Mobile Connect for iOS 5.0

User Guide

SONICWALL®

Contents

1

Introduction to Mobile Connect

SonicWall Mobile Connect for iOS is an application for Apple iPhone, iPod touch, and iPad that enables secure, mobile connections to private networks protected by SonicWall security appliances.

Topics:

- How Mobile Connect Works
- New Features in Mobile Connect 5.0
- 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, and so on), 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 like the iPhone, iPod touch and iPad. 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 application for iPhone, iPod touch, and iPad 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.

The Mobile Connect client certificate importer capability allows you to obtain digital security certificates, issued by certification authorities, to confirm your identify. They contain information used to protect data or to establish secure network connections. The certificates are securely stored so that only Mobile Connect has access to them for your protection. No other applications have access to your client certificates.

After installing the SonicWall Mobile Connect application from the App Store:

1. Ensure that the SonicWall Secure Mobile Access (SMA), or firewall appliance, that will be used by Mobile Connect to the network, is connected.

2. Configure Network Information (server name, username, password, and so on).
3. 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 Mobile Connect 5.0.

- **iOS 11 Compatibility** - Mobile Connect has adopted the bold, dynamic new style elements introduced in iOS 11 including large title bars, landscape tab bars and more.
- **Client Certificate Importer** - Allows a user to import client certificates for logging into remote servers. These digital certificates are sent from the client to the server at the start of a session. They prove the identification of the user. You can import client certificates from apps such as Mail, Outlook, or web browsers like Safari. Supported starting in Mobile Connect 5.0.4.
- **Network Extension Support** - Mobile Connect also leverages Apple's current VPN framework, called Network Extension, to allow for more reliable VPN connectivity on iOS devices. After upgrading to the 5.0 version, Mobile Connect may need to be re-provisioned, including updating VPN connection configurations and certificates.
- **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 Touch ID Support** - Mobile Connect now supports Touch ID for VPN connections to supported SMA 1000 series servers.
- **Face ID Support** - Mobile Connect now supports Face ID for VPN connections to supported SMA 100 and SMA 1000 series servers.
- **Global HA Support** - Mobile Connect contains updates for the global high availability and disaster recovery capabilities for VPN connections to SMA 1000 Series servers running 12.1 or newer firmware.
- **Localization** - Mobile Connect now supports Korean and Chinese languages.
- **SAML Authentication** - Latest Mobile Connect support SAML authentication with SMA100 and SMA1000 as well, enabling Mobile Connect to authenticate against third-party SAML IdP servers.

Additional Feature Information

SonicWall Mobile Connect continues to support the following features:

- **Slide Over** and **Split View** - Mobile Connect supports Slide Over and Split View multitasking on iPad.
- **Touch ID Support** - Apple's Touch ID is a seamless way to use your fingerprint as a passcode. On Touch ID enabled devices, Mobile Connect permits Touch ID to be used as a substitute for username and

password authentication if allowed by the VPN server. Instead of manually typing in the username and password on the login screen, a user can simply authenticate with their fingertip. Requires compatible server software with configured Touch ID policy.

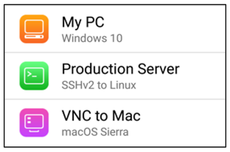
- **Face ID Support** - Apple's Face ID is a seamless way to use facial recognition as a passcode. On Face ID enabled devices, Mobile Connect permits Face ID to be used as a substitute for username and password authentication if allowed by the VPN server. Instead of manually typing in the username and password on the login screen, a user can simply authenticate using Face ID. Requires compatible server software with configured Face ID policy.
- **Files Bookmarks** - Files bookmarks are supported for FTP and SFTP servers in addition to CIFS servers.
- **HTML5 Bookmarks with SSO** - Mobile Connect supports in-app access with Single Sign-On for HTML5 Bookmarks including RDP, VNC, and SSH.

  The following third party apps are supported:

  - Microsoft Remote Desktop
  - ServerAuditor
  - vSSH

  HTML5 Bookmarks are displayed natively within Mobile Connect and provide a seamless and more secure user experience, including support for Single Sign-On.

Native HTML5 Bookmarks:

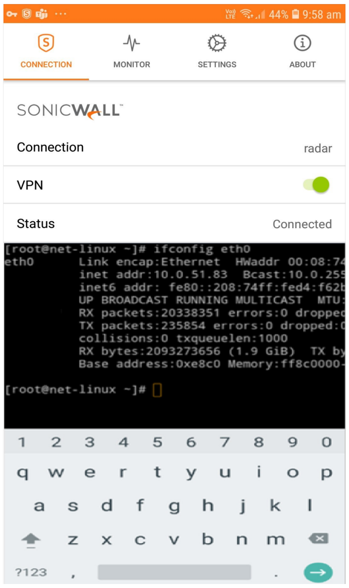


My PC
Windows 10

Production Server
SSHv2 to Linux

VNC to Mac
macOS Sierra

SSH Bookmark:



Connection radar

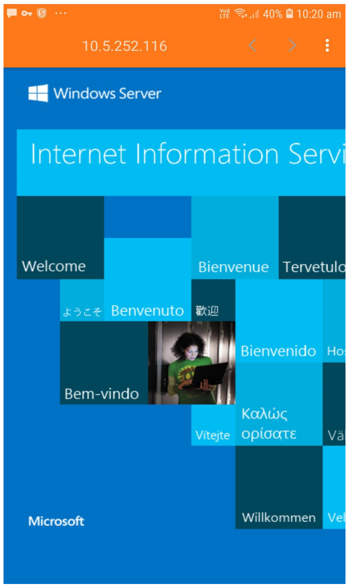
VPN

Status Connected

```
[root@net-linux ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:08:74
          inet addr:10.0.51.83  Bcast:10.0.255
          inet6 addr: fe80::208:74ff:fed4:f62b
          UP BROADCAST RUNNING MULTICAST  MTU:
          RX packets:20338351 errors:0 dropped
          TX packets:235854 errors:0 dropped:0
          collisions:0 txqueuelen:1000
          RX bytes:2093273656 (1.9 GiB)  TX by
          Base address:0xe8c0 Memory:ff8c0000-

[root@net-linux ~]#
```

RDP Bookmark:



Supported Platforms

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

- Apple Product Support
- SonicWall Appliance Support
- Required Network Information

Apple Product Support

SonicWall Mobile Connect is supported on the following devices:

- iPhone 12 running iOS 14.x or later
- iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max - running iOS 13 or higher
- iPhone XS, XS Max, and XR - running iOS 12 or higher
- iPhone X - running iOS 11 or higher
- iPhone 8 and 8 Plus - running iOS 11 or higher
- iPhone 7 and 7 Plus - running iOS 10 or higher
- iPhone 6s and 6s Plus - running iOS 9 or higher
- iPhone 6 and 6 Plus - running iOS 9 or higher
- iPhone 5, 5c and 5s - running iOS 9 or higher
- iPhone 4 and 4S - running iOS 9 or higher
- iPad Pro - running iOS 9 or higher
- iPad Air 2 - running iOS 9 or higher
- iPad Air (5th generation) - running iOS 9 or higher
- iPad (4th generation) - running iOS 9 or higher
- iPad (3rd generation) - running iOS 9 or higher
- iPad 2 - running iOS 9 or higher
- iPad mini 4 - running iOS 9 or higher
- iPad mini 3 - running iOS 9 or higher
- iPad mini (2nd generation) - running iOS 9 or higher
- iPad mini - running iOS 9 or higher
- iPod touch (5th generation or later) - running iOS 9 or higher

ⓘ **NOTE:** Devices running iOS 8 or earlier with earlier versions of SonicWall Mobile Connect cannot update to Mobile Connect 5.0.0 for iOS from the App Store unless they are upgraded to iOS 9 or newer.

SonicWall Appliance Support

SonicWall Mobile Connect 5.0.10 for iOS is a free app, but requires a concurrent license on one of the following SonicWall solutions to function properly:

- SonicWall firewall appliances including the NSa, NSA, TZ, SOHO, and SuperMassive™ 9000 series platforms running SonicOS 6.5 or higher. This includes SonicWall firewalls running SonicOS 7.0 or higher.
- Secure Mobile Access (SMA) 100 Series appliances running 9.0 or higher.
- Secure Mobile Access (SMA) 1000 Series appliances running 12.1 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** - 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. The administrator controls the number of domains listed, in addition to **Choose during login**.
- **Protocol** - You are required to select the type of protocol. However SonicWall SMA 1000 series do not support and display this information.

2

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

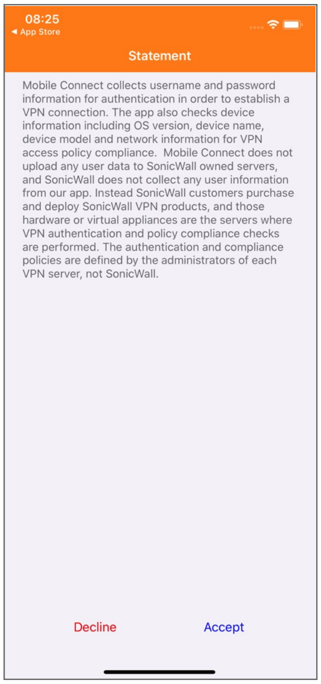
SonicWall Mobile Connect is installed through the Apple App Store.

To download and install the Mobile Connect app:

1. On your iPhone, iPod touch, or iPad, tap the App Store icon.
2. Go to the Search tab, type in ***SonicWall Mobile Connect,*** and tap **Search**.
3. In the search results, select **SonicWall Mobile Connect**.
4. Tap **Get** to **Install**. When the installation is complete on your device, the SonicWall Mobile Connect icon appears on your device.

ⓘ **NOTE:** If you encounter an error when attempting to download Mobile Connect, see iTunes Store Customer Support, where you can find troubleshooting procedures and instructions on how to report the issue using your iTunes account: http://www.apple.com/support/itunes/.

5. Tap **Accept** for the Mobile Connect privacy policy **Statement**.



Mobile Connect collects username and password information for authentication in order to establish a VPN connection. The app also checks device information including OS version, device name, device model and network information for VPN access policy compliance. Mobile Connect does not upload any user data to SonicWall owned servers, and SonicWall does not collect any user information from our app. Instead SonicWall customers purchase and deploy SonicWall VPN products, and those hardware or virtual appliances are the servers where VPN authentication and policy compliance checks are performed. The authentication and compliance policies are defined by the administrators of each VPN server, not SonicWall.

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

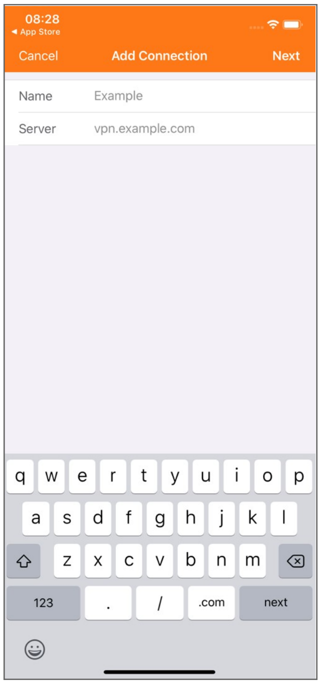
Creating Firewall or SMA 100 Series Connections

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

1. The first time you launch Mobile Connect, tap **Add Connection**.

   ⓘ | **NOTE:** If you don't have any connections, you'll bypass step 2 and see the editor screen under step 5.

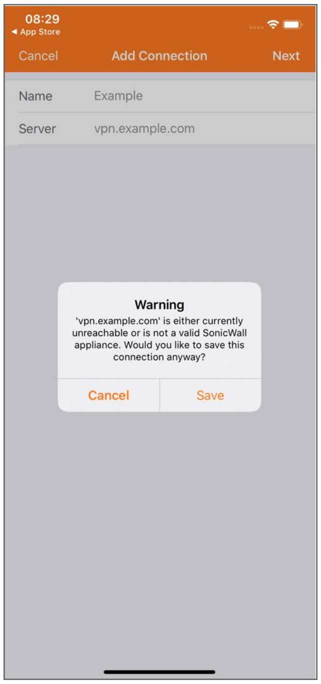
2. Then, tap **Create a new connection**. The info icon takes you to the same place.
3. In the **Name** field, type in a descriptive name for the connection.
4. In the **Server** field, type in the URL or IP address of the server (appliance).
5. Tap **Next**. Mobile Connect attempts to contact the SonicWall appliance.



Name Example

Server vpn.example.com

6. 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.



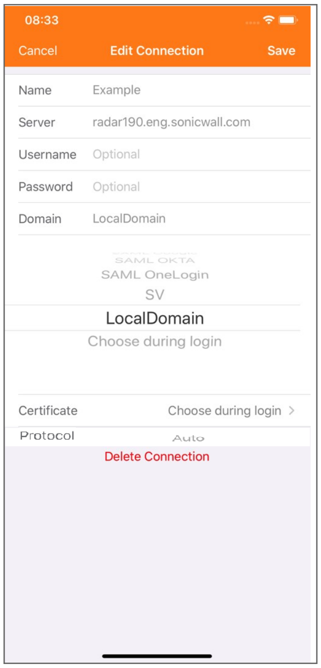
Name Example

Server vpn.example.com

Warning

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

7. If Mobile Connect successfully contacts the server after you enter your **Name** and **Server** name, choose your **Domain** name by tapping on the Domain field and selecting from the picker. You can then choose how to obtain your client certificate by tapping on one of the following:
   - **Choose during login** - You will be prompted to select a certificate if the server requires one.
   - **None** - If the server requires a certificate, login will be canceled. Then tap **Save**.



Name Example

Server radar190.eng.sonicwall.com

Username Optional

Password Optional

Domain LocalDomain

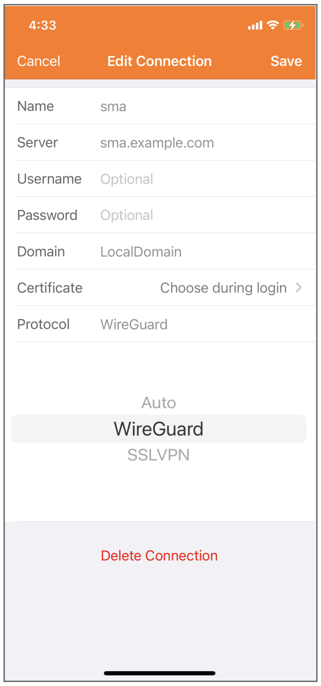
Certificate Choose during login

Protocol Auto

IMPORTANT: The **Domain** field is auto-populated with the default domain from the server. To select a different domain, tap **Domain** to display the available options in the picker, and then select the correct domain.

NOTE: Entering your Username and Password is optional during this step. If the previous screenshot does not match what is displayed on your device, you are connecting to the SonicWall SMA 1000 Series. See Creating SMA 1000 Series Connections.

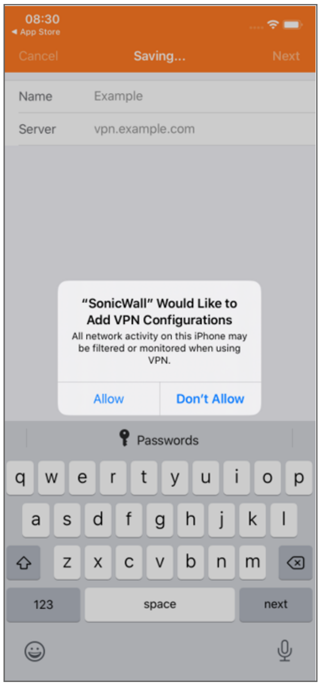
8. The **Protocol** field is auto-populated with the default VPN from the server. To select a different VPN, click **Protocol** to display a drop-down menu of the available options and then select the required VPN.
   - **Auto**: Selecting **Auto** connects the VPN according the preference setting of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



Name	sma
Server	sma.example.com
Username	Optional
Password	Optional
Domain	LocalDomain
Certificate	Choose during login >
Protocol	WireGuard

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

9. iOS may present a security prompt to allow SonicWall Mobile Connect to add VPN Configurations.



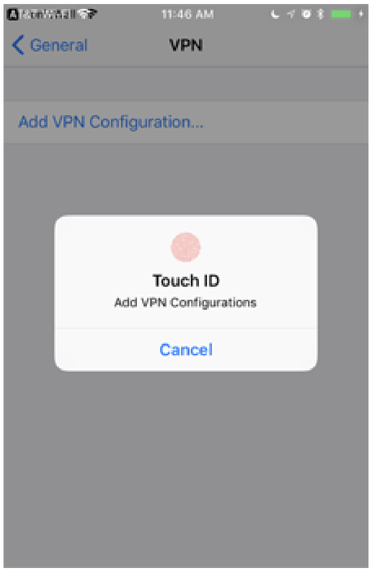
Name Example

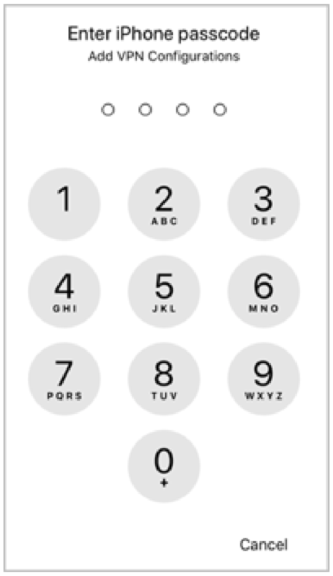
Server vpn.example.com

“SonicWall” Would Like to Add VPN Configurations

All network activity on this iPhone may be filtered or monitored when using VPN.

10. If prompted, tap **Allow**. The iOS Settings app opens and you may be prompted for your Touch ID, Face ID, or passcode to grant the permission.



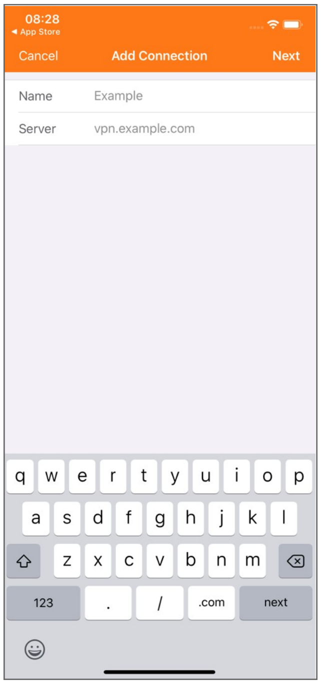


11. Enter Touch ID, Face ID, or your passcode as required. The Mobile Connect Connections screen where you select the server connection is then displayed.

Creating SMA 1000 Series Connections

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

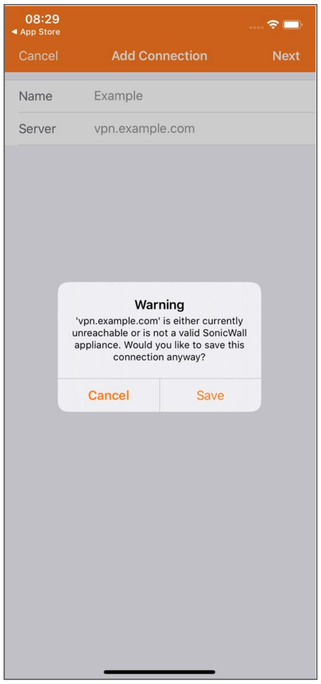
1. The first time you launch Mobile Connect, tap **Add Connection**.



Name Example

Server vpn.example.com

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**. 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**.



Name Example

Server vpn.example.com

Warning

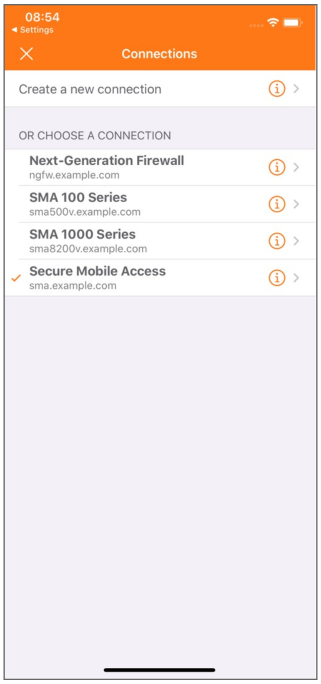
'vpn.example.com' is either currently unreachable or is not a valid SonicWall appliance. Would you like to save this connection anyway?

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

Initiating a Connection

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

connections screen



08:54

◂ Settings

Connections

Create a new connection

OR CHOOSE A CONNECTION

Next-Generation Firewall
ngfw.example.com

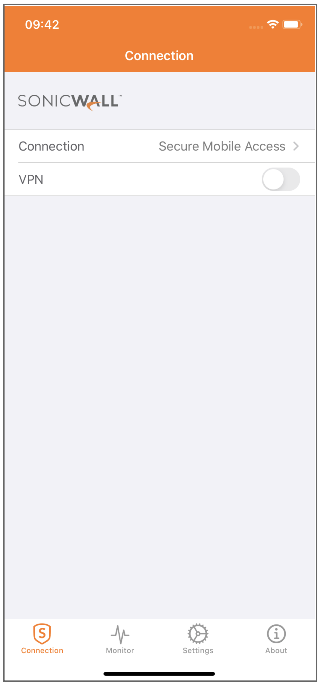
SMA 100 Series
sma500v.example.com

SMA 1000 Series
sma8200v.example.com

✓ Secure Mobile Access
sma.example.com

To initiate a Mobile Connect session:

1. Tap the connection in the list that you want to initiate. The Connection page displays.



09:42

Connection

SONICWALL

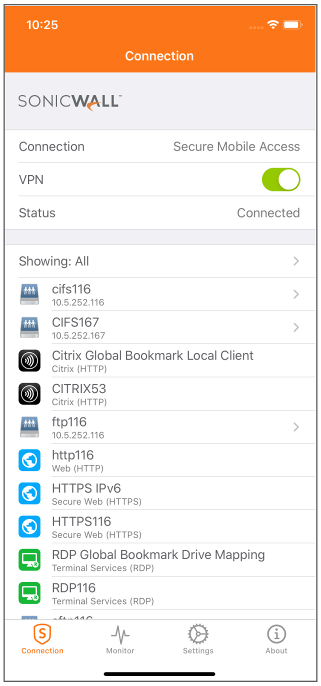
Connection Secure Mobile Access

VPN

2. Tap the **VPN** switch to enable the VPN.

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

4. When the connection is successfully established, the **Status** row changes to **Connected** and the VPN switch is on.



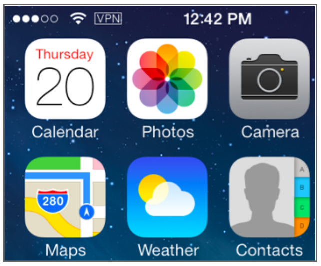
Connection	Secure Mobile Access
VPN	
Status	Connected

Showing: All

- cifs116 10.5.252.116
- CIFS167 10.5.252.167
- Citrix Global Bookmark Local Client Citrix (HTTP)
- CITRIX53 Citrix (HTTP)
- ftp116 10.5.252.116
- http116 Web (HTTP)
- HTTPS IPv6 Secure Web (HTTPS)
- HTTPS116 Secure Web (HTTPS)
- RDP Global Bookmark Drive Mapping Terminal Services (RDP)
- RDP116 Terminal Services (RDP)

Any bookmarks defined for the portal are displayed following the Status row. You can launch a bookmark by tapping on it.

5. Press the Home button on your iPhone, iPod touch, or iPad to display its home screen. You can now navigate to other applications to access your Intranet network. The status bar at the top of the iPhone, iPod touch or iPad displays a VPN icon to indicate that the Mobile Connect session is still connected.



If the VPN connection is interrupted, the VPN icon disappears and you are no longer able to access the Intranet network. This can happen if your device's connection transitions from wireless to cellular or to another network type.

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

Configuring Connect on Demand

The Connect on Demand feature provides the ability for Mobile Connect to automatically establish a VPN connection when you attempt to access a domain on the private network. This provides a seamless VPN connectivity experience without the need to manually launch Mobile Connect.

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

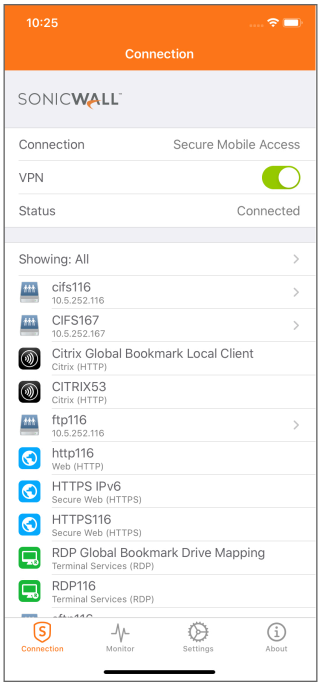
See the following:

- Connect on Demand to SMA 1000 Series
- Connect on Demand to SMA 100 and SMA 1000 Series

Connect on Demand to SMA 1000 Series

The easiest way to determine if Connect on Demand is available for your SMA 1000 Series connection is to look at the Connection screen when a VPN is connected. If the information indicator ⓘ › appears at the right side of the **Status** row, Connect on Demand can be configured while connected.

info indicator



Connection: Secure Mobile Access
VPN
Status: Connected

Showing: All

cifs116
10.5.252.116

CIFS167
10.5.252.167

Citrix Global Bookmark Local Client
Citrix (HTTP)

CITRIX53
Citrix (HTTP)

ftp116
10.5.252.116

http116
Web (HTTP)

HTTPS IPv6
Secure Web (HTTPS)

HTTPS116
Secure Web (HTTPS)

RDP Global Bookmark Drive Mapping
Terminal Services (RDP)

RDP116
Terminal Services (RDP)

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

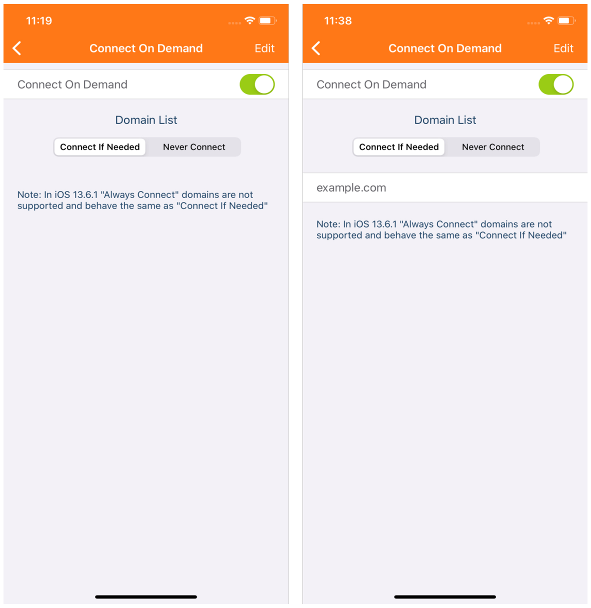
- The VPN tunnel must not be configured for Redirect-All mode.
- The realm must be configured to use client certificates, for authentication. Chained authentication (where a second authentication server is used) does not support Connect on Demand.
- A valid client certificate for the realm must be present. See Importing Certificates to the iOS Device for more information.
- The user must successfully connect to the appliance at least one time.

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

- The VPN server's SSL certificate is untrusted.
- Personal Device Authorization is enabled on the server and the device has not been authorized.
- Two-factor user authentication is required such as a one-time password.

To configure Connect on Demand to SonicWall SMA 1000 Series:

1. Tap the information indicator ⓘ › in the Status row on the Connection tab that displays the Connect On Demand screen.



Note: In iOS 13.6.1 "Always Connect" domains are not supported and behave the same as "Connect If Needed"

example.com

Note: In iOS 13.6.1 "Always Connect" domains are not supported and behave the same as "Connect If Needed"

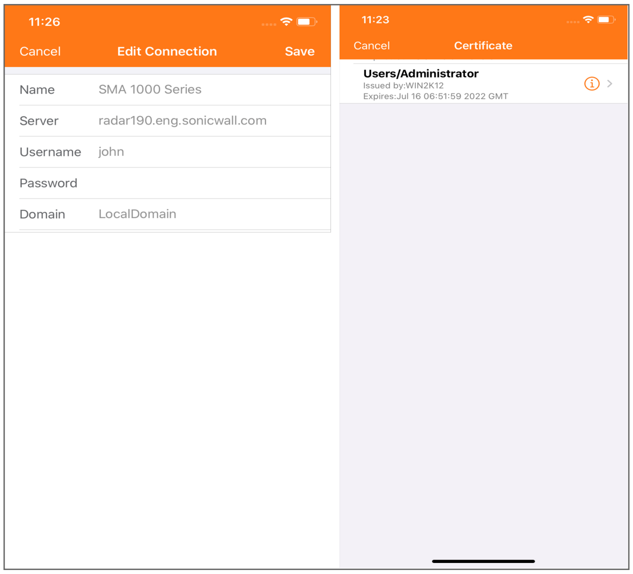
2. Tap **Connect on Demand**.
3. Set **Domain List** to one of the following:
   a. Set **Domain List** to **Connect If Needed** to have Mobile Connect establish a VPN connection when accessing a resource with any of the domain suffixes listed.
   b. Set **Domain List** to **Never Connect** to disable Connect on Demand for the domain suffixes listed.

ⓘ **NOTE: Always Connect** domains are no longer supported in iOS. They behave the same as **Connect if Needed**.

Connect on Demand to SMA 100 and SMA 1000 Series

On SonicWall SMA 100 Series and SonicWall SMA 1000 Series, client certificate authentication is available as a second factor authentication method in addition to standard user name and password authentication. If a client certificate is required during authentication, the user is automatically prompted to select a client certificate from the iOS device.

selecting a certificate

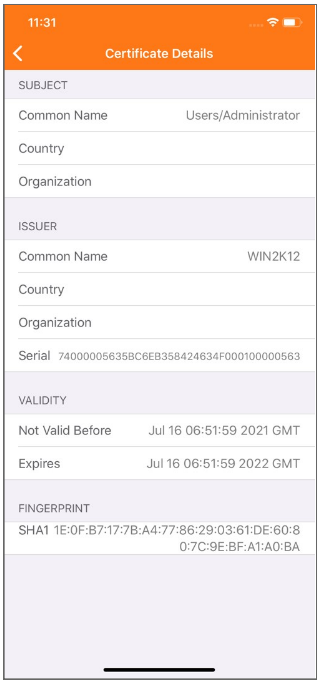


Name SMA 1000 Series
Server radar190.eng.sonicwall.com
Username john
Password
Domain LocalDomain

Users/Administrator
Issued by:WIN2K12
Expires:Jul 16 06:51:59 2022 GMT

Tapping on the information indicator ⓘ › that appears to the right of the client certificate displays additional details for the client certificate.

certificate details



11:31

Certificate Details

SUBJECT

Common Name Users/Administrator

Country

Organization

ISSUER

Common Name WIN2K12

Country

Organization

Serial 74000005635BC6EB358424634F000100000563

VALIDITY

Not Valid Before Jul 16 06:51:59 2021 GMT

Expires Jul 16 06:51:59 2022 GMT

FINGERPRINT

SHA1 1E:0F:B7:17:7B:A4:77:86:29:03:61:DE:60:80:7C:9E:BF:A1:A0:BA

By default, a VPN configuration uses the client certificate setting of **Choose during login**.

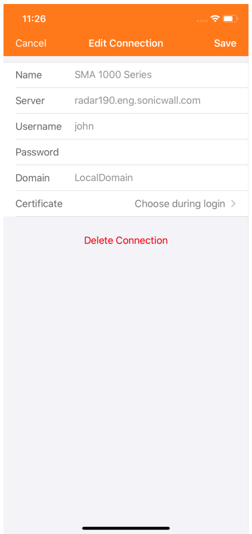
To support Connect on Demand, a VPN configuration on the SonicWall SMA 1000 and SMA 100 Series must meet the following requirements:

- The user's effective client certificate enforcement policy, configured at the domain or user level, must be enabled to use client certificates for authentication.
- The user's effective user name and password caching policy (configured at the global, group, or user level) must be set to **Allow saving of username and password**.
- The valid client certificate for the user must be present on the iOS device.
- The iOS VPN connection profile must have the user name and password configured, and the appropriate client certificate must be selected. See Importing Certificates to the iOS Device for more information.

To configure Connect on Demand to SonicWall SMA 100 and SMA 1000 Series:

1. Tap **Certificate** on the Edit Connection screen.
2. Select a client certificate from the list.

   The Connect On Demand setting is displayed.


11:26

Cancel Edit Connection Save

Name SMA 1000 Series

Server radar190.eng.sonicwall.com

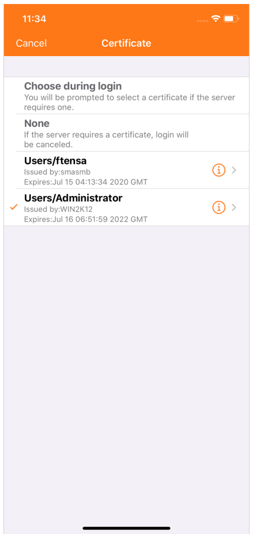
Username john

Password

Domain LocalDomain

Certificate Choose during login >

Delete Connection


11:34

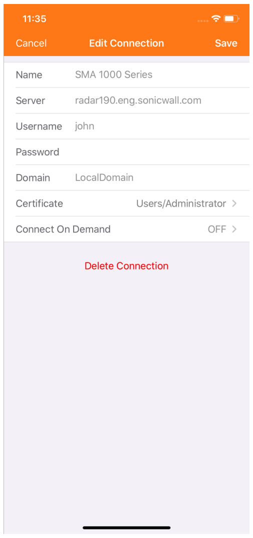
Cancel Certificate

Choose during login
You will be prompted to select a certificate if the server requires one.

None
If the server requires a certificate, login will be canceled.

Users/ftensa
Issued by:smasmb
Expires:Jul 15 04:13:34 2020 GMT

✓ **Users/Administrator**
Issued by:WIN2K12
Expires:Jul 16 06:51:59 2022 GMT


11:35

Cancel Edit Connection Save

Name SMA 1000 Series

Server radar190.eng.sonicwall.com

Username john

Password

Domain LocalDomain

Certificate Users/Administrator >

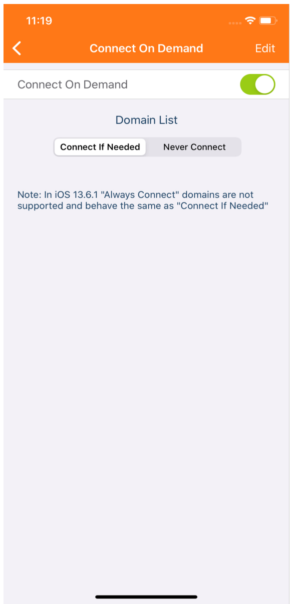
Connect On Demand OFF >

Delete Connection

3. Tap **Connect On Demand** on the Edit Connection screen to enable Connect On Demand and display the Connect On Demand screen.

4. In the **Connect On Demand** screen, set **Domain List** to **Connect If Needed** to have Mobile Connect establish a VPN connection when accessing a resource with any of the domain suffixes listed.

   Setting **Domain List** to **Never Connect** disables Connect on Demand for the domain suffixes listed.


11:19

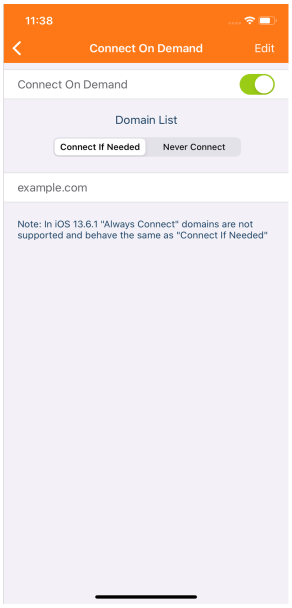
< Connect On Demand Edit

Connect On Demand ●

Domain List

Connect If Needed | Never Connect

Note: In iOS 13.6.1 "Always Connect" domains are not supported and behave the same as "Connect If Needed"


11:38

< Connect On Demand Edit

Connect On Demand ●

Domain List

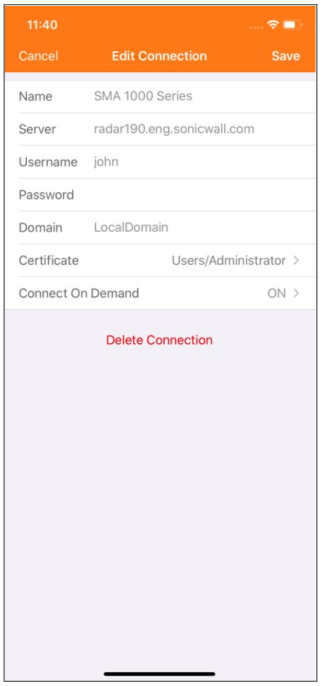
Connect If Needed | Never Connect

example.com

Note: In iOS 13.6.1 "Always Connect" domains are not supported and behave the same as "Connect If Needed"

5. If more than one domain is listed, tap a domain name to enable Connect on Demand for an individual domain.

   ⓘ **NOTE: Always Connect** domains are no longer supported in iOS. They behave the same as **Connect if Needed**.



Name	SMA 1000 Series
Server	radar190.eng.sonicwall.com
Username	john
Password	
Domain	LocalDomain
Certificate	Users/Administrator
Connect On Demand	ON

Configuring Trusted Network Detection

The Apple Trusted Network Detection (TND) enhancement to the iOS Connect On Demand feature has the following properties:

- Can be used only with Connect on Demand.
- Extends the Connect on Demand functionality by determining whether the user is on a trusted network.
- Is configured with the Apple Configurator 2.
- Is used for wireless connections only. When operating over other types of network connections, Connect on Demand does not use TND to determine whether a VPN should be connected.

Connect On Demand starts a VPN connection whenever a user tries to access a destination with a hostname specified in the domains list. For example, if ***.example.com** is in the **Always Connected** list, when a user accesses **internal.example.com**, the client starts a VPN connection regardless of the network to which the device is currently connected. TND compares the VPN and local DNS servers and DNS suffixes to determine whether to use Mobile Connect and dial the VPN, as shown in the following table:

DNS Comparison And Effect On Login

DNS suffixes	DNS servers	Login
None	None	Refused - no VPN
None	Same	Refused - no VPN
Same	Same	Refused - no VPN

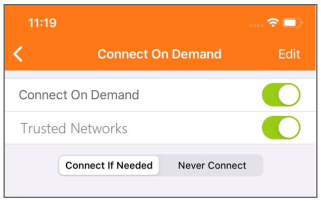
Same	Same and others	Allowed
Same	Different	Allowed
Different	Same	Allowed
Partial match	Partial match	Allowed

A partial match means that if there are two DNS servers configured for TND, but only one DNS server matches the actual network environment, then the login will still be allowed.

Consult documentation from Apple Inc. for more information about Trusted Network Detection and Connect on Demand.

To determine if TND is available for your connection, tap the information indicator in the Status row on the Connection tab. This displays the **Trusted Networks** button used to enable/disable TND, if available.

Trusted Networks Button



To configure TND:

1. Tap the information indicator ⓘ > in the Status row on the Connection tab.
2. Ensure that **Connect On Demand** is turned on.
3. Turn on **Trusted Networks**.

   ⓘ | **NOTE:** Trusted Network Detection is available only for connections to SonicWall SMA 1000 Series.

Using Apple Configurator 2 with Mobile Connect

Apple Configurator 2 makes it easy for admin to configure togther and deploy iPhone, iPad, and iPod touch in business and education. It lets administrators of enterprise environments create configuration profiles for iOS devices that provide the ability to preconfigure the device settings for enterprise policies, such as VPN configuration, security policies, wireless settings, and so on. Information about downloading Apple Configurator is available here Mac App Store-Apple Configurator.

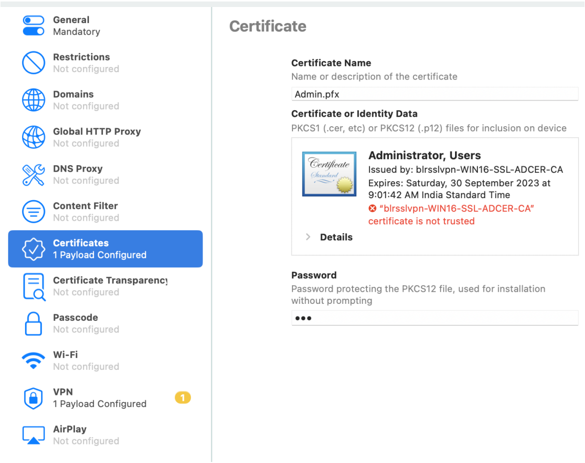
For more information, refer to:

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

To Configure a Mobile Connect Profile Using Apple Configurator 2:

1. Download, install, and launch Apple Configurator 2.
2. In Apple Configurator 2, choose **File** > **New Profile**.

   A new configuration profile document window appears.
3. In the **General**, fill in the mandatory fields.
4. If the user authentication type is certificate, go to the **Certificates** page, and do the following:

   Certificate Name
   Name or description of the certificate
   Admin.pfx

   Certificate or Identity Data
   PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device

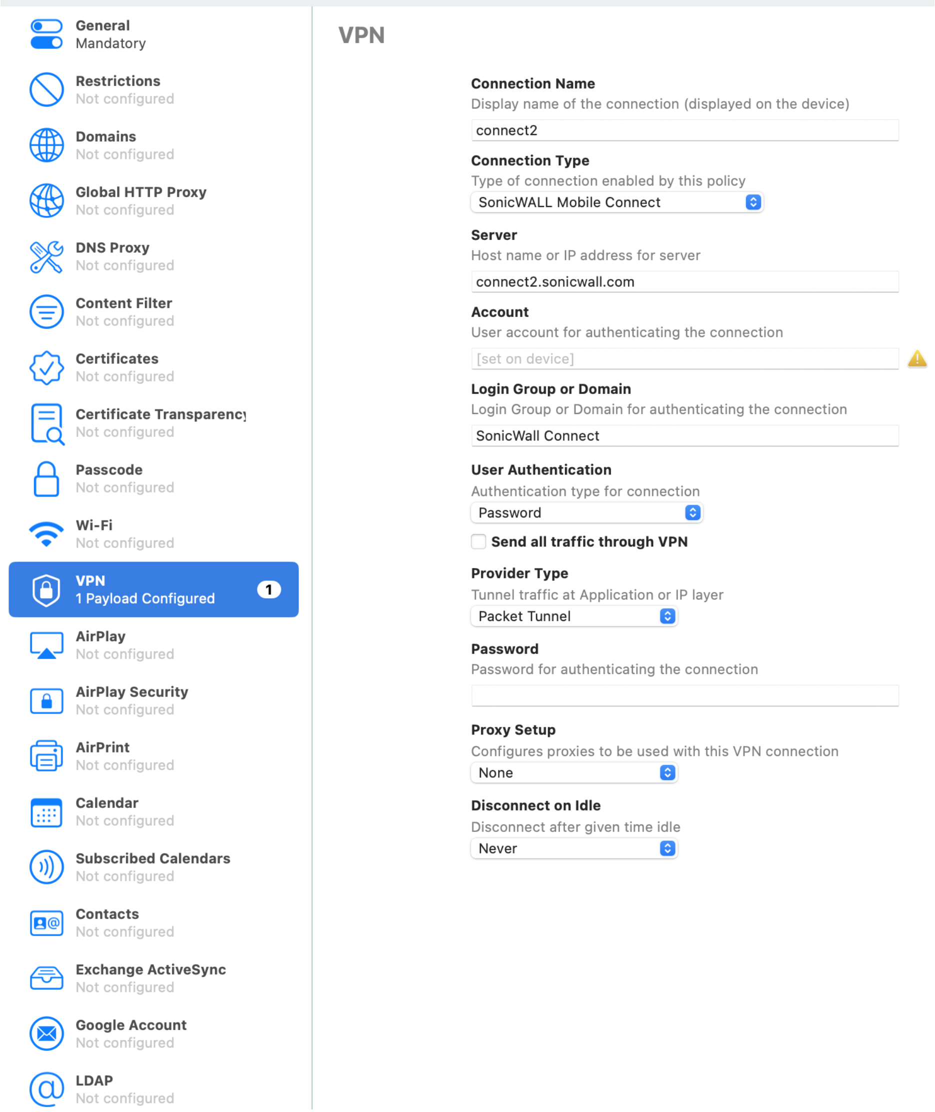
   Administrator, Users
   Issued by: blrsslvpn-WIN16-SSL-ADCER-CA
   Expires: Saturday, 30 September 2023 at 9:01:42 AM India Standard Time
   ⊗ "blrsslvpn-WIN16-SSL-ADCER-CA" certificate is not trusted
   › **Details**

   Password
   Password protecting the PKCS12 file, used for installation without prompting
   •••

   a. Enter a **Certificate Name**.

   b. Browse and select the **Certificate or Identity Data**.

   c. Enter a **Password** to open the protected certificate without prompting to enter the password.
5. Go to **VPN** and click **Configure** the following settings:



VPN

Connection Name
Display name of the connection (displayed on the device)
connect2

Connection Type
Type of connection enabled by this policy
SonicWALL Mobile Connect

Server
Host name or IP address for server
connect2.sonicwall.com

Account
User account for authenticating the connection
[set on device] ⚠

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

User Authentication
Authentication type for connection
Password

☐ **Send all traffic through VPN**

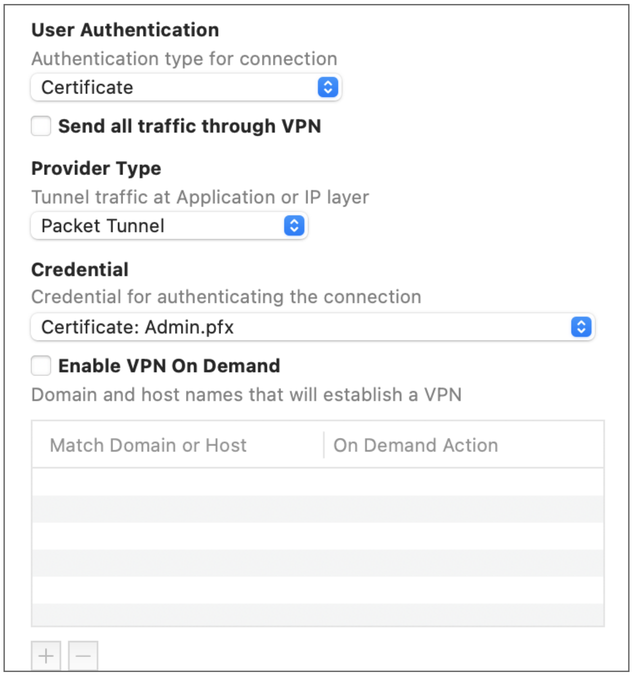
Provider Type
Tunnel traffic at Application or IP layer
Packet Tunnel

Password
Password for authenticating the connection

Proxy Setup
Configures proxies to be used with this VPN connection
None

Disconnect on Idle
Disconnect after given time idle
Never

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

Settings	Description
User Authentication	• If you select **Password**, in the **Password** field, enter the password for the user account. • If you select **Certificate**, in the **Credential** select the uploaded certificate.  **User Authentication** Authentication type for connection Certificate □ **Send all traffic through VPN** **Provider Type** Tunnel traffic at Application or IP layer Packet Tunnel **Credential** Credential for authenticating the connection Certificate: Admin.pfx □ **Enable VPN On Demand** Domain and host names that will establish a VPN Match Domain or Host | On Demand Action
Provider Type	Select the **Packet Tunnel** from the drop-down menu.
Proxy Setup	Leave the with default value or set any custom value from the drop-down menu.
Disconnect on Idle	Leave the with default value or set any custom value from the drop-down menu.

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

Configuring Per App VPN

This section describes how Mobile Connect supports the iOS Per App VPN features. Per App VPN is only supported for Mobile Connect VPN connections to SMA 1000 Series appliances that have been configured for Application Access Control.

Per App VPN requires the use of a Mobile Device Management (MDM) solution. In addition, the Per App VPN is only supported with MDM managed apps as well as Safari through a list of MDM managed web domains. Please refer to your MDM solution provider's documentation for how to configure Per App VPN with their solution.

The following are known limitations with using Per App VPN and Mobile Connect:

- Application access control Zone classification could fail if the MDM solution does not successfully install managed applications and configure Per App VPN rules for managed applications.
- Custom VPN connections are not installed for MDM managed VPN connections when connecting to SMA 1000 Series appliances.
- VPN on Demand connections may fail to connect if device authorization is enabled on the SMA 1000 Series appliance. This is due to the fact that user interaction will be required in the application.

3

Settings, Bookmarks, Files, and Certificates

This section describes the configurable elements that are accessed from the Settings screen in Mobile Connect, such as connection settings, URL control, bookmarks, files bookmarks, and how to use Mobile Connect Client Certificate Importer.

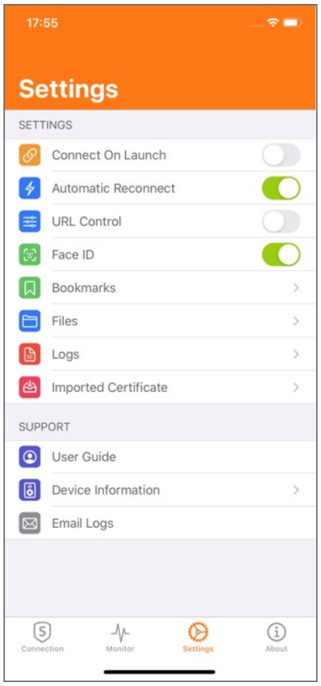
Topics:

- Settings Overview
- URL Control Syntax and Parameters
- Using Bookmarks
- Using Files
- Importing Certificates to the iOS Device

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 information, and email logs.

settings screen



17:55

Settings

SETTINGS

- Connect On Launch ○
- Automatic Reconnect ●
- URL Control ○
- Face ID ●
- Bookmarks >
- Files >
- Logs >
- Imported Certificate >

SUPPORT

- User Guide
- Device Information >
- Email Logs

The available settings and selections are described below:

- Settings Section
- Support Section

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
`name`	The unique name of the VPN connection entry that is created and appears in the Mobile Connect Connections list. Mobile Connect accepts the name only if it is unique. Letters are case sensitive.
`server`	The domain name or IP address of the SonicWall appliance to which you wish to connect. For example: `vpn.example.com`
`username`	**Optional**: The username used in the VPN connection.
`password`	**Optional**: The password used in the VPN connection.
`realm`	**Optional**: The realm used in the VPN connection profile. Applies to SMA 1000 Series connections only.
`domain`	**Optional**: The domain used in the VPN connection profile. Applies to SMA 100 Series and Firewall connections only.
`sessionid`	**Optional**: The session ID or Team ID used for authentication.
`connect`	**Optional**: If presented and the value is non-null, the connection is initiated if the profile was successfully added.
`callbackurl`	**Optional**: The callback URL to be opened by Mobile Connect after the `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%202&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
```

ⓘ **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: `vpn.example.com`
`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 connect command has been processed. See Using the callbackurl Command Parameter for full details of `callbackurl` 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%202&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 `callbackurl` is opened by Mobile Connect after the disconnect command has been processed. See Using the callbackurl Command Parameter for full details of `callbackurl` 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 or iOS web clip.

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

Examples:

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%24
ERROR_CODE%24
```

Callback URL (2):

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

Corresponding full URL with URL encoded `callbackurl` value:

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

Callback URL (3):

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

Corresponding full URL with URL encoded callbackurl value:

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

Using Bookmarks

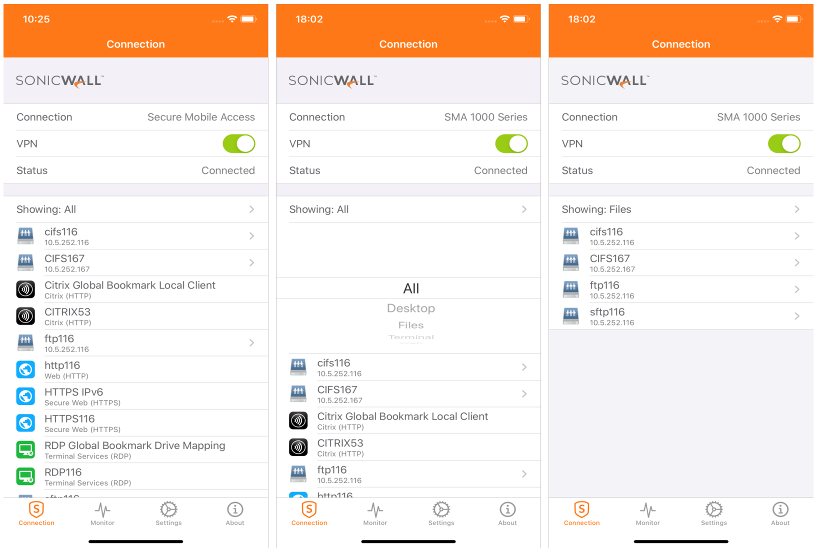
Topics:

- Showing and Filtering Bookmarks
- Supported Bookmark Types

Showing and Filtering Bookmarks

The Mobile Connect **Connection** screen displays the configured bookmarks. The list of bookmarks can be filtered by tapping the **Showing: *<bookmark type>*** row that is displayed when there are more than five bookmarks. This lets you filter long lists of bookmarks by type. Select the type of bookmarks to display or select **All** to display all bookmarks.

showing bookmarks



Connection Secure Mobile Access
VPN
Status Connected

Showing: All
cifs116 10.5.252.116
CIFS167 10.5.252.167
Citrix Global Bookmark Local Client Citrix (HTTP)
CITRIX53 Citrix (HTTP)
ftp116 10.5.252.116
http116 Web (HTTP)
HTTPS IPv6 Secure Web (HTTPS)
HTTPS116 Secure Web (HTTPS)
RDP Global Bookmark Drive Mapping Terminal Services (RDP)
RDP116 Terminal Services (RDP)

Connection SMA 1000 Series
VPN
Status Connected

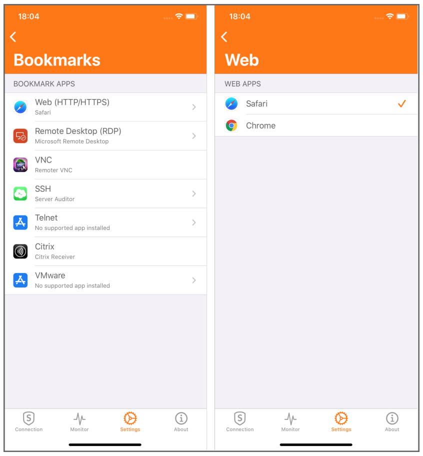
Showing: All
All
Desktop
Files
Terminal
cifs116 10.5.252.116
CIFS167 10.5.252.167
Citrix Global Bookmark Local Client Citrix (HTTP)
CITRIX53 Citrix (HTTP)
ftp116 10.5.252.116
http116

Connection SMA 1000 Series
VPN
Status Connected

Showing: Files
cifs116 10.5.252.116
CIFS167 10.5.252.167
ftp116 10.5.252.116
sftp116 10.5.252.116

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

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



BOOKMARK APPS
Web (HTTP/HTTPS) Safari
Remote Desktop (RDP) Microsoft Remote Desktop
VNC Remoter VNC
SSH Server Auditor
Telnet No supported app installed
Citrix Citrix Receiver
VMware No supported app installed

WEB APPS
Safari ✓
Chrome

Supported Bookmark Types

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

ⓘ **NOTE:** In Mobile Connect iOS 5.0, only Web and Desktop bookmarks are supported on the SonicWall SMA 1000 Series.

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:

- 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

ⓘ | **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 RDP applications and minimum supported versions.

RDP Applications And Minimum Supported Versions

Application	Minimum supported version
Microsoft Remote Desktop	8.1.35
Parallels Client (legacy 2X)	15.0.3883

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 iOS

VNC Bookmarks

VNC Bookmark Portal Names And Internal Types

Portal name	Internal type

Virtual Network Computing (VNC)	VNC
Virtual Network Computing (VNC – HTML5)	VNCHTML5

ⓘ | **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 Minimum Supported Versions

Application	Minimum supported version
Remoter VNC	4.8.10

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 Minimum Supported Version

Application	Minimum supported version
Citrix Receiver	7.3

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 and the provided “Name or IP Address” (HostID) is passed as the parameter to display in the browser.

Browser Types And Minimum Supported Versions

Browser type	Minimum supported version
Any browser	—
Safari	Any
Google Chrome	61.0.3163.73

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 fully on the OS to determine and launch the proper application. The bookmark is expected to be properly configured for launch. The Mobile Connect application 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

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

The applications and versions are:

Terminal Applications And Minimum Supported Versions

Application	Minimum supported version
ServerAuditor	2.2.2
vSSH	1.11
vSSH Lite	1.11

Using Files

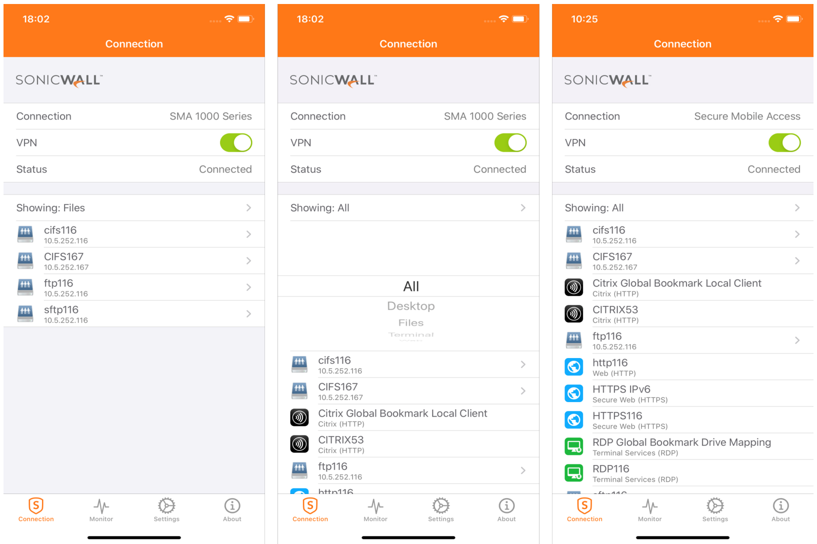
Mobile Connect 5.0 supports secure mobile access to files through File bookmarks. File bookmarks allow secure access to files by first checking and enforcing the server configured file policy, and then securely downloading and displaying the file within the Mobile Connect application.

Server configured policies include control over whether a file can be printed, copied to the clipboard, opened in a third-party application, or securely cached on the iOS device. File bookmarks can also be created to folders or file share root directories to allow directory navigation.

> ⓘ **NOTE:** In Mobile Connect for iOS 5.0, File bookmarks are supported only on the SonicWall SMA 100 Series. Support for File bookmarks in SMA 1000 Series 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: Files** row that is displayed when there are more than five bookmarks. See Showing Files bookmarks.

showing files bookmarks



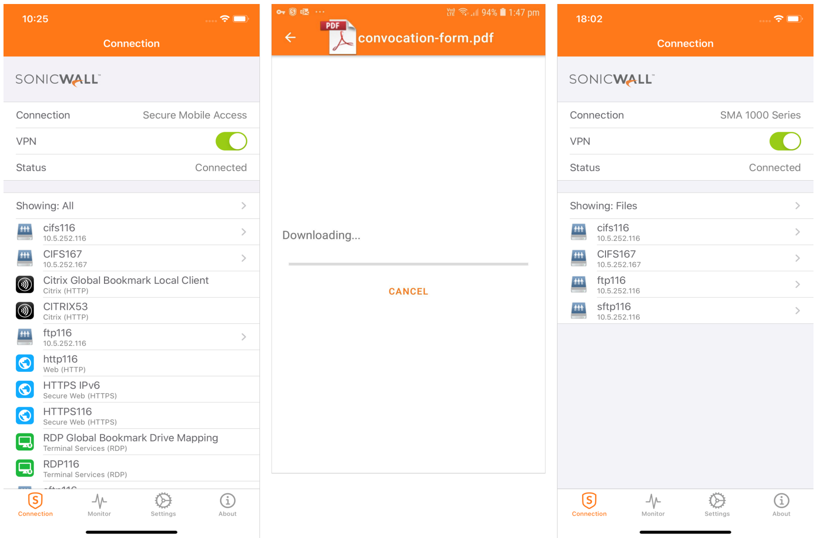
Connection: SMA 1000 Series
VPN: on
Status: Connected
Showing: Files
cifs116 10.5.252.116
CIFS167 10.5.252.167
ftp116 10.5.252.116
sftp116 10.5.252.116

Connection: SMA 1000 Series
VPN: on
Status: Connected
Showing: All
All
Desktop
Files
Terminal
cifs116 10.5.252.116
CIFS167 10.5.252.167
Citrix Global Bookmark Local Client Citrix (HTTP)
CITRIX53 Citrix (HTTP)
ftp116 10.5.252.116
http116

Connection: Secure Mobile Access
VPN: on
Status: Connected
Showing: All
cifs116 10.5.252.116
CIFS167 10.5.252.167
Citrix Global Bookmark Local Client Citrix (HTTP)
CITRIX53 Citrix (HTTP)
ftp116 10.5.252.116
http116 Web (HTTP)
HTTPS IPv6 Secure Web (HTTPS)
HTTPS116 Secure Web (HTTPS)
RDP Global Bookmark Drive Mapping Terminal Services (RDP)
RDP116 Terminal Services (RDP)

Selecting 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. After the file is downloaded, it is displayed within the Mobile Connect application. See Downloading a file using a File bookmark.

downloading a file using a file bookmark



10:25

Connection

SONICWALL

Connection	Secure Mobile Access
VPN	On
Status	Connected

Showing: All

- cifs116 – 10.5.252.116
- CIFS167 – 10.5.252.167
- Citrix Global Bookmark Local Client – Citrix (HTTP)
- CITRIX53 – Citrix (HTTP)
- ftp116 – 10.5.252.116
- http116 – Web (HTTP)
- HTTPS IPv6 – Secure Web (HTTPS)
- HTTPS116 – Secure Web (HTTPS)
- RDP Global Bookmark Drive Mapping – Terminal Services (RDP)
- RDP116 – Terminal Services (RDP)

94% 1:47 pm

convocation-form.pdf

Downloading...

CANCEL

18:02

Connection

SONICWALL

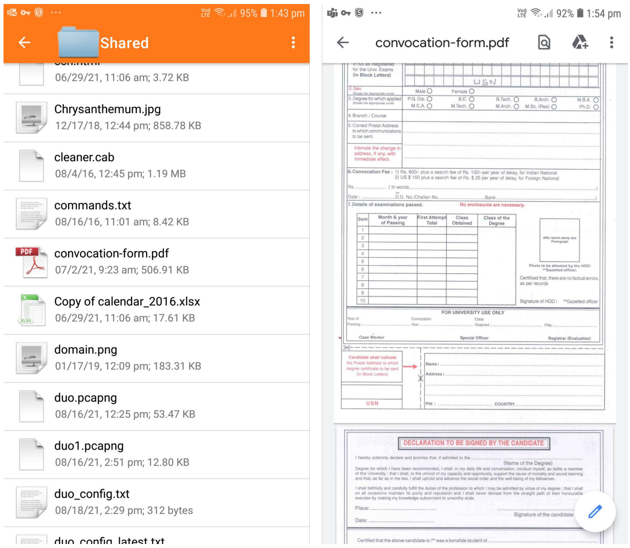
Connection	SMA 1000 Series
VPN	On
Status	Connected

Showing: Files

- cifs116 – 10.5.252.116
- CIFS167 – 10.5.252.167
- ftp116 – 10.5.252.116
- sftp116 – 10.5.252.116

Selecting a File bookmark to a folder or directory allows directory browsing, including download and viewing of any file in the folder. Each attempt to browse a file folder or view a file queries the server to enforce access policies. See Browsing folders and viewing files.

browsing folders and viewing files



95% 1:43 pm

Shared

	06/29/21, 11:06 am; 3.72 KB
Chrysanthemum.jpg	12/17/18, 12:44 pm; 858.78 KB
cleaner.cab	08/4/16, 12:45 pm; 1.19 MB
commands.txt	08/16/16, 11:01 am; 8.42 KB
convocation-form.pdf	07/2/21, 9:23 am; 506.91 KB
Copy of calendar_2016.xlsx	06/29/21, 11:06 am; 17.61 KB
domain.png	01/17/19, 12:09 pm; 183.31 KB
duo.pcapng	08/16/21, 12:25 pm; 53.47 KB
duo1.pcapng	08/16/21, 2:51 pm; 12.80 KB
duo_config.txt	08/18/21, 2:29 pm; 312 bytes
duo_config_latest.txt	

92% 1:54 pm

convocation-form.pdf

For information about supported file types and other actions you can take on files, see Files Features.

Files Features

A number of file types are supported with features allowing you to perform many important functions with the files you access via Files bookmarks.

See the following:

- Supported File Types
- Unsupported File Types
- File Policies and Actions

Supported File Types

Mobile Connect supports the file types natively supported by Apple iOS, as shown in Supported file types.

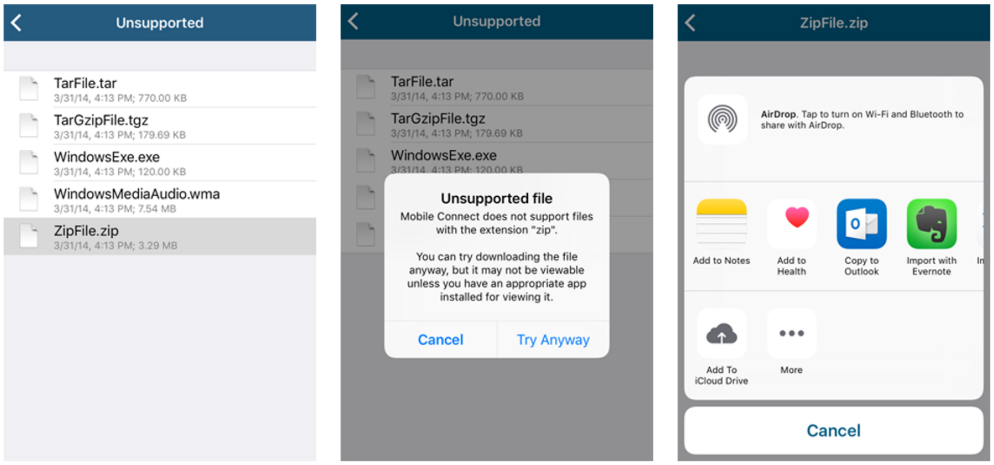
supported file types

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
Keynote presentations	.key
Pages documents	.pages
Numbers spreadsheets	.numbers
Web pages	.htm, .html
Text and Rich-text files	.txt, .rtf
Pages documents	.pages
Numbers spreadsheets	.numbers
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 identifying 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



TarFile.tar
3/31/14, 4:13 PM; 770.00 KB

TarGzipFile.tgz
3/31/14, 4:13 PM; 179.69 KB

WindowsExe.exe
3/31/14, 4:13 PM; 120.00 KB

WindowsMediaAudio.wma
3/31/14, 4:13 PM; 7.54 MB

ZipFile.zip
3/31/14, 4:13 PM; 3.29 MB

Unsupported file

Mobile Connect does not support files with the extension "zip".

You can try downloading the file anyway, but it may not be viewable unless you have an appropriate app installed for viewing it.

AirDrop. Tap to turn on Wi-Fi and Bluetooth to share with AirDrop.

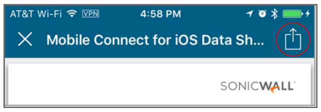
File Policies and Actions

On iOS, policies can be configured on the server to control the actions you can take with a file, including:

- Print
- Copy to the clipboard
- Open in a third-party application
- Securely cached on the device

If a file has an Allow policy (Allow Print, Allow Copy, or Allow Open In) enabled, a **Share** button is displayed in the top right of the navigation bar when the file is viewed.

share button



See the following sections:

- Allow All Actions
- Allow Print

- Allow Copy
- Allow Open in an Application

Importing Certificates to the iOS Device

Most Mobile Device Management products can push client certificates to the iOS device, but due to iOS security restrictions, SonicWall Mobile Connect accesses client certificates by importing them into the application keychain.

There are three ways to import client certificates to the iOS device using Mobile Connect. They are Apple Configurator 2, Mobile Device Management, and the Mobile Connect Client Certificate Importer feature.

Topics:

- Using Apple Configurator 2 with Mobile Connect
- Using Mobile Device Management for Certificate Import
- Using Mobile Connect Client Certificate Importer

Using Apple Configurator 2 with Mobile Connect

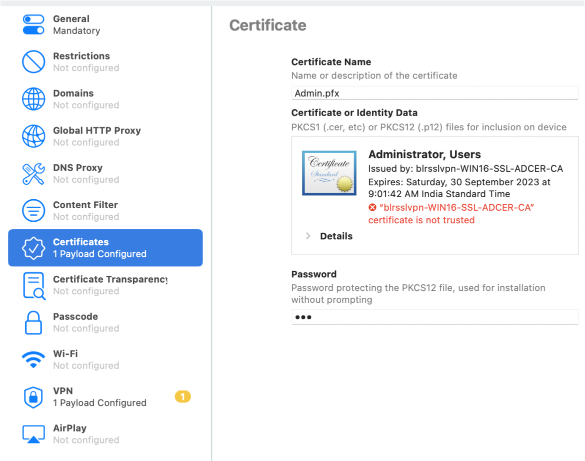
Apple Configurator 2 makes it easy for admin to configure togther and deploy iPhone, iPad, and iPod touch in business and education. It lets administrators of enterprise environments create configuration profiles for iOS devices that provide the ability to preconfigure the device settings for enterprise policies, such as VPN configuration, security policies, wireless settings, and so on. Information about downloading Apple Configurator is available here Mac App Store-Apple Configurator.

For more information, refer to:

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

To Configure a Mobile Connect Profile Using Apple Configurator 2:

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



Certificate

Certificate Name
Name or description of the certificate
Admin.pfx

Certificate or Identity Data
PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device

Administrator, Users
Issued by: blrsslvpn-WIN16-SSL-ADCER-CA
Expires: Saturday, 30 September 2023 at 9:01:42 AM India Standard Time
⊗ "blrsslvpn-WIN16-SSL-ADCER-CA" certificate is not trusted

› Details

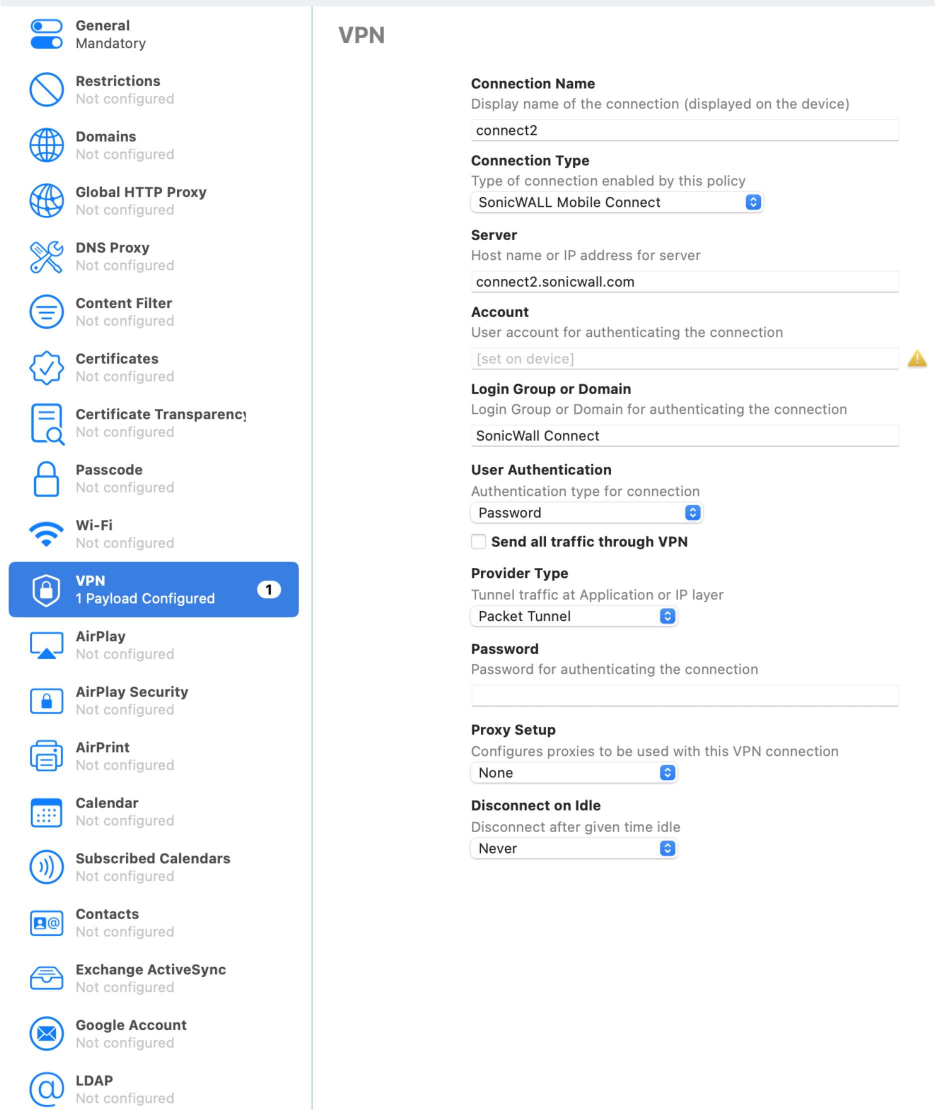
Password
Password protecting the PKCS12 file, used for installation without prompting
•••

a. Enter a **Certificate Name**.

b. Browse and select the **Certificate or Identity Data**.

c. Enter a **Password** to open the protected certificate without prompting to enter the password.

5. Go to **VPN** and click **Configure** the following settings:



VPN

Connection Name
Display name of the connection (displayed on the device)
connect2

Connection Type
Type of connection enabled by this policy
SonicWALL Mobile Connect

Server
Host name or IP address for server
connect2.sonicwall.com

Account
User account for authenticating the connection
[set on device]

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

User Authentication
Authentication type for connection
Password

☐ **Send all traffic through VPN**

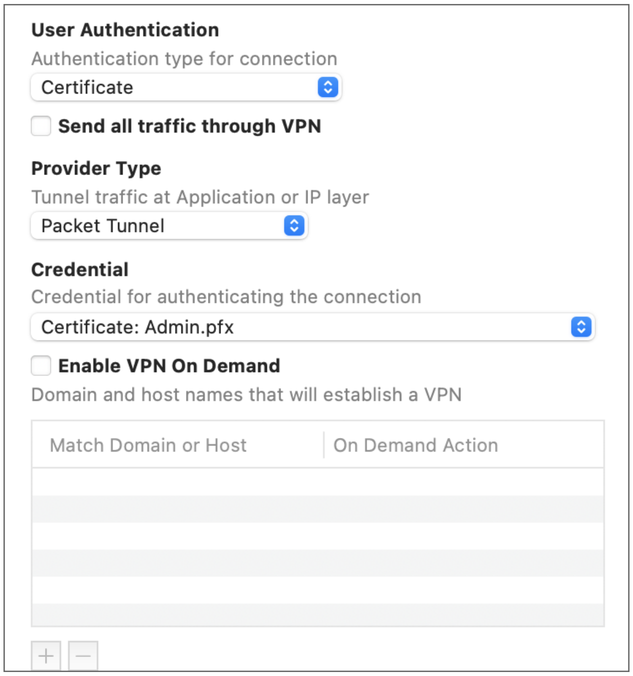
Provider Type
Tunnel traffic at Application or IP layer
Packet Tunnel

Password
Password for authenticating the connection

Proxy Setup
Configures proxies to be used with this VPN connection
None

Disconnect on Idle
Disconnect after given time idle
Never

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

Settings	Description
User Authentication	• If you select **Password**, in the **Password** field, enter the password for the user account. • If you select **Certificate**, in the **Credential** select the uploaded certificate.  **User Authentication** Authentication type for connection Certificate □ **Send all traffic through VPN** **Provider Type** Tunnel traffic at Application or IP layer Packet Tunnel **Credential** Credential for authenticating the connection Certificate: Admin.pfx □ **Enable VPN On Demand** Domain and host names that will establish a VPN Match Domain or Host | On Demand Action + −
Provider Type	Select the **Packet Tunnel** from the drop-down menu.
Proxy Setup	Leave the with default value or set any custom value from the drop-down menu.
Disconnect on Idle	Leave the with default value or set any custom value from the drop-down menu.

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

Using Mobile Device Management for Certificate Import

Importing a client certificate using Mobile Device Management:

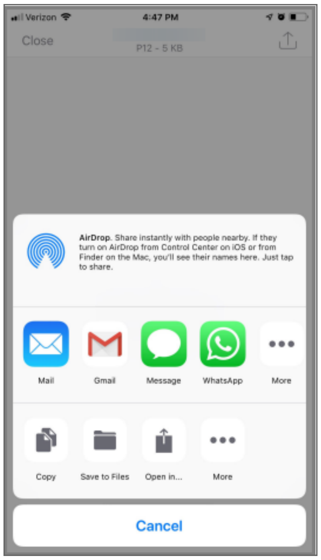
1. Email your ***.mobileprovision*** file (from the "**How to create...**" section) to an address which is configured in **Apple Mail** on the iOS device.
2. Open the mail on the iOS device.
3. Tap on the attached ***.mobileprovision*** file in the email.
   The Settings app should launch automatically and show a security prompt. The exact prompt will vary depending on how many VPN and certificate payloads are being imported, whether the iOS device is

controlled by Mobile Device Management, and whether the profile is signed. You may be required to authenticate on the iOS device.

Using Mobile Connect Client Certificate Importer

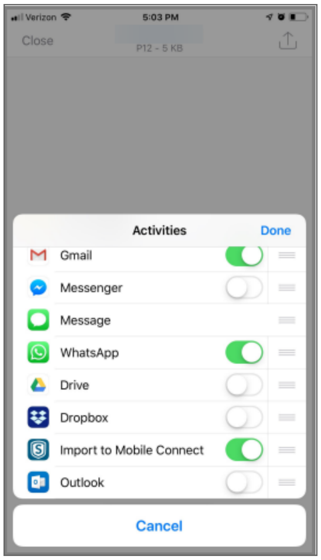
Importing a client certificate using Mobile Connect Client Certificate Importer:

1. From your iOS device, open the administrator email message that contains an attached client certificate and private key in a **p12** file format, for example: ***cert.p12***.
2. If using the standard Apple Mail app, press and hold the attachment. In **Outlook**, and in other apps, press the **Share** button with the up arrow.
3. Tap the three dots (...) labeled **More** in the middle row to get to the **Activities** list.



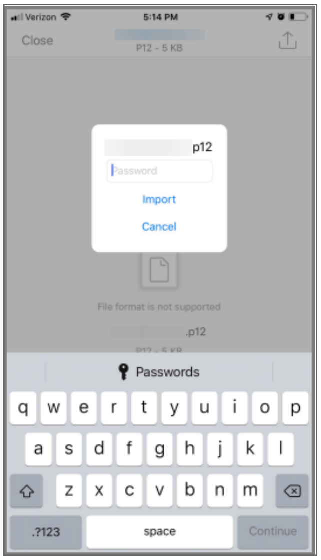
AirDrop. Share instantly with people nearby. If they turn on AirDrop from Control Center on iOS or from Finder on the Mac, you'll see their names here. Just tap to share.

4. Enable the **Import to Mobile Connect** toggle next to the app icon and tap **Done**.



5. Tap the **Import to Mobile Connect** icon in the app **Activities** menu.

6. Enter the **p12** file password (if prompted) and tap **Import** to get the certificate.



7. A checkmark verifies that the certificate is successfully imported.

ⓘ **NOTE:** After completing this process, the certificate is available in Mobile Connect whenever a server requires the user to provide it.

ⓘ **TIP:** A **.p12** file follows the PKCS #12 standard for storing cryptography objects as a single file. Each **.p12** file bundles a private key with a corresponding X.509 certificate.

4

Monitoring and Troubleshooting

This section discusses the Monitoring screen and provides troubleshooting tips, including how to contact Support from within Mobile Connect.

Topics:

Monitoring Mobile Connect

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

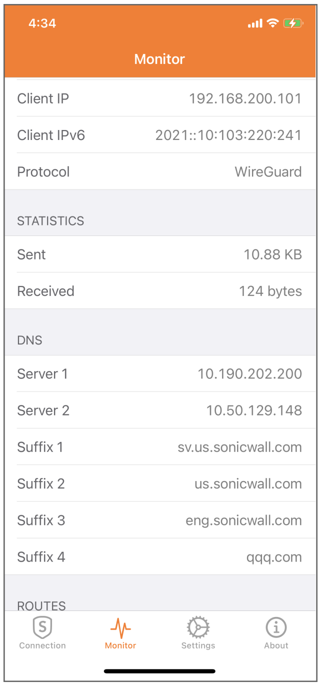
ⓘ **NOTE:** Displaying the protocol information in Monitor when connected to different appliances:

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



4:34

Monitor

Client IP	192.168.200.101
Client IPv6	2021::10:103:220:241
Protocol	WireGuard

STATISTICS

Sent	10.88 KB
Received	124 bytes

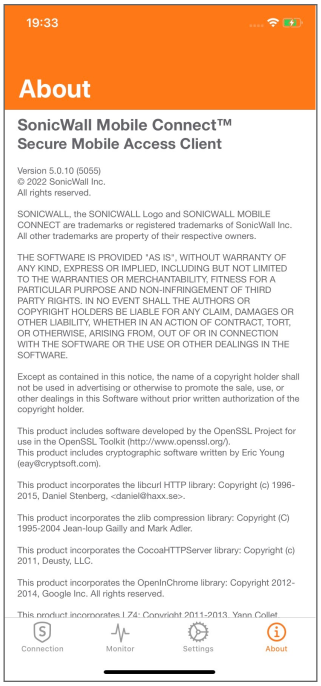
DNS

Server 1	10.190.202.200
Server 2	10.50.129.148
Suffix 1	sv.us.sonicwall.com
Suffix 2	us.sonicwall.com
Suffix 3	eng.sonicwall.com
Suffix 4	qqq.com

ROUTES

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

About Screen



About

SonicWall Mobile Connect™
Secure Mobile Access Client

Version 5.0.10 (5055)
© 2022 SonicWall Inc.
All rights reserved.

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

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

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

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product incorporates the libcurl HTTP library: Copyright (c) 1996-2015, Daniel Stenberg, <daniel@haxx.se>.

This product incorporates the zlib compression library: Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler.

This product incorporates the CocoaHTTPServer library: Copyright (c) 2011, Deusty, LLC.

This product incorporates the OpenInChrome library: Copyright 2012-2014, Google Inc. All rights reserved.

This product incorporates LZ4: Copyright 2011-2013, Yann Collet.

Troubleshooting Mobile Connect

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

1. Double-check that you have entered the server name properly in the connection configuration.
2. Go to the Safari browser on your iPhone, iPod touch, or iPad 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 Safari browser and you still cannot establish a Mobile Connect connection, notify SonicWall Support, as follows:
   a. On the Settings tab, enable **Debug Logging**.
   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 **Email Logs**. An email launches 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

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

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

ⓘ | **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 iOS   User Guide
Updated - October 2023
Software Version - 5.0
232-004058-00 Rev F

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