Configuring Network Access Manager

This chapter provides an overview of the Network Access Manager configuration and provides instructions for adding and configuring user policies and network profiles. This chapter contains these sections:

Introduction

The Network Access Manager is client software that provides a secure Layer 2 network in accordance with policies set forth by the enterprise network administrators. The Network Access Manager detects and selects the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks. The Network Access Manager manages user and device identity and the network access protocols required for secure access. It works intelligently to prevent end users from making connections that are in violation of administrator-defined policies.

The Network Access Manager component of the AnyConnect Secure Mobility Client supports these main features:

- Wired (IEEE 802.3), wireless (IEEE 802.11) and some Mobile Broadband (3G) network adapters on Windows 7. For the complete list of supported adapters, see *Release Notes for Cisco AnyConnect Secure Mobility Client, Release 3.1*.
- Pre-login authentication using Windows machine credentials
- Single sign-on user authentication using Windows logon credentials
- Simplified and easy-to-use IEEE 802.1X configuration
- IEEE MACsec wired encryption and enterprise policy control
- EAP methods:
  - EAP-FAST, PEAP, EAP-TTLS, EAP-TLS, and LEAP (EAP-MD5, EAP-GTC, and EAP-MSCHAPv2 for IEEE 802.3 wired only)
- Inner EAP methods:
  - PEAP—EAP-GTC, EAP-MSCHAPv2, and EAP-TLS

  - EAP-TTLS—EAP-MD5 and EAP-MSCHAPv2 and legacy methods (PAP, CHAP, MSCHAP, and MSCHAPv2)
  - EAP-FAST—GTC, EAP-MSCHAPv2, and EAP-TLS
- Encryption modes:
  - Static WEP (Open or Shared), dynamic WEP, TKIP, and AES
- Key establishment protocols:
  - WPA, WPA2/802.11i, and CCKM (selectively, depending on the IEEE 802.11 NIC card)

Note The only adapter supported for CCKM is the Cisco CB21AG on Windows XP

- Smartcard provided credentials. AnyConnect supports Smartcards in the following environments:
  - Microsoft CAPI 1.0 and CAPI 2.0 (CNG) on Windows XP, 7 & Vista
  - Windows logon does not support ECDSA certificates, therefore Network Access Manager's Single Sign-On (SSO) does not support ECDSA client certificates.

Note Network Access Manager is not supported on MAC or Linux.

Suite B and FIPS

The following features are FIPS-certified, and any exceptions are listed:

- ACS and ISE doesn't support SuiteB, but FreeRADIUS 2.x + OpenSSL 1.x does. Microsoft NPS 2008 supports Suite-B in part (the NPS's certificate still has to be RSA).
- 802.1X/EAP supports transitional Suite B profile only (as defined in RFC5430); there no support for TLS 1.2.
- MACsec is FIPS-compliant on Windows 7 only.
- Elliptic Curve Diffie-Hellman (ECDH) key exchange for Windows 7 and XP.
- ECDSA client certificates are supported on Windows 7 and Vista only.
- ECDSA CA certificates in OS store are supported on Windows 7 and Vista only
- ECDSA CA certificates in the network profile (PEM encoded) are supported on Windows XP/7/Vista
- Server's ECDSA certificate chain verification is supported on Windows XP/7/Vista

Single Sign On "Single User" Enforcement

Microsoft Windows XP, Windows-7 and Vista allow multiple users to be logged on concurrently, but AnyConnect Network Access Manager restricts network authentication to a single user. AnyConnect Network Access Manager can only be active for one user per desktop/server, regardless of how many users are logged on. Single User login Enforcement implies that only one user can be logged into the system at any one time and that Administrators can't force a logoff of the currently logged in user.

When the Network Access Manager client module is installed on Windows desktops the default behavior is to enforce single user logon. When installed on servers the default behavior is to relax the single user login enforcement. In either case a registry key can be modified or added to change the default behavior.

Single Sign-On Single user enforcement has the following features and restrictions:

- Windows administrators are restricted from forcing logoff of currently logged on users
- RDP to a connected workstation is supported for the same user
- To be considered the same user, credentials must be in the same format. For example, me/mydomain is not the same as me@mydomain.com.
- Smart card users must also have the same PIN to be considered the same user.

Configuring Single Sign-On Single User Enforcement

To change how a Window's workstation or server handles multiple users, change the value of EnforceSingleLogon in the registry. Network Access Manager does not add that key to Windows XP, but you can add it, if you wish to change Windows logon access.

On Windows 7, The registry key is **EnforceSingleLogon**, and is in the same registry location as the OverlayIcon key:

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

On Windows XP, The registry key is:

```
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\acnamsso
```

To configure single or multiple user logon, add a DWORD named EnforceSingleLogon, and give it a value of 1 or 0.

For both Windows 7 and XP:

- 1 restricts logon to a single user
- 0 allows multiple users logged on

The default configuration for workstations is 1; the default for servers is 0. If you are using single sign on for your workstation or server, you must set the value of EnforceSingleLogon to 1 for both the workstation and server.

Guidelines

Windows Network Status Task Tray Icon

Network Access Manager overrides Windows network management. After installing Network Access Manager, the Windows networking icon in the task bar may confuse users, because the user can no longer use the network status icon to connect to networks.

You can remove the Windows network icon from the task bar by setting 'Remove the networking icon' in a Windows group policy. This setting only affects the tray icon, the user can still create native wireless networks using the Control Panel.

Hidden Networks and Network Selection for Windows 7

Network Access Manager only tries to connect to the networks that are configured in the Network Access Manager's network scan list.

On Windows 7, Network Access Manager probes for hidden SSIDs. When the first hidden SSID is found, it stops looking. When multiple hidden networks are configured, Network Access Manager selects the SSID as follows:

- The first administrator-defined hidden corporate network.
- The administrator-defined hidden network.
- The first user-defined hidden network.

We recommend having only one hidden Corporate network at your site, since Network Access Manager can only probe one non-broadcasting SSID at a time.

Networks Defined by Windows

If the user defined networks in Windows before Network Access Manager was installed, then the Windows connection manager may occasionally try to make a connection to that network. This may cause a momentary loss of network connectivity and/or longer initial connection times.

- Turn off Connect Automatically when this network is in range for all Windows-defined networks.
- Delete all the Windows-defined networks.

System Requirements for the Network Access Manager

The Network Access Manager module requires the following:

- ASDM version 6.8

  Note The standalone Network Access Manager editor is a supported alternative for configuring a Network Access Manager profile. For security reasons, AnyConnect does not accept Network Access Manager profiles edited outside AnyConnect profile editors.

- The following operating systems support the Network Access Manager:
  - Windows 7 x86 (32-bit) and x64 (64-bit)
  - Windows Vista SP2 x86 (32-bit) and x64 (64-bit)
  - Windows XP x86 SP3 (32-bit)
  - Windows Server 2003 SP2 x86 (32-bit), IPv6 and Suite-B are not supported
  - Windows Server 2008 R2

Licensing and Upgrading Requirements

The AnyConnect Network Access Manager is licensed without charge for use with Cisco wireless access points, wireless LAN controllers, switches, and RADIUS servers. No AnyConnect Essentials or Premium license is required. A current SmartNet contract is required on the related Cisco equipment.

Deploying Network Access Manager

Network Access Manager is deployed as part of AnyConnect. For information about how to install AnyConnect, along with Network Access Manager and other modules, see "Deploying the AnyConnect Secure Mobility Client" section on page 2-1.

Creating a Network Access Manager Profile

Network Access Manager profiles are deployed on the endpoints as part of AnyConnnect, so that the Network Access Manager can enforce administratively defined end user requirements and authentication policies, and make the pre-configured network profiles available to end users.

Use the Network Access Manager profile editor to create and configure one or more Network Access Manager profiles. AnyConnect includes the profile editor as part of ASDM, and as a standalone Windows version. Refer to Chapter 2, "Deploying the AnyConnect Secure Mobility Client" for profile editor requirements and deployment instructions.

Note Until you upload a client image, you will not be able to create a client profile.

Adding a New Profile from ASDM

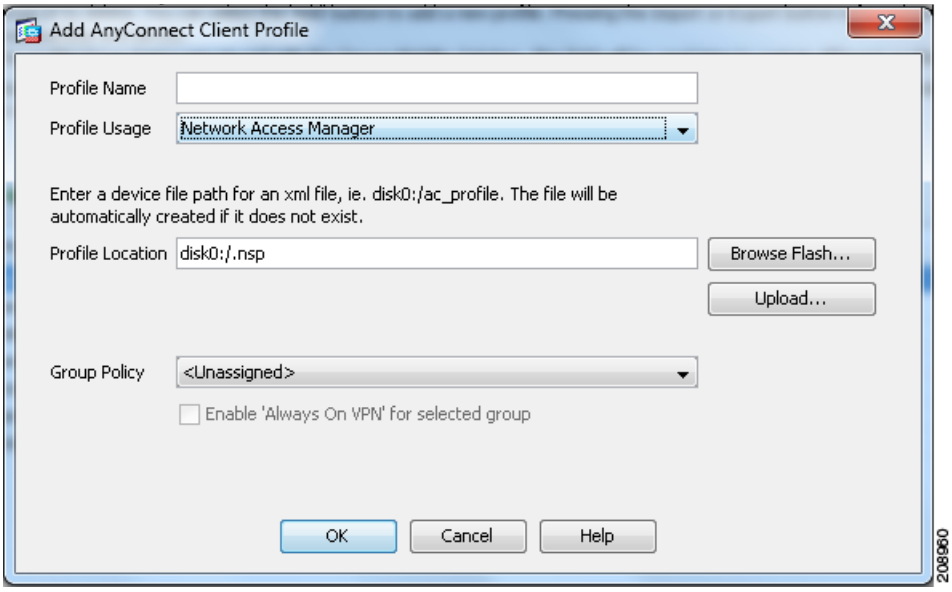
Follow these steps to add a new Network Access Manager client profile to the ASA from ASDM.

Step 1 Open ASDM and select Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.

Step 2 Click **Add**.

Step 3 The Add AnyConnect Client Profile window opens (see Figure 4-1).

Figure 4-1 Add AnyConnect Client Profile Window



Step 4 Enter a profile name.

Step 5 From the Profile Usage drop-down list, choose **Network Access Manager**.

Step 6 (Optional) In the Profile Location field, click **Browse Flash** and select a device file path for the XML file on the ASA.

Step 7 (Optional) If you created a Network Access Manager profile with the stand-alone editor, click **Upload** to use that profile definition.

Step 8 (Optional) Choose an AnyConnect group policy from the drop-down list.

Step 9 Click **OK**.

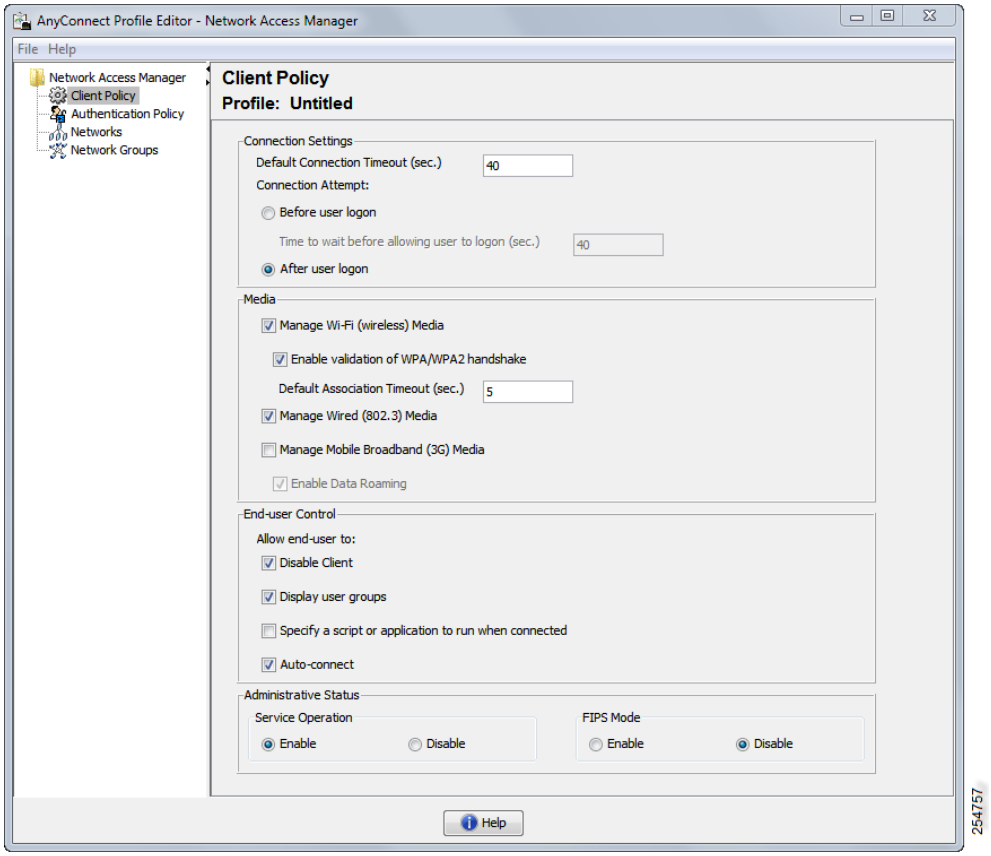
Configuring a Network Access Manager Profile

Network Access Manager profiles are configured in the Network Access Manager profile editor, which is available in the ASDM and also as a stand-alone Windows application.

Client Policy Window

The Client Policy window enables you to configure the client policy options (see Figure 4-2).

Figure 4-2 Client Policy Window



Four sections are included:

- Connection Settings—Allows you to define whether a network connection is attempted before or after the user logs on.
  - Default Connection Timeout—The number of seconds to use as the connection timeout for user-created networks. The default value is 40 seconds.
  - Before User Logon—Connect to the network before the user logs on. The user logon types that are supported include user account (Kerberos) authentication, loading of user GPOs, and GPO-based logon script execution.

    If you choose Before User Logon, you also get to set Time to Wait Before Allowing a User to Logon:

    Time to Wait Before Allowing User to Logon—Specifies the maximum (worst case) number of seconds to wait for the Network Access Manager to make a complete network connection. If a network connection cannot be established within this time, the Windows logon process continues with user log on. The default is 5 seconds.

Note If the Network Access Manager is configured to manage wireless connections, set *Time to wait before allowing user to logon* to 30 seconds or more because of the additional time it may take to establish a wireless connection. You must also account for the time required to obtain an IP address via DHCP. If two or more network profiles are configured, you may want to increase the value to cover two or more connection attempts.

  - After User Logon—Specifies that the Network Access Manager will attempt to establish a network connection after the user logs on to Windows.

- Media—Specifies which types of media are controlled by the Network Access Manager client.
  - Manage Wi-Fi (wireless) Media— Enables management of WiFi media and, optionally, validation of WPA/WPA2 handshake.

    The IEEE 802.11i Wireless Networking standard specifies that the supplicant, in this case the Network Access Manager, must validate that the access point's RSN IE (Robust Secure Network Information Exchange) that was sent in the IEEE 801.X protocol packet's EAPOL Key data during key derivation matches the access point's RSN IE found in the beacon/probe response frame. If you enable the validation of WPA/WPA2 handshake, you must specify the default association timeout. If you uncheck the enable validation of WPA/WPA2 handshake setting, this validation step is skipped.

    Note Some adapters do not consistently provide the access point's RSN IE, so the authentication attempt fails, and the client will not connect.

  - Manage Wired (IEEE 802.3) Media—Enables management of wired connections.
  - Manage Mobile Broadband (3G) Media - Enables management of Windows 7 Mobile Broadband Adapters, and whether to allow data roaming. This feature is in a beta release state.

    Note Cisco TAC does not provide support for beta releases.

- End-user Control—Allows you to configure the following control for users:
  - Disable Client—Allows users to disable and enable the Network Access Manager's management of wired and wireless media using the AnyConnect UI.
  - Display User Groups—Makes user-created groups (created from CSSC 5.x) visible and capable of a connection, even though they do not correspond to administrator-defined groups.
  - Specify a Script or Application To Run When Connected—Allows users to specify a script or application to run when the network connects.

Note The scripting settings are specific to one user-configured network and allow the user to specify a local file (.exe,.bat, or .cmd) to run when that network gets to a connected state. To avoid conflicts, the scripting feature only permits users to configure a script or application for user-defined networks and not for administrator-defined networks. The feature does not allow users to alter administrator networks regarding the running of scripts; therefore, the interface for administrator networks is not available to the user. Also, if you do not allow users to configure a running script, the feature is not seen in the Network Access Manager GUI.

  - Auto-connect—If selected, the Network Access Manager automatically connects to a network without a user needing to choose it. The default is automatic connection.

- Administrative Status
  - Service Operation—If you disable the service, clients who use this profile will not be able to connect to establish layer 2 connections.
  - FIPS Mode— Federal Information Processing Standard (FIPS 140-2 Level 1) is a U.S. government standard that specifies security requirements for cryptography modules. If you enable FIPS mode, the Network Access Manager performs cryptographic operations in a way that meets the government requirements. Refer to Chapter 9, "NGE, FIPS and Additional Security" for additional information.

    FIPS is supported by Network Access Manager for MACsec or Wifi, depending on the type of software and hardware, as show in the following table:

Table 4-1 FIPS support by Network Access Manager

Media/Operating System	Windows XP/2003	Windows 7/Vista
Wired with MACsec	Not FIPS compliant	FIPS compliant when an Intel HW MACsec capable NIC, or when any non-hardware MACsec is used
WiFi	FIPS compliant when a 3eti driver is installed	Not FIPS compliant

Authentication Policy Window

The Authentication Policy window allows you to create association and authentication network filters, which apply to all network connections. If you do not check any of the association or authentication modes, the user cannot connect to an authenticating wi-fi network. If you choose a subset of the modes, the user can connect to networks for those types only. Select each desired association or authentication mode, or choose Select All.

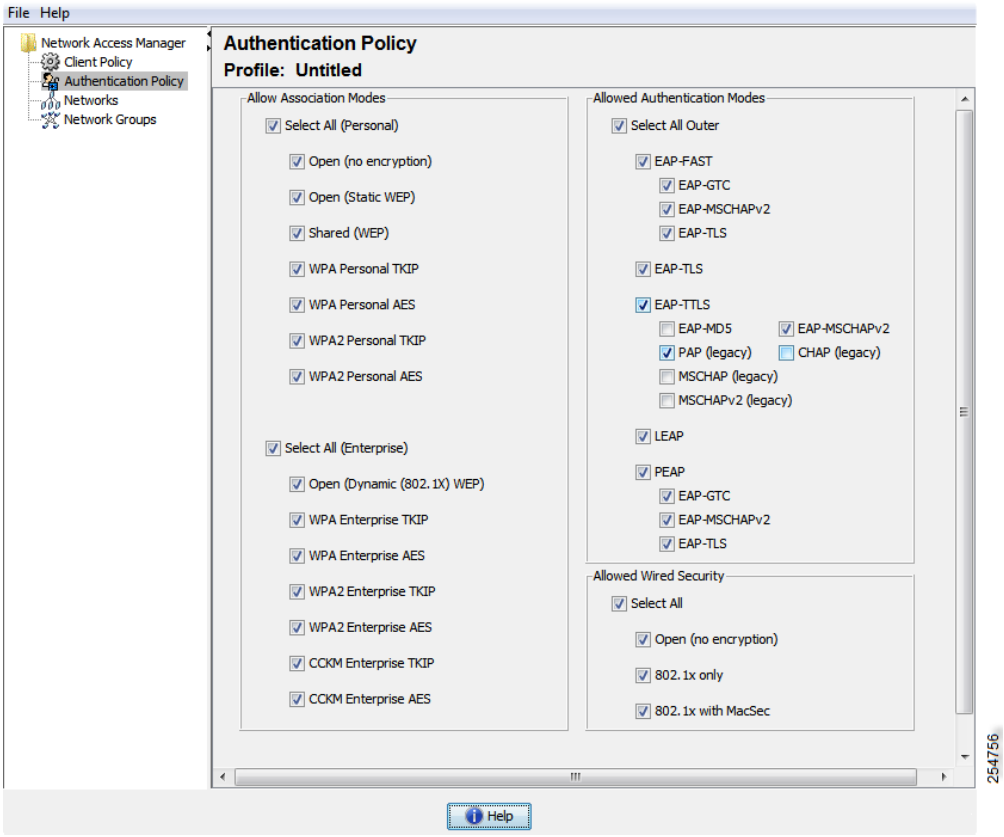
Note that the inner methods can also be restricted to only specific authentication protocols. The inner methods are shown indented under the outer methods (tunneling) in the Allowed Authentication Modes pane.

The mechanism for choosing the authentication protocol is integrated with the current client authentication database. A secure wireless LAN deployment does not require the creation of a new authentication system for users.

The EAP methods available for inner tunneling are based on the inner method credential type and the outer tunneling method. In the following list, each outer tunnel method lists the types of inner methods that are supported for each credential type.

- PEAP
  - Password credentials: EAP-MSCHAPv2 or EAP-GTC
  - Token credentials: EAP-GTC
  - Certificate credentials: EAP-TLS
- EAP-FAST
  - Password credentials: EAP-MSCHAPv2 or EAP-GTC
  - Token credentials: EAP-GTC
  - Certificate credentials: EAP-TLS
- EAP-TTLS
  - Password credentials: EAP-MSCHAPv2, EAP-MD5, PAP (L), CHAP (L), MSCHAP (L), MSCHAP-v2 (Legacy)
  - Token credentials: PAP (Legacy). The default token option that NAM supports is PAP, since challenge/response methods are not well suited for token-based authentication.
  - Certificate credentials: N/A

Figure 4-3 Authentication Policy Window



Networks Window

The Networks window allows you to configure pre-defined networks for your enterprise user. You can either configure networks that are available to all groups, or create groups with specific networks. The Networks window runs a wizard that sometimes adds panes to the existing window, and you advance to more configuration options by clicking **Next**.

A group, fundamentally, is a collection of configured connections (networks). Every configured connection must belong to a group or a member of all groups.

Note For backward compatibility, the administrator-created networks deployed with the Cisco Secure Services Client are treated as hidden networks, which do not broadcast SSIDs. However, user networks are treated as networks which broadcast their SSIDs.

Only administrators can create a new group. If no groups are defined in the configuration, the profile editor creates an auto-generated group. The auto-generated group contains networks that are not assigned to any administrator-defined group. The client attempts to make a network connection using the connections defined in the active group. Depending on the setting of the *Create networks* option in the Network Groups window, end users can add user networks to the active group or delete user networks from the active group.

Networks that are defined are available to all groups at the top of the list. Because you control what networks are in the global Networks, you can specify the enterprise networks that an end user can connect to, even in the presence of user-defined networks. An end user cannot modify or remove administrator-configured networks.

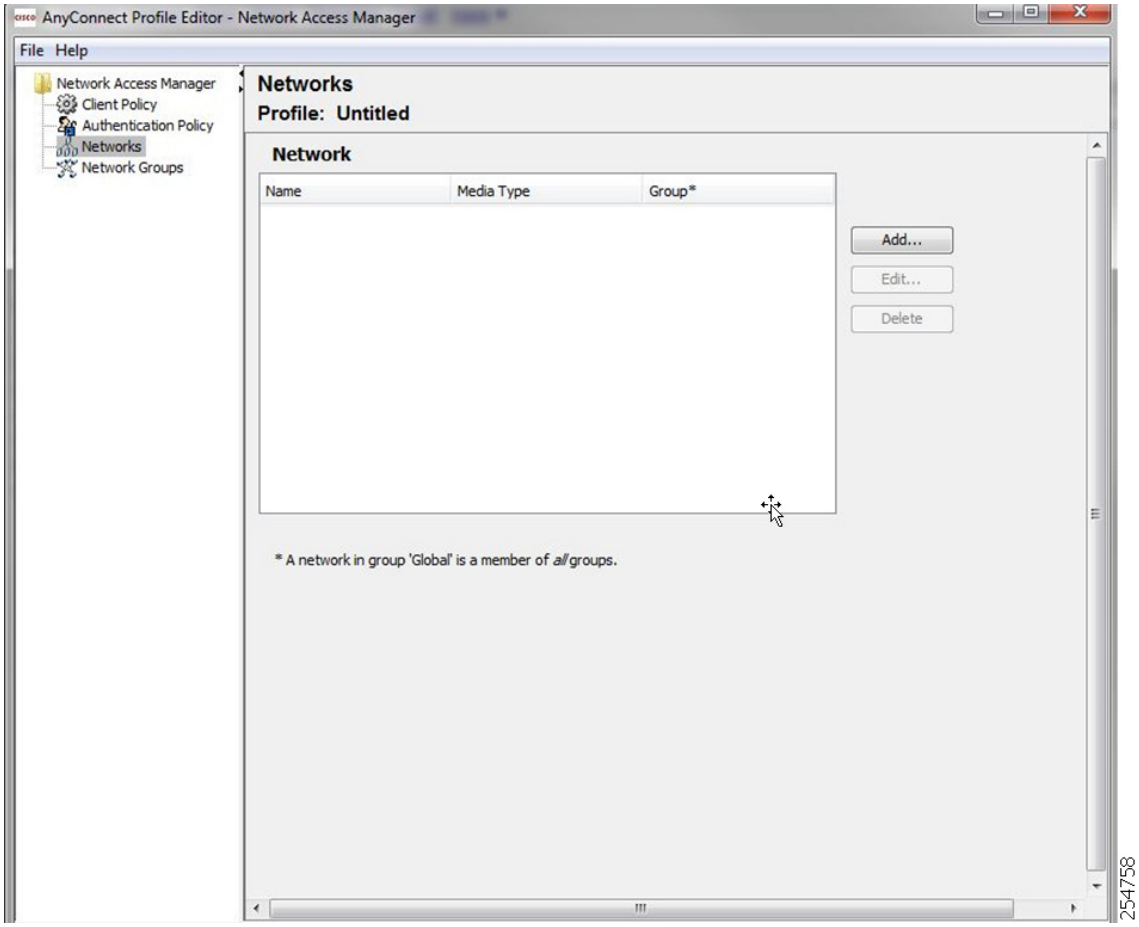
Note End users may add networks to groups, except for networks in the globalNetworks section, because these networks exist in all groups, and you can only create them using the profile editor.

It is important to note that a typical end user of an enterprise network does not need knowledge of groups in order to use this client. The active group is the first group in the configuration, but if only one is available, the client is unaware and does not display the active group. However, if more than one group exists, the UI displays a combo box indicating that the active group is selected. Users can then choose from the active group, and the setting persists across reboots. Depending on the setting of the *Create networks* option in the Network Groups window, end users can add or delete their own networks without using groups.

Note A group selection is maintained across reboots and network repairs (done while right clicking on the tray icon and choosing **Network Repair**). When the Network Access Manager is repaired or restarted, the Network Access Manager starts using the previously active group.

When you choose **Networks** from the Network Access Manager menu, the window shown in Figure 4-4 appears.

Figure 4-4 Networks Window



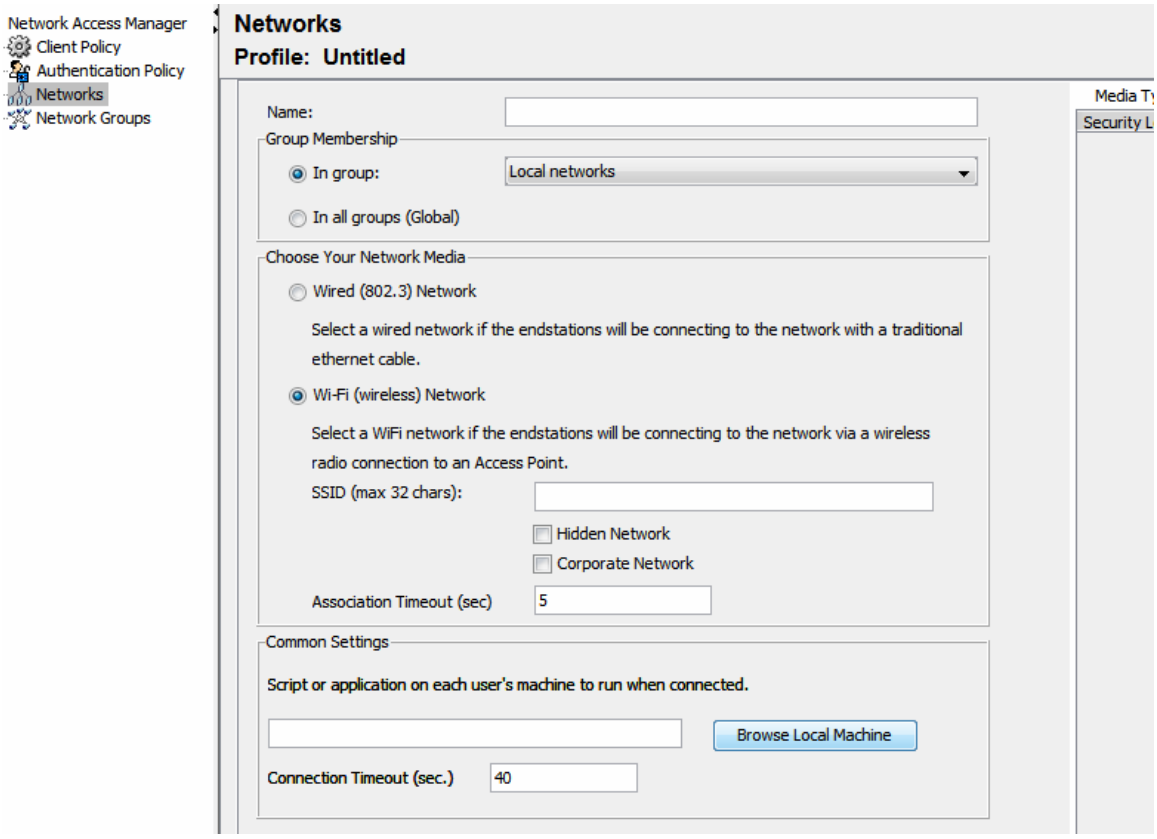
Choose from one of the following actions:

- Click **Add** to create a new network. If you choose to create a new network, use the information in the following sections to configure the client profile, starting with the Networks - Media Type Page section below.
- Choose a network you want to change and click **Edit**.
- Choose a network you want to remove and click **Delete**.

Networks - Media Type Page

The Networks window Media Type page enables you to create or edit a wired or a wireless network. The settings vary depending on whether you choose wired or wireless. Figure 4-5 shows the window that appears if you choose a Wi-Fi network, but this section covers both wired and Wi-Fi options.

Figure 4-5 Media Type Page



Four sections are included in the first dialog:

- Group Membership—Select which network group or groups this profile should be available to.
- Name - Enter the name that is displayed for this network.
- Network Media—Select Wired or Wi-Fi (wireless). If you choose Wi-Fi, you can also configure the following parameters:
  - At the SSID parameter, enter the SSID (Service Set Identifier) of your wireless network.
  - Choose **Hidden Network** to allow a connection to a network even if it is not broadcasting its SSID.
  - Choose **Corporate Network** to force a connection to a network configured as Corporate first, if a corporate network is in proximity. When Corporate network uses a non-broadcasting (hidden) SSID, and is configured as hidden, NAM will actively probe for hidden SSIDs, and establish the connection when a corporate SSID is in range.
  - Association Timeout—Enter the length of time that Network Access Manager waits for association with a particular wireless network before it re-evaluates the available networks. The default association timeout is 5 seconds.
- Common Settings—
  - Script or application—Enter the path and filename of the file that you want to run on the local system, or browse to a folder and select one. The following rules apply to scripts and applications:

Files with .exe, .bat, or .cmd extensions are accepted.

Users may not alter the script or application defined in an administrator-created network.

You may only specify the path and script or application filename using the profile editor. If the script or application does not exist on a user's machine, an error message appears. The user is informed that the script or application does not exist on their machine and that they need to contact their system administrator.

You must specify the full path of the application that you want to run, unless the application exists in the user's path. If the application exists in the user's path, you can specify only the application or script name.

– Connection Timeout—Enter the number of seconds that the Network Access Manager waits for a network connection to be established before it tries to connect to another network (when the connection mode is automatic) or uses another adapter.

Note Some smartcard authentication systems require almost 60 seconds to complete an authentication. When using a smartcard, you may need to increase the Connection Timeout value, especially if the smartcard may have to try several networks before making a successful connection.

When you have completed configuring networks, click **Next** to display the Security Level pane of the Networks wizard.

Networks - Security Level Page

In the Security Level page of the Networks wizard, choose Open Network, Authentication Network, or (displayed for Wireless Network Media only) Shared Key Network. The configuration flow for each of those network types is different, and are described in the following sections.

- Configuring Authenticating Network—Recommended for a **secure enterprises**.
- Configuring Open Network—Not recommended, but can be used to provide guest access through captive portal environment.
- Configuring Shared Key Network—Recommended for wireless networks such as **small offices** or home offices.

Configuring Authenticating Network

If you chose Authenticating Network in the Security Level section, additional panes appear, which are described below. When you are done configuring settings on this pane, click the **Next** button or select the Connection Type tab to open the Network Connection Type dialog.

802.1X Settings Pane

Adjust the IEEE 802.1X settings according to your network configuration:

- authPeriod(sec.)—When authentication begins, this time determines how long the supplicant waits in between authentication messages before it times out and requires the authenticator to initiate authentication again.
- heldPeriod(sec)—When authentication fails, this time defines how long the supplicant waits before another authentication attempt can be made.

- startPeriod(sec)—The interval, in seconds, between the retransmission of EAPOL-Start messages if no response to any EAPOL-Start messages is received from the authenticator.
- maxStart—The number of times the supplicant will initiate authentication with the authenticator by sending an IEEE 801.X protocol packet, EAPOL Key data, EAPoL-Start before the supplicant assumes there is no authenticator present. When this happens, the supplicant allows data traffic.

Tip You can configure a single authenticating wired connection to work with both open and authenticating networks by carefully setting the startPeriod and maxStart such that the total time spent trying to initiate authentication is less than the network connection timer (startPeriod x maxStart < Network Connection Timer).

Note: In this scenario, you should increase the network connection timer by (startPeriod x maxStart) seconds to give the client enough time to acquire a DHCP address and finish the network connection.

Conversely, administrators who want to allow data traffic if and only after authentication succeeds should make sure that the startPeriod and maxStart is such that the total time spent trying to initiate authentication is greater than the network connection timer (start Period x maxStart > Network Connection Timer).

Security Pane

Only appears for wired networks.

In the Security pane, select values for the following parameters:

- Key Management—Use the drop-down list to determine which Key Management Protocol you want to use with your MACsec-enabled wired network.
  - None—No key management protocols are used, and no wired encryption is performed.
  - MKA—The supplicant attempts to negotiate a MACsec key agreement protocol policies and encryption keys. MACsec is MAC Layer Security, which provides MAC layer encryption over wired networks. The MACsec protocol represents a means to secure MAC level frames with encryption and relies on the MACsec Key Agreement (MKA) Entity to negotiate and distribute the encryption keys.

    Note Refer to IEEE-802.1X-Rev for a detailed definition of MACsec Key Agreement and IEEE 802.1AE-2006 for a detailed definition of the MACsec encryption protocol. Additionally, refer to http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/deploy_guide_c17-663760.html for further information about MACsec, including benefits and limitations, functional overview, design considerations, deployment, and troubleshooting.

- Encryption
  - None—Data traffic is integrity checked but not encrypted.
  - MACsec: AES-GCM-128—This option is only available if you chose MKA for Key Management. It causes data traffic to be encrypted using AES-GCM-128.

Port Authentication Exception Policy Pane

Only appears for wired networks.

The Port Authentication Exception Policy allows you to tailor the IEEE 802.1X supplicant's behavior during the authentication process. If port exceptions are not enabled, the supplicant continues its existing behavior and only opens the port upon successfully completing the full configuration (or as described earlier in this section, after the maxStarts number of authentications are initiated without a response from the authenticator). Choose from one of the following options:

- Allow data traffic before authentication—This option allows data traffic prior to an authentication attempt.
- Allow data traffic after authentication even if:
  - EAP Fails—When selected, the supplicant attempts authentication. But if authentication fails, the supplicant allows data traffic despite authentication failure.
  - EAP succeeds but key management fails—When selected, the supplicant attempts to negotiate keys with the key server but allows data traffic if the key negotiation fails for any reason. This setting is only valid when key management is configured. If key management is set to none, the check box is grayed out.

Note MACsec requires ACS version 5.1 or later and a MACsec capable switch. Refer to the *Catalyst 3750-X and 3560-X Switch Software Configuration Guide* for ACS or switch configuration.

Association Mode

Only appears for wireless networks.

Choose the association mode, options are :

- WEP
- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA 2 Enterprise (TKIP)
- WPA 2 Enterprise (AES)
- CCKM (TKIP) - (requires Cisco CB21AG Wireless NIC)
- CCKM (AES) - (requires Cisco CB21AG Wireless NIC)

Configuring Open Network

An open network uses no authentication or encryption. Follow these steps if you want to create an open (non-secure) network.

Step 1 Choose **Open Network** from the Security Level page. This choice provides the least secure network and is recommended for guest access wireless networks.

Step 2 Click **Next**.

Step 3 Determine a connection type. Refer to the Networks - Network Connection Type Pane.

Clicking **Next** or selecting the Connection Type tab opens the Network Connection Type dialog.

Configuring Shared Key Network

Wi-Fi networks may use a shared key to derive an encryption key for use when encrypting data between end points and network access points. Using a shared key with WPA or WPA2 Personal provides a medium level security class that is suitable for small or home offices.

Note Shared key security is not recommended for enterprise wireless networks.

Follow these steps if you want Shared Key Network as your security level.

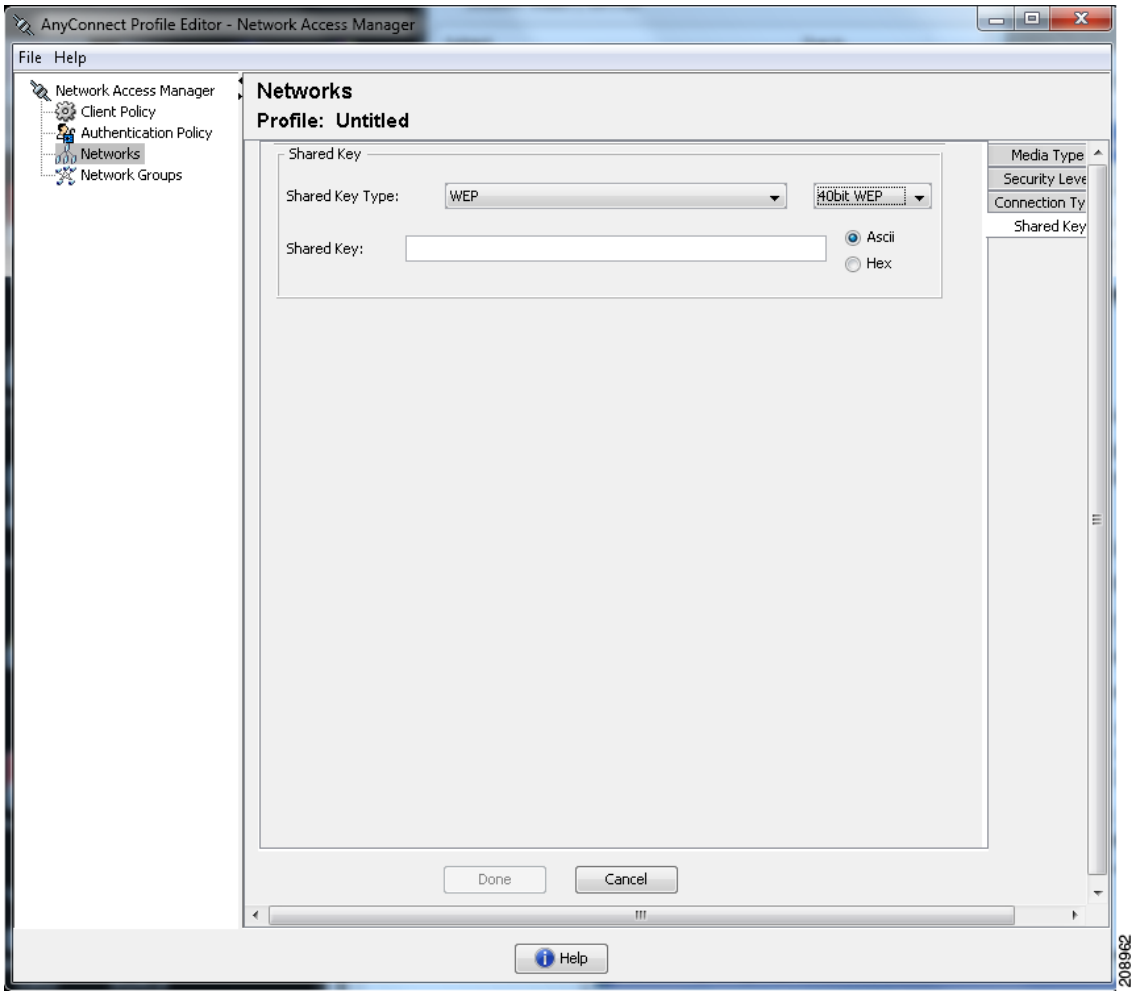
Step 1 Choose **Shared Key Network**.

Step 2 Click **Next** on the Security Level window.

Step 3 Specify **User Connection** or **Machine Connection**. Refer to the "Networks - Network Connection Type Pane" section on page 4-18 for more information.

Step 4 Click **Next**. The Shared Key pane appears (see Figure 4-6).

Figure 4-6 Shared Key Pane



Step 5 Shared Key Type—Specify the shared key association mode which determines the shared key type. The choices are as follows:

- WEP—Legacy IEEE 802.11 open-system association with static WEP encryption.
- Shared—Legacy IEEE 802.11 shared-key association with static WEP encryption.
- WPA/WPA2-Personal—A Wi-Fi security protocol that derives encryption keys from a passphrase pre-shared key (PSK).

Step 6 If you chose Legacy IEEE 802.11 WEP or Shared Key, choose 40 bit, 64 bit, 104 bit, or 128 bit. A 40- or 64-bit WEP key must be 5 ASCII characters or 10 hex digits. A 104- or 128-bit WEP key must be 13 ASCII characters or 26 hex digits.

Step 7 If you chose WPA or WPA2 Personal, choose the type of encryption to use (TKIP/AES) and then enter a shared key. The key must be entered as 8 to 63 ASCII characters or exactly 64 hexadecimal digits. Choose **ASCII** if your shared key consists of ASCII characters. Choose **Hexadecimal** if your shared key includes 64 hexadecimal digits.

Step 8 Click **Done**. Click **OK**.

Networks - Network Connection Type Pane

This section describes the Network Connection Type pane of the Networks window, which follows Security Level in the Network Access Manager profile editor. The pane for an Open Network is shown in Figure 4-7.Choose one of the following connection types:

- Machine Connection—The machine's Windows Active Directory ID is used for authorization. Machine connection is typically used when user credentials are not required for a connection. Choose this option if the end station should log onto the network even when a user is logged off and user credentials are unavailable. This option is typically used for connecting to domains and to get GPOs and other updates from the network before the user has access.

  Note VPN start before login (SBL) will fail if no known network is available. But if you configure Network Access Manager for *Before user logon*, and machine connection authorization, the Network Access Manager will ask the user for network information, and the VPN SBL will succeed.

- User Connection—User credentials are used for authorization.

  If *Before user logon* was selected in the Client Policy pane, Network Access Manager gathers the user's credentials after the user enters their logon credentials on the Windows start screen. Network Access Manager establishes the network connection while Windows is starting the user's windows session.

  If *After user logon* was selected in the Client Policy pane, Network Access Manager starts the connection after the user logs on to Windows.

  When the user logs off, the current user network connection is terminated. If there are machine network profiles are available, NAM will reconnect to a machine network.

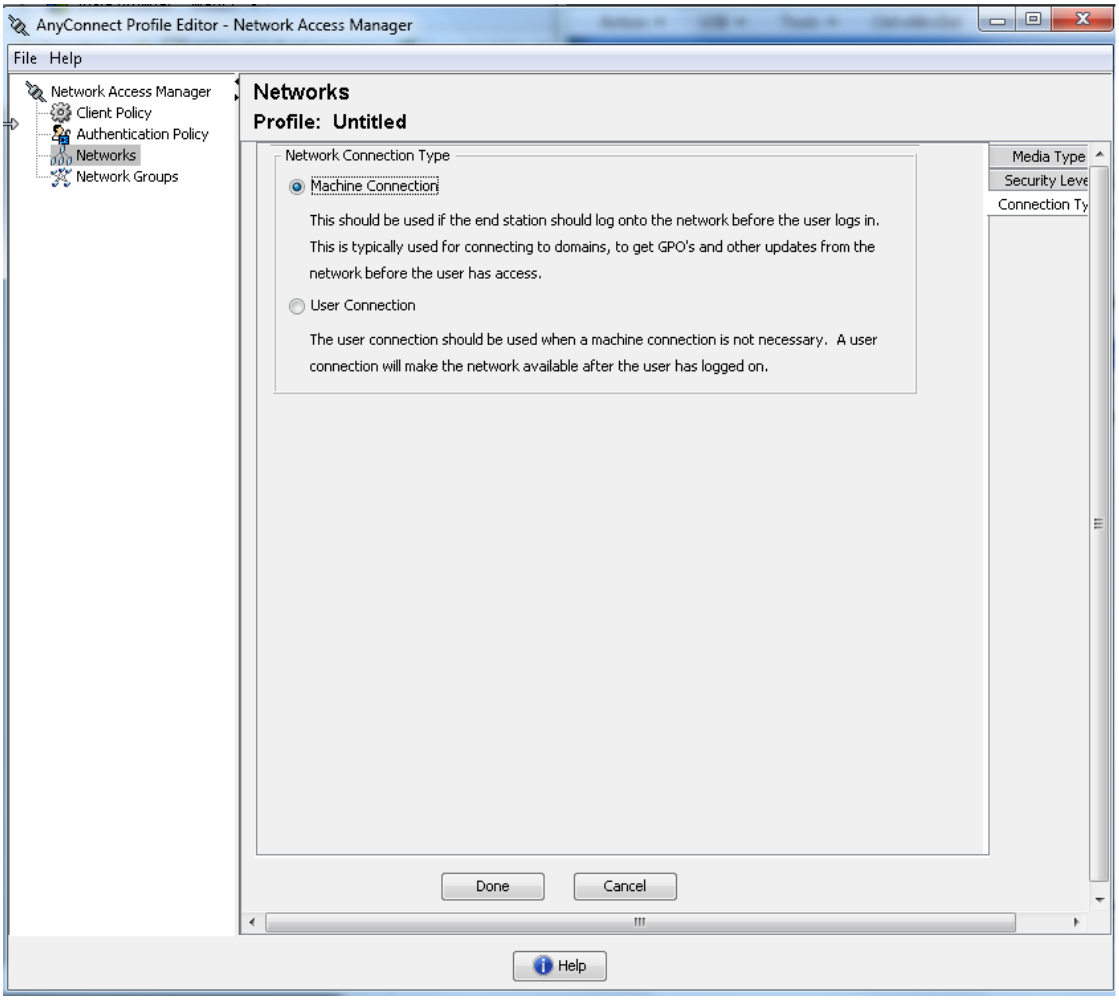
- Machine and User Connection—Only available when configuring an *Authenticating Network*, as selected in the Security Level pane. Machine ID and user credentials are both used, however, the machine part is only valid when a user is not logged onto the PC. The configuration is the same for the two parts, but the authentication type and credentials for machine connection can be different from the authentication type and credentials for the user connection.

  Choose this option to keep the PC connected to the network at all times using the Machine Connection when a user is not logged in and using the User Connection when a user has logged in.

  When EAP-FAST is configured as the EAP method (in the next pane), EAP chaining is supported. That means that Network Access Manager will verify that the machine and the user are known entities, and managed by the corporation, which is useful for Bring Your Own Device (BYOD).

  When you choose the Network Connection Type, additional tabs are displayed in the Networks dialog, which allow you to set EAP methods and credentials for the chosen Network Connection Type.

Figure 4-7 Network Connection Type Pane for Open Networks



Networks - User or Machine Authentication Page

After choosing the Network Connection Type, you chose the authentication method(s) for those connection types. After you select an authentication method, the center of the window adapts to the method you chose, and you are required to provide additional information.

Note If you have enabled MACsec, ensure that you select an EAP method that supports MSK key derivation, such as PEAP, EAP-TLS, or EAP-FAST.

You may have additional configuration in this pane, depending on which EAP Method you chose.

- EAP-GTC—See Configuring EAP-GTC, page 4-21
- EAP-TLS—See Configuring EAP-TLS, page 4-22.
- EAP-TTLS—See Configuring EAP-TTLS, page 4-22.
- PEAP—See Configuring PEAP Options, page 4-24.
- EAP-FAST—See Configuring EAP-FAST Settings, page 4-25.
- LEAP—See Configuring LEAP Settings, page 4-27

EAP Overview

EAP is an IETF RFC that addresses the requirements for an authentication protocol to be decoupled from the transport protocol carrying it. This decoupling allows the transport protocols (such as IEEE 802.1X, UDP, or RADIUS) to carry the EAP protocol without changes to the authentication protocol.

The basic EAP protocol is relatively simple and made up of four packet types:

- EAP request—The authenticator sends the request packet to the supplicant. Each request has a type field that indicates what is being requested, such as the supplicant identity and EAP type to use. A sequence number allows the authenticator and the peer to match an EAP response to each EAP request.
- EAP response—The supplicant sends the response packet to the authenticator and uses a sequence number to match the initiating EAP-request. The type of the EAP response generally matches the EAP request, unless the response is a negative (NAK).
- EAP success—The authenticator sends a success packet upon successful authentication to the supplicant.
- EAP failure—The authenticator sends a failure packet to the supplicant if authentication failed.

When EAP is in use in an IEEE 802.11X system, the access point operates in an EAP pass-through mode. In this mode, the access point checks the code, identifier, and length fields and then forwards the EAP packets received from the supplicant to the AAA server. Packets received from the AAA server at the authenticator are forwarded to the supplicant.

Configuring EAP-GTC

EAP-GTC is an EAP authentication method based on simple username and password authentication. Without using the challenge-response method, both username and password are passed in clear text. This method is recommended for either inside a tunneling EAP method (see tunneling EAP methods below) or with a OTP (token).

EAP-GTC does not provide mutual authentication. It only authenticates clients, so a rogue server may potentially obtain users' credentials. If mutual authentication is required, EAP-GTC is used inside tunneling EAP methods, which provide server authentication.

No keying material is provided by EAP-GTC; therefore, you cannot use this method for MACsec. If keying material for further traffic encryption is required, EAP-GTC is used inside tunneling EAP methods, which provides the keying material (and inner and outer EAP methods crytobinding, if necessary).

You have two password source options:

- Authenticate using a Password—Suitable only for well protected wired environments
- Authenticate using a Token—More secure because of the short lifetime (usually about 10 seconds) of a token code or it is a OTP

Note Neither the Network Access Manager, the authenticator, nor the EAP-GTC protocol can distinguish between password and token code. These options only impact the credential's lifetime within the Network Access Manager. While a password can be remembered until logout or longer, the token code cannot (because the user is prompted for token code with every authentication).

If a password is used for authentication, you can use this protocol for authentication against the database with hashed (or irreversibly encrypted) passwords since it is passed to the authenticator in clear text. We recommend this method if a possibility of a database leak exists.

Configuring EAP-TLS

EAP-Transport Layer Security (EAP-TLS) is an IEEE 802.1X EAP authentication algorithm based on the TLS protocol (RFC 2246). TLS uses mutual authentication based on X.509 digital certificates. The EAP-TLS message exchange provides mutual authentication, cipher suite negotiation, key exchange, verification between the client and the authenticating server, and keying material that can be used for traffic encryption.

The list below provides the main reasons why EAP-TLS client certificates can provide strong authentication for wired and wireless connections:

- Authentication occurs automatically, usually with no intervention by the user.
- No dependency on a user password.
- Digital certificates provide strong authentication protection.
- Message exchange is protected with public key encryption.
- Not susceptible to dictionary attacks.
- The authentication process results in a mutually determined key for data encryption and signing.

EAP-TLS contains two options:

- Validate Server Certificate—Enables server certificate validation.
- Enable Fast Reconnect—Enables TLS session resumption which allows for much faster reauthentication by using abbreviated TLS handshake as long as TLS session data is preserved on both the client and the server.

Note The *Disable when using a Smart Card* option is not available for machine connection authentication.

Configuring EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) is a two-phase protocol that expands the EAP-TLS functionality. Phase 1 conducts a complete TLS session and derives the session keys used in Phase 2 to securely tunnel attributes between the server and the client. You can use the attributes tunneled during Phase 2 to perform additional authentications using a number of different mechanisms.

The Network Access Manager does not support the cryptobinding of the inner and outer methods used during EAP-TTLS authentication. If cryptobinding is required, you must use EAP-FAST. Cryptobinding provides protection from a special class of man-in-the-middle attacks where an attacker hijacks the user's connection without knowing the credentials.

The authentication mechanisms that can be used during Phase 2 include these protocols:

- PAP (Password Authentication protocol)—Uses a two-way handshake to provide a simple method for the peer to prove its identity. An ID/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or failed. If mutual authentication is required, then you must configure EAP-TTLS to validate the server's certificate at Phase 1.

  Because a password is passed to the authenticator, you can use this protocol for authentication against a database with hashed (or irreversibly encrypted) passwords. We recommend this method when a possibility of a database leak exists.

  Note You can use EAP-TTLS PAP for token and OTP-based authentications.

- CHAP (Challenge Handshake Authentication Protocol)—Uses a three-way handshake to verify the identity of the peer. If mutual authentication is required, you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method, you are required to store clear text passwords in the authenticator's database.
- MS-CHAP (Microsoft CHAP)—Uses a three-way handshake to verify the identity of the peer. If mutual authentication is required, you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least NT-hash of the password in the authenticator's database.
- MS-CHAPv2—Provides mutual authentication between peers by including a peer challenge in the response packet and an authenticator response in the success packet. The client is authenticated before the server. If the server needs to be authenticated before the client (to prevent dictionary attacks), you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least NT-hash of the password in the authenticator's database.

EAP-TTLS Configuration

- EAP—Allows use of these EAP methods:
  - EAP-MD5 (EAP-Message Digest 5)—Uses a three-way handshake to verify the peer's identity (similar to CHAP). Using this challenge-response method, you are required to store the clear text password in the authenticator's database.
  - EAP-MSCHAPv2—Uses a three-way handshake to verify the identity of the peer. The client is authenticated before the server. If the server needs to be authenticated before the client (such as for the prevention of a dictionary attack), you should configure EAP-TTLS to validate the server's certificate at Phase 1. Using this challenge-response method on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.
- EAP-TTLS Settings
  - Validate Server Identity—Enables server certificate validation.
  - Enable Fast Reconnect—Enables outer TLS session resumption only, regardless of whether the inner authentication is skipped or is controlled by the authenticator.

Note *Disable when using a Smart Card* is not available on machine connection authentication.

- Inner Methods—Specifies the inner methods used after the TLS tunnel is created. Only available for Wi-Fi Media Type.

Configuring PEAP Options

Protected EAP (PEAP) is a tunneling TLS-based EAP method. It uses TLS for server authentication before the client authentication for the encrypting of inner authentication methods. The inner authentication occurs inside a trusted cryptographically protected tunnel and supports a variety of different inner authentication methods, including certificates, tokens, and passwords. The Network Access Manager does not support the cryptobinding of the inner and outer methods used during PEAP authentication. If cryptobinding is required, you must use EAP-FAST. Cryptobinding provides protection from a special class of man-in-the-middle attacks where an attacker hijacks the user's connection without knowing the credentials.

PEAP protects the EAP methods by providing these services:

- TLS tunnel creation for the EAP packets
- Message authentication
- Message encryption
- Authentication of server to client

You can use these authentication methods:

- Authenticate using a Password
  - EAP-MSCHAPv2—Uses a three-way handshake to verify the identity of the peer. The client is authenticated before the server. If the server needs to be authenticated before the client (such as for the prevention of a dictionary attack), you must configure PEAP to validate the server's certificate. Using the challenge-response method based on the NT-hash of the password, you are required to store either the clear text password or at least the NT-hash of the password in the authenticator's database.
  - EAP-GTC (EAP Generic Token Card)—Defines an EAP envelope to carry the username and password. If mutual authentication is required, you must configure PEAP to validate the server's certificate. Because the password is passed to the authenticator in clear text, you can use this protocol for authentication against the database with hashed (or irreversibly encrypted) passwords. We recommend this method if a possibility of a database leak exists.
- EAP-TLS, using a Certificate
  - EAP-TLS—Defines an EAP envelope to carry the user certificate. In order to avoid a man-in-the-middle attack (the hijacking of a valid user's connection), we recommend that you do not mix PEAP [EAP-TLS] and EAP-TLS profiles meant for authentication against the same authenticator. You should configure the authenticator accordingly (not enabling both plain and tunneled EAP-TLS).

PEAP Configuration

- PEAP-EAP settings
  - Validate Server Identity—Enables server certificate validation.

  - Enable Fast Reconnect—Enables outer TLS session resumption only. The authenticator controls whether or not the inner authentication is skipped.
  - Disable when using a Smart Card—Don't use Fast Reconnect when using a smart card for authentication. Smart cards only apply to user connections.
  - Authenticate using a Token and EAP GTC—Not available for machine authentication.
- Inner methods based on Credentials Source
  - Authenticate using a password for EAP-MSCHAPv2 and/or EAP-GTC
  - EAP-TLS, authenticate using a Certificate
  - Authenticate using a Token and EAP-GTC—Not available for machine authentication.

Note Before user log on, smart card support is not available on Windows Vista and Windows 7.

Configuring EAP-FAST Settings

EAP-FAST is an IEEE 802.1X authentication type that offers flexible, easy deployment and management. It supports a variety of user and password database types, server-initiated password expiration and change, and a digital certificate (optional).

EAP-FAST was developed for customers who want to deploy an IEEE 802.1X EAP type that does not use certificates and provides protection from dictionary attacks.

As of AnyConnect 3.1, EAP chaining is supported when both machine and user connections are configured. That means that Network Access Manager will verify that the machine and the user are known entities, and managed by the corporation, which is useful for Bring Your Own Device (BYOD). For more information about EAP chaining, see RFC 3748.

EAP-FAST encapsulates TLS messages within EAP and consists of three protocol phases:

1. A provisioning phase that uses Authenticated Diffie-Hellman Protocol (ADHP) to provision the client with a shared secret credential called a Protected Access Credential (PAC).
2. A tunnel establishment phase in which the PAC is used to establish the tunnel.
3. An authentication phase in which the authentication server authenticates the user's credentials (token, username/password, or digital certificate).

Unlike the other two tunneling EAP methods, EAP-FAST provides cryptobinding between inner and outer methods, preventing the special class of the man-in-the-middle attacks where an attacker hijacks a valid user's connection.

EAP-FAST Configuration

- EAP-FAST Settings
  - Validate Server Identity—Enables server certificate validation. Enabling this introduces two extra dialogs in the management utility and adds additional Certificate panes into the Network Access Manager Profile Editor task list.
  - Enable Fast Reconnect—Enables session resumption. The two mechanisms to resume the authentication sessions in EAP-FAST include user authorization PAC, which substitutes the inner authentication, or TLS session resumption, which allows for abbreviated outer TLS handshake. This Enable Fast Reconnect parameter enables or disables both mechanisms. The authenticator decides which one to use.

Note The machine PAC provides abbreviated TLS handshake and eliminates inner authentication. This control is handled by the enable/disable PAC parameter.

Note The *Disable when using a Smart Card* option is only available for user connection authorization.

- Inner methods based on Credentials Source—Enables you to authenticate using a password or certificate.
  - Authenticate using a password for EAP-MSCHAPv2 or EAP-GTC. EAP-MSCHAPv2 provides mutual authentication, but it authenticates the client before authenticating the server. If you want mutual authentication with the server being authenticated first, configure EAP-FAST for authenticated provisioning only, and verify the server's certificate. Using the challenge-response method based on the NT-hash of the password, EAP-MSCHAPv2 requires you to store either the clear text password, or at least the NT-hash of the password, in the authenticator's database. Since the password is passed to the authenticator in clear text within EAP-GTC, you can use this protocol for authentication against the database with hashed (or irreversibly encrypt) exists.

    If you are using password-based inner methods, an additional option is available to allow unauthenticated PAC provisioning.
  - Authenticate using a certificate—Decide the following criteria for authenticating using a certificate: when requested, send the client certificate in the clear, only send client certificates inside the tunnel, or send client certificate using EAP-TLS in the tunnel.
  - Authenticate Using a Token and EAP-GTC
- Use PACs—You can specify the use of PAC for EAP-FAST authentication. PACs are credentials that are distributed to clients for optimized network authentication.

  Note Typically, you use the PAC option because most authentication servers use PACs for EAP-FAST. Before removing this option, verify that your authentication server does not use PACs for EAP-FAST; otherwise, the client's authentication attempts will be unsuccessful. If your authentication server supports authenticated PAC provisioning, we recommend that you disable unauthenticated provisioning. Unauthenticated provisioning does not validate server's certificates, thus allowing rogue authenticators to mount a dictionary attack.

  You can manually provide one or more specific PAC files for distribution and authentication by selecting the PAC Files pane and clicking **Add**. You can also highlight a PAC file and click **Remove** to remove a PAC file from the list.

  Password protected—If the PAC was exported as password protected, check the **Password Protected** check box and provide the password that matches the one with which PAC is encrypted.

Configuring LEAP Settings

LEAP (Lightweight EAP) supports wireless networks. It is based on the Extensible Authentication Protocol (EAP) framework, and was developed by Cisco to create a protocol that was more secure than WEP.

Note LEAP is subject to dictionary attacks unless you enforce strong passwords and periodically expiring passwords. Cisco recommends that you use EAP-FAST, PEAP or EAP-TLS, whose authentication methods are not susceptible to dictionary attacks. For more information about LEAP security issues, see http://www.cisco.com/en/US/tech/tk722/tk809/technologies_security_notice09186a00801aa80f.html.

LEAP Settings, which are only available for User Authentication:

- Extend user connection beyond log off—For User authentication only, keeps the connection open when the user logs off. If the same user logs back on the network connection will still be active.

Defining Networks Credentials

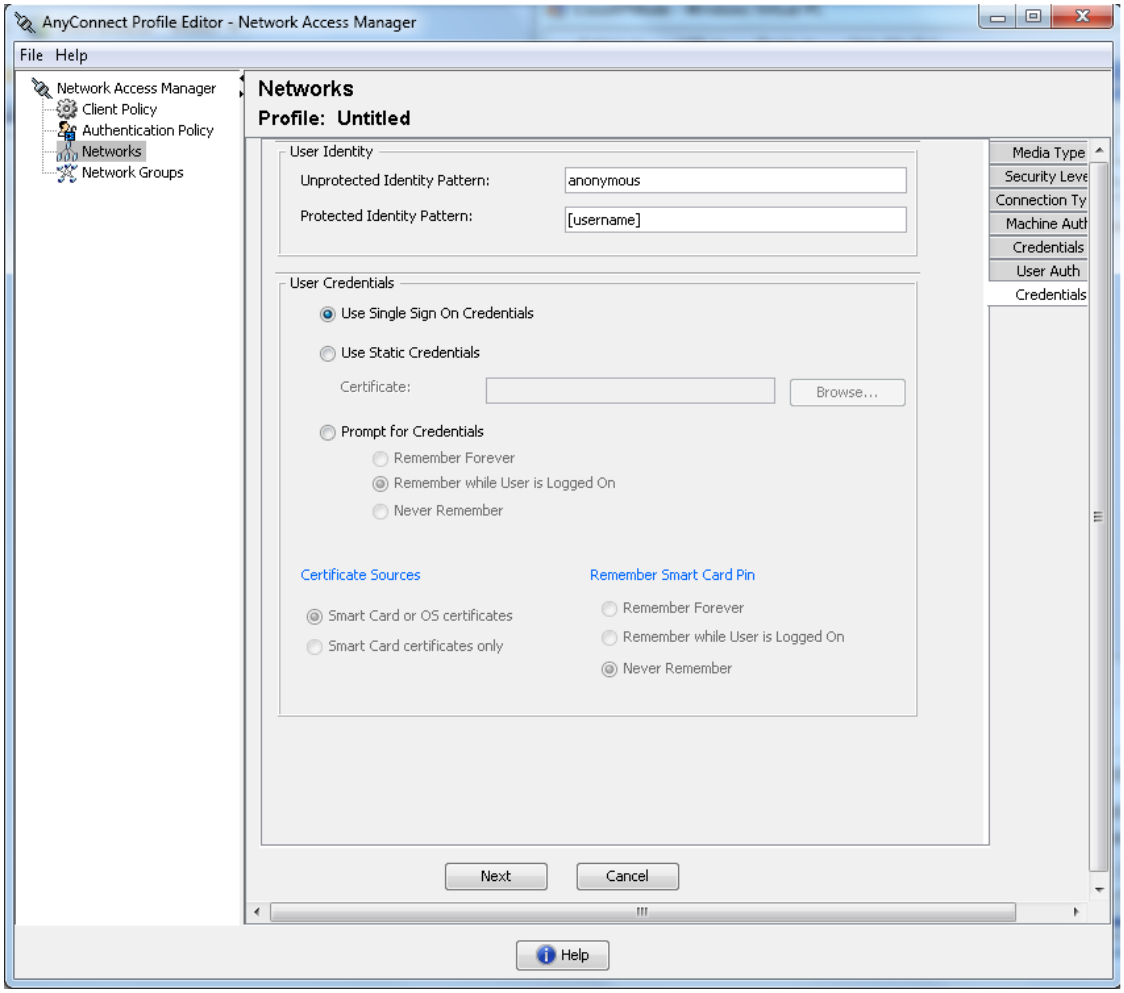
On the Networks > Credentials pane, you specify whether to use user and/or machine credentials, and configure trusted server validation rules.

- Configuring User Credentials
- Configuring Machine Credentials
- Configuring Trusted Server Validation Rules

Configuring User Credentials

On the Credentials pane, you can specify the desired credentials to use for authenticating the associated network (see Figure 4-8).

Figure 4-8 User Credentials Pane for EAP-TLS



Step 1 You must identify a user identity for the Protected Identity Pattern. The Network Access Manager supports the following identity placeholder patterns:

- [username]—Specifies the username. If a user enters username@domain or domain\username, the domain portion is stripped off.
- [raw]—Specifies the username, exactly as entered by the user.
- [domain]—Specifies the domain of the user's PC.

For user connections, when the [username] and [domain] placeholder patterns are used, the following conditions apply:

- If a client certificate is used for authentication, the placeholder values for [username] and [password] are obtained from various X509 certificate properties. The properties are analyzed in the order described below, according to the first match. For example, if the identity is userA@cisco.com (where username=userA and domain=cisco.com) for user authentication and hostA.cisco.com (where username=hostA and domain=cisco.com) for machine authentication, the following properties are analyzed:

  User certificate based authentication:

- SubjectAlternativeName: UPN = userA@cisco.com
- Subject = .../CN=userA@cisco.com/...
- Subject = userA@cisco.com
- Subject = .../CN=userA/DC=cisco/DC=com/...
- Subject = userA (no domain)

Machine certificate based authentication:

- SubjectAlternativeName: DNS = hostA.cisco.com
- Subject = .../DC=hostA.cisco.com/...
- Subject = .../CN=hostA.cisco.com/...
- Subject = hostA.cisco.com

- If the credential source is the end user, the placeholder's value is obtained from the information the user enters.
- If the credentials are obtained from the operating system, the placeholder's value is obtained from the logon information.
- If the credentials are static, no placeholders should be used.

Sessions that have yet to be negotiated experience identity request and response in the clear without integrity protection or authentication. These sessions are subject to snooping and packet modification. Typical unprotected identity patterns are as follows:

- anonymous@[domain]—Often used in tunneled methods to hide the user identity when the value is sent in clear text. The real user identity is provided in the inner method as the protected identity.
- [username]@[domain]—For non-tunneled methods

Note Unprotected identity is sent in clear text. If the initial clear text identity request or response is tampered with, the server may discover that it cannot verify the identity once the TLS session is established. For example, the user ID may be invalid or not within the realm handled by the EAP server.

The protected identities present clear text identity in a different way. To protect the userID from snooping, the clear text identity may only provide enough information to enable routing of the authentication request to the correct realm. Typical protected identity patterns are as follows:

- [username]@[domain]
- the actual string to use as the user's identity (no placeholders)

An EAP conversation may involve more than one EAP authentication method, and the identities claimed for each of these authentications may be different (such as machine authentication followed by user authentication). For example, a peer may initially claim the identity of nouser@cisco.com to route the authentication request to the cisco.com EAP server. However, once the TLS session has been negotiated, the peer may claim the identity of johndoe@cisco.com. Thus, even if protection is provided by the user's identity, the destination realm may not necessarily match, unless the conversation terminates at the local authentication server.

Step 2 Provide further user credential information:

- Use Single Sign On Credentials—Obtains the credentials from the operating system's logon information. If logon credentials fail, the Network Access Manager temporarily (until next logon) switches and prompts the user for credentials with the GUI.

- Use Static Credentials—Obtains the user credentials from the network profiles that this profile editor provides. If static credentials fail, the Network Access Manager will not use the credentials again until a new configuration is loaded.
- Prompt for Credentials—Obtains the credentials from the end user with the AnyConnect GUI as specified here:
  - Remember Forever—The credentials are remembered forever. If remembered credentials fail, the user is prompted for the credentials again. Credentials are preserved in the file and encrypted using a local machine password.
  - Remember while User is Logged On—The credentials are remembered until the user logs off. If remembered credentials fail, the user is prompted for credentials again.
  - Never Remember—The credentials are never remembered. The Network Access Manager prompts the user each time it needs credential information for authentication.

Step 3 Determines which certificate source to use for authentication when certificates are required:

- Smart Card or OS certificates—The Network Access Manager uses certificates found in the OS Certificate Stores or on a Smart Card.
- Smart Card certificates only— The Network Access Manager only uses certificates found on a Smart Card.

Step 4 At the Remember Smart Card Pin parameter, determine how long the Network Access Manager remembers the PIN used to retrieve the certificate off a smart card. Refer to Step 2 for the available options.

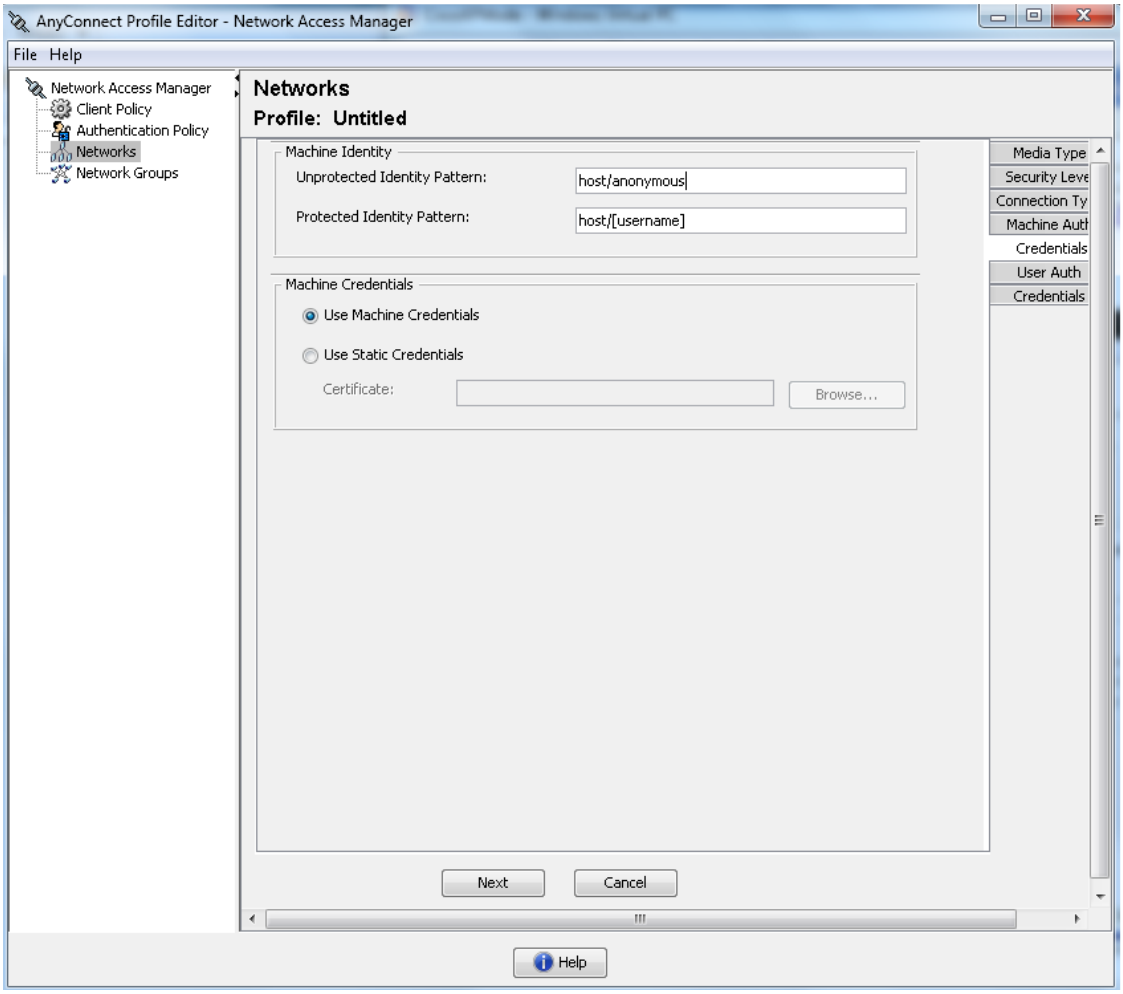
Note The PIN is never preserved longer than a certificate itself.

Some smart cards may take longer than others to connect, depending on the smart card chip and the driver, aka the Cryptographic service provider (CSP) and the Key storage provider (KSP). You may need to increase the connection timeout to give the network enough time to perform the smart card-based authentication.

Configuring Machine Credentials

With the Credentials panel you can specify the desired machine credentials (see Figure 4-9).

Figure 4-9 Machine Credentials



Step 1 You must a machine identity for the Protected Identity Pattern. The Network Access Manager supports the following identity placeholder patterns:

- [username]—Specifies the username. If a user enters username@domain or domain\username, the domain portion is stripped off.
- [raw]—Specifies the username, exactly as entered by the user.
- [domain]—Specifies the domain of the user's PC.

For machine connections, whenever the [username] and [domain] placeholders are used, these conditions apply:

- If a client certificate is used for authentication, the placeholder values for [username] and [password] are obtained from various X509 certificate properties. The properties are analyzed in the order described below, according to the first match. For example, if the identity is userA@cisco.com (where username=userA and domain=cisco.com) for user authentication and hostA.cisco.com (where username=hostA and domain=cisco.com) for machine authentication, the following properties are analyzed:

  User certificate based authentication:

- SubjectAlternativeName: UPN = userA@cisco.com
- Subject = .../CN=userA@cisco.com/...
- Subject = userA@cisco.com
- Subject = .../CN=userA/DC=cisco.com/...
- Subject = userA (no domain)

Machine certificate based authentication:

- SubjectAlternativeName: DNS = hostA.cisco.com
- Subject = .../DC=hostA.cisco.com/...
- Subject = .../CN=hostA.cisco.com/...
- Subject = hostA.cisco.com

- If a client certificate is not used for authentication, the credentials are obtained from the operating system, and the [username] placeholder represents the assigned machine name.

Sessions that have yet to be negotiated experience identity request and response in the clear without integrity protection or authentication. These sessions are subject to snooping and packet modification. Typical unprotected machine identity patterns are as follows:

- host/anonymous@[domain]
- the actual string to send as the machine's identity (no placeholders)

The protected identities present clear text identity in a different way. To protect the userID from snooping, the clear text identity may only provide enough information to enable routing of the authentication request to the correct realm. Typical protected machine identity patterns are as follows:

- host/[username]@[domain]
- the actual string to use as the machine's identity (no placeholders)

An EAP conversation may involve more than one EAP authentication method, and the identities claimed for each of these authentications may be different (such as machine authentication followed by user authentication). For example, a peer may initially claim the identity of nouser@cisco.com to route the authentication request to the cisco.com EAP server. However, once the TLS session has been negotiated, the peer may claim the identity of johndoe@cisco.com. Thus, even if protection is provided by the user's identity, the destination realm may not necessarily match, unless the conversation terminates at the local authentication server.

Step 2 Provide further Machine Credential information:

- Use Machine Credentials—Obtains the credentials from the operating system.
- Use Static Credentials—If you choose to use static credentials, you can specify an actual static password to send in the deployment file. Static credentials do not apply for certificate-based authentication.

Configuring Trusted Server Validation Rules

When the Validate Server Identity option is configured for the EAP method, the Certificate panel is enabled to allow you to configure validation rules for Certificate Server or Authority. The outcome of the validation determines whether the certificate server or the authority are trusted.

To define certificate server validation rules, follow these steps:

Step 1 When the optional settings appear for the **Certificate Field** and the **Match** columns, click the drop-down arrows and highlight the desired settings.

Step 2 Enter a value in the Value field.

Step 3 Under Rule, click **Add**.

Step 4 In the Certificate Trusted Authority portion, choose one of the following options:

- Trust any Root Certificate Authority (CA) Installed on the OS—If chosen, only the local machine or certificate stores are considered for the server's certificate chain validation.
- Include Root Certificate Authority (CA) Certificates

Note If you choose Include Root Certificate Authority (CA) Certificates, you must click on **Add** to import the CA certificate into the configuration.

Network Groups Window

On the Network Groups window, you assign network connections to particular groups (see Figure 4-10). Classifying connections into groups provides multiple benefits:

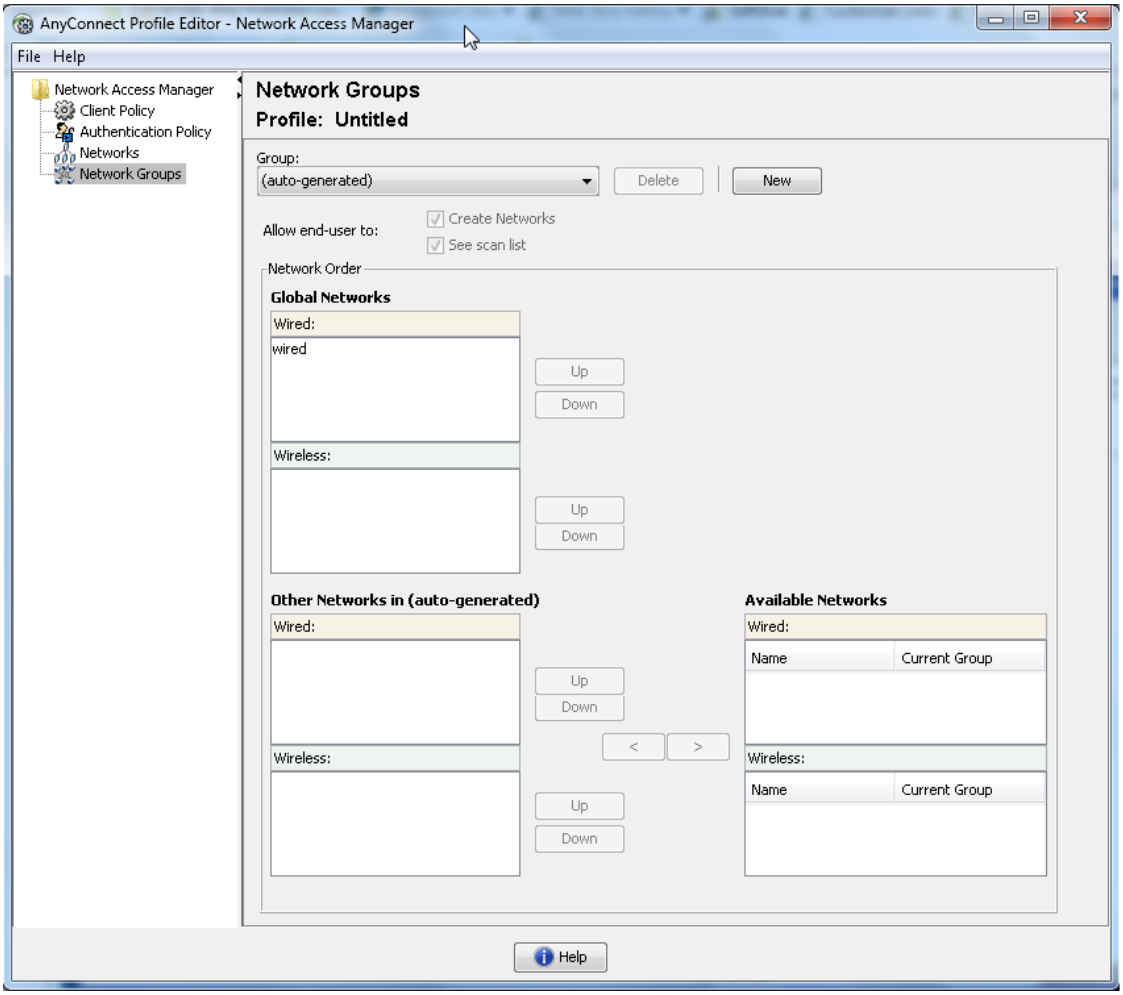
- Improved user experience when attempting to make a connection. When multiple hidden networks are configured, the client walks through the list of hidden networks in the order that they are defined until a successful connection is made. In such instances, groups are used to greatly reduce the amount of time needed to make a connection.
- Easier management of configured connections. This benefit allows you to separate administrator networks from user networks if you want and allows users who have multiple roles in a company (or who often visit the same area) to tailor the networks in a group to make the list of selectable networks more manageable.

Networks defined as part of the distribution package are locked, preventing the user from editing the configuration settings or removing the network profiles.

You can define a network as global. When doing so, it appears in the Global Networks section. This section is split between the wired and wireless network types. You can only perform sort order edits on this type of network.

All non-global networks must exist in a group. There is one group created by default, and the user can delete that group if all networks are global.

Figure 4-10 Network Groups Window



Step 1 Choose a Group by selecting it in the drop-down list.

Step 2 Choose **Create networks** to allow the end user to create networks in this group. When deployed, if you uncheck this, the Network Access Manager deletes any user-created networks from this group, which may force the user to re-enter network configuration in another group.

Step 3 Choose **See scan list** to allow end users to view the scanlist when the group is selected as the active group using the AnyConnect GUI. Alternatively, clear the check box to restrict users from viewing the scan list. For instance, if you want to prevent users from accidentally connecting to nearby devices, you should restrict scan list access.

Note These settings are applied on a per group basis.

Step 4 Use the **Right** and **Left arrows** to insert and remove a network from the group selected in the Group drop-down list. If a network is moved out of the current group, it is placed into the default group. When the default group is being edited, you cannot move a network from it (using the > button).

Note Within a given network, the display name of each network must be unique; therefore, any one group cannot contain two or more networks with the same display name.

Step 5 Use the **Up and Down arrows** to change the priority order of the networks within a group.