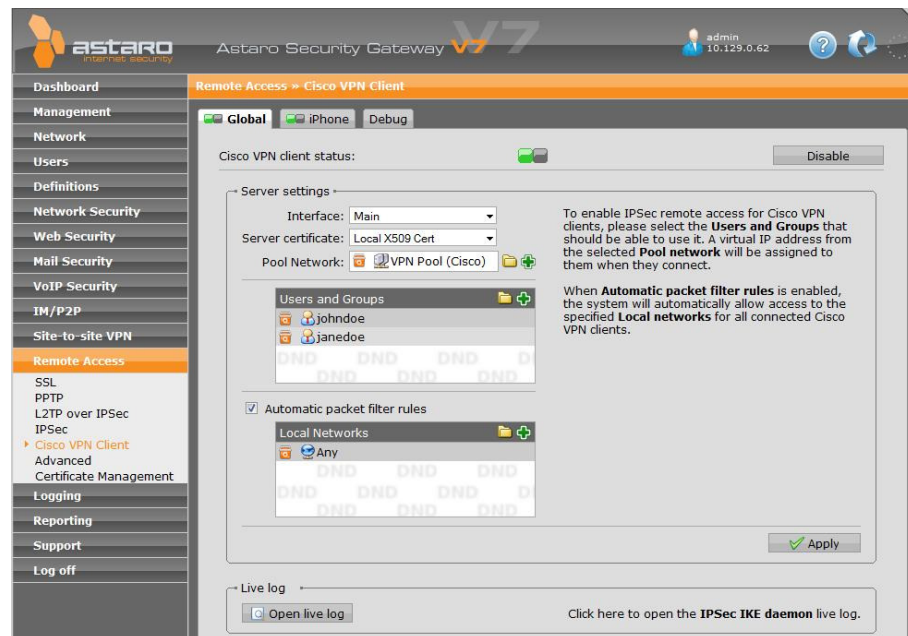


iPhone VPN Overview

The Apple iPhone supports VPN Roadwarrior tunnels using three different technologies, PPTP, L2TP, and IPSEC. While iPhone users can take advantage of all connection methods to connect to Astaro installations, this guide will outline how to make use of the 3rd Party IPSEC client that is included in iPhone OS 2.0 and beyond in order to create a secure connection to an Astaro device. This allows users to securely access the Astaro WebAdmin, SSH to internal servers, check email over encrypted connections, and surf to internal sites via a browser, to name just a few useful functions. In order to configure this connectivity, your Astaro platform must be setup to accept Cisco VPN Client communications, and the iPhone functionality of this engine must be enabled (figure 1).

*For dedicated, detailed guides on Roadwarrior IPSEC setup of your Astaro installation, there are more detailed, published guides for advanced options available on our knowledgebase at www.astaro.com/kb. In this guide, we will show some overview and basic screenshot information from the Astaro platform itself, but will focus mainly on the client-side configuration steps and procedure.



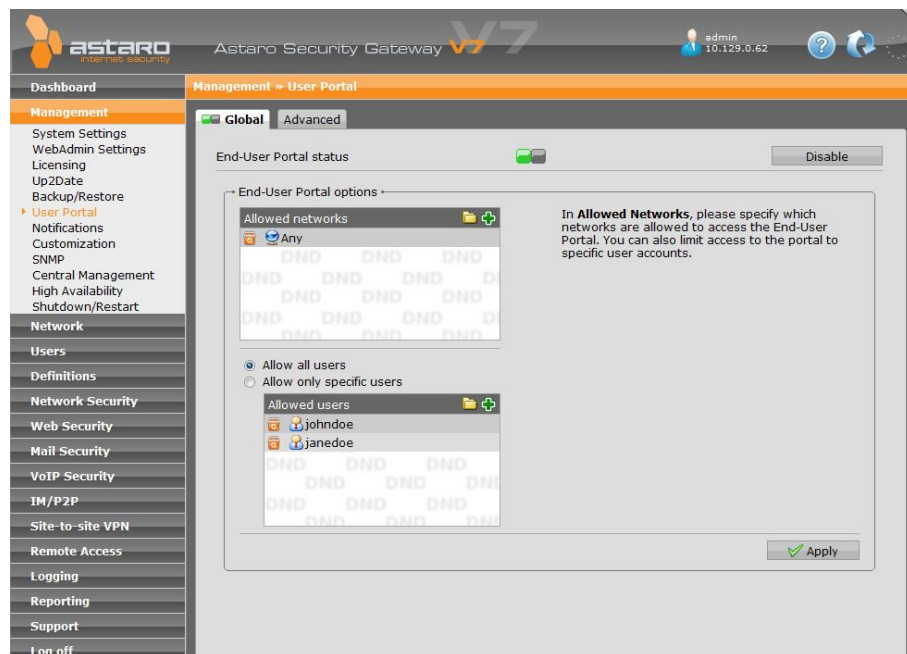
(Figure 1 - Astaro ready for iPhone connections)

Configuring iPhone for IPSEC connectivity to Astaro

After quickly configuring your Astaro platform to support incoming IPSEC Roadwarrior connections, you require just a few steps to setup your iPhone to connect to it. In this example, we'll show you how to configure your iPhone for IPSEC connectivity.

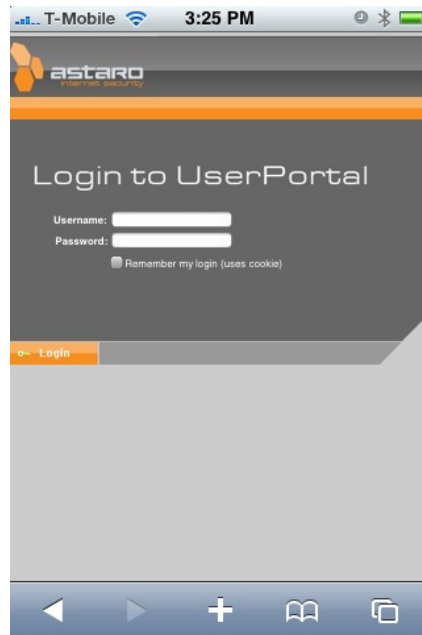
1) Inside WebAdmin of your ASG, it takes just a few simple clicks to enable the IPSEC access for the Cisco client installed on your iPhone. You can set the users that are allowed to connect, and optionally restrict what resources are accessible after the connection is established, for each user or the entire pool of IPSEC Roadwarriors. This is useful if you do not want users to have full visibility to the entire Internal network after connecting, but rather wish to strictly control what can be accessed, even using this secured method.

2) For iPhone users to be able to install and configure the IPSEC connectivity, the Astaro UserPortal must be enabled for the user(s) that wish to use this functionality. Simply enable the UserPortal (figure 2) and ensure the necessary users are able to access it via the configuration options.



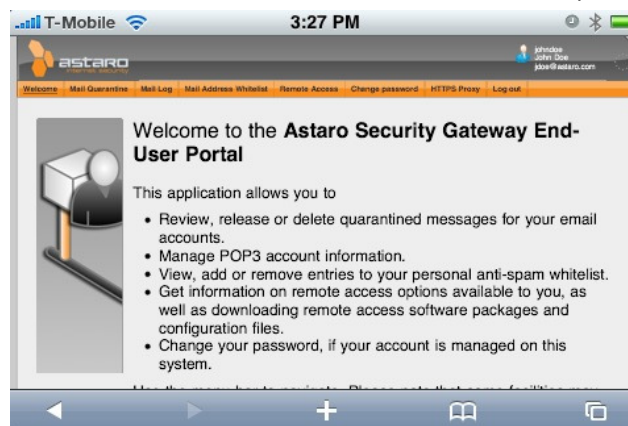
(Figure 2 - Astaro UserPortal enabled by Administrator)

3) Using your iPhone browser, navigate to the IP address or hostname of the Astaro UserPortal as communicated by the administrator (for example <https://ourastaro.ourcompany.com>), and login with the required directory or local-user credentials to access your personalized portal (figure 3).



(Figure 3 – UserPortal login screen)

4) Upon logging into the Astaro UserPortal, a welcome screen will greet the user and provide options depending on the configuration of the Astaro device, and the permissions of the user granted to them by the Administrator. Select “Remote Access” from the menu choices at the top.



(Figure 4 – The UserPortal welcome screen)

5) For the section of the Remote Access screen that deals with the iPhone VPN Configuration, specify an export password for the client configuration and certificate which will be imported into your iPhone. You will require this password just once in a few moments, during this setup process. Now click "install" to begin the automated client installation (Figure 4).



(Figure 4 – iPhone VPN package installer)

6) Once the install process has been started, wait just a few seconds, then click "install" on the resulting screen that appears (Figure 5). When prompted again to confirm this process, select "Install Now" (Figure 6).



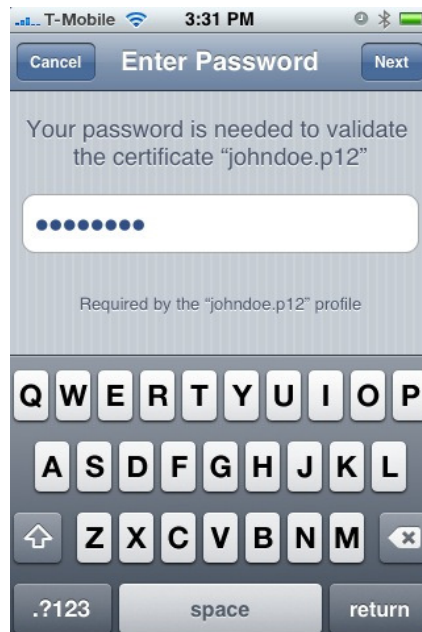
(Figure 5 – Installation prompt)



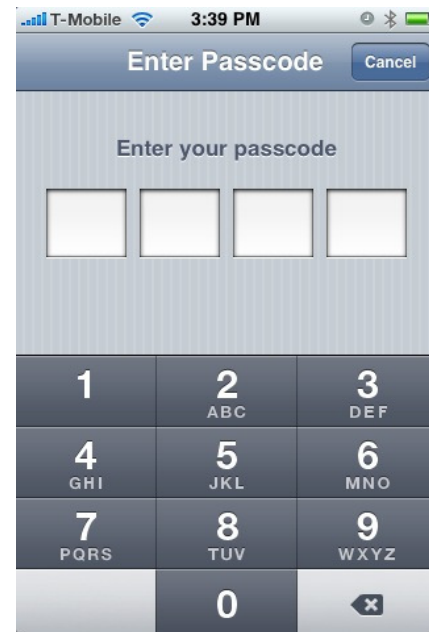
(Figure 6 – Confirming the installer)

7) The installation package downloaded from the Astaro UserPortal contains all the technical information necessary to build the configuration on the iPhone, such as encryption strength, tunnel parameters, and IP address information. Users do not need to know this information. As the installation happens, you will be prompted for the password which you manually set during the export of the client installer from the UserPortal (Figure7). In this example we used simple "password".

*Note: If you protect your iPhone using a "lock password", the OS will prompt you for this (Figure 8) during the install process. If you do not use a lock code on your phone, this screen will not present itself.



(Figure 7 – Export Password)



(Figure 8 – optional iPhone code)

8) That's it! The setup is complete (Figure 9). All that remains is to connect.



(Figure 9 – Setup Complete)

9) To start the connection, on the main menu select Settings, and enter the General options area (Figure 10). Go to Network setup --> VPN (Figure 11).



(Figure 10 – Network Settings)



(Figure 11 – VPN Settings)

10) In this VPN area (Figure 13) set the VPN button to "On" to connect.



(Figure 13 – VPN Startup)

11) Once connected (Figure 14), status information will verify your successful session to your Astaro (Figure 15).



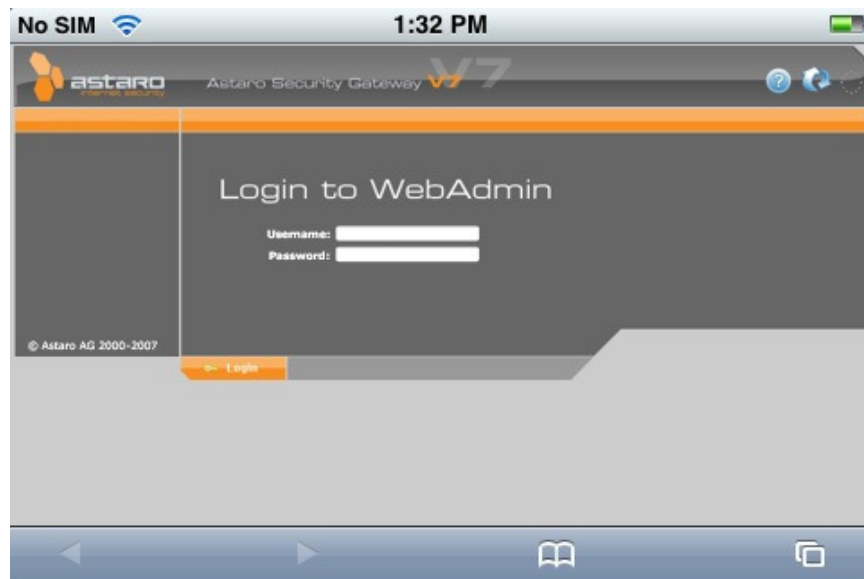
(Figure 14 - Connection Established)



(Figure 15 – Connection Status)

12) Now that you are connected you can conduct secure communications to the LAN resources at the other end of the tunnel.

For example, for security reasons you might disallow access to your Astaro's WebAdmin GUI from the Internet, so you must come from the private side in order to access it. Connecting over a VPN places you virtually in the LAN, so you can access your WebAdmin without making it publicly available (Figure 16).



Congratulations, you have now completed setup of IPSEC VPN from your iPhone to your Astaro product!