SONICWALL

View Page online: https://www.sonicwall.com/support/knowledge-base/how-to-create-a-connection-in-sonicwall-mobile-connect-with-ios/170503735978974

How to create a connection in SonicWall Mobile Connect with iOS

Description

This document outlines how to create a connection in SonicWall Mobile Connect. SonicWall Mobile Connect is a unified SSL-VPN client that can connect to our Next Generation Firewall (NGFW) appliances running SonicOS Enhanced and SMB Secure Remote Access (SRA-series) appliances.

Resolution

Step 1: Launch the application.

From the iOS home screen, launch the Mobile Connect application.

When you first open the application, a popup will prompt you to enable Mobile Connect in iOS. Simply tap the 'Enable' option to continue.

Step 2a (UTM only. See Step 2b for SMB SSL-VPN): Tap "Add connection".

Tap on "Add connection" to create a new connection. Give the connection a name, and enter a server IP or FQDN. Connection names cannot match the name of any VPN connection added in the iOS Settings app. This must be a unique name, as Mobile Connect is integrated with iOS, and connections can be established without opening Mobile Connect. Once a name and IP/FQDN have been provided, tap Next.

Note: If you are running an SMB SSLVPN appliance or a UTM appliance with SSL-VPN services over a custom port, ensure that you specify the port. Example: sslvpn.example.com:4433.

Step 2b (SMB SSL-VPN only. See Step 2a for UTM SSL-VPN): Tap "Add connection".

Tap on "Add connection" to create a new connection. Give the connection a name, and enter a server IP or FQDN. Connection names cannot match the name of any VPN connection added in the iOS Settings app. This must be a unique name, as Mobile Connect is integrated with iOS, and connections can be established without opening Mobile Connect. SMB SSL-VPN appliances can be configured with multiple Portals and Domains. Domains can be tied to multiple Portals, but in some scenarios they may only be accessible via a specific Portal. If this is the case with your appliance, one of two steps can be taken:

a. Assign the Domain to the VirtualOffice Portal as well as your custom Portal. This will allow users to log in using your custom Domain from the default VirtualOffice Portal as well as your custom Portal.
b. Configure your custom Portal with a Virtual Host. Example: mycustomportal.example.com will go to your custom Portal (and display any Domain assigned to it) while sslvpn.example.com goes to the default VirtualOffice Portal (and displays any Domains assigned to it). You must be able to resolve the chosen Virtual Host name externally in order for users to reach the custom Portal using the Virtual Host domain name. In this case, to authenticate to the custom Domain you'll need to enter the Virtual Host domain name as the server name.

If one of the above steps isn't taken, the Domain you'd like to log into may not be available in the Domain list, thus you will not be able to authenticate to it.

Once a name and IP/FQDN have been provided, tap Next.

Notes:
a. If you are running an SMB SSLVPN appliance or a UTM appliance with SSL-VPN services over a custom port, ensure that you specify the port. Example: sslvpn.example.com:4433.
b. Full Portal URLs are not supported in Mobile Connect. The proper format is IP address or FQDN, along with a port number if necessary. (Ex: 1.2.3.4, 1.2.3.4:4433, example.com, sslvpn.example.com:4433). Do not enter a server address with a Portal URL behind it (Ex: sslvpn.example.com/portal/mycustomportal)

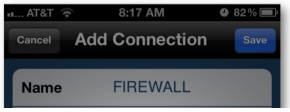
Step 3: Certificate verification.

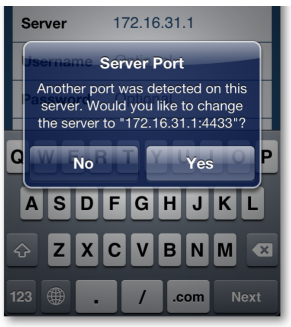
At this time, Mobile Connect will attempt to verify the server's identity. If a self-signed or otherwise un-trusted certificate is found, you will be prompted to continue or cancel the connection. An option to view the certificate details is available.

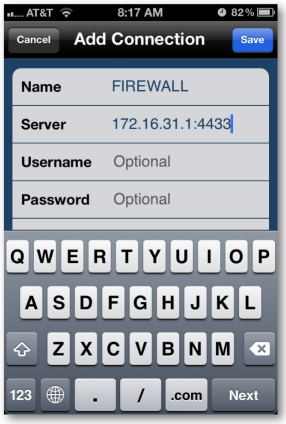
Step 4: Server Port detection (applicable to UTM-SSLVPN only).

In this example, Mobile Connect is connecting to a UTM appliance with SSL-VPN functionality enabled on the default port 4433 and WAN management is enabled on the default port of 443. Although the port can be specified in Step 2, Mobile Connect will try to detect if the SSL-VPN service is running on another port, and will offer to change it automatically, as shown below. Tap "Yes" to allow Mobile Connect to change the port for you.

Note: This step is only applicable to UTM-SSLVPN. If you are running an SMB SSLVPN appliance over a custom port, ensure that you specify the port in Step 2.



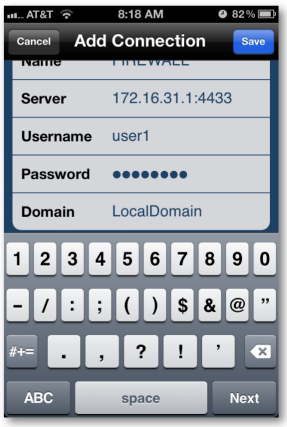




Step 5: Provide your credentials.

Credentials can be specified before saving the connection profile, or when you connect. In this example, credentials have been specified before saving the connection profile. Once you're ready to save the profile, tap "Save".

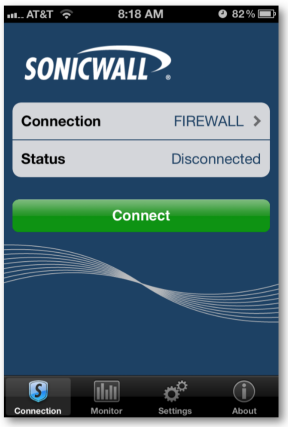
UTM/NGFW appliances have a single Domain to log into, so no further steps are required before saving the connection profile.

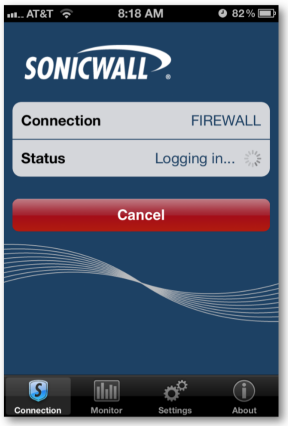


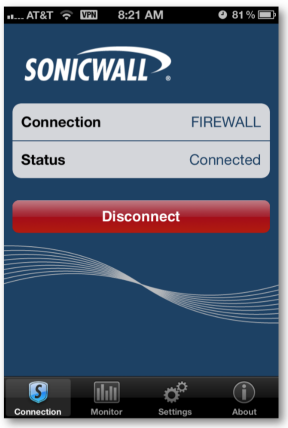
For SSL-VPN apliances

Step 6: Initiate a connection.

After tapping "Save", you'll be back on the Connection tab. Tap "Connect" to initiate a connection.

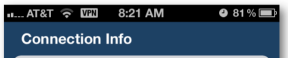


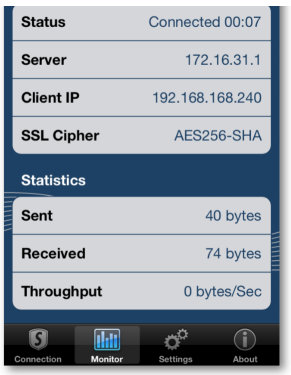


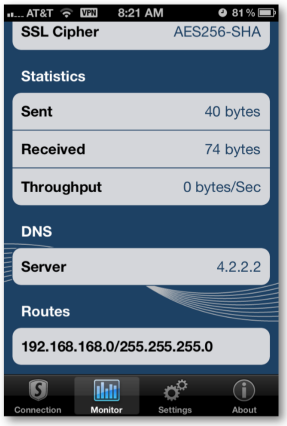


Step 7: Viewing connection details using the Monitor tab.

Tap on the Monitor tab to view connection details.




Status
Connected 00:07
Server
172.16.31.1
Client IP
192.168.168.240
SSL Cipher
AES256-SHA
Statistics
Sent
40 bytes
Received
74 bytes
Throughput
0 bytes/Sec
Connection
Monitor
Settings
About


AT&T
VPN
8:21 AM
81 %
SSL Cipher
AES256-SHA
Statistics
Sent
40 bytes
Received
74 bytes
Throughput
0 bytes/Sec
DNS
Server
4.2.2.2
Routes
192.168.168.0/255.255.255.0
Connection
Monitor
Settings
About