APPENDIX C

Communicating User Guidelines

Consider communicating the following guidelines to your VPN users or use this section as a reference when responding to user requests for guidance. The following topics are covered:

Apple MobileMe Conflicts with AnyConnect

If users of MobileMe have configured "Back to my Mac," they will encounter connection problems with AnyConnect. Both AnyConnect and MobileME use the virtual adapter named "utun0." MobileMe starts before AnyConnect when the computer boots, so it always gets the utun0 interface first, which causes Cisco AnyConnect to fail. Neither application can be configured to use a different interface, such as "utun1."

Mac users must turn off “Back to my Mac” before connecting to the AnyConnect VPN. Once the VPN has connected, they can re-enable “Back to my Mac.”

Responding to a TUN/TAP Error Message with Mac OS X 10.5

During the installation of AnyConnect on Mac OS X 10.5 and earlier versions, the following error message sometimes appears:

```
A version of the TUN virtual network driver is already installed on this system that is
incompatible with the AnyConnect client. This is a known issue with OS X version 10.5 and
prior, and has been resolved in 10.6. Please uninstall any VPN client, speak with your
System Administrator, or reference the AnyConnect Release Notes for assistance in
resolving this issue.
```

Mac OS X 10.6 resolves this issue because it provides the version of the TUN/TAP virtual network driver that AnyConnect requires.

Versions of Mac OS X earlier than 10.6 do not include a TUN/TAP virtual network driver, so AnyConnect installs its own on these operating systems. However, some software such as Parallels, software that manages data cards, and some VPN applications install their own TUN/TAP driver. The AnyConnect installation software displays the error message above because the driver is already present, but its version is incompatible with AnyConnect.

To install AnyConnect, you must remove the TUN/TAP virtual network driver.

Note Removing the TUN/TAP virtual network driver can cause issues with the software on your system that installed the driver in the first place.

To remove the TUN/TAP virtual network driver, open the console application and enter the following commands:

sudo rm -rf /Library/Extensions/tap.kext

sudo rm -rf /Library/Extensions/tun.kext

sudo rm -rf /Library/StartupItems/tap

sudo rm -rf /Library/StartupItems/tun

sudo rm -rf /System/Library/Extensions/tun.kext

sudo rm -rf /System/Library/Extensions/tap.kext

sudo rm -rf /System/Library/StartupItems/tap

sudo rm -rf /System/Library/StartupItems/tun

After entering these commands, restart Mac OS, then re-install AnyConnect.

64-bit Internet Explorer Not Supported

AnyConnect installation via WebLaunch does not support 64-bit versions of Internet Explorer. If using Windows on x64 (64-bit), use the 32-bit version of Internet Explorer or Firefox to install WebLaunch. At this time, Firefox is available only in a 32-bit version.

Avoiding the Wireless Hosted Network

Using the Windows 7 Wireless Hosted Network feature can make AnyConnect unstable. When using AnyConnect, we do not recommend enabling this feature or running front-end applications (such as Connectify or Virtual Router) that enable it.

Start Before Logon and DART Installation

The Start Before Logon component requires that AnyConnect be installed first.

If SBL or DART is manually uninstalled from an endpoint that then connects, these components will be re-installed. This behavior occurs only if the head-end configuration specifies that these components be installed and if the preferences (set on the endpoint) permit upgrades.

Responding to a Quarantine State

An endpoint that does not comply with corporate policies for access shows a network status of *Quarantined* on the AnyConnect Connection tab.

An ACL assigned to a dynamic access policy applied to a quarantined session typically grants access only to remediation services such as antivirus and antispyware updates.

A session in a quarantined state must have sufficient time to remediate the endpoint. Following this time period, the user must click **Reconnect** to exit the state and start a new posture assessment.

Using the AnyConnect CLI Commands to Connect

The Cisco AnyConnect VPN Client provides a command line interface (CLI) for users who prefer to enter client commands instead of using the graphical user interface. The following sections describe how to launch the CLI command prompt and the commands available through the CLI:

Launching the Client CLI Prompt, page C-3

Using the Client CLI Commands, page C-3

Preventing a Windows Popup Message When ASA Terminates Session, page C-5

Launching the Client CLI Prompt

To launch the CLI command prompt:

Windows—Locate the file *vpncli.exe* in the Windows folder C:\Program Files\Cisco\Cisco AnyConnect VPN Client. Double-click the file *vpncli.exe*.

For Linux and Mac OS X—Locate the file *vpn* in the folder /opt/cisco/anyconnect/bin/. Execute the file *vpn*.

Using the Client CLI Commands

If you run the CLI in interactive mode, it provides its own prompt. You can also use the command line. Table 3-1 shows the CLI commands.

Table 3-1 AnyConnect Client CLI Commands

Command	Action
connect *IP address or alias*	Client establishes a connection to a specific ASA.
disconnect	Client closes a previously established connection.
stats	Displays statistics about an established connection.
quit	Exits the CLI interactive mode.
exit	Exits the CLI interactive mode.

The following examples show the user establishing and terminating a connection from the command line:

Windows

connect 209.165.200.224
Establishes a connection to a security appliance with the address 209.165. 200.224. After contacting the requested host, the AnyConnect client displays the group to which the user belongs and asks for the user's username and password. If you have specified that an optional banner be displayed, the user must respond to the banner. The default response is **n**, which terminates the connection attempt. For example:

```
VPN> connect 209.165.200.224
    >>contacting host (209.165.200.224) for login information...
    >>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
    >>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour. The system will not be available during that time.

accept? [y/n] y
    >> notice: Authentication succeeded. Checking for updates...
    >> state: Connecting
    >> notice: Establishing connection to 209.165.200.224.
    >> State: Connected
    >> notice: VPN session established.
VPN>
```

stats
Displays statistics for the current connection; for example:

```
VPN> stats
[ Tunnel Information ]

    Time Connected:01:17:33
    Client Address:192.168.23.45
    Server Address:209.165.200.224

[ Tunnel Details ]

    Tunneling Mode:All Traffic
    Protocol: DTLS
    Protocol Cipher: RSA_AES_256_SHA1
    Protocol Compression: None

[ Data Transfer ]
```

```
    Bytes (sent/received): 1950410/23861719
    Packets (sent/received): 18346/28851
    Bypassed (outbound/inbound): 0/0
    Discarded (outbound/inbound): 0/0

[ Secure Routes ]

    Network     Subnet
    0.0.0.0     0.0.0.0
VPN>
```

disconnect
Closes a previously established connection; for example:

```
VPN> disconnect
    >> state: Disconnecting
    >> state: Disconnected
    >> notice: VPN session ended.
VPN>
```

quit or **exit**

Either command exits the CLI interactive mode; for example:

```
quit
goodbye
    >>state: Disconnected
```

Linux or Mac OS X

/opt/cisco/anyconnect/bin/vpn connect 1.2.3.4
Establishes a connection to an ASA with the address *1.2.3.4*.

/opt/cisco/anyconnect/bin/vpn connect some_asa_alias
Establishes a connection to an ASA by reading the profile and looking up the alias *some_asa_alias* in order to find its address.

/opt/cisco/anyconnect/bin/vpn stats
Displays statistics about the vpn connection.

/opt/cisco/anyconnect/bin/vpn disconnect
Disconnect the vpn session if it exists.

Preventing a Windows Popup Message When ASA Terminates Session

If you terminate an AnyConnect session by issuing a session reset from the ASA, the following Windows popup message displays to the end user:

```
The secure gateway has terminated the vpn connection. The following message was
received for the gateway: Administrator Reset
```

It could be undesirable for this message to appear. For example, when the VPN tunnel is initiated using the CLI command. You can prevent the message from appearing by restarting the client CLI after the client connects. The following example shows the CLI output when you do this:

```
C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client>vpncli
Cisco AnyConnect Secure Mobility Client (version 3.0.1).
Copyright (c) 2004 - 2011 Cisco Systems, Inc.
All Rights Reserved.
  >> state: Connected
  >> state: Connected
```

```
  >> notice: Connected to asa.cisco.com.
  >> notice: Connected to asa.cisco.com.
  >> registered with local VPN subsystem.
  >> state: Connected
  >> notice: Connected to asa.cisco.com.
  >> state: Disconnecting
  >> notice: Disconnect in progress, please wait...
  >> state: Disconnected
  >> notice: On a trusted network.
  >> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

Alternatively, in the Windows registry, you can create a 32-bit double value with the name SuppressModalDialogs on the endpoint device in the following locations. The client checks for the name, but ignores its value:

- 64-bit Windows:

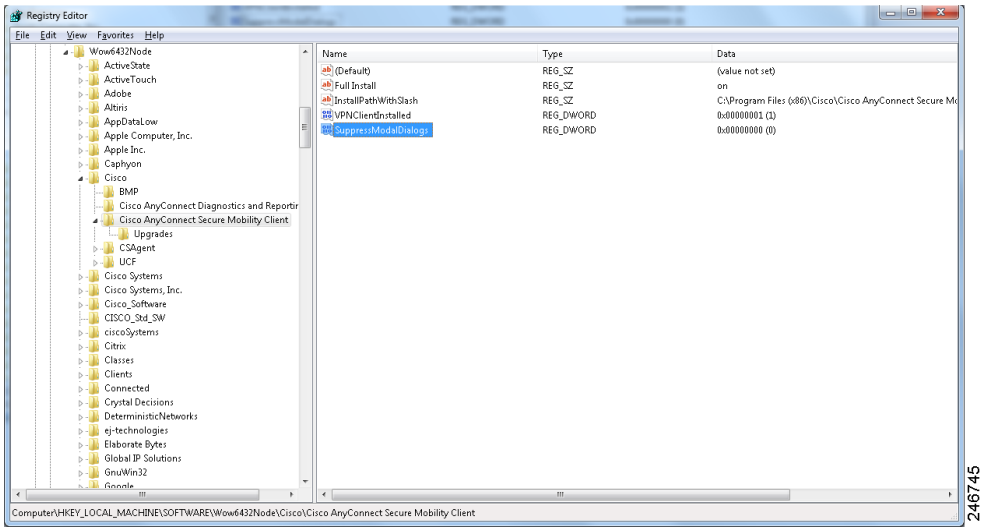
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\
  Cisco AnyConnect Secure Mobility Client

- 32-bit Windows:

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

Figure C-1 shows the registry value for 64-bit Windows:

Figure C-1 Registry Value to Suppress Windows Popup Message



Setting the Secure Connection (Lock) Icon

The Lock icon indicates a secure connection. Windows XP automatically hides this icon among those that have not been recently used. Users can prevent Windows XP from hiding this icon by following this procedure:

Step 1 Go to the taskbar where the tray icons are displayed and right click the left angle bracket (<).

Step 2 Select **Customize Notifications...**

Step 3 Select **Cisco Systems AnyConnect VPN Client** and set to **Always Show**.

AnyConnect Hides the Internet Explorer Connections Tab

Under certain conditions, AnyConnect hides the Connections tab located in Internet Explorer Tools, Internet Options. When exposed, this tab lets the user set proxy information. Hiding this tab prevents the user from intentionally or unintentionally circumventing the tunnel. The tab lockdown is reversed on disconnect, and it is superseded by any administrator-defined policies regarding that tab. The conditions under which this lockdown occurs are either of the following:

- The ASA configuration specifies Connections tab lockdown.
- The ASA configuration specifies a private-side proxy.
- A Windows group policy previously locked down the Connections tab (overriding the **no lockdown** ASA group policy setting).

Using a Windows Remote Desktop

Using one of these three methods, you can access a network computer remotely while the connection is being managed by the Network Access Manager on that network computer:

- Network Profiles with Machine-only Authentication
- Network Profiles with Machine and User Authentication
- Network Profiles with User-only Authentication

Network Profiles with Machine-only Authentication

To use this method, the Network Access Manager must be configured for machine authentication. Refer to “Defining the Networks Machine or User Authentication” on page 4-18 for the configuration details. When a user logs in remotely, the Network Access Manager remains authenticated with the machine’s credentials. No attempt is made to authenticate with the user’s credentials or to reauthenticate with the machine’s credentials.

Network Profiles with Machine and User Authentication

To use this method, the Network Access Manager must be configured for machine authentication plus user authentication. Refer to "Defining the Networks Machine or User Authentication" on page 4-18 for the configuration details. Without any users logged in, the Network Access Manager authenticates with the machine's credentials.

For Vista or Windows 7, when a user logs in, whether locally or remotely, the Network Access Manager authenticates only the first user session, ignoring subsequent logon sessions while the first session persists. When the first logon session ends, the Network Access Manager stops the user connection and reverts to a machine connection. The Network Access Manager tracks the first succeeding logon attempt after the original session ended as the user session, regardless of whether the secondary sessions were present when the first session ended. Because the Network Access Manager ignores subsequent logon sessions while the first session is operational, any secondary sessions created after the first session will momentarily lose their network connection when the original session is destroyed or when a subsequent logon attempt is made. If the first user is logged on locally, a remote desktop session will not result in the reauthentication of this user.

Note Only the first logon user session has access to the AnyConnect GUI.

For Windows XP, the number of user sessions are limited to 1, either local or remote; therefore, a new user logon always results in a previous user logoff. If the user is logged on locally, a remote desktop session with the same user will not result in the reauthentication of this user.

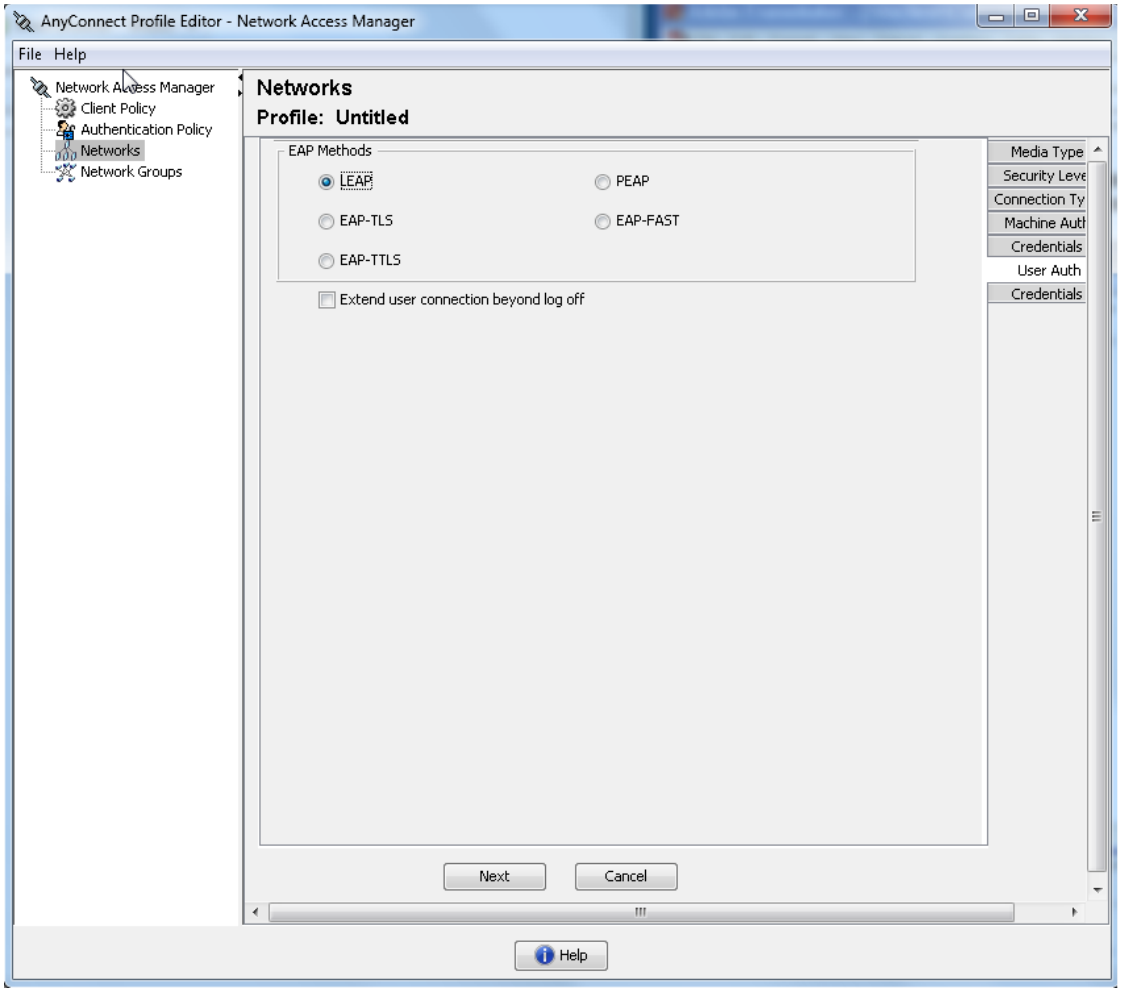
Note When using machine and user authentication, complications may occur. For example, depending on the configuration, the machine and the user profiles may assign the computer to different networks (usually VLANs, referred to here as *user VLAN* and *machine VLAN*). Therefore, if the network computer is connected as a machine on the machine VLAN (user logged off) and later it is accessed remotely, the computer connects as a user VLAN. For that reason, you may need to re-establish the remote desktop session with a different IP address on a different VLAN (the user VLAN).

Network Profiles with User-only Authentication

To use this method, the Network Access Manager must be configured for user-only authentication. Refer to "Defining the Networks Machine or User Authentication" on page 4-18 for the configuration details. Normally with this configuration and without any users logged in, the Network Access Manager cannot establish a network connection; therefore, a remote desktop connection is not possible. Now when users log on, they can establish a remote desktop connection. This remote session will not result in the re-authentication of the user.

The extendUserConnectionBeyondLogoff parameter (see Figure C-2) makes it possible to configure a user authentication so that it remains active (connected) even after the local user has logged off. Therefore, you do not need machine authentication solely to support remote desktop functionality.

Figure C-2 GUI Location of Extend User Connection Beyond Logoff Parameter



If a reauthentication that requires credentials occurs while the user is logged out and if the Network Access Manager no longer has access to the required credentials (such as a user certificate), the Network Access Manager cannot reauthenticate the connection. Consequently, the authentication attempt times out, and the authenticator eventually disconnects the client. When this occurs, the Network Access Manager re-evaluates the available connections and attempts to make a network connection from the available machine connections.

For Vista or Windows 7, when a user logs in, whether locally or remotely, the Network Access Manager authenticates only the first user session, ignoring subsequent logon sessions while the first session persists. When the first logon session ends, the Network Access Manager stops the user connection and reverts to a machine connection. The Network Access Manager tracks the first succeeding logon attempt after the original session ended as the user session, regardless of whether the secondary sessions were present when the first session ended. Because the Network Access Manager ignores subsequent logon sessions while the first session is operational, any secondary sessions created after the first session will momentarily lose their network connection when the original session is destroyed or when a subsequent logon attempt is made. If the first user is logged on locally, a remote desktop session will not result in the reauthentication of this user.

Note Only the first logon user session has access to the AnyConnect GUI.

For Windows XP, the number of user sessions are limited to 1, either local or remote; therefore, a new user logon always results in a previous user logoff. If the user is logged on locally, a remote desktop session with the same user will not result in the reauthentication of this user.

When using machine and user authentication, complications may occur. For example, depending on the configuration, the machine and the user profiles may put the computer on different networks (usually VLANs, referred to here as user VLAN and machine VLAN). Therefore, if the network computer is connected as a machine on the machine VLAN (user logged off) and later it is accessed remotely, the computer connects as a user VLAN. For that reason, you may need to re-establish the remote desktop session with a different IP address on a different VLAN (the user VLAN).

Credential Provider on Microsoft Vista and Win7

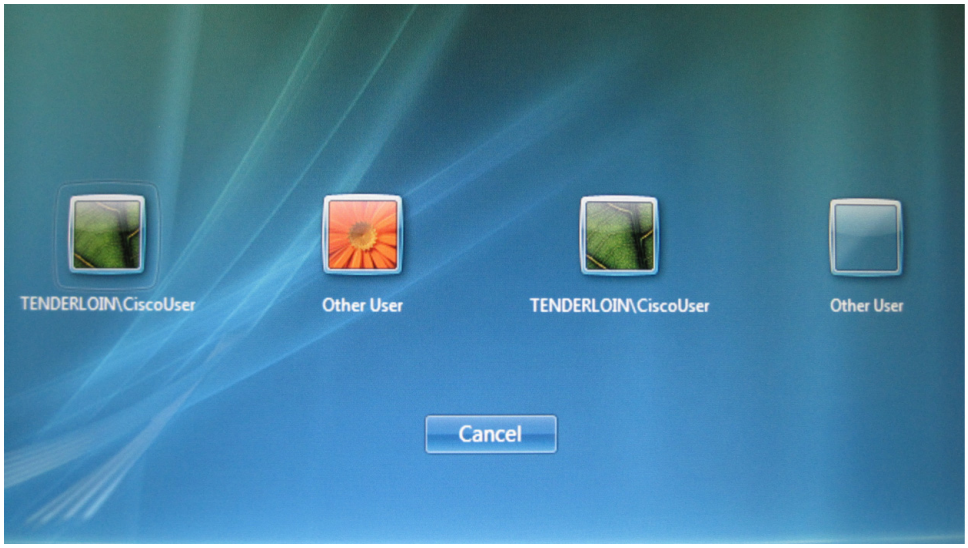
To provide single sign-on (SSO) user authentication using Windows logon credentials on Microsoft Vista and Windows 7, the Network Access Manager module implements a password (logon) credential provider. The credential provider (CP) captures the Windows credentials during the logon process and provides notifications when users log in or out of the system to allow the Network Access Manager service to switch between machine and user authentication.

For AnyConnect 3.0, the Network Access Manager CP is implemented as a wrapper around the Microsoft Password Credential Provider, which is filtered out by the Network Access Manager CP to prevent multiple sets of logon tiles from displaying. If this filtering is not done, a logon tile is displayed for each CP.

If a third-party CP is installed on a system, the Network Access Manager does not detect this, and the user may be presented with multiple sets of logon tiles. If users choose the third-party CP to log on, the Network Access Manager is unable to obtain the Windows credentials, thus preventing the single sign-on user authentication operation.

Figure C-3 shows the logon screen from a system with both the Network Access Manager CP and a third-party CP installed.

Figure C-3 AnyConnect Icon Without the Overlay



You have two options for this issue:

1. For the user to distinguish between tiles, the Network Access Manager CP provides the option to overlay the AnyConnect icon over the logon tile. A small AnyConnect icon is placed in the lower-right corner of the login tile bitmaps. Users can then see their login tile images and still be aware that AnyConnect is active. Without this Anyconnect icon, users cannot determine if login tiles are managed by AnyConnect or not.

   By default, the CP operates as described above. Users can change a value in the registry to disable it, and then the CP will not overlay the AnyConnect icon on login tiles. They would display exactly as they would if AnyConnect was not installed.

   To disable this option, the following registry value is used:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\
   {B12744B8-5BB7-463a-B85E-BB7627E73002}\OverlayIcon]
   ```

   OverLayIcon is a REG_DWORD where a value of 0 disables the overlay icon, and a value of 1 enables the overlay icon. This default value is 1 and is set by the AnyConnect installer. If a registry key is missing or incorrect, the CP assumes the value of 1.

   Sometimes Windows presents a tile labeled “other users” and in some cases, no picture appears in the associated tile. What appears inside the tile frame is whatever appears in the background of the window on which the tiles are placed; therefore, the tiles may appear empty or transparent. For technical reasons, the CP is unable to overlay an icon on an empty tile, so the CP must provide its own bitmap when this occurs.

   By default, the CP uses a stock image embedded in the CP executable file. Users may provide a picture to use in place of the stock empty tile by saving the picture in a .bmp file and adding a registry string value that provides the location of the file.

   To set the bitmap file location, the following registry value must be added:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\
   {B12744B8-5BB7-463a-B85E-BB7627E73002}\OverlayEmptyTile]
   ```

OverlayEmptyTile is a REG_SZ value that contains a full path to the bitmap file. Example: "C:\users\jsmith\Pictures\MyEmptyTile.bmp"

Note The file must be a Windows .bmp file.

If overlays are disabled (using the overlayicon registry setting), the OverlayEmptyTile option is ignored, and users cannot provide an empty tile bitmap if they disable the icon overlay. The OverlayEmptyTile value is not provided by the AnyConnect installer.

Figure C-4 shows the logon screen from a system with both the Network Access Manager CP and a third-party CP installed. In this example, the AnyConnect icon is displayed on the logon tile, indicating the Network Access Manager CP.

Figure C-4 Anyconnect Icon With Overlay

2. To prevent third-party credential provider's logon tiles from being displayed, the Network Access Manager CP can filter these tiles out.

   To set this option, you must add the following registry value:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticati
   on\Credential Providers\ {B12744B8-5BB7-463a-B85E-BB7627E73002}\Filters]
   ```

   Any credential provider that needs to be filtered out is added as a key with its specific GUID in the Filters key.

   Note The *Filters* value is not provided by the Anyconnect installer.

When GPO Configured for SSO

When GPO wired or wireless profiles are configured for SSO, winlogon short-circuits the Credential Provider querying process and directly loads the native L2NA credential provider in addition to the Network Access Manager CP. This presents the user with two sets of tiles. If GPO profiles are not configured for SSO, the logon process works as expected, the Microsoft CP is filtered out by the Network Access Manager CP, and the user is presented with a single set of tiles.

SmartCard CP

The Microsoft Smartcard Credential Provider is not wrapped by the Network Access Manager CP; therefore, prelogon smartcard based certificate authentication is not supported on post XP platforms for AnyConnect 3.0.

Network Access Manager CP Pre-logon Status Display

When the Connection Settings value *Before User Logon* is specified as part of the Client Policy, the Network Access Manager CP displays a status dialog box to inform the user of the connection status. This dialog box will be displayed after the user credentials are received by the CP and is displayed until the connection is successful, or until the value chosen by the *Time to Wait Before Allowing User to Logon* has expired. You can cancel this dialog box at any time.

Cipher Requirements Running Internet Explorer on Windows XP

With Windows XP, the Internet Explorer browser is not capable of using AES and requires either RC4 or 3DES. If remote users disable RC4 and 3DES in the SSL settings page, the AnyConnect connection fails. For a successful AnyConnect connection using Internet Explorer, remote users must not specify AES as the only cipher in the SSL settings for IE.