CHAPTER 4

# 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) and wireless (IEEE 802.11) network adapters
- 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 on Windows XP, 7 & Vista
  - Keychain via Tokend on Mac OS X, 10.4 and higher

**Note** AnyConnect does not support Smart cards on Linux or PKCS #11 devices.

# System Requirements for the Network Access Manager

The Network Access Manager module requires the following:

- ASDM version 6.4(0)104 or later.

**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 with a standard editor.

- 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)

## 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.

# Pre-deploying Network Access Manager

When you pre-deploy the Network Access Manager, you install it on the endpoint before the AnyConnect client makes its initial connection to the ASA. You need to install the AnyConnect Secure Mobility Client on the endpoint before you install the Network Access Manager modules. See the "Deploying the AnyConnect Secure Mobility Client" section on page 2-1for instructions on installing the AnyConnect Secure Mobility Client.

# Stopping and Starting the Network Access Manager

Users with local administrator privileges can start and stop the Network Access Manager. Users without local administrator privileges cannot start and stop the Network Access Manager without using the service password defined in the Authentication panel of the profile editor.

# Profile Editor

The Network Access Manager profile editor is designed for you to create configuration profiles and create pre-configured client profiles. This configuration is deployed on the endpoints so that the Network Access Manager can enforce administratively defined end user and authentication policies and make the pre-configured network profiles available to end users. To use the profile editor, create settings for a profile, save it, and then place the configurations onto the client. AnyConnect includes the profile editor inside ASDM, but a standalone version is also available. Refer to Chapter 2, "Deploying the AnyConnect Secure Mobility Client" for profile editor requirements and deployment instructions.

## Adding a New Profile

Follow these steps to add a new profile for the Network Access Manager.

**Step 1** Click **Configuration** in the ASDM toolbar.

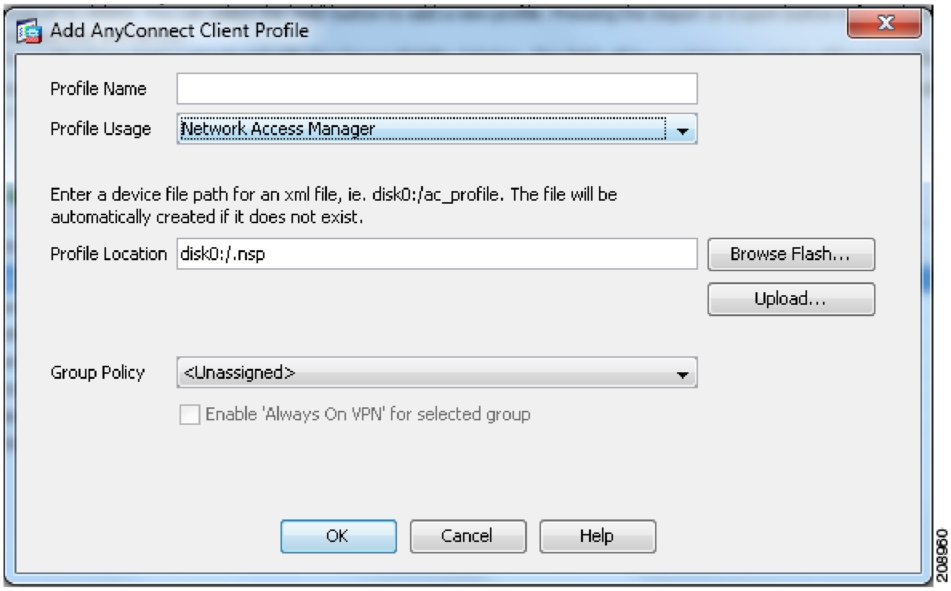
**Step 2** Click **Remote Access VPN** in the leftmost navigation area.

**Step 3** Click **Network Client Access**.

**Step 4** Click **AnyConnect Client Profile**. The profile window appears.

**Step 5** Click **Add**. The Add AnyConnect Client Profile window appears (see Figure 4-1).

*Figure 4-1 Add AnyConnect Client Profile Window*



Add AnyConnect Client Profile

Profile Name

Profile Usage: Network Access Manager

Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.

Profile Location: disk0:/.nsp

Group Policy: <Unassigned>

□ Enable 'Always On VPN' for selected group

**Step 6** Enter a profile name.

**Note** When using the Standalone Profile Editor to create a Network Access Manager profile, you are required to use **configuration.xml** as the entry in the **Profile Name** field. The profile editor copies this file to the newConfigFiles directory. To initiate the process, the user must repair the Network Access Manager. When the Network Access Manager restarts, it will validate the new configuration file and move it to the Network Access Manager/system directory.

**Step 7** From the Profile Usage drop-down list, choose **Network Access Manager** and click **OK**.

**Step 8** (Optional) In the Profile Location parameter, establish a device file path for the XML file.

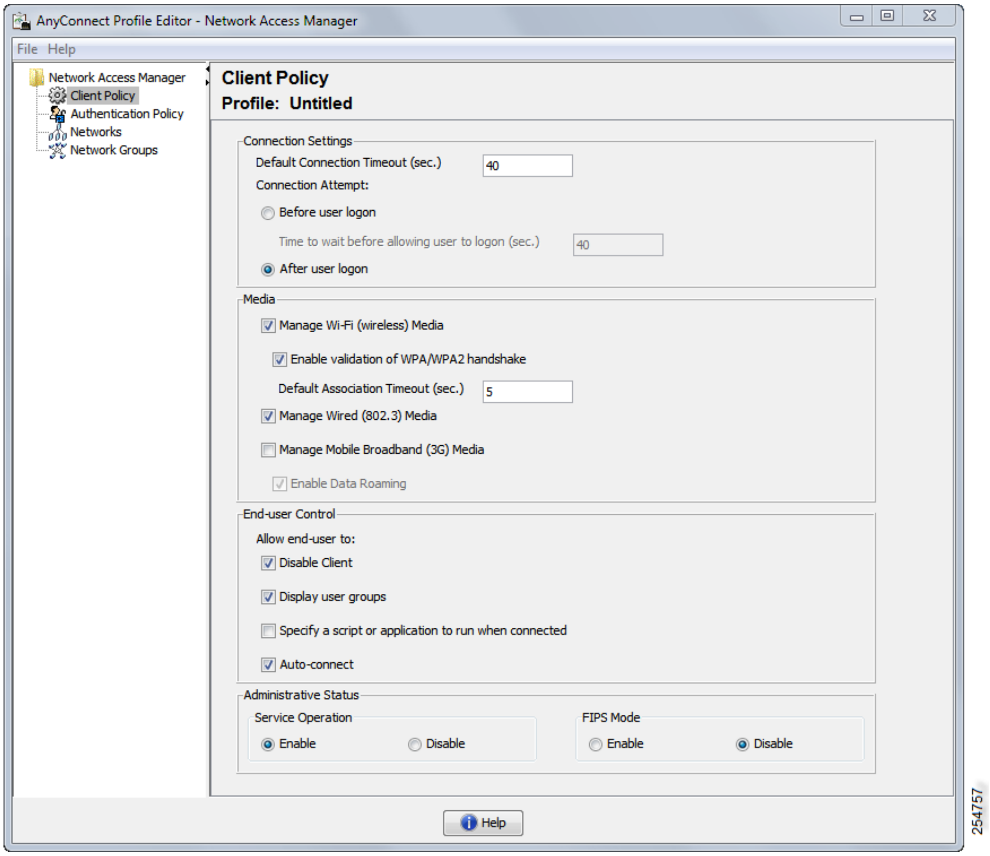
**Step 9** (Optional) Choose an AnyConnect group policy from the drop-down list.

**Step 10** Click **OK**.

# Configuring a Client Policy

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

*Figure 4-2 Client Policy Window*



**Client Policy**
**Profile: Untitled**

Connection Settings
Default Connection Timeout (sec.) 40
Connection Attempt:
○ Before user logon
Time to wait before allowing user to logon (sec.) 40
● After user logon

Media
☑ Manage Wi-Fi (wireless) Media
☑ Enable validation of WPA/WPA2 handshake
Default Association Timeout (sec.) 5
☑ Manage Wired (802.3) Media
□ Manage Mobile Broadband (3G) Media
☑ Enable Data Roaming

End-user Control
Allow end-user to:
☑ Disable Client
☑ Display user groups
□ Specify a script or application to run when connected
☑ Auto-connect

Administrative Status
Service Operation: ● Enable ○ Disable
FIPS Mode: ○ Enable ● Disable

Four sections are included:

- Administrative Status
  - You can switch the Network Access Manager functionality on or off with the Service Operation parameter. If you choose to disable the service, the Network Access Manager cannot manage network connections on the client.
  - You can switch FIPS mode on or off. Federal Information Processing Standard (FIPS 104-2) 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. The normal FIPS mode of operation is disabled. Refer to the "Enabling FIPS and Additional Security" section on page 8-1 for additional information.
- Connection Settings—Allows you to define whether a network with a user connection component is attempted before or after the user logs on.
  - Default Connection Timeout—Specifies the number of seconds to use as the connection timeout parameter for user-created networks. The default value is 40 seconds.
  - Before User Logon—Specifies that you want the Network Access Manager to attempt the user connection immediately, before Windows user logon procedures take place. Windows logon procedures include user account (kerberos) authentication, loading of user GPOs, and GPO-based logon script execution.

- Time to Wait Before Allowing User to Logon—Specify 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, we suggest you use 30 seconds or more because it takes additional time 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 you want the Network Access Manager to attempt the user connection after a Windows user logon procedure.

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

    The IEEE 802.11i Wireless Networking standard specifies the supplicant must validate that the access point's RSN IE sent in the 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** However, 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 the Network Access Manager's management of wired media.
- End-user Control—Allows you to determine 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.

# Configuring an Authentication Policy

This window allows you to define global association and authentication network policies. These policies apply to all networks that the user can create. The policies allows you to limit the type of network a user can create with the GUI. If you do not check any of the association or authentication modes, the user cannot create any networks. If you choose a subset of the modes, the user can create networks for these types and not the unchecked ones. Choose each desired association or authentication mode or choose **Select All**.

When you choose Authentication Policy from the Network Access Manager menu, the window shown in Figure 4-3 appears.

Depending upon the customer requirements, different authentication mechanisms are used in a secure mobility environment, but all of the mechanisms use IEEE 802.1X, EAP, and RADIUS as their supporting protocols. These protocols allow the control of access based upon the successful authentication of the wireless LAN client and allow the wireless LAN network to be authenticated by the user.

This system also provides the other elements of AAA, authorization and accounting, through policies communicated through RADIUS and RADIUS accounting.

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

## EAP

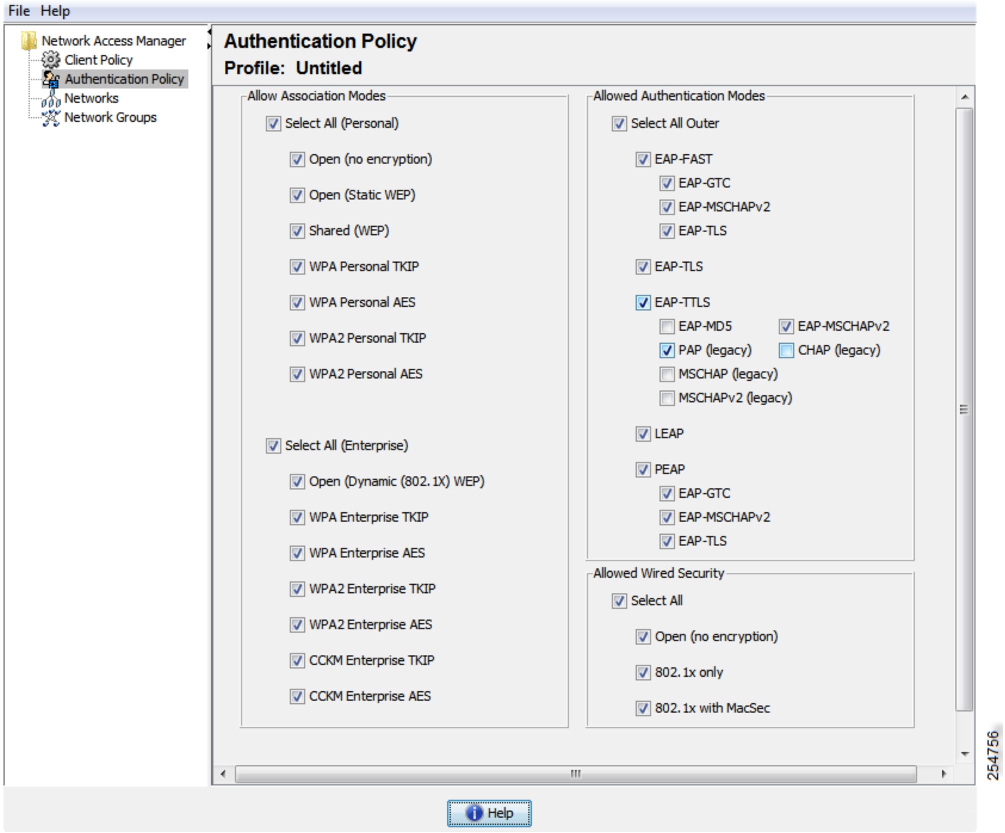
EAP is an IEFT RFC that addresses the requirements for an authentication protocol to be decoupled from the transport protocol carrying it. This decoupling allows the transport protocols (such as IEEE 802.1X, UDP, or RADIUS) to carry the EAP protocol without changes to the authentication protocol.

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 NAK.
- EAP success—The authenticator sends the success packet upon successful authentication to the supplicant.
- EAP failure—The authenticator sends the failure packet upon successful authentication to the supplicant.

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.

*Figure 4-3 Authentication Policy Window*



**Authentication Policy**
**Profile: Untitled**

Allow Association Modes

- ☑ Select All (Personal)
  - ☑ Open (no encryption)
  - ☑ Open (Static WEP)
  - ☑ Shared (WEP)
  - ☑ WPA Personal TKIP
  - ☑ WPA Personal AES
  - ☑ WPA2 Personal TKIP
  - ☑ WPA2 Personal AES
- ☑ Select All (Enterprise)
  - ☑ Open (Dynamic (802.1X) WEP)
  - ☑ WPA Enterprise TKIP
  - ☑ WPA Enterprise AES
  - ☑ WPA2 Enterprise TKIP
  - ☑ WPA2 Enterprise AES
  - ☑ CCKM Enterprise TKIP
  - ☑ CCKM Enterprise AES

Allowed Authentication Modes

- ☑ Select All Outer
  - ☑ EAP-FAST
    - ☑ EAP-GTC
    - ☑ EAP-MSCHAPv2
    - ☑ EAP-TLS
  - ☑ EAP-TLS
  - ☑ EAP-TTLS
    - □ EAP-MD5 ☑ EAP-MSCHAPv2
    - ☑ PAP (legacy) □ CHAP (legacy)
    - □ MSCHAP (legacy)
    - □ MSCHAPv2 (legacy)
  - ☑ LEAP
  - ☑ PEAP
    - ☑ EAP-GTC
    - ☑ EAP-MSCHAPv2
    - ☑ EAP-TLS

Allowed Wired Security

- ☑ Select All
  - ☑ Open (no encryption)
  - ☑ 802.1x only
  - ☑ 802.1x with MacSec

Refer to the following for a description of the options on this page:

- for personal or enterprise association modes—Defining Networks Security Level
- for allowed authentication modes—Defining the Networks Machine or User Authentication
- for allowed wired security—Defining the Networks Connection Type

# Configuring Networks

The Networks window allows you to configure networks that are pre-defined for your enterprise user. You can either configure networks that are available to all groups or create groups with specific networks.

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 globalNetworks, 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 remove administrator-configured networks.

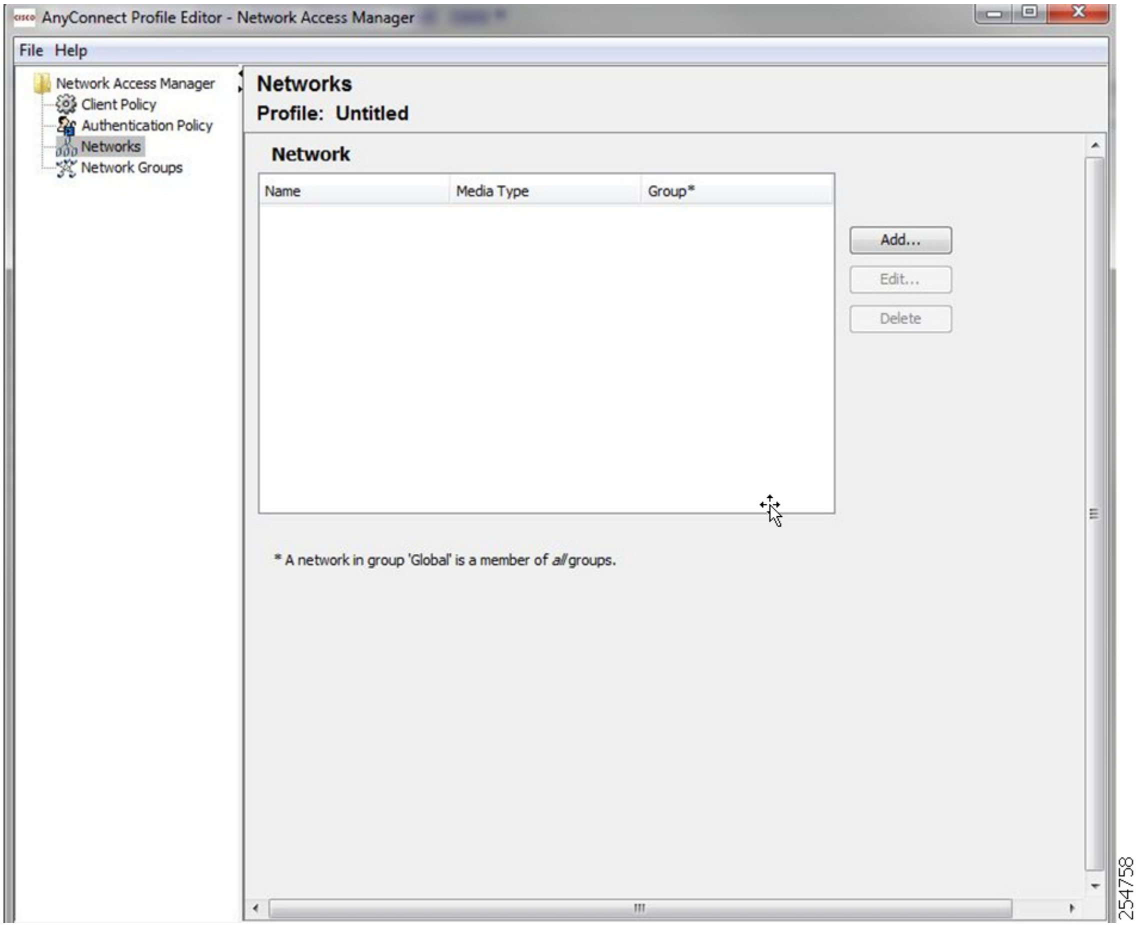
**Note** End users may add networks to groups, except for networks in the globalNetworks section, because these networks exist in all groups, and you can only create them using the profile editor.

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*



Networks

Profile: Untitled

Network

| Name | Media Type | Group* |
|---|---|---|

* A network in group 'Global' is a member of *all* groups.

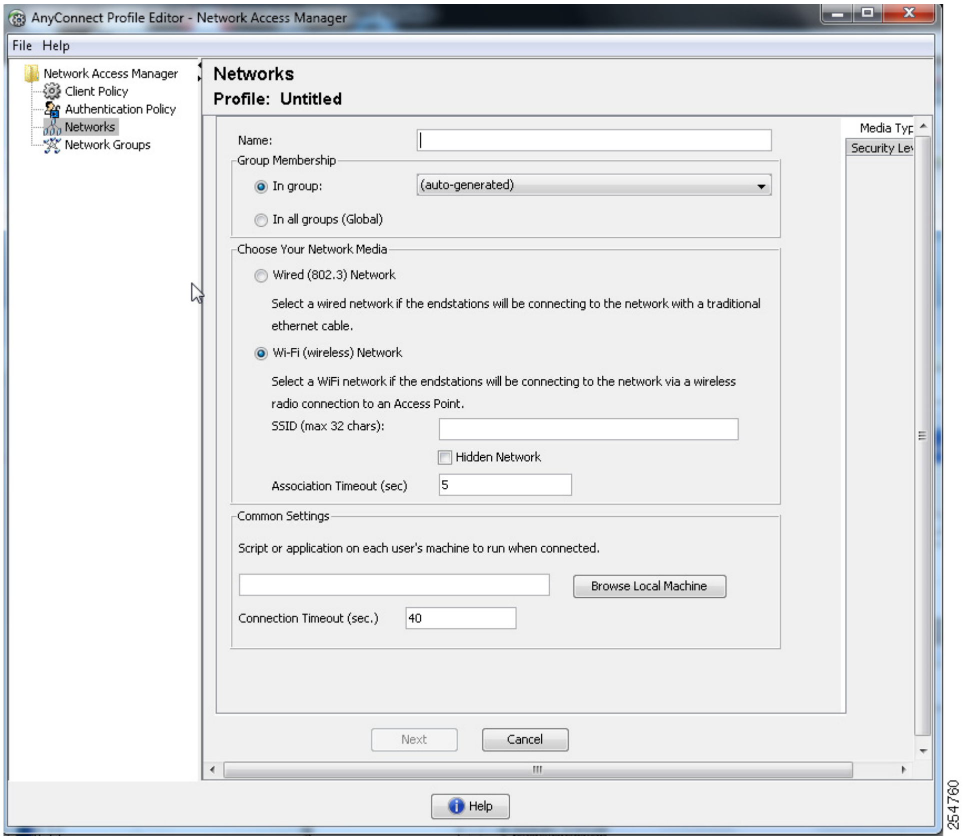
Choose from one of the following actions:

- Click **Add** to create a new network. If you choose to create a new network, follow the steps in the Defining Networks Media Types section below.
- Choose a network you want to change and click **Edit**.
- Choose a network you want to remove and click **Delete**.

# Defining Networks Media Types

This window panel enables you to create or edit a wired or a wireless network. The settings vary somewhat 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 Panel*



**Networks**
**Profile: Untitled**

Name:

Group Membership
● In group: (auto-generated)
○ In all groups (Global)

Choose Your Network Media
○ Wired (802.3) Network
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.
● Wi-Fi (wireless) Network
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.
SSID (max 32 chars):
□ Hidden Network
Association Timeout (sec) 5

Common Settings
Script or application on each user's machine to run when connected.
Browse Local Machine
Connection Timeout (sec.) 40

**Step 1** In the Name field, enter the name that is displayed for this network.

**Step 2** (Wi-Fi Only) At the SSID parameter, enter the SSID of your wireless network.

**Step 3** (Wi-Fi only) Choose **Hidden Network** if the network is not broadcasting its SSID.

**Note** The Network Access Manager's selection algorithm is optimized to make more use of the network scan list. For networks that broadcast their SSIDs, the Network Access Manager only attempts connection with these networks when they show up in the network scan list.

**Step 4** (Wi-Fi Only) At the Association Timeout parameter, 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.

**Step 5** In the Common Settings section, you can enter the path and filename of the file that you want to run or you can browse to the location and select the file to run.

The following applies 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.

**Step 6** In the Connection Timeout parameter, 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.

**Step 7** Click **Next**.

# Defining Networks Security Level

You can define the type of security level for your wired or wireless network. In the Security Level area, choose the desired network type:

- Using Authenticating Wired Networks—Recommended for secure enterprise wired network.
- Using an Open Network—Not recommended but can be used for guest access on a wired network.
- Using a Shared Key—Recommended for wireless networks such as small offices or home offices.
- Using Authenticating WiFi Networks—Recommended for secure enterprise wireless networks.

## Using Authenticating Wired Networks

Follow these steps if you want to use IEEE 802.1X authentication as your security level.

**Step 1** Choose **Authenticating Network**.

**Note** Make sure you chose Wired (802.3) Network on the Network Media Type panel (shown in Figure 4-5).

**Step 2** 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)—After sending an EAPoL-Start to initiate an authentication attempt with the authenticator, this timer defines how long the supplicant will wait for the authenticator to respond before initiating authentication again (such as sending the next EAPoL-Start).
- maxStart—The number of times the supplicant will initiate authentication with the authenticator by sending an 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).

**Step 3** Choose from the following level of security:

- Key Management—Use the drop-down list to determine which Key Management Protocol you want to use with your 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 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—Data traffic is encrypted using AES-GCM-128.

**Step 4** Choose **Port Authentication Exception Policy**. By enabling the Port Authentication Exception Policy, you have the ability 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—When selected, this exception 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.

## Using an 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 panel. 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 "Defining the Networks Connection Type" section on page 4-17.

## Using a Shared Key

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

**Note** This setting is not recommended for enterprise wireless networks.

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

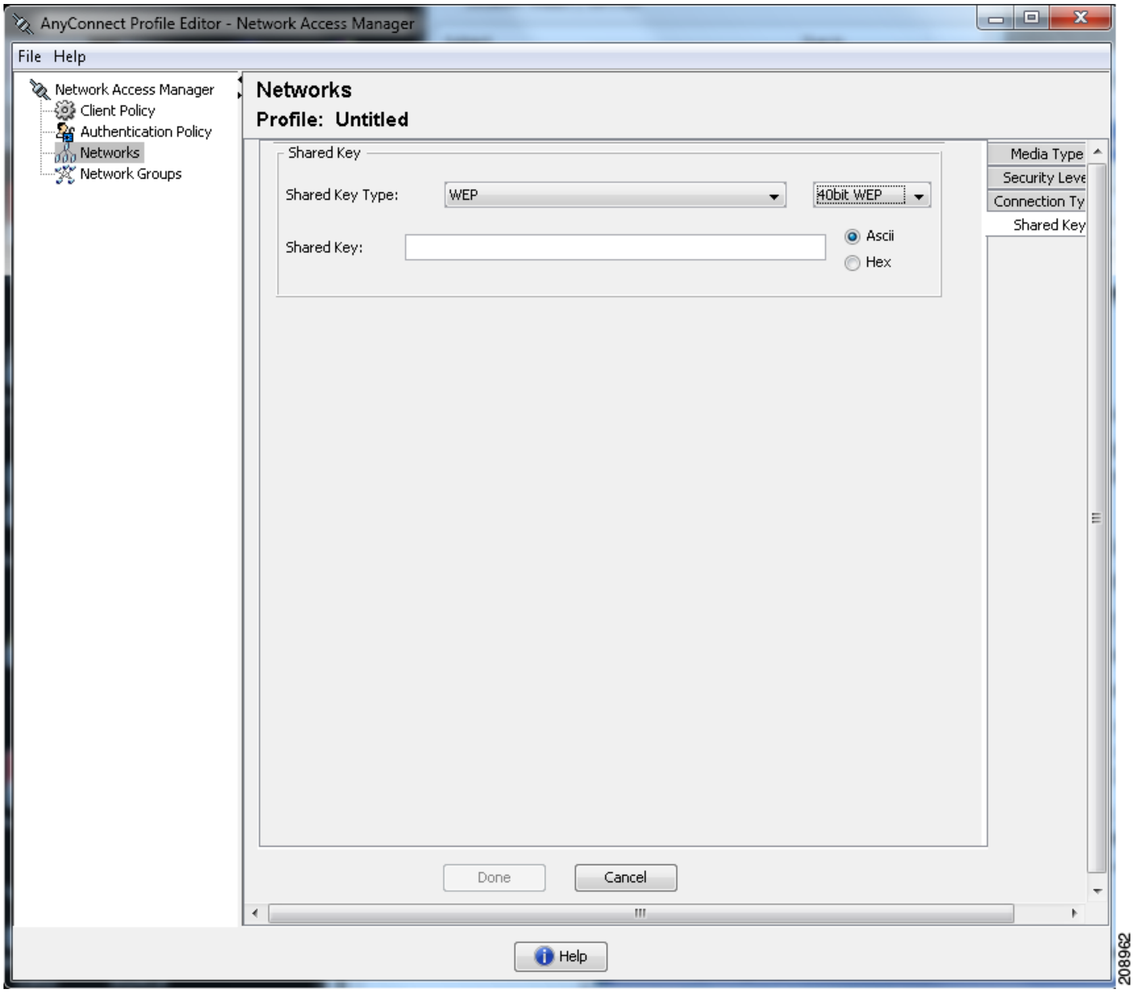
**Step 1** Choose **Shared Key Network**.

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

**Step 3** Specify **User Connection** or **Machine Connection**. Refer to the "Defining the Networks Connection Type" section on page 4-17 for more information.

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

*Figure 4-6 Shared Key Panel*



Shared Key

Shared Key Type: WEP 40bit WEP

Shared Key:

● Ascii
○ Hex

**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.
- WPA/WPA2-Personal—A Wi-Fi security protocol that derives encryption keys from a passphrase pre-shared key (PSK).

**Step 6** If you choose 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.

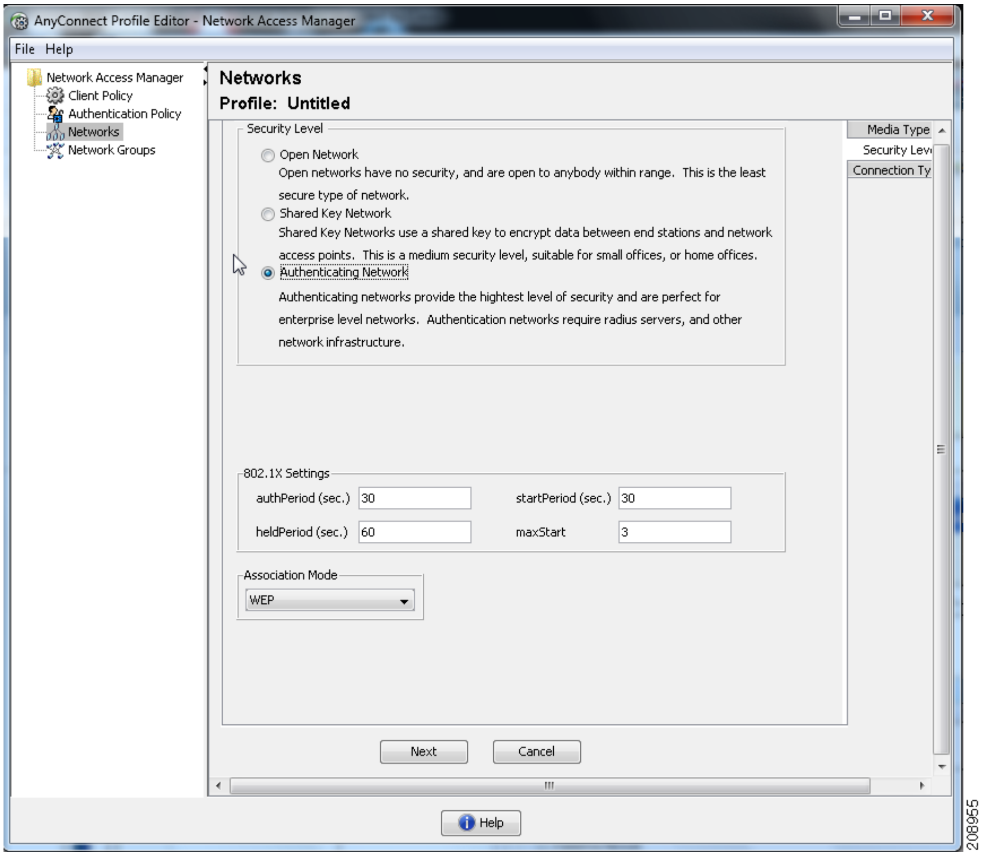
**Step 7** If you choose WPA or WPA2 Personal, choose the type of encryption to use (TKIP/AES) and then enter a shared key. The key must be entered as 8 to 63 ASCII characters or exactly 64 hexadecimal digits. Choose **ASCII** if your shared key consists of ASCII characters. Choose **Hexadecimal** if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

# Using Authenticating WiFi Networks

If you choose Authenticating Network, you can create secure wireless networks based on IEEE 802.1X and EAP.

Follow these steps if you want Authenticating Networks as your security level (see Figure 4-7).

***Figure 4-7 Authenticating Network Security Level***



Networks
Profile: Untitled

Security Level

○ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

○ Shared Key Network
Shared Key Networks use a shared key to encrypt data between end stations and network access points. This is a medium security level, suitable for small offices, or home offices.

● Authenticating Network
Authenticating networks provide the hightest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

| | | | |
|---|---|---|---|
| authPeriod (sec.) | 30 | startPeriod (sec.) | 30 |
| heldPeriod (sec.) | 60 | maxStart | 3 |

Association Mode: WEP

**Step 1** Choose **Authenticating Networks**.

**Step 2** Although the default values should work for most networks, you have the option to configure the IEEE 802.1X settings to suit your environment, if necessary:

- 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. The default is 30 seconds.
- heldPeriod(sec)—When authentication fails, this time defines how long the supplicant waits before another authentication attempt can be made. The default is 60 seconds.
- startPeriod(sec)—After sending an EAPoL-Start to initiate an authentication attempt with the authenticator, this timer defines how long the supplicant will wait for the authenticator to respond before initiating authentication again (such as sending the next EAPoL-Start). The default is 30 seconds.

- maxStart—The number of consecutive times the supplicant will initiate authentication with the authenticator by sending an EAPoL-Start (without receiving a response from the authenticator) before the supplicant assumes there is no authenticator present. When this happens, the supplicant allows data traffic. The default is 3 times.

**Note** For this section, authentication begins when the authenticator sends the client supplicant an EAP identity request.

**Step 3** For Association Mode, specify the type of wireless security to use.

# Defining the Networks Connection Type

With the Connection Type panel, you can choose the type of network connection and specify when connection attempts using this network are allowed (see Figure 4-8). The machine connection option defines the connection as a machine connection type. You can use machine connection at any time, but you typically use it whenever user credentials are not required for a connection. The User Connection option defines the connection as a user connection type. The user can make connections only after initiating a logon attempt with the PC. While not required, user connections usually use the logged on user’s credentials to establish a connection.

A machine and user network contains a machine part and a user part; 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.

- Machine 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** You should consider that if you want VPN start before login (SBL) to operate as expected, a network connection must exist when the user attempts to start the VPN. If the Network Access Manager is installed, you must deploy machine connection to ensure that an appropriate connection is available.

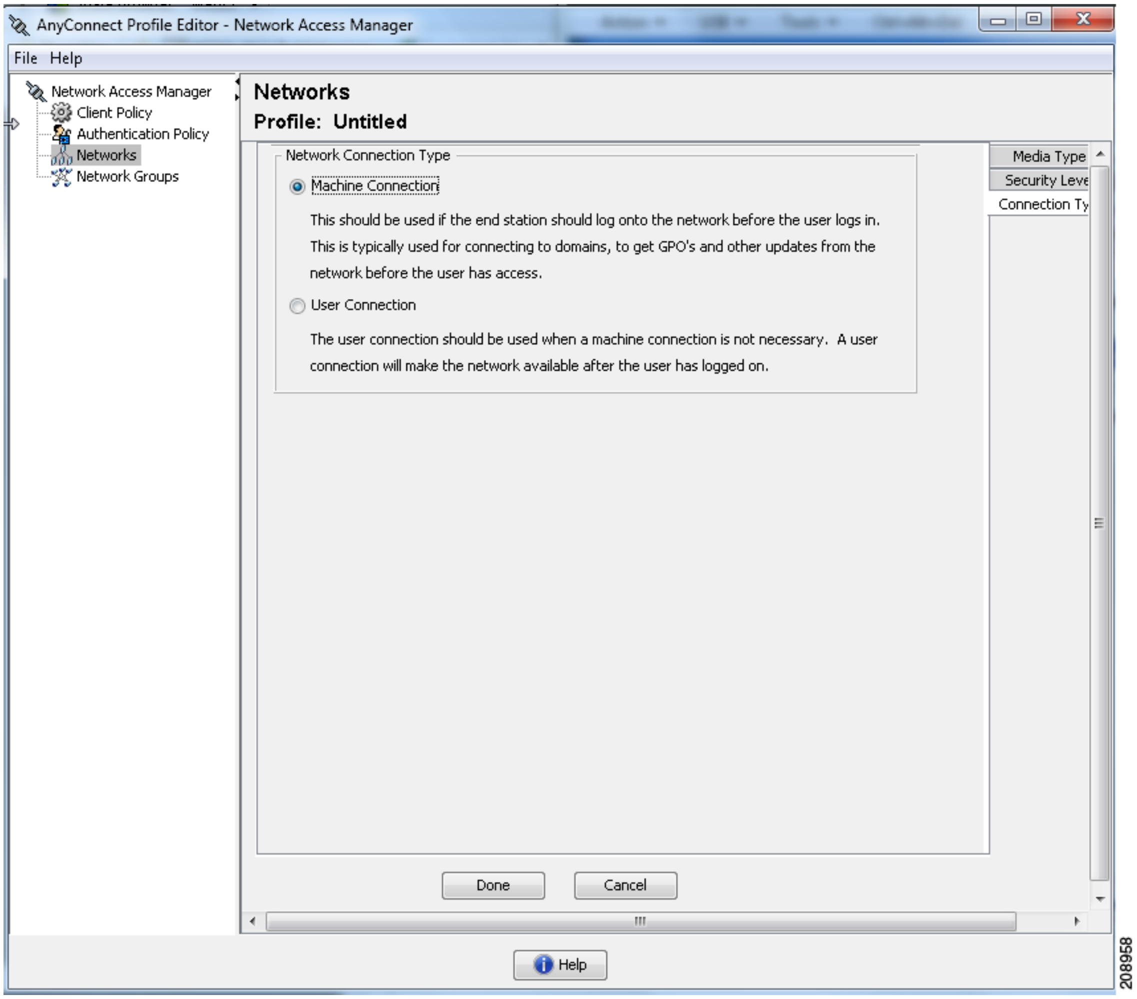
- User Connection—Choose this option when a machine connection is unnecessary. A user connection makes the network available after the user has initiated a logon attempt with the PC. When the user subsequently logs off, the network connection is terminated unless the connection is configured to extend the connection beyond user logoff.

  **Note** The Client Policy Connection settings determine whether a user is considered as logged in by the Network Access Manager (refer to the “Configuring a Client Policy” section on page 4-4). If Connection Settings are set to *Attempt connection before user logon*, the Network Access Manager attempts to use the credentials the user entered to make a network connection prior to actual logon. If Connection Settings is set to *Attempt connection after user logon*, the Network Access Manager waits until user has actually logged in to make a network connection.

- Machine and 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.

**Note** For open and shared key networks, the Machine and User Connection option is not available.

***Figure 4-8 Network Connection Type Panel***



Network Connection Type

● Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

○ User Connection

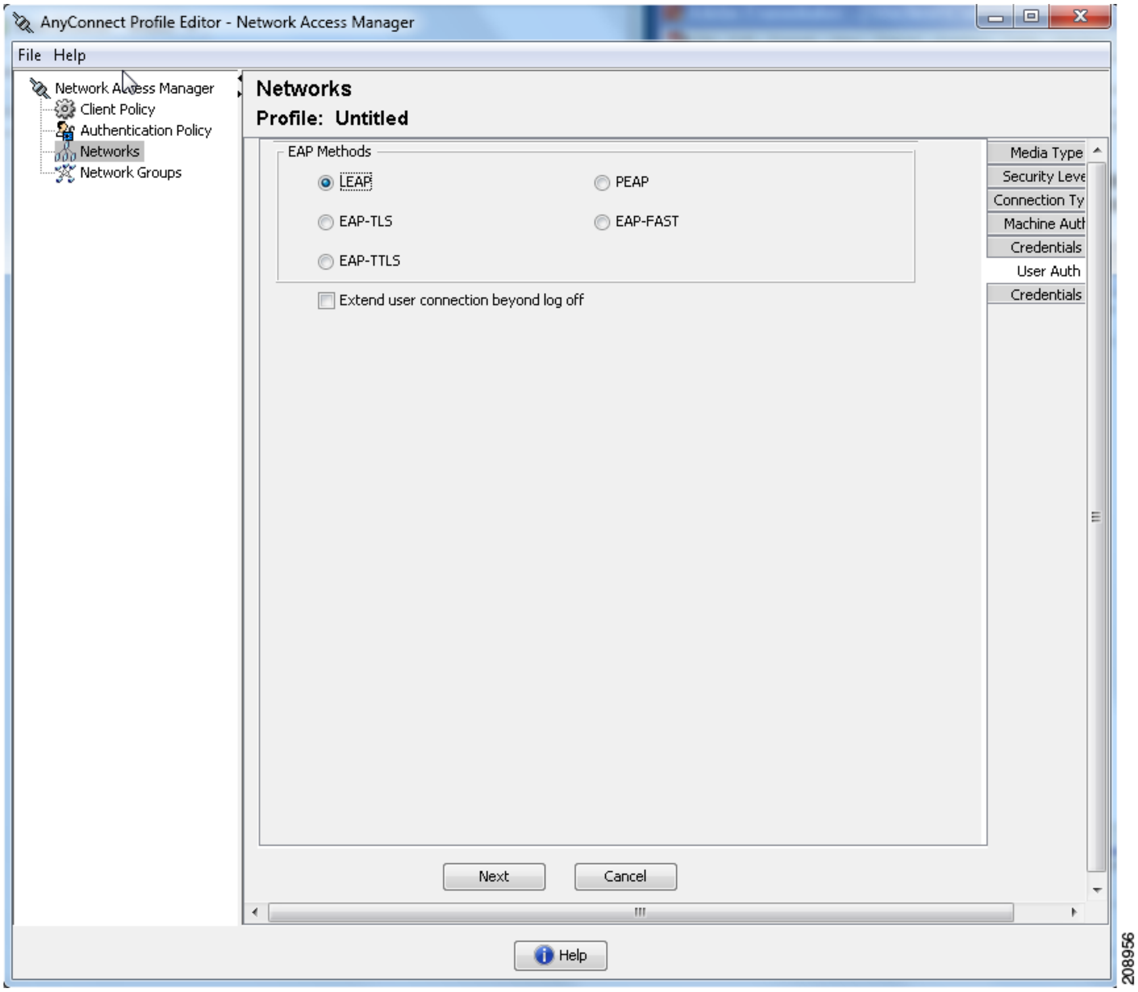
The user connection should be used when a machine connection is not necessary. A user connection will make the network available after the user has logged on.

# Defining the Networks Machine or User Authentication

With the Machine Authentication or User Authentication panel, you can choose the authentication method for the machine or user (see Figure 4-9). When you specify your authentication method, the center of the window adapts to the method you choose, and you are required to provide additional information for EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, or EAP-GTC.

Refer to the "Using a Windows Remote Desktop" section on page C-7 for information on accessing a network computer remotely while the connection is being managed by the Network Access Manager on that network computer. It discusses network profiles using machine, user, or machine and user authentication.

*Figure 4-9 Machine or User Authentication Panel*



Networks

Profile: Untitled

EAP Methods

● LEAP ○ PEAP

○ EAP-TLS ○ EAP-FAST

○ EAP-TTLS

□ Extend user connection beyond log off

**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 if you choose an EAP option.

- EAP-GTC—See the "Configuring EAP-GTC" section on page 4-20
- EAP-TLS—See the "Configuring EAP-TLS" section on page 4-20.
- EAP-TTLS—See the "Configuring EAP-TTLS" section on page 4-21.
- PEAP—See the "Configuring PEAP Options" section on page 4-22.
- EAP-FAST—See the "Configuring EAP-FAST Settings" section on page 4-23.

## 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 authentication.

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

## 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—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** The *Disable when using a Smart Card* option is not available on machine authentication.Before user log on, smart card support is not available on Windows Vista and Windows 7.

- Inner Methods—Specifies the inner methods used after the TLS tunnel is created.

## 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:

- 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.

- Token
  - EAP-GTC—Defines an EAP envelope to carry a token code or OTP.
- 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 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.
- The *Disable when using a Smart Card* and the *Authenticate using a Token and EAP GTC* options are not available for machine authentication.
- Inner methods based on Credentials Source—Enables you to choose to authenticate using a password or a certificate.
  - Authenticate using a password for EAP-MSCHAPv2 or EAP-GTC
  - EAP-TLS, using Certificate
  - Authenticate using a Token and EAP-GTC

**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.

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.

The EAP-FAST Settings panel enables you to configure the EAP-FAST settings:

- EAP-FAST Settings
  - Validate Server Identity—Enables server certificate validation. Enabling this introduces two extra dialogs in the management utility and adds additional Certificate panels 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** Before user log on, smart card support is not available on Windows Vista and Windows 7.

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

- 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, you should 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 encrypted) passwords. We recommend this method if a possibility of a database leak exists.

    If you are using password based inner methods, an additional option for using Protected Access Credential (PAC) applies. Choose to allow or disallow 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 panel 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.

# Defining Networks Credentials

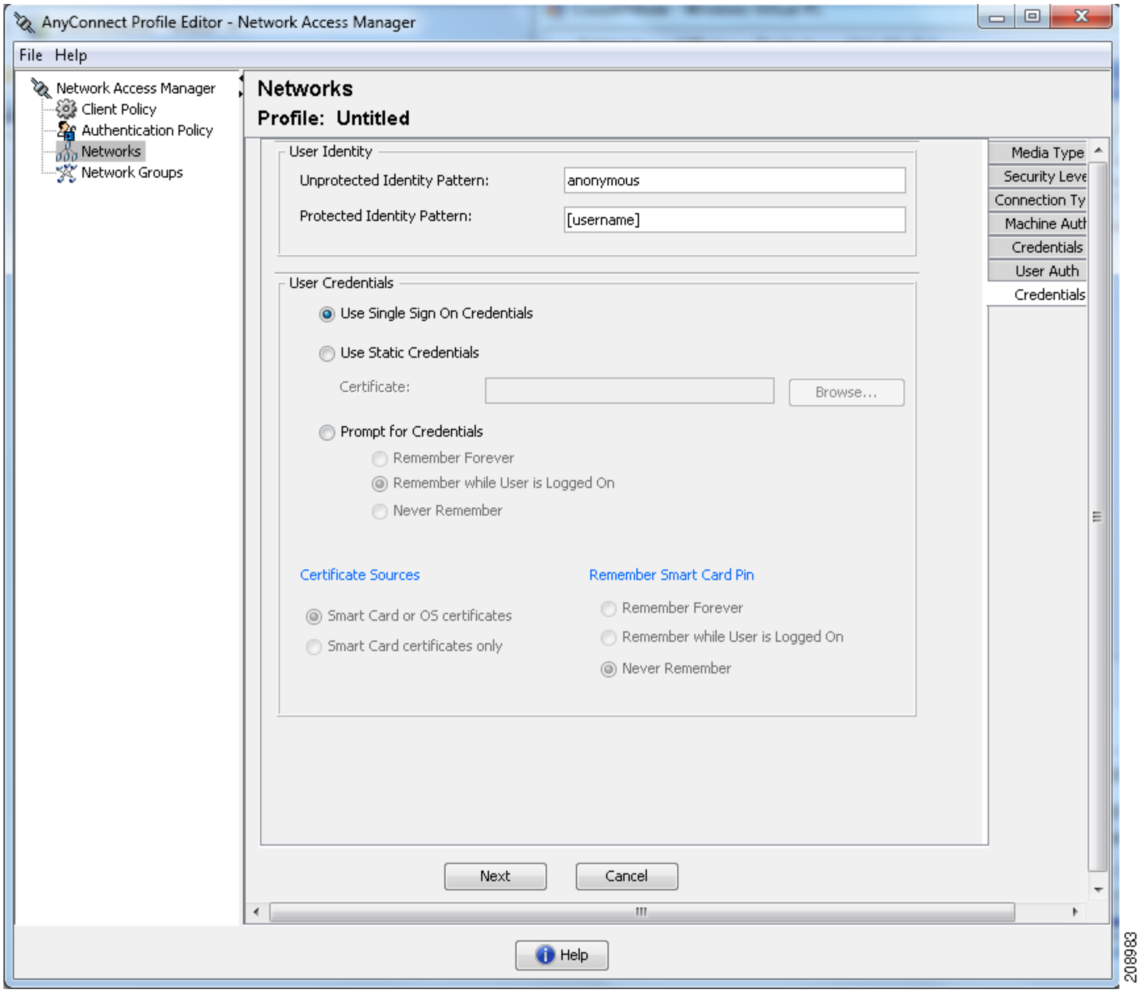
Within Network Credentials, you can establish user or machine credentials and establish trusted server validation rules.

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

## Configuring User Credentials

With the Credentials panel you can specify the desired credentials to use for authenticating the associated network (see Figure 4-10).

*Figure 4-10 User Credentials Panel*



Networks
Profile: Untitled

User Identity
Unprotected Identity Pattern: anonymous
Protected Identity Pattern: [username]

User Credentials
● Use Single Sign On Credentials
○ Use Static Credentials
Certificate:
○ Prompt for Credentials
○ Remember Forever
● Remember while User is Logged On
○ Never Remember

Certificate Sources
● Smart Card or OS certificates
○ Smart Card certificates only

Remember Smart Card Pin
○ Remember Forever
○ Remember while User is Logged On
● Never Remember

**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, 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 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.

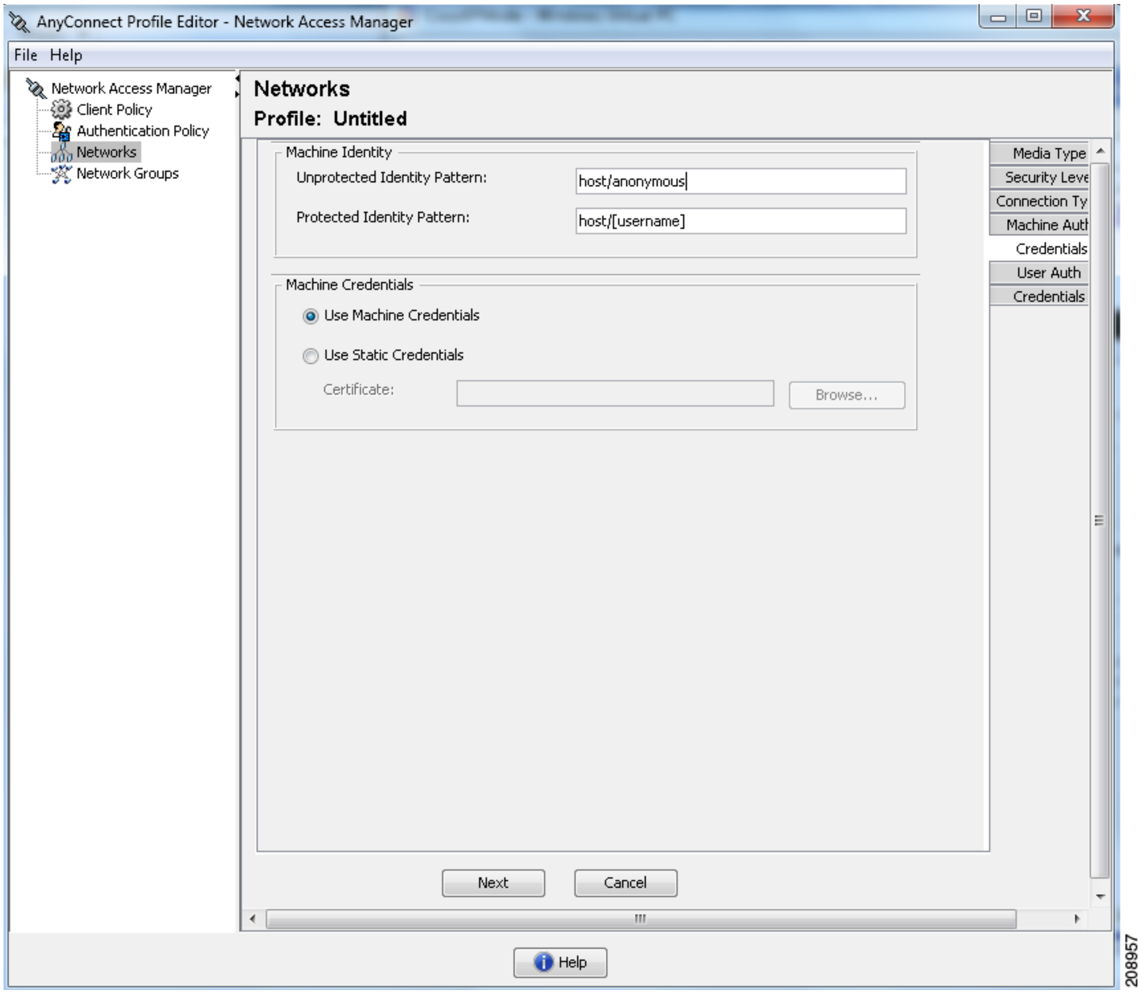
**Step 4** At the Remember Smart Card Pin parameter, determine how long the Network Access Manager remembers the PIN used to retrieve the certificate off a smart card. Refer to Step 2 for the available options.

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

## Configuring Machine Credentials

With the Credentials panel you can specify the desired machine credentials (see Figure 4-11).

*Figure 4-11 Machine Credentials*



AnyConnect Profile Editor - Network Access Manager

Networks
Profile: Untitled

Machine Identity
Unprotected Identity Pattern: host/anonymous
Protected Identity Pattern: host/[username]

Machine Credentials
● Use Machine Credentials
○ Use Static Credentials
Certificate:

**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.

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.

# Defining Network Groups

With the Network Groups panel you can assign network connections to a particular group (see Figure 4-12). Classifying connections into groups provides multiple benefits:

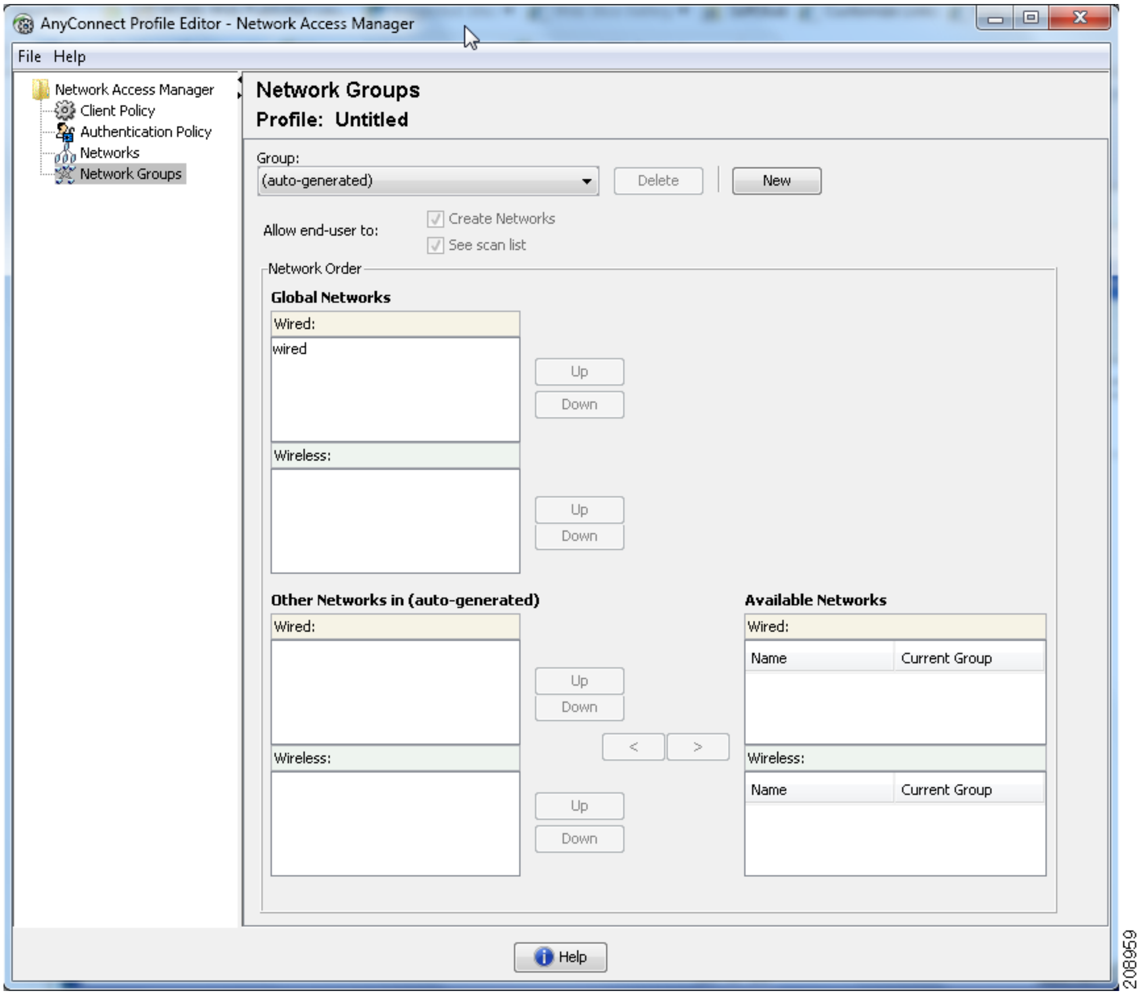
- Improved user experience when attempting to make a connection. When multiple hidden networks are configured, the client walks through the list of hidden networks in the order that they are defined until a successful connection is made. In such instances, groups are used to greatly reduce the amount 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. If the network has not been added, it is added to a predefined Default group.

*Figure 4-12 Network Groups Window*



Group: (auto-generated)

Allow end-user to: ☑ Create Networks ☑ See scan list

Global Networks — Wired: wired

**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.