SonicWall™ Mobile Connect for Android 4.0

User Guide
## Contents

**Introduction to Mobile Connect** .......................................................... 5  
How Mobile Connect Works ....................................................................... 5  
New Features in Mobile Connect 4.0 ......................................................... 6  
Supported Platforms ................................................................................. 7  
  Android Product Support ........................................................................ 7  
  SonicWall Appliance Support ................................................................. 8  
Required Network Information ................................................................. 8

**Installing and Connecting** ....................................................................... 9  
Installing Mobile Connect ........................................................................ 9  
Creating and Saving Connections ............................................................. 10  
  Creating Firewall or SMA 100 Series / SRA Connections ...................... 11  
  Creating SMA 1000 Series / E-Class SRA Connections ....................... 13  
Initiating a Connection ............................................................................. 14  
  Connecting to a Firewall or SMA 100 Series / SRA Appliance .............. 14  
  Connecting to an SMA 1000 Series / E-Class SRA Appliance .............. 18  
Configuring Client Certificates ................................................................. 25  
  Client Certificates with SMA 1000 Series / E-Class SRA .................... 25  
  Client Certificates with SMA 100 Series / SRA .................................... 27  
Using the Mobile Connect Widget ............................................................. 30

**Settings, Bookmarks, and Files** ............................................................. 31  
Settings Overview .................................................................................. 31  
  Settings Section .................................................................................... 32  
  Support Section .................................................................................... 33  
  Additional Settings for SMA 1000 Series / E-Class SRA ....................... 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 ..................................................................................... 38  
  Showing and Filtering Bookmarks ......................................................... 38  
  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 ......................................................................... 51  
Viewing the App List after Connecting ..................................................... 52  
About Learning Mode (Administrators Only) ............................................. 53
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.

Topics:
- How Mobile Connect Works on page 5
- New Features in Mobile Connect 4.0 on page 6
- Supported Platforms on page 7

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 4.0

This section describes the enhancements included in the Mobile Connect 4.0 release.

- **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 now 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 now 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**

<table>
<thead>
<tr>
<th>Native HTML5 Bookmarks:</th>
<th>SSH Bookmark:</th>
<th>RDP Bookmark:</th>
</tr>
</thead>
<tbody>
<tr>
<td>My PC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Production Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VNC to Mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSHv2 to Linux</td>
<td></td>
<td></td>
</tr>
<tr>
<td>macOS Sierra</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Supported Platforms**

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

- Android Product Support on page 7
- SonicWall Appliance Support on page 8
- Required Network Information on page 8

**Android Product Support**

SonicWall Mobile Connect requires the Android 4.1 or newer platform and a cellular or Wi-Fi connection.

SonicWall Mobile Connect has been verified to run on the following Android devices running the official Android 4.1 or newer platform:

- Dell Venue 7
- Dell Venue 8
- Huawei Nexus 6P
- ASUS Nexus 7
- ASUS FonePad
- LG Nexus 4
- Samsung Nexus 10
- Samsung Galaxy S2
- Samsung Galaxy S3
- Samsung Galaxy S4
- Samsung Galaxy S5
- Samsung Galaxy Tab
SonicWall Mobile Connect for Android 4.0 User Guide

Introduction to Mobile Connect

SonicWall Mobile Connect is a free app, but minimally requires a concurrent user license on one of the following SonicWall solutions. However, in order to use the new Mobile Connect features properly, the newer versions of these OS types are required.

- SonicWall firewall appliances including the TZ, NSA, E-Class NSA, and SuperMassive™ 9000 Series running SonicOS 5.8.1.0 or higher
- SonicWall Secure Mobile Access 100 Series / SRA appliances running 7.5 or higher
- SonicWall Secure Mobile Access 1000 Series / E-Class SRA appliances running 10.7 or higher.

To support Per App VPN, the appliance must be running SonicWall Secure Mobile Access (SMA) 11.0 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 on page 8.

- **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.
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 on page 9
- Creating and Saving Connections on page 10
- Initiating a Connection on page 14
- Configuring Client Certificates on page 25
- Using the Mobile Connect Widget on page 30

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:

Amazon Appstore:

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:


**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 / SRA Connections on page 11
- Creating SMA 1000 Series / E-Class SRA Connections on page 13
Creating Firewall or SMA 100 Series / SRA Connections

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

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.

![Screen capture of SonicWall Mobile Connect interface showing username and password fields](image.png)

**NOTE:** If the previous screenshot does not match what is displayed on your device, you are connecting to a SonicWall SMA 1000 Series / E-Class SRA appliance. See [Creating SMA 1000 Series / E-Class SRA Connections](#) on page 13.

6 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**.

![Screen capture of SonicWall Mobile Connect interface showing domain selection](image.png)
Creating SMA 1000 Series / E-Class SRA Connections

To create and save a new connection to a SonicWall SMA 1000 Series / E-Class SRA appliance:

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.

   ![Warning Message]

   
   Warning
   ‘vpn.example.com’ is either currently unreachable or is not a valid SonicWall appliance. Would you like to save this connection anyway?

   CANCEL  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 / SRA Appliance on page 14
- Connecting to an SMA 1000 Series / E-Class SRA Appliance on page 18

Connecting to a Firewall or SMA 100 Series / SRA Appliance

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.

3. The first time you initiate a connection, a Connection Request message displays. Tap OK to continue.
4 When the connection is successfully established, the **Status** changes to **Connected** and the VPN switch remains in the ON position.

![Connection Screen]

**NOTE:** If this sequence of events does not match what is displayed on your device, you are connecting to a SonicWall SMA 1000 Series / E-Class SRA appliance. See [Connecting to an SMA 1000 Series / E-Class SRA Appliance](#) on page 18.

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 / E-Class SRA Appliance

After you save a new SMA 1000 Series / E-Class SRA 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

After you save a new SMA 1000 Series / E-Class SRA 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.
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.

![Login Group Selection]

**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 / SRA appliance. See Connecting to a Firewall or SMA 100 Series / SRA Appliance on page 14.

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 / E-Class SRA server 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 / E-Class SRA server with Application Access Control configured, a notification about Data Privacy with a list of the applications under control is displayed. Optionally, clear the checkboxes 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.

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.

**NOTE:** SonicWall SMA 1000 Series / E-Class SRA connections do not currently support Files bookmarks.
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 / E-Class SRA appliances and SMA 100 Series / SRA appliances.

Topics:
- [Client Certificates with SMA 1000 Series / E-Class SRA](#) on page 25
- [Client Certificates with SMA 100 Series / SRA](#) on page 27

### Client Certificates with SMA 1000 Series / E-Class SRA

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**

![No certificates found dialog]

The app SonicWall has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future. The app has identified the requesting server as ora-k609-eng.sonicwall.com, but you should only give access to the certificate if you trust the app.

You can install certificates from a PKCS#12 file with a .p12 or a .pfx extension located in external storage.

[INSTALL]

[CANCEL]
Client Certificates with SMA 100 Series / SRA

On SonicWall SMA 100 Series / SRA appliances, 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. See Editing the connection to change the certificate.
Editing the connection to change the certificate
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**

The app SonicWall has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future. The app has identified the requesting server as secNUL.ing.sonicwall.com, but you should only give the app access to the certificate if you trust the app.

You can install certificates from a PKCS#12 file with a .pfx or a .p12 extension located in external storage.
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
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 on page 31
- URL Control Syntax and Parameters on page 34
- Using Bookmarks on page 38
- Using Files on page 43

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** on page 32
- **Support Section** on page 33
- **Additional Settings for SMA 1000 Series / E-Class SRA** on page 33

## 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** on page 34.

- **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.

  ![Note](image)

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

- **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 / SRA appliance, 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.

  ![Note](image)

  **NOTE:** Bookmarks are supported on all supported firmware versions on SonicWall SMA 100 Series / SRA appliances and SonicWall SMA 1000 Series / E-Class SRA appliances, 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** on page 38.

- **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** on page 43.

- **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:

- **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 / E-Class SRA

Connections to SonicWall SMA 1000 Series / E-Class SRA appliances 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 / E-Class SRA server 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 / SRA appliance.
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 on page 34
- Using the connect Command on page 35
- Using the disconnect Command on page 36
- Using the callbackurl Command Parameter on page 37

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...]
```

<table>
<thead>
<tr>
<th>Command parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>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.</td>
</tr>
<tr>
<td>server</td>
<td>The domain name or IP address of the SonicWall appliance to which you wish to connect. For example: vpn.example.com</td>
</tr>
<tr>
<td>username</td>
<td>Optional: The username used in the VPN connection.</td>
</tr>
<tr>
<td>password</td>
<td>Optional: The password used in the VPN connection.</td>
</tr>
<tr>
<td>realm</td>
<td>Optional: The realm used in the VPN connection profile. Applies to SMA 1000 Series / E-Class SRA connections only.</td>
</tr>
<tr>
<td>domain</td>
<td>Optional: The domain used in the VPN connection profile. Applies to SMA 100 Series / SRA and Firewall connections only.</td>
</tr>
<tr>
<td>sessionid</td>
<td>Optional: The session ID or Team ID used for authentication.</td>
</tr>
<tr>
<td>connect</td>
<td>Optional: If presented and the value is non-null, the connection is initiated if the profile was successfully added.</td>
</tr>
<tr>
<td>callbackurl</td>
<td>Optional: The callback URL to be opened by Mobile Connect after the addprofile command has been processed. See Using the callbackurl Command Parameter on page 37 for full details of the callback URL syntax and options.</td>
</tr>
</tbody>
</table>

Examples:

Following are examples of the addprofile command:

```
mobileconnect://addprofile/?name=Example&server=vpn.example.com
```
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...]
```

<table>
<thead>
<tr>
<th>Connect command parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>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.</td>
</tr>
<tr>
<td>server</td>
<td>The domain name or IP address of the SonicWall appliance in which you wish to connect. For example: vpn.example.com</td>
</tr>
<tr>
<td>username</td>
<td>Optional: The username used in the VPN connection.</td>
</tr>
<tr>
<td>password</td>
<td>Optional: The password used in the VPN connection.</td>
</tr>
<tr>
<td>realm</td>
<td>Optional: The realm used in the VPN connection profile. Applies to SMA 1000 Series / E-Class SRA connections only.</td>
</tr>
<tr>
<td>domain</td>
<td>Optional: The domain used in the VPN connection profile. Applies to SMA 100 Series / SRA and Firewall connections only.</td>
</tr>
<tr>
<td>sessionid</td>
<td>Optional: The session ID or Team ID used for authentication.</td>
</tr>
<tr>
<td>connect</td>
<td>Optional: If presented and the value is non-null, the connection is initiated if the profile was successfully added.</td>
</tr>
<tr>
<td>callbackurl</td>
<td>Optional: The callback URL is opened by Mobile Connect after the connect command has been processed. See Using the callbackurl Command Parameter on page 37 for full details of callbackurl syntax and options.</td>
</tr>
</tbody>
</table>
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%202&server=vpn.example.com
mobileconnect://connect?name=SRA%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

<table>
<thead>
<tr>
<th>Command parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callbackurl</td>
<td>Optional: The URL defined for callbackurl is opened by Mobile Connect after the disconnect command has been processed. See Using the callbackurl Command Parameter on page 37 for full details of callbackurl syntax and options.</td>
</tr>
</tbody>
</table>

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>
```

**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

<table>
<thead>
<tr>
<th>Dynamic token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>$ERROR_CODE$</code></td>
<td>The numerical value of the error from the failed connection attempt.</td>
</tr>
<tr>
<td><code>$ERROR_MESSAGE$</code></td>
<td>The string value of the error message from the failed connection attempt.</td>
</tr>
<tr>
<td><code>$LOGIN_GROUP$</code></td>
<td>The string value of the authentication login group or realm. Applies to SMA 1000 Series / E-Class SRA connections only.</td>
</tr>
<tr>
<td><code>$COMMUNITY$</code></td>
<td>The string value of authentication community. Applies to SMA 1000 Series / E-Class SRA connections only.</td>
</tr>
<tr>
<td><code>$ZONE$</code></td>
<td>The string value of EPC (End Point Control) zone. Applies to SMA 1000 Series / E-Class SRA connections only.</td>
</tr>
<tr>
<td><code>$TUNNEL_IP$</code></td>
<td>The string value of the Mobile Connect IPv4 client address.</td>
</tr>
<tr>
<td><code>$TUNNEL_MODE$</code></td>
<td>One of split, split-nonlocal, redirectall, or redirectall-nonlocal, depending on the tunnel mode. Applies to SonicWall SMA 1000 Series / E-Class SRA connections only.</td>
</tr>
<tr>
<td><code>$ESP_ENABLED$</code></td>
<td>One of yes or no, depending on if ESP (Encapsulating Security Payload) is enabled. Applies to SonicWall SMA 1000 Series / E-Class SRA 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.</td>
</tr>
</tbody>
</table>

**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:**

```
```

---

**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** on page 38
- **Supported Bookmark Types** on page 40

---

**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

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

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.
Supported Bookmark Types

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

Topics:
- Desktop Bookmarks on page 40
- Web Bookmarks on page 41
- Mobile Connect Bookmarks on page 42
- Terminal Bookmarks on page 42

Desktop Bookmarks

Desktop bookmarks have a name that appears on the user portal, and an internal type. Several types of desktop bookmarks are supported:
- RDP Bookmarks on page 40
- VNC Bookmarks on page 41
- Citrix Bookmarks on page 41

RDP Bookmarks

RDP bookmark portal names and internal types

<table>
<thead>
<tr>
<th>Portal name</th>
<th>Internal type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Services (RDP – ActiveX)</td>
<td>RDPSActiveX</td>
</tr>
<tr>
<td>Terminal Services (RDP – Java)</td>
<td>RDPSJava</td>
</tr>
<tr>
<td>Terminal Services (RDP – HTML5)</td>
<td>RDPSHTML5</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Application</th>
<th>Android version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parallels 2X RDP</td>
<td>14.1.3379</td>
</tr>
<tr>
<td>Remote RDP Lite</td>
<td>4.3.12</td>
</tr>
<tr>
<td>Remote RDP</td>
<td>4.3.15</td>
</tr>
<tr>
<td>Remote RDP Enterprise</td>
<td>4.3.15</td>
</tr>
<tr>
<td>Microsoft Remote Desktop</td>
<td>8.1.27</td>
</tr>
</tbody>
</table>

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 2X client does not accept screen resolution settings on Android
VNC Bookmarks

VNC bookmark portal names and internal types

<table>
<thead>
<tr>
<th>Portal name</th>
<th>Internal type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Network Computing (VNC)</td>
<td>VNC</td>
</tr>
<tr>
<td>Virtual Network Computing (VNC – HTML5)</td>
<td>VNCHTML5</td>
</tr>
</tbody>
</table>

**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.

**Application and versions**

<table>
<thead>
<tr>
<th>Application</th>
<th>Android version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNC Viewer for Android</td>
<td>0.5.0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Portal name</th>
<th>Internal type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Portal (Citrix)</td>
<td>Citrix</td>
</tr>
<tr>
<td>Citrix Portal (Citrix)</td>
<td>Citrix_https</td>
</tr>
</tbody>
</table>

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

**Application and versions**

<table>
<thead>
<tr>
<th>Application</th>
<th>Android version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Receiver</td>
<td>3.8.1</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Portal name</th>
<th>Internal type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web (HTTP)</td>
<td>HTTP</td>
</tr>
<tr>
<td>Secure Web (HTTPS)</td>
<td>HTTPS</td>
</tr>
<tr>
<td>External Web Site</td>
<td>URL</td>
</tr>
<tr>
<td>External Web Site</td>
<td>URL_https</td>
</tr>
</tbody>
</table>
These bookmarks launch in an associated web browser and the provided “Name or IP Address” (HostID) is passed as the parameter to display in the browser.

**Browser types and versions**

<table>
<thead>
<tr>
<th>Browser type</th>
<th>Android version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any browser</td>
<td>Yes</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>47.0.2526.83</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Portal name</th>
<th>Internal type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Connect</td>
<td>MC</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Portal name</th>
<th>Internal type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>Telnet</td>
</tr>
<tr>
<td>Telnet (HTML5)</td>
<td>TelnetHTML5</td>
</tr>
<tr>
<td>Secure Shell Version 1 (SSHv1)</td>
<td>SSH</td>
</tr>
<tr>
<td>Secure Shell Version 2 (SSHv2)</td>
<td>SSHv2</td>
</tr>
<tr>
<td>Secure Shell Version 2 (HTML5)</td>
<td>SSHv2HTML5</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Application</th>
<th>Android version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectBot</td>
<td>1.8.6</td>
</tr>
<tr>
<td>JuiceSSH - SSH Client</td>
<td>2.1.12</td>
</tr>
</tbody>
</table>

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

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

Mobile Connect 4.0 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.

NOTE: In SonicWall Mobile Connect for Android 4.0, File bookmarks are supported only on the SonicWall SMA 100 Series / SRA appliances. Support for File bookmarks in SMA 1000 Series / E-Class SRA and Next Generation Firewall appliances is expected in a future release.

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 / SRA appliance. 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 on page 45.
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 on page 45
- Unsupported File Types on page 45
- File Policies on page 47

Supported File Types

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

Supported file types

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

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**

Mobile Connect does not find any appropriate app to view this file. You can try downloading the file anyway, but it may not be viewable on your device.
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

![Image showing the Mobile Connect app interface with a file policy notification]

The file is not allowed to be opened in external apps
Application Access Control

Mobile Connect 4.0 and higher supports the Application Access Control feature in SonicWall Secure Mobile Access 11.0 and higher on SonicWall SMA 1000 Series / E-Class SRA appliances.

Topics:
- About Application Access Control on page 48
- Logging in and Registering your Device on page 49
- Controlling App Behavior on page 51
- Viewing the App List after Connecting on page 52
- About Learning Mode (Administrators Only) on page 53

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 / E-Class SRA 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 / E-Class SRA server 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**

![Authorize your device](image)

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**

Before you are permitted to use this device to access the VPN network you must agree to the following:
1. This device belongs to you and is not a shared device or a public kiosk type device.
2. You will comply with all corporate policies regarding access of company data and resources from this personal device.
3. You will always keep the credentials for this device safe.

As part of this authorization process, a unique identifier of your device will be collected and stored by your administrator. This unique identifier is verified every time you log in to the VPN network. The company will not share information coming from your personal device with entities outside the corporation unless legally required to do so.

Do you agree to these terms and conditions? If authorization has expired, please review and tap Accept.

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 / E-Class SRA appliance administrator.

**Trusted app list**

The following list of trusted apps are permitted to access the corporate network. All other apps that try to access the corporate network will be blocked. You can block trusted apps from sending data to the corporate network by unselecting them. You can continue to use all the apps on your device to access sites that are not on the corporate network.

1. Clear the checkbox 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 / E-Class SRA server.
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**

![Application Control help screen]

**About Learning Mode (Administrators Only)**

Designated administrators can use Android devices as trusted learning devices when working with SonicWall SMA 1000 Series / E-Class SRA 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 / E-Class SRA server, 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 / E-Class SRA administrator.

For more information about configuring Application Access Control on the SMA 1000 Series / E-Class SRA appliances 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 on page 54
- Troubleshooting Mobile Connect on page 57

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 / SRA appliance running SRA 7.5 or higher with compression enabled. Traffic over the VPN tunnel is compressed using the LZ4 algorithm.

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

**About screen**

![About screen](image)

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**

![Key icon in notification panel](image)
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**

![Network monitoring dialog](image)

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

**VPN status**

![VPN status](image)
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**

![Disconnect VPN dialog](image)

**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](#) on page 58
- [General Troubleshooting](#) on page 59
Failed End Point Control Check

End Point Control can prevent the connection when the server is an SMA 1000 Series / E-Class SRA appliance or SMA 100 Series / SRA appliance. 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 - SraEpcManager - Allow Profile: {AndroidEPCExamplePolicy:[Literal=EQUIPMENTID,1,1234567890]}
2014-07-10 13:08:23:977 DEBUG Thread-142 - SraEpcManager - Recurring Mode: 1
2014-07-10 13:08:24:200 DEBUG Thread-142 - SraEvaluator - DeviceID<abcda50e-e13b-1234-b89d-b3da7384a2f5>, expect<1234567890>
When the server is either an SMA 1000 Series / E-Class SRA appliance or an SMA 100 Series / SRA appliance, 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.
Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, refer to https://support.sonicwall.com/contact-support.

To view the SonicWall End User Product Agreement (EUPA), see https://www.sonicwall.com/legal/eupa.aspx. Select the language based on your geographic location to see the EUPA that applies to your region.