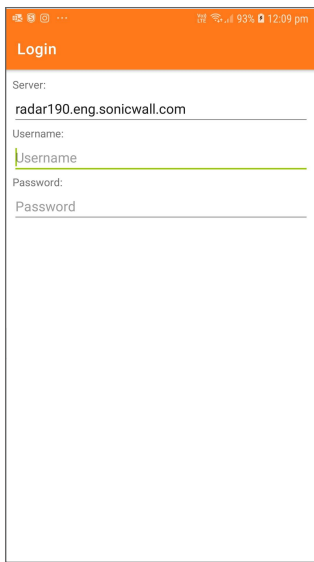


NOTE: If the screenshot above does not match what is displayed on your device, you are connecting to a SonicWall firewall or SMA 100 Series. See [Connecting to a Firewall or SMA 100 Series](#).

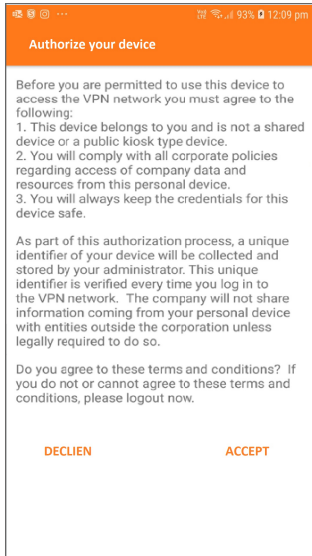
5. If the Login Group you connect to is not listed, select Other to manually type in the group name.



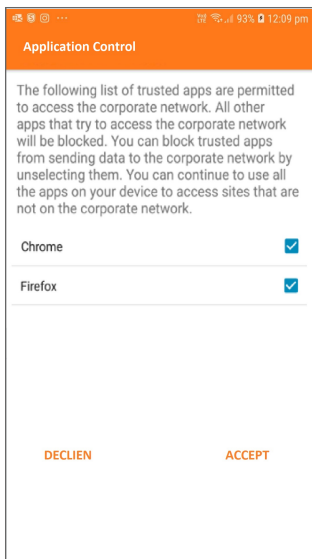
6. Enter your username and password if prompted (depending on whether the SonicWall appliance you are connecting to allows for saving usernames and passwords).



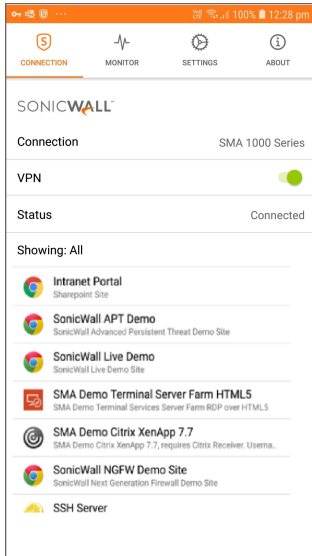
7. If this is the first time you have connected to an SMA 1000 Series Appliance with **Personal Device Authorization** enabled, you are prompted to register your device. A similar prompt appears when the terms and conditions have changed. To continue, tap **Accept** to agree to the terms and conditions.



- When connecting to an SMA 1000 Series Appliance with **Application Access Control** configured, a notification about Data Privacy with a list of the applications under control is displayed. Optionally, clear the check boxes next to any of the displayed apps if you are only using them for personal use and you do not want their traffic sent to the corporate network. Then tap **Accept** to accept the terms and continue.

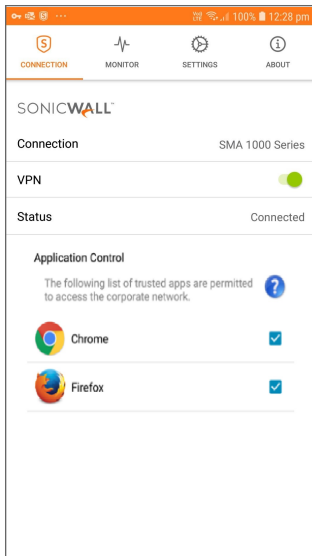


- When the connection is successfully established, the **Status** changes to **Connected** and the VPN switch remains in the ON position.



Any bookmarks defined for the portal are displayed below the Status line, and allow you to navigate directly to the bookmark's destination. Bookmarks only appear after a VPN connection is established to a server that is running firmware that supports Mobile Connect bookmarks, and bookmarks have been defined for that user.

If Application Access Control is configured on the server, the list of Bookmarks is replaced by a list of apps that are allowed to access the corporate network.



10. Press the **Home** button to return to your device's home screen. You can now navigate to other apps to access your Intranet network.



The status bar displays a VPN icon  to indicate that the session is still connected.

If the VPN connection is interrupted, the VPN icon will disappear and you will no longer be able to access the Intranet network. This can happen if your device's connection transitions to a different network connection (for example, from Wi-Fi to cellular).

Return to Mobile Connect to reestablish the connection. Optionally, you can configure the **Automatic Reconnect** option on the Settings screen to have Mobile Connect automatically attempt to reestablish interrupted connections.

Configuring Client Certificates

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

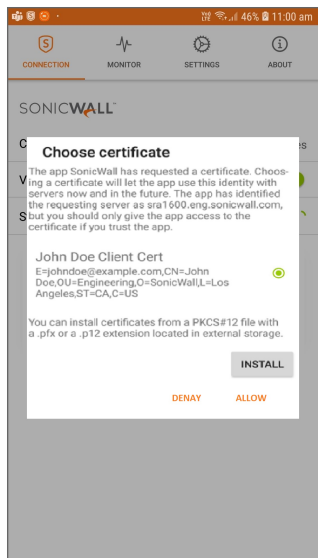
Topics:

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

Client Certificates with SMA 1000 Series

If a client certificate is required during authentication, you are automatically prompted to select a client certificate from the Android device client certificate store.

Choose Certificate



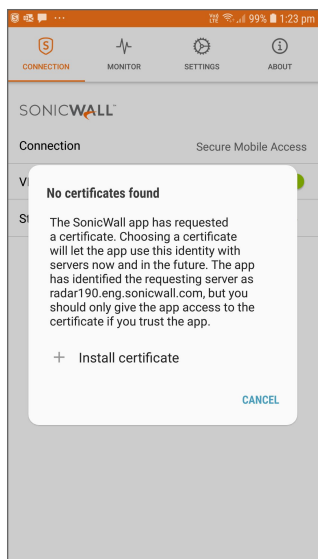
Select the client certificate from the list of certificates and tap **Allow**.

By default, a VPN connection prompts you to select the client certificate during authentication. 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, edit the connection and tap the **Forget Selections** button.

If no client certificates are installed, an Android *No certificates found* dialog appears with an option to install a PKCS#12 file located in external storage.

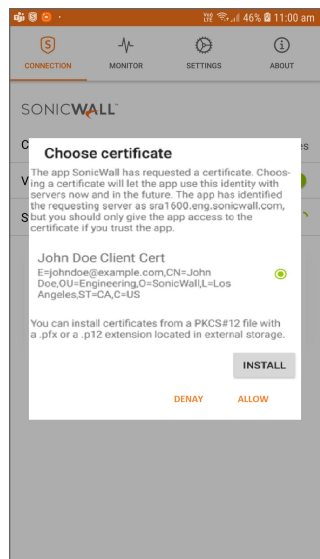
No Certificates Found



Client Certificates with SMA 100 Series

On SonicWall SMA 100 Series, client certificate authentication is available as a two factor authentication method in addition to standard user name and password authentication. If a client certificate is required during authentication, you are automatically prompted to select a client certificate from the Android device client certificate store.

Choose Certificate

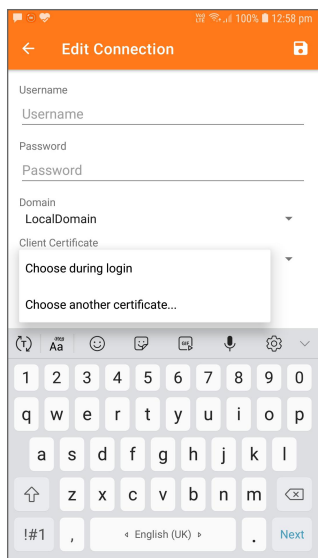


Select the client certificate from the list of certificates and tap **Allow**.

By default, the client certificate is set to **Choose during login** for a VPN connection. If you successfully authenticate with a client certificate, the VPN connection profile is automatically updated to set the client certificate to the one that was chosen.

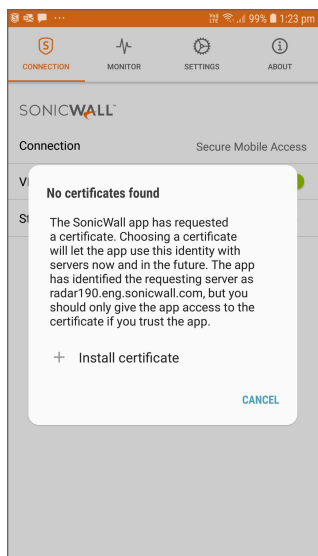
To reset the client certificate selection, edit the connection and tap the Client Certificate, then set it back to **Choose during login**.

Edit Connection



If no client certificates are installed, an Android No certificates found dialog appears with an option to install a PKCS#12 file located in external storage.

No certificates found

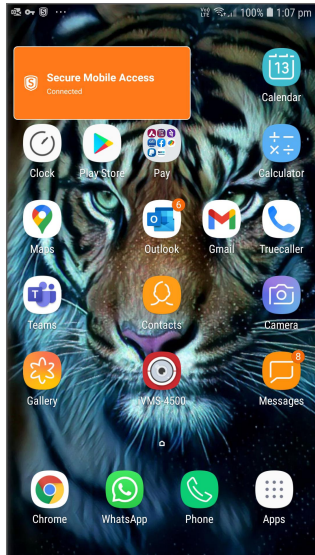


Using the Mobile Connect Widget

When the SonicWall Mobile Connect app is installed, a widget for Android is also created in the widgets screen. It can then be dragged from the widgets tab to the home screen. This widget is used as follows:

- The widget shows the connection status (connected, disconnected, connecting, etc.)
- Tap the icon to establish a tunnel when disconnected.
- Tap the icon to disconnect the tunnel when connected.
- Tap any other area of the widget to launch the Mobile Connect client.

Mobile Connect Widget



Installing and Using the Quick Settings Tile

On Android 9.0 (Pie) or higher including Android 12.x, a Quick Settings Tile can be used to connect and disconnect Mobile Connect. The tile must be installed before it can be used.

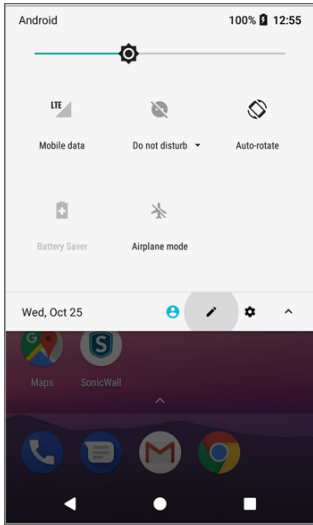
Installing the Quick Settings Tile

To install the Quick Settings Tile:

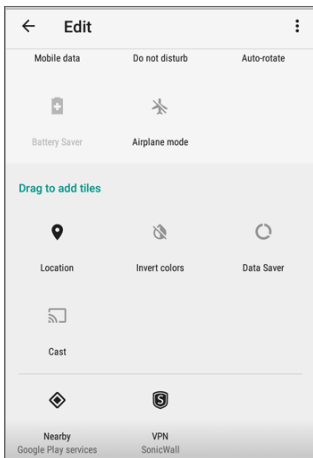
1. Drag down from the top of the screen to reveal **Quick Settings**, then drag down again to reveal the **Edit**

button  .

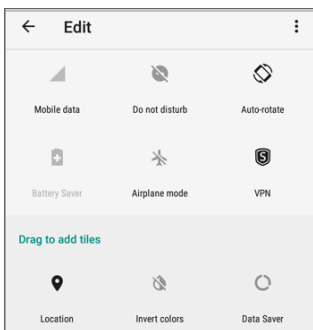
2. Tap the **Edit** button.



3. Scroll down to locate the **SonicWall Mobile Connect** icon in the bottom section.



4. Long-press the **SonicWall Mobile Connect** icon. Once it becomes highlighted, drag it to the top section.

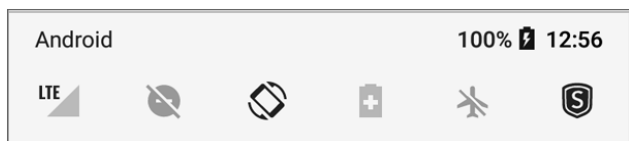


5. Press the **Back** or **Home** button to exit the Quick Settings editor.

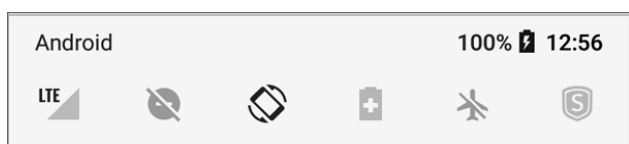
Using the Quick Settings Tile

Once the tile is installed, it will change colors to indicate whether the tunnel is connected.

Connected



Disconnected

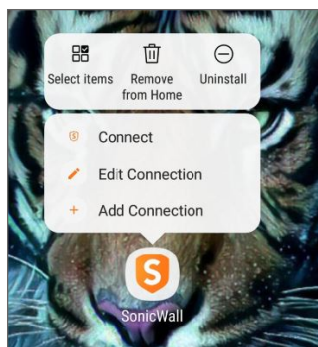


Simply tap the icon to connect or disconnect the tunnel.

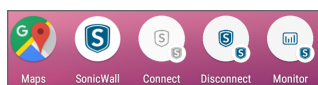
Using App Shortcuts

On Android 9 (Pie) or higher including Android 12.x, the Mobile Connect launcher icon provides shortcuts for easy access to frequently-used features, such as Connect, Disconnect, Bookmarks, and Monitor.

To reveal these shortcuts, long-press the **SonicWall Mobile Connect** icon:



Individual shortcuts may be pinned to the launcher by dragging them out of the App Shortcuts menu:



Settings, Bookmarks, and Files

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

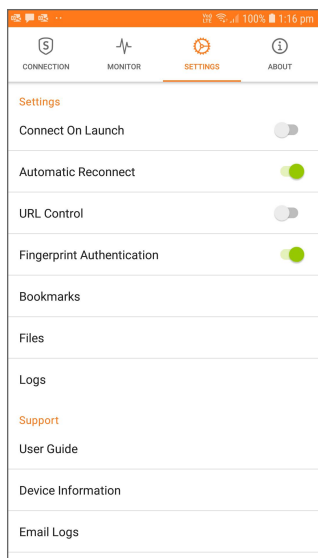
Topics:

- [Settings Overview](#)
- [URL Control Syntax and Parameters](#)
- [Using Bookmarks](#)
- [Using Files](#)

Settings Overview

SonicWall Mobile Connect provides several settings for connection and logging options. The Settings screen also provides Support information that includes a User Guide, device and connection information, and an option to email the log files to SonicWall Support.

Settings Screen



The available settings and selections are described below:

- [Settings Section](#)
- [Support Section](#)
- [Additional Settings for SMA 1000 Series](#)

Settings Section

The following options are controlled from the **Settings** section of the Settings screen:

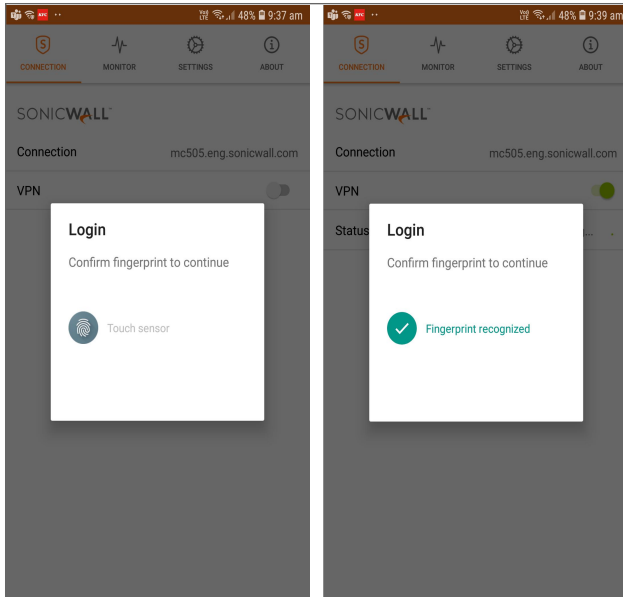
- **Connect on Launch** - Sets Mobile Connect to automatically initiate a connection to the last-used profile when the application is launched.
- **Automatic Reconnect** - Sets Mobile Connect to automatically attempt to reconnect if the connection is lost. The SSL VPN connection can be disrupted when your device's connection transitions to a different network type (for example, from wireless to cellular). 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](#).

- **Fingerprint Authentication** - Set Mobile Connect to prompt for Fingerprint Authentication during username/password authentication. Requires connection to servers that have a configured Fingerprint Authentication policy.

① **NOTE:** This setting only appears on Android devices that have fingerprint sensors running Android 6.0 or newer.

Logging In With Fingerprint Authentication



- **Bookmarks** - Displays centrally configured shortcuts, called bookmarks, to VPN resources like web pages, Remote Desktop servers, files, and terminal servers. These bookmarks, which are displayed on the main Connection tab when the VPN is connected, provide one-touch access to frequently used applications.

If using an SMA 100 Series, pulling down the Connection screen and releasing it refreshes the bookmarks. Mobile Connect supports Remote Desktop options like screen size and enable/disable audio as long as both the server bookmark and third party application support the option.

① **NOTE:** Bookmarks are supported on all supported firmware versions on SonicWall SMA 100 Series and SonicWall SMA 1000 Series, and on Next Generation Firewall appliances running SonicOS 5.9.0.2 and higher. SonicOS only supports bookmarks when using RDP-Java, VNC, Telnet, or SSHv2 on Mobile Connect.

Additional information about bookmarks is provided in [Using Bookmarks](#).

- **Files** - The **Delete Cached Files** option deletes all cached files that have been downloaded and stored on the device. Note that cached files are encrypted on the device for added security. Additional information about Files is provided in [Using Files](#).
- **Logs** - Provides the following options:
 - **Debug Logging** - Enables full debug log messages of Mobile Connect activity. Leave this setting disabled unless instructed to enable it by SonicWall Support staff.
 - **Clear Logs** - Deletes all log files saved on the device.

Support Section

The following selections are available in the **Support** section of the Settings screen:

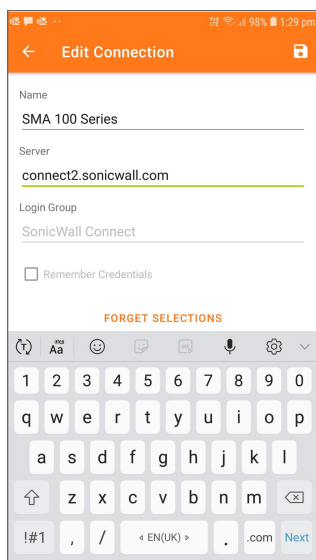
- **User Guide** - Displays the SonicWall Mobile Connect User Guide.
- **Device Information** - Displays information about the iOS device, wireless connection, cellular connection, Bluetooth connection, and DNS servers.
- **Email Logs** - Creates an email to send the Mobile Connect log files to SonicWall Support staff. Tap **Send** to send the email.

Additional Settings for SMA 1000 Series

Connections to SonicWall SMA 1000 Series have two additional options that are available on the **Edit Connection** screen.

To view these options:

1. Go to the **Connection** screen and tap and hold on the Connection line to display the **Edit Connection** screen.



2. The following options can be configured:
 - **Remember Credentials** - Enables saving of user authentication credentials for the VPN connection. This is enabled by default and can be controlled by the SMA 1000 Series Appliance setting. This feature requires version 10.7 or higher.
 - **Forget Selections** - Mobile Connect remembers the Login Group that you specified when configuring the connections. To change to a different Login Group, tap **Forget Selections**. The next time you connect to the server, you will be prompted to select a new Login Group.

NOTE: If this option is not displayed, you are connecting to either a SonicWall firewall or SMA 100 Series.

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:

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

addprofile command parameters

Command parameter	Description
<code>name</code>	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.
<code>server</code>	The domain name or IP address of the SonicWall appliance to which you wish to connect. For example: <code>vpn.example.com</code>
<code>username</code>	Optional: The username used in the VPN connection.
<code>password</code>	Optional: The password used in the VPN connection.
<code>realm</code>	Optional: The realm used in the VPN connection profile. Applies to SMA 1000 Series connections only.
<code>domain</code>	Optional: The domain used in the VPN connection profile. Applies to SMA 100 Series and Firewall connections only.
<code>sessionid</code>	Optional: The session ID or Team ID used for authentication.
<code>connect</code>	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 `addprofile` command has been processed. See [Using the callbackurl Command Parameter](#) for full details of the callback URL syntax and options.

Examples:

Following are 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:

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

connect command parameters

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 SonicWall appliance 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 on page 45 for full details of <code>callbackurl</code> syntax and options.

Examples:

Following are 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:

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

disconnect command parameters

Command parameter	Description
callbackurl	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:

Following are 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.

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 application that is opened by the callback URL. Tokens are evaluated in place, in the same order that 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:

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

- ① **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 <code>yes</code> or <code>no</code> , 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:

Following are examples using `callbackurl`:

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%24ERROR_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%24ERROR_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
```

Using Bookmarks

This section describes how to view and filter the list of bookmarks, and provides information about the types of bookmarks and associated applications that are supported by Mobile Connect.

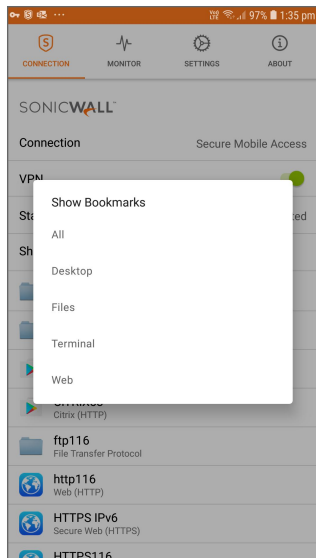
Topics:

- [Showing and Filtering Bookmarks](#)
- [Supported Bookmark Types](#)

Showing and Filtering Bookmarks

The **Mobile Connect Connection** screen displays the configured bookmarks. When there are more than five bookmarks, the bookmarks are replaced by a Filter screen that groups bookmarks by type. Select the type of bookmarks to display or select **All** to display all bookmarks.

showing and filtering bookmarks

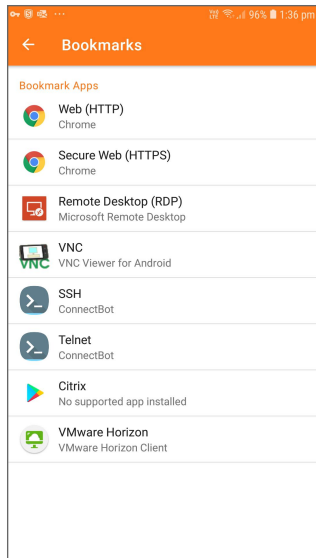


NOTE: When connected to a SonicWall Secure Mobile Access appliance with Application Access Control enabled, the Bookmarks list is replaced by a list of trusted apps that can access the corporate network

Selecting a bookmark for an app that is not installed prompts you to install the app. Apps referenced by bookmarks also can be installed at any time using the **Settings > Bookmarks** screen.

In addition to installing apps for bookmarks, the **Settings > Bookmarks** screen is also used to select and install apps for bookmarks that support multiple third-party apps. For example, you might select Chrome or Firefox for a Web bookmark.

bookmark apps



Supported Bookmark Types

This section describes the types of bookmarks and associated applications that are supported by Mobile Connect.

Topics:

- [Desktop Bookmarks](#)
- [Web Bookmarks](#)
- [Mobile Connect Bookmarks](#)
- [Terminal Bookmarks](#)

Desktop Bookmarks

Desktop bookmarks have a name that appears on the user portal, and an internal type.

Several types of desktop bookmarks are supported:

Topics:

- [RDP Bookmarks](#)
- [VNC Bookmarks](#)
- [Citrix Bookmarks](#)

RDP Bookmarks

RDP Bookmark Portal Names And Internal Types

Portal name	Internal type
Terminal Services (RDP – ActiveX)	RDP5ActiveX
Terminal Services (RDP – Java)	RDP5Java
Terminal Services (RDP – HTML5)	RDP5HTML5

① | **NOTE:** RDP (HTML5) bookmarks are launched within Mobile Connect and do not launch a third-party app.

RDP bookmark types attempt to launch with the associated RDP application, as configured in the **Settings** screen. See the RDP applications and versions table.

RDP Applications And Versions

Application	Android version
Parallels Client (Legacy)	14.1.3379
Remote RDP Lite	4.3.12
Remote RDP	4.3.15
Remote RDP Enterprise	4.3.15
Microsoft Remote Desktop	8.1.27

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters varies based on the application. For example:

- Parallels Client does not accept screen resolution settings on Android

VNC Bookmarks

VNC Bookmark Portal Names And Internal Types

Portal name	Internal type
Virtual Network Computing (VNC)	VNC
Virtual Network Computing (VNC – HTML5)	VNCHTML5

① | **NOTE:** VNC (HTML5) bookmarks are launched within Mobile Connect and do not launch a third-party app.

VNC bookmark types attempt to launch with the associated VNC application as configured in the **Settings** screen.

VNC Applications And Versions

Application	Android version
VNC Viewer for Android	0.5.0

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters varies based on the application.

Citrix Bookmarks

Citrix Bookmark Portal Names And Internal Types

Portal name	Internal type
Citrix Portal (Citrix)	Citrix
Citrix Portal (Citrix)	Citrix_https

Citrix bookmark types attempt to launch with the associated Citrix application.

Citrix Application And Version

Application	Android version
Citrix Receiver	3.8.1

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters varies based on the application.

Web Bookmarks

Web bookmarks have a name that appears on the user portal, and an internal type.

Web Bookmark Portal Names And Internal Types

Portal name	Internal type
Web (HTTP)	HTTP
Secure Web (HTTPS)	HTTPS
External Web Site	URL
External Web Site	URL_https

These bookmarks launch in an associated web browser, or in the Mobile Connect in-app browser (if configured on the server), and the provided "Name or IP Address" (HostID) is passed as the URL to display in the browser.

Browser Types And Versions

Browser type	Android version
Any browser	Yes
Google Chrome	47.0.2526.83

Mobile Connect Bookmarks

Mobile Connect bookmarks have a name that appears on the user portal, and an internal type.

Mobile Connect Bookmark Portal Names And Internal Types

Portal name	Internal type
Mobile Connect	MC

The Mobile Connect bookmark type relies on the operating system to determine and launch the proper application. The bookmark is expected to be properly configured for launch. The Mobile Connect app attempts to launch it as is. (For example, `telnet://server`).

Terminal Bookmarks

Terminal bookmarks have a name that appears on the user portal, and an internal type.

Terminal Bookmark Portal Names And Internal Types

Portal name	Internal type
Telnet	Telnet
Telnet (HTML5)	TelnetHTML5
Secure Shell Version 1 (SSHv1)	SSH
Secure Shell Version 2 (SSHv2)	SSHv2
Secure Shell Version 2 (HTML5)	SSHv2HTML5

① | **NOTE:** The Telnet (HTML5) & SSH (HTML5) bookmarks are launched within Mobile Connect and do not launch a third-party app.

The applications and versions used are shown in the Terminal applications and versions table.

Terminal Applications And Versions

Application	Android version
ConnectBot	1.8.6
JuiceSSH - SSH Client	2.1.12

Proper formatting is required for ConnectBot SSH (server bookmark field requires `username@server`).

① | **NOTE:** Some supported third party apps may not yet be available in the Amazon Appstore.

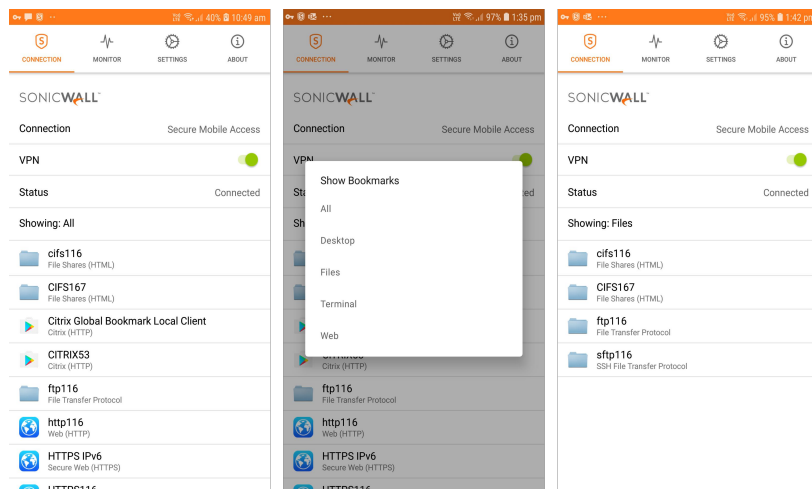
Using Files

Mobile Connect 5.0 supports secure mobile access to files through File bookmarks. File bookmarks allow secure access to files by first checking and enforcing the server configured file policy, and then securely downloading and displaying the file within the Mobile Connect application.

Granular policy controls can be configured to allow other Android apps to use each file. On Android, policies include control over whether a file may be opened in a third-party application, or securely cached on the Android device. File bookmarks can also be created to folders or file share root directories to allow directory navigation.

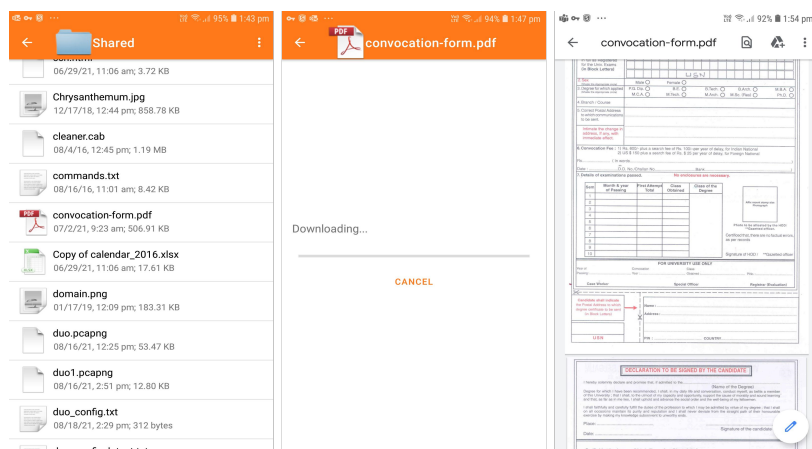
When File bookmarks are configured for the user on the server appliance, they appear in the list of bookmarks after the VPN is established and can be filtered by selecting the **Showing** row that is displayed when there are more than five bookmarks. See Showing Files bookmarks.

Showing Files Bookmarks



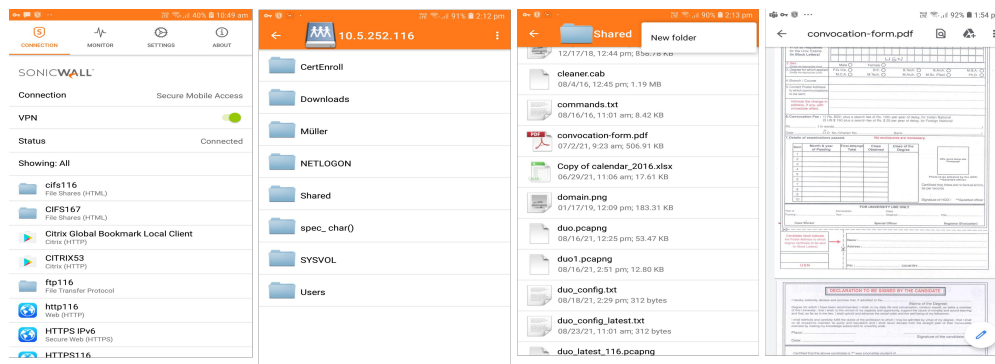
Tapping a File bookmark queries the server and enforces any file policies configured on the server for that File bookmark. If the file is not already cached on the device, the file is securely downloaded from the SMA 100 Series. Once the file is downloaded, it is opened in the Android default file viewer app for that file type.

Tapping A File Bookmark



Tapping a File bookmark to a folder or directory allows for directory browsing and file download and viewing of any file in the folder. All attempts to browse a file folder or view a file query the server to enforce access policies. On Android, the default file viewer app is automatically launched after a file is downloaded.

Browsing Folders And Viewing Files



For information about supported file types and other actions you can take on files, see [File Types and Policies](#).

File Types and Policies

A number of file types are supported natively on Android and third-party apps can open other file types. Policies on the server control whether a file can be opened with a third-party app.

See the following:

- [Supported File Types](#)
- [Unsupported File Types](#)
- [File Policies](#)

Supported File Types

Mobile Connect supports the file types natively supported by Android, as shown in the Supported file types table.

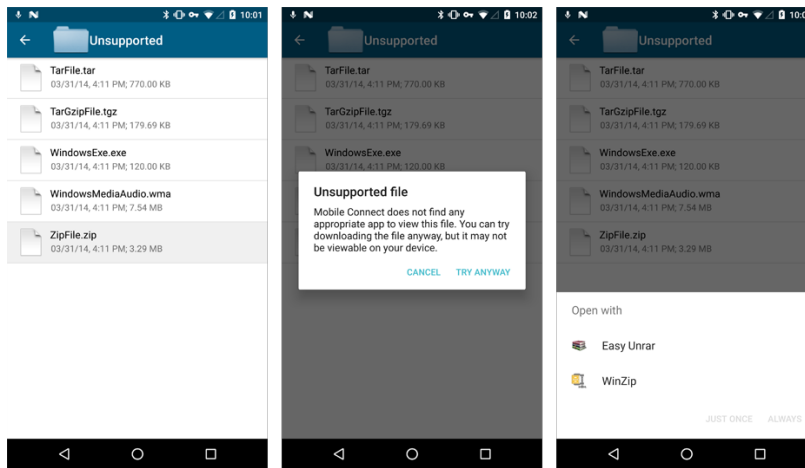
Supported File Types

File type	File extension
Images	.jpg, .jpeg, .tif, .tiff, .png
Music	.mp3, .m4a, .wav
Movies	.mov, .mp4
Microsoft Word documents	.doc, .docx
Microsoft Excel spreadsheets	.xls, .xlsx
Microsoft PowerPoint presentations	.ppt, .pptx
Adobe PDF	.pdf
Web pages	.htm, .html
Text and Rich-text files	.txt, .rtf

Unsupported File Types

If a file type is not supported, an *Unsupported file* message is displayed, indicating that the file might not be viewable unless another application is installed that can view the file. Tap **Try Anyway** to try opening the file with another application that might be registered to handle that file type. See Trying to open an unsupported file.

Trying To Open An Unsupported File

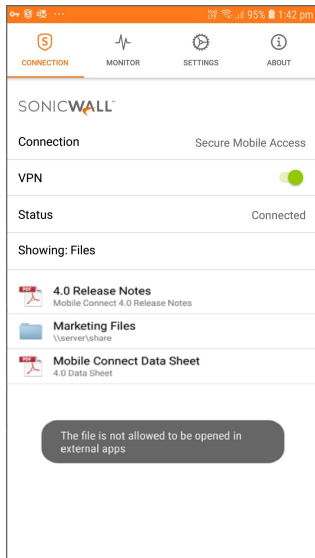


File Policies

On Android, server-configured policies control whether a file can be opened in a third-party app or securely cached on the device.

For example, if a file has the *Allow Open In* policy disabled, the file cannot be viewed on an Android device. Mobile Connect launches third-party apps to view all file types, so the *Allow Open In* policy must be enabled to view a file.

File Policy - File Not Allowed



Application Access Control

Mobile Connect 5.0 and higher supports the Application Access Control feature in SonicWall Secure Mobile Access 11.4 and higher on SonicWall SMA 1000 Series.

Topics:

- [About Application Access Control](#)
- [Logging in and Registering your Device](#)
- [Controlling App Behavior](#)
- [Viewing the App List after Connecting](#)
- [About Learning Mode \(Administrators Only\)](#)

About Application Access Control

Application Access Control allows remote access administrators to control exactly which resources on the corporate network each application (app) can access. Meanwhile, the device owner can still use their personal Android device for their own activities such as personal email, financial data, pictures, music, accessing third party web sites, etc.

If the SMA 1000 Series administrator has configured this feature, you will log in to a **Login Group** that allows a list of trusted apps to access corporate resources. The specific version of each app is included in the configuration.

The Application Access Control rule list controls the following:

- Which applications can send data through the VPN tunnel
- Which destinations on the corporate network those applications are allowed to access

When connected to a SonicWall SMA 1000 Series Appliance running SonicWall Secure Mobile Access 11.0 or higher with Application Access Control configured, device traffic is handled in four ways:

1. For applications listed and selected in the application list, traffic destined for the corporate network from those applications is allowed to enter the VPN tunnel. The application ID and signature are used by the server to identify the application.

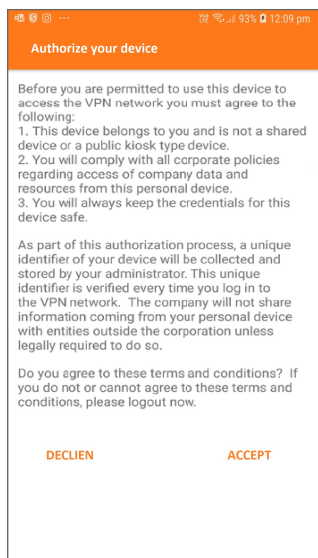
2. For applications that are on that list and are not selected (or any other application on the device), traffic destined for the corporate network is blocked and/or dropped by Mobile Connect and does NOT enter the tunnel.
3. All applications (regardless of whether or not they are on the application list) send traffic out the default interface of the device if the traffic is NOT destined for the corporate network.
4. The information status symbol 'i' displays on applications that are learned by the appliance but still have at least one version pending approval.

Logging in and Registering your Device

The first time you connect and log in, you must agree to the displayed terms and conditions. These include:

- The device belongs to you and is not a shared device.
- You will comply with all corporate policies.
- You will keep the device credentials safe.
- The device identifier can be collected and stored by the server administrator.

Agreeing To Terms



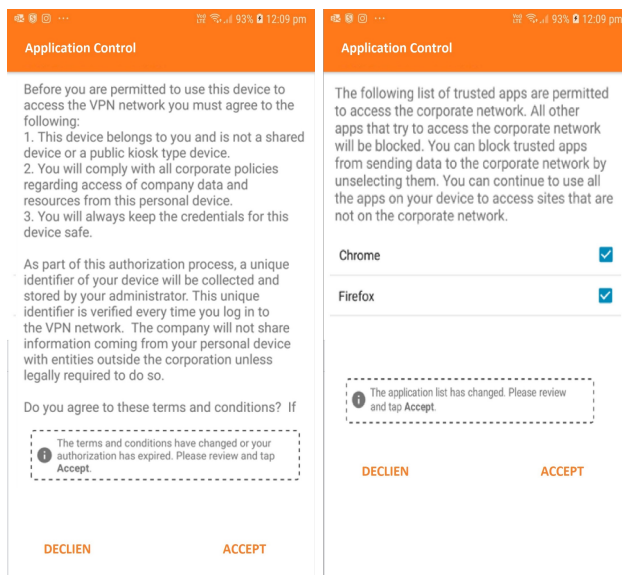
To agree and continue, tap **ACCEPT**.

Your device is then registered with the server, and will be recognized in later connections.

Multiple personal devices can be authorized for a single user, and a single personal device may be registered by multiple users.

If the policy or list of trusted apps changes, you are asked to re-accept the terms and conditions.

Changes In Terms Or Trusted Apps



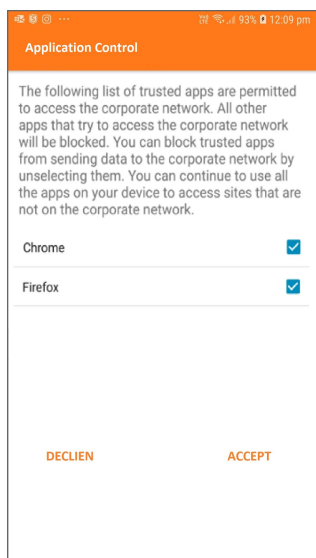
To agree and continue, tap **ACCEPT**.

Controlling App Behavior

The list of trusted apps is displayed on your device after you agree to the terms and conditions.

NOTE: To request that additional apps be added to the trusted apps list, contact the SonicWall SMA 1000 Series administrator.

Trusted App List



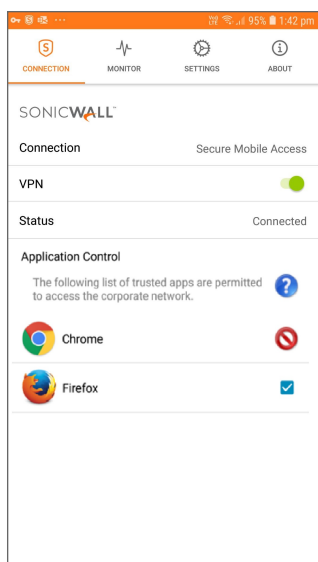
To control app behavior:

1. Clear the check box next to the app to prevent the app from sending data to the corporate network. Typically, you would do this for any application that is only being used for personal tasks or information.
2. Tap **ACCEPT** to continue with the connection to the SMA 1000 Series Appliance.



Viewing the App List after Connecting


The Application Control section of an active connection screen displays the list of apps that are known by the server.

App List With Mixed Status

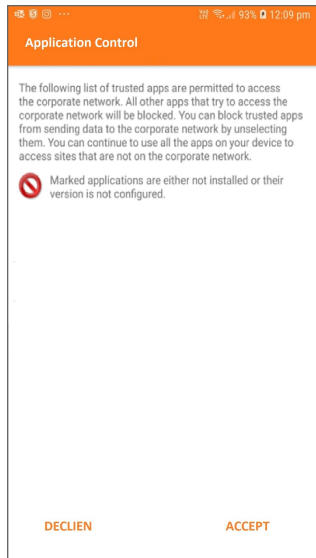


A status indicator is displayed next to each app.

- A check mark  indicates that the app is installed on your device and is permitted to access the corporate network.
- A red circle with a slash  indicates one of the following conditions:
 - The version of the app on your device is not the same as the approved version in the server.
 - The app is approved by the server, but it is not installed on your device.

Tapping the **Application Control** help icon  displays information about Application Control. Tap **OK** to exit the help screen.

Application Control Help



About Learning Mode (Administrators Only)

Designated administrators can use Android devices as trusted learning devices when working with SonicWall SMA 1000 Series appliances running Secure Mobile Access 11.0 and higher with Application Access Control enabled. A trusted learning device is assigned special privileges to perform signature lookups as a part of the process of learning application version information. When the trusted learning device is connected to the SMA 1000 Series Appliance, apps that need versions to be learned are displayed. After launching the app, a '!' "pending approval" icon displays next to the app name. The app can then be approved by the SMA 1000 Series administrator.

For more information about configuring Application Access Control on the SMA 1000 Series running SMA 11.0 and higher, see the *SonicWall Secure Mobile Access Application Access Control Feature Guide*, available on the SonicWall Support portal.

Monitoring and Troubleshooting

This section discusses the Mobile Connect Monitor screen and provides troubleshooting tips.

Topics:

- [Monitoring Mobile Connect](#)
- [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.

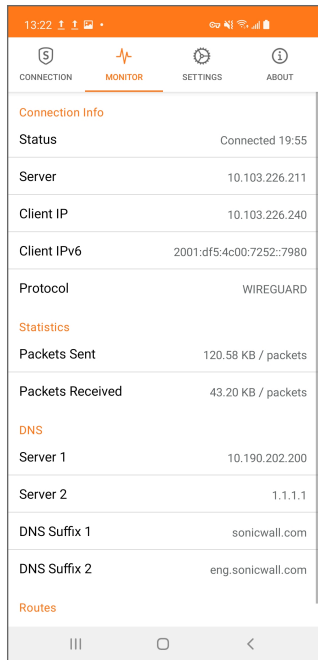
① | **NOTE:** Displaying the protocol information in **Monitor** when connected to different appliances:

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.

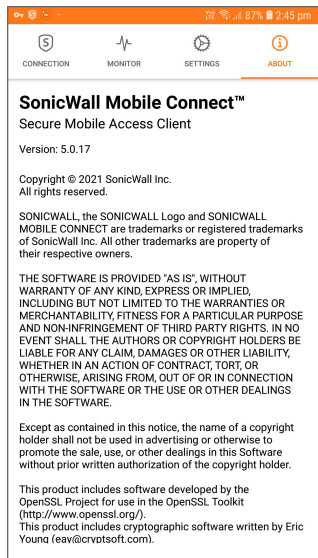
When you are connected to SonicWall SMA 1000 Series, you will not see the **Protocol** information.

Monitor Screen



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

About Screen



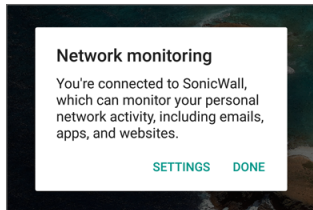
When a Mobile Connect session is active, the Android notifications panel includes a key icon indicating that the VPN is connected.

Key Icon In Notification Panel



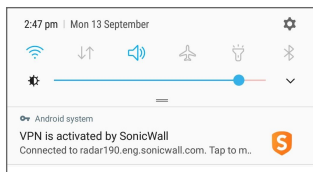
Tapping on the **Network may be monitored** message in the Android notification panel displays a dialog that the device is connected to SonicWall.

Network Monitoring Dialog



Tapping **Settings** opens the VPN section of the Android Settings app and shows the status of Mobile Connect.

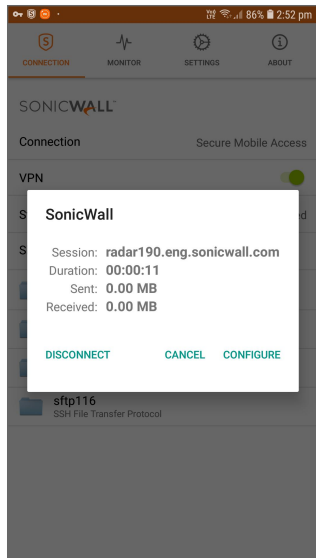
VPN Status



Tapping the SonicWall row in the VPN list displays a dialog that provides two buttons:

- **Cancel** - Closes the dialog.
- **Disconnect** - Disconnects the Mobile Connect session.

Disconnect VPN Dialog



Troubleshooting Mobile Connect

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

Topics:

- [Failed End Point Control Check](#)
- [General Troubleshooting](#)

Failed End Point Control Check

End Point Control can prevent the connection when the server is an SMA 1000 Series or SMA 100 Series. During the connection process, the connection status displays **EPC checking...** while the End Point Security policy checks are performed. If the device is not compliant because a security check failed, an error message is then displayed.

EPC checking

You can view the Mobile Connect log for more detailed information about which check failed. For example, you might see the following if an EPC policy was set up to restrict access to only a single device ID (EQUIPMENT ID).

```
2014-07-10 13:08:23:974 DEBUG Thread-142 - SmaEpcManager - Allow Profile:
{AndroidEPCExamplePolicy:[Literal=EQUIPMENTID,1,1234567890]}
2014-07-10 13:08:23:976 DEBUG Thread-142 - SmaEpcManager - Deny Profile: {}
```



```
2014-07-10 13:08:23:977 DEBUG Thread-142 - SmaEpcManager - Recurring Mode: 1
2014-07-10 13:08:23:978 DEBUG Thread-142 - SmaEpcManager - Recurring Period: 1
2014-07-10 13:08:24:200 DEBUG Thread-142 - SmaEvaluator - Evaluate literal:
Literal=EQUIPMENTID,1,1234567890
2014-07-10 13:08:24:200 DEBUG Thread-142 - SmaEvaluator - DeviceID<abcda50e-
e13b-1234-b89d-b3da7384a2f5>, expect<1234567890>
2014-07-10 13:08:24:201 INFO Thread-142 - SmaEpcManager - Failed allow profile:
Literal=EQUIPMENTID,1,1234567890
```

When the server is either an SMA 1000 Series or an SMA 100 Series, policies can be created to check different attributes of the Android device, including:

- Rooted or Not Rooted
- Client certificate installed
- Android OS version
- Device ID / Equipment ID
- Anti-Virus App
- Personal Firewall App
- Application
- Directory name
- File name

See the *SonicWall SMA Administration Guide* for the server for complete information about End Point Control policy options.

General Troubleshooting

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 web browser on your device and attempt to navigate to the SMA appliance 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. On the **Settings** tab, 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 return to the **Settings** tab and tap the **Email Logs** button. 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 tap **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 Android User Guide

Updated - December 2023

Software Version - 5.0

232-004062-00 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