EMC²
where information lives

EMC Global Networks and Telecommunications

AnyConnect SSL VPN Remote Access

Upgrade guide for current SSL VPN users

GNT - Architecture and Engineering

EMC
GNT

Contents

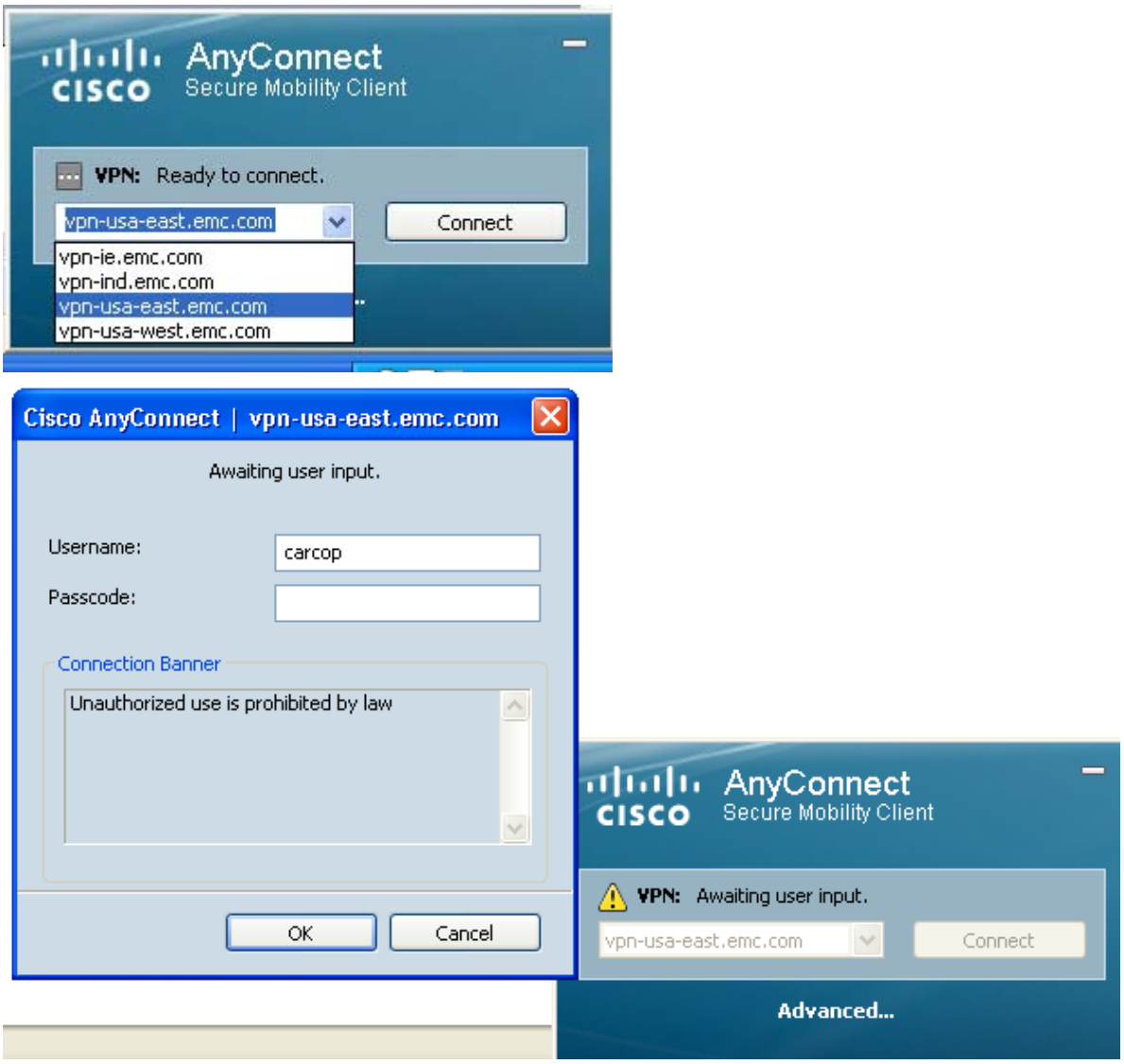
Overview

We are deploying a newer version of the AnyConnect Client known as the Cisco AnyConnect Secure Mobility Client v3.0 which looks very different from what the early adopters of SSL VPN have come accustomed to. This guide will explain the differences and the upgrade process.

Figure 1 Current AnyConnect Client

EMC²
where information lives

Figure 2 New AnyConnect v3.0 Secure Mobility Client



Changes to the Client & Upgrade

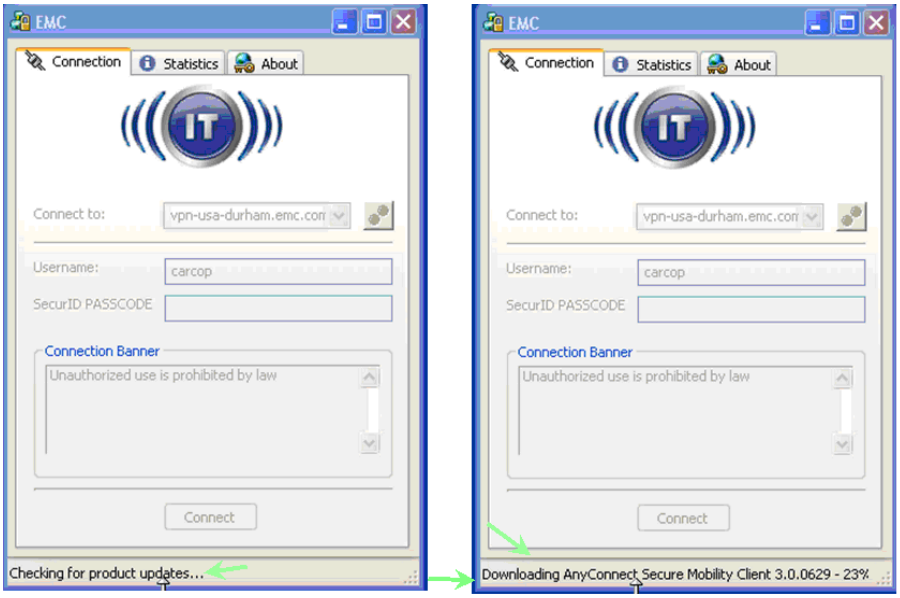
On the surface the changes are mostly aesthetic with a cleaner smaller user interface; however the basic behavior is identical in terms of VPN connectivity. The newer client does position us to offer additional features such as Wireless integration so that older VPN Client is no longer required and this will be addressed in the very near future.

We will be installing the new v3.0 client on all VPN head ends across all our gateways making the upgrade process automatic.

If you are watching the session establishment closely during the upgrade you will notice that the time to establish the connection will be a little longer than usual but any new sessions hereon after should be restored to normal

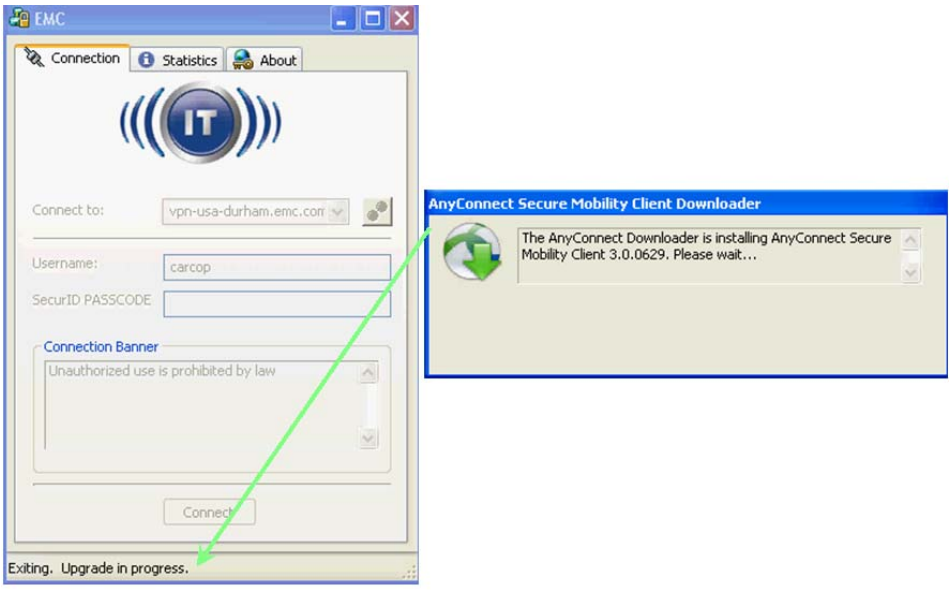
After logging in as normal, the current client will check with the gateway for any updates. The current client will find a major upgrade to the Cisco AnyConnect Secure Mobility Client v3.0 and begin the download.

Figure 3 AnyConnect update check and download



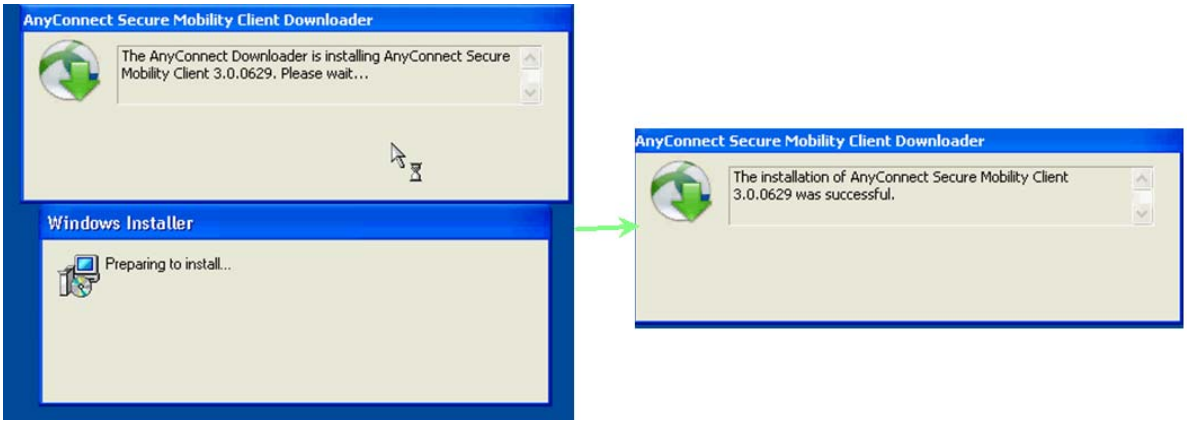
After the new client download is completed the installation package is automatically launched and the installation begins.

Figure 4 Client Upgrade.



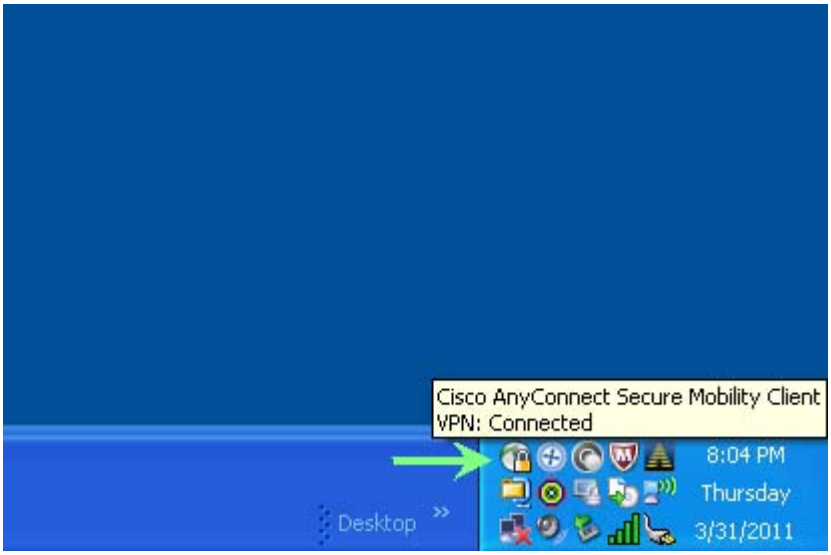
During the installation the old client will be removed and replace with the newer version. Please do not manually install the newer client and attempt to go back since this will cause instability.

Figure 5 Install process



After the install completes you are connnected and ready to access the network. Note that the icon in the tray has changed from v2.5 to v3.0

Figure 6 New Client sent to tray

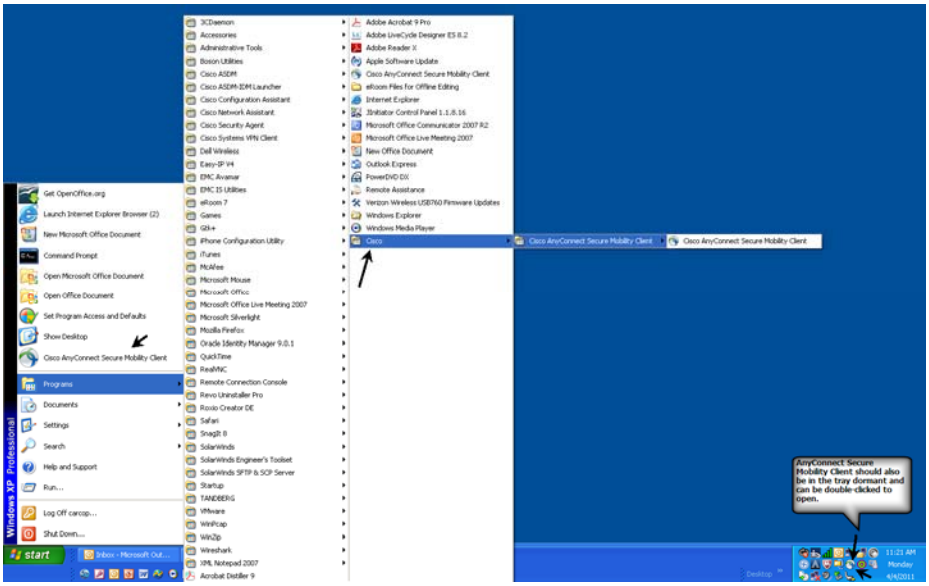


.

Launching AnyConnect Secure Mobility

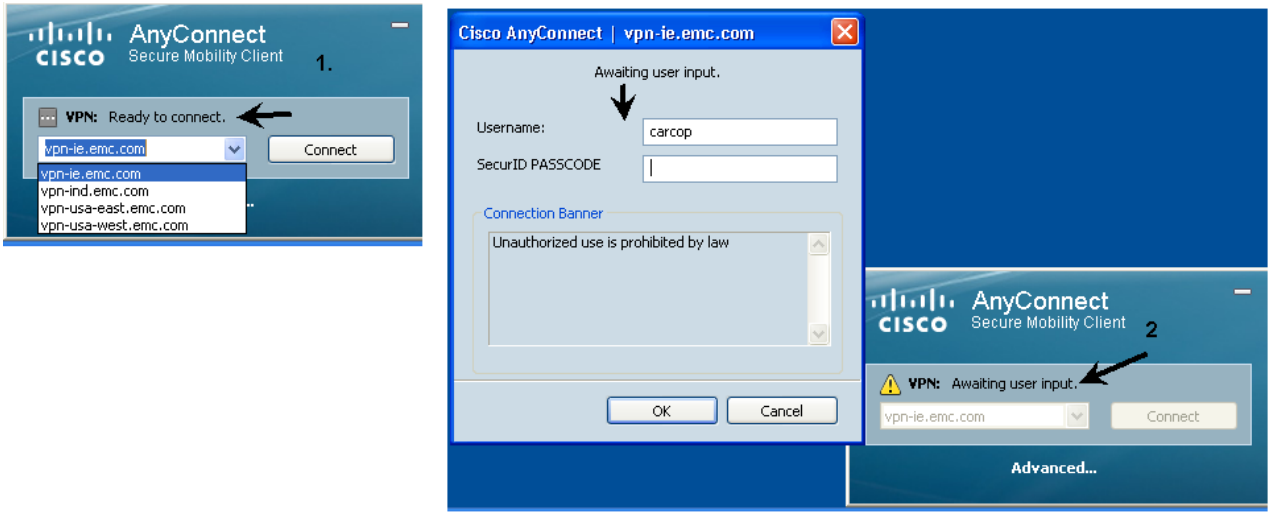
The only change in launching the new client is that the icons and naming convention is different.

Figure 7 AnyConnect Launch locations



Once launched the available gateways will be located in the pull-down identical to the earlier client, the login form will fly out which is a new behavior, this keeps the client footprint much smaller.

Figure 8 AnyConnect login

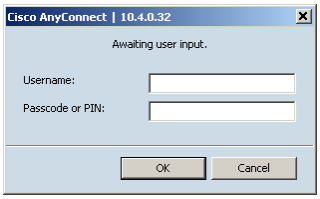


Once connected to the VPN Gateway you will be prompted to login with your Username and SecurID Passcode.

- ⇒ Users with physical fobs in hand will enter the Pin combined with the Token code in the same manner used with the legacy VPN Client.
- ⇒ Users that have migrated to using the Soft Token solution on their laptop only need to enter the Pin since AnyConnect will pull the token code automatically for you.

- ⇒ Users that have Soft Token installed on another device such as an iPhone enter the pin onto that device and the output generated by Soft Token is entered into the 'PIN or Passcode' field.

Figure 9 Soft Token Prompt



After successfully logging in, you will need to acknowledge the following banner's to complete the connection.

- ⇒ The first banner is simply informing you of which gateway you have connected to.
- ⇒ The second banner is informing you of the security posture and policies assigned to the session.

Figure 10 Gateway banner

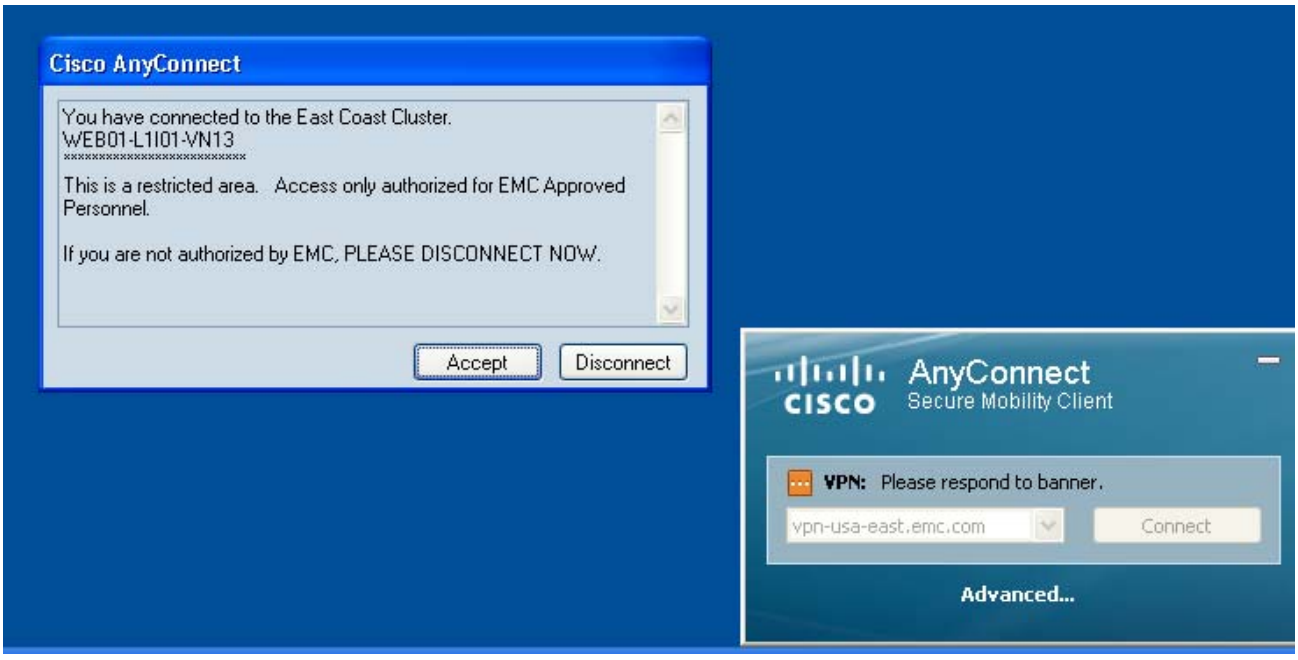
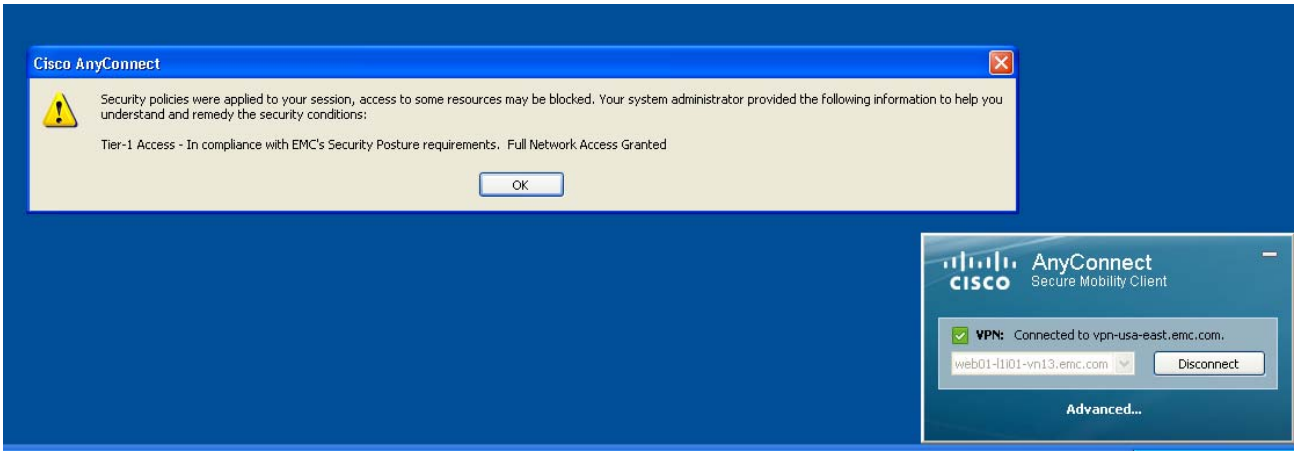
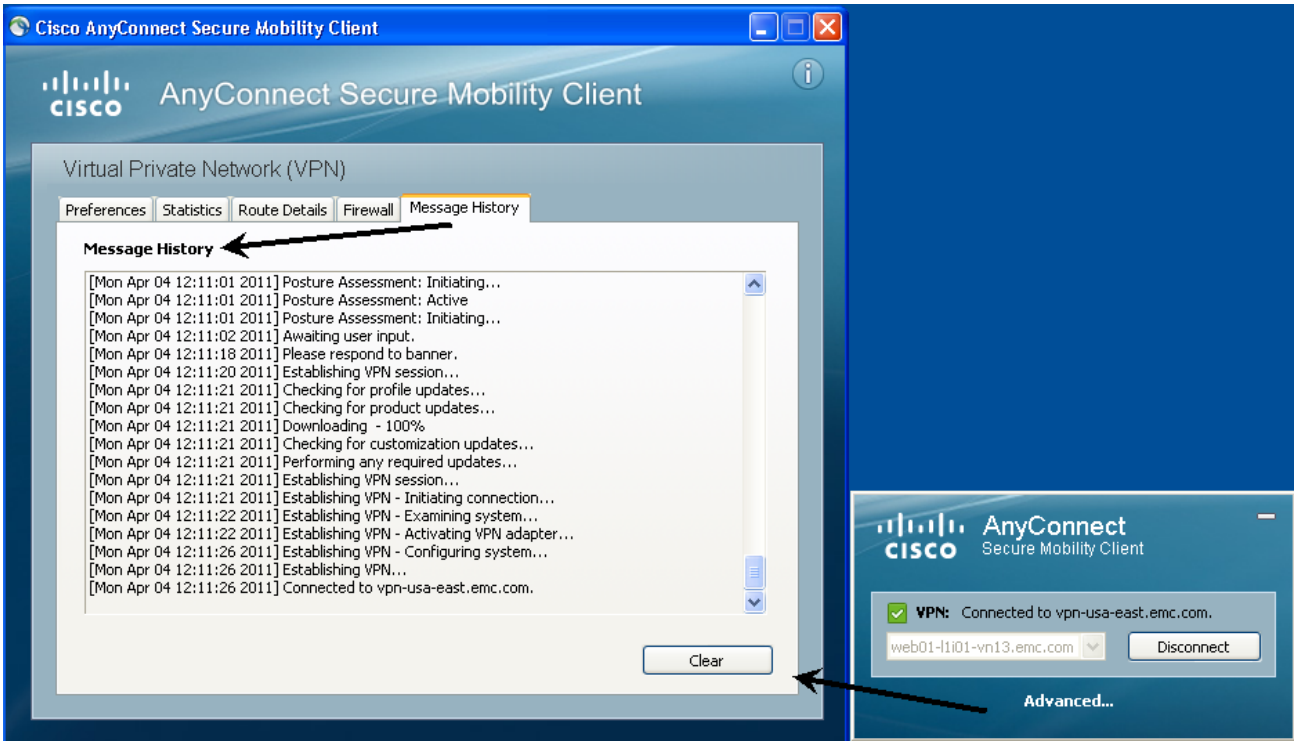


Figure 11 Security Posture banner



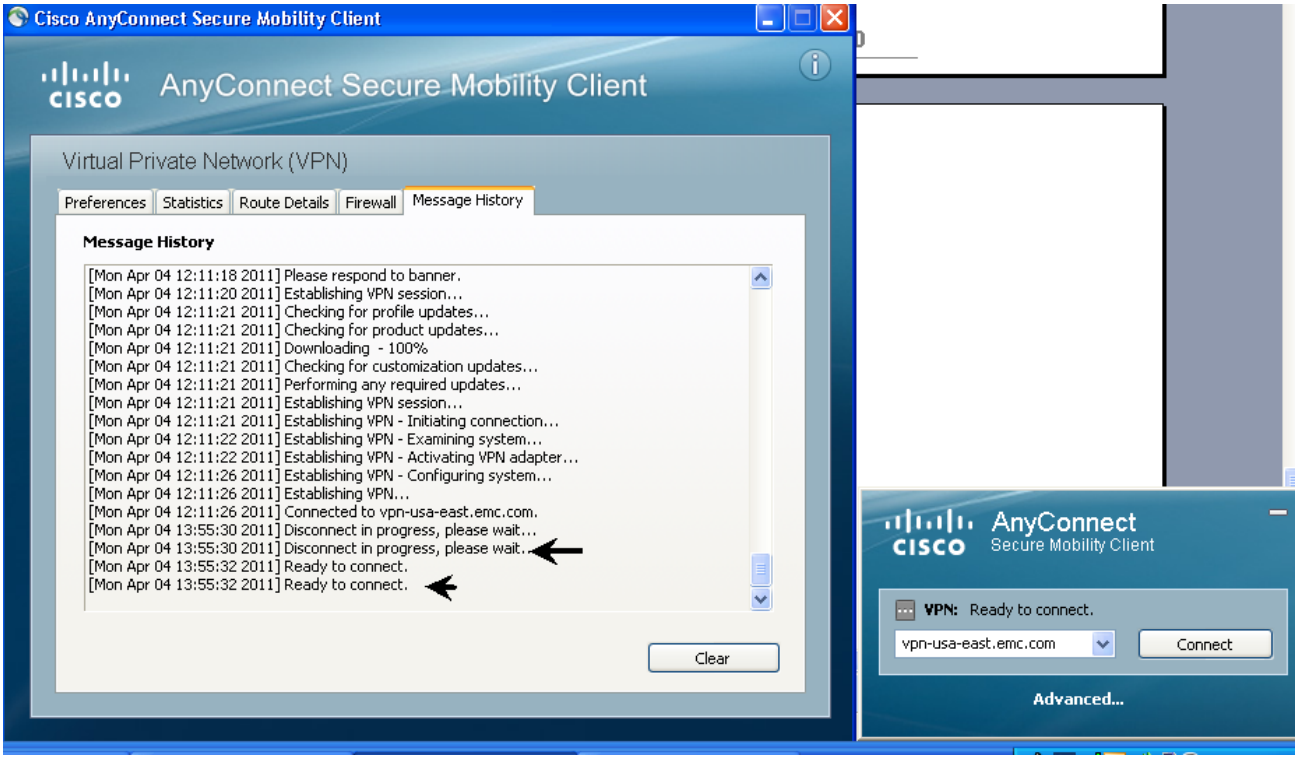
After accepting the banner's the AnyConnect client will transition to only an icon in your taskbar. You can open the client if you wish to view your connection status and statistics.

Figure 12 AnyConnect Connection Status



It is highly recommended that you gracefully disconnect your session when you wish to terminate your session.

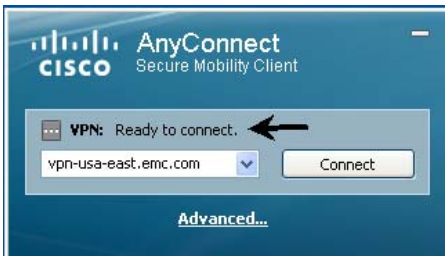
Figure 13 AnyConnect Disconnect and connection status.



Troubleshooting

The AnyConnect Client should always be in a 'Ready to connect' state before attempting to connect to EMC. The client determines if network connectivity is available.

Figure 14 AnyConnect Ready to Connect



If there no network connectivity the Client will report this also.

Figure 15 AnyConnect No Network Connectivity / Verify your network connection

If the client is reporting No Network Connectivity and asking you to verify your connection and before calling the help desk please open a command prompt and perform an ‘ipconfig’ to list your current IP address. If you have an IP address, ensure that address resolution from your network provider is operational by performing an ‘nslookup’ on the gateway you are attempting to connect to as shown below.

Figure 16 Open a command window

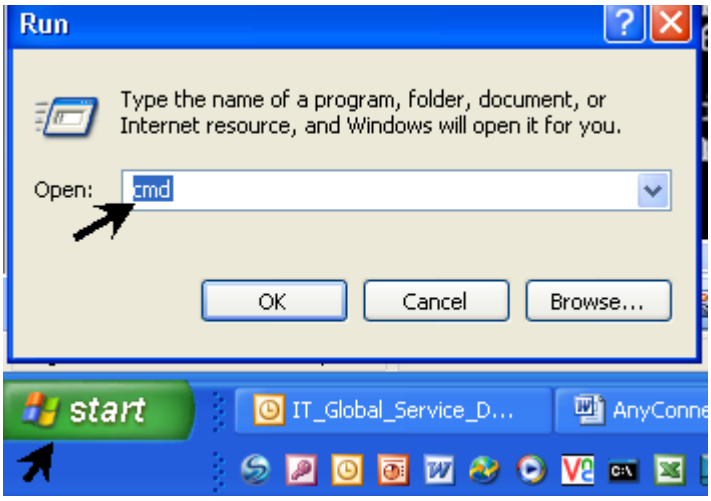


Figure 17 ipconfig & nslookup troubleshooting