Configure 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.

- About Network Access Manager, on page 1
- Network Access Manager Deployment, on page 4
- Disable DHCP Connectivity Testing, on page 5
- Network Access Manager Profile, on page 5

About Network Access Manager

Network Access Manager is client software that provides a secure Layer 2 network in accordance with its policies. It detects and selects the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks. 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 is designed to be single homed, allowing only one network connection at a time. Also, wired connections have higher priority than wireless so that if you are plugged into the network with a wired connection, the wireless adapter becomes disabled with no IP address.

If your wired or wireless network settings or specific SSIDs are pushed from a group policy, they can conflict with the proper operation of the Network Access Manager. With the Network Access Manager installed, a group policy for wireless settings is not supported.

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

Note If you are using ISE posture on a Windows OS, Network Access Manager must be installed prior to starting AnyConnect ISE Posture.

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

- Captive Portal Detection. Refer to Captive Portal Detection Requirements with Network Access Manager, on page 8. Captive Portal Detection is not supported on Windows 7.

- Transport Layer Security (TLS) Protocol Version 1.2.
- Wired (IEEE 802.3) and wireless (IEEE 802.11) network adapters.
- Some Mobile Broadband (3G) network adapters with Windows 7 or later. (Requires a WAN adapter that supports Microsoft Mobile Broadband APIs.)
- Pre-login authentication using Windows machine credentials.
- Single sign-on user authentication using Windows logon credentials.
- Simplified 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.
- AnyConnect supports smartcard-provided credentials in the following environments:
  - Microsoft CAPI 1.0 and CAPI 2.0 (CNG) on Windows.
  - Windows logon does not support ECDSA certificates; therefore, the Network Access Manager Single Sign-On (SSO) does not support ECDSA client certificates.

Note WPA3 Enhanced Open (OWE) and WPA3 Personal (SAE) support added to Network Access Manager with Cisco Secure Client Release 5.0.02075.

Suite B and FIPS

The following features are FIPS-certified on Windows 7 or later, and any exceptions are listed:

- ACS and ISE do not support Suite B, but FreeRADIUS 2.x with OpenSSL 1.x does. Microsoft NPS 2008 supports Suite B in part (the NPS certificate still has to be RSA).
- 802.1X/EAP supports the transitional Suite B profile only (as defined in RFC 5430).
- MACsec is FIPS-compliant.
- Elliptic Curve Diffie-Hellman (ECDH) key exchange is supported.

- ECDSA client certificates are supported.
- ECDSA CA certificates in the OS store are supported.
- ECDSA CA certificates in the network profile (PEM encoded) are supported.
- Server’s ECDSA certificate chain verification is supported.

Single Sign On "Single User" Enforcement

Microsoft Windows allows multiple users to be logged on concurrently, but AnyConnect Network Access Manager restricts network authentication to a single user. AnyConnect Network Access Manager can be active for one user per desktop or server, regardless of how many users are logged on. Single user login enforcement implies that only one user can be logged in to the system at any one time and that administrators cannot force the currently logged-in user to log off.

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, you can modify or add a registry to change the default behavior.

Restrictions

- Windows administrators are restricted from forcing currently logged-on users to log off.
- 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, user/example is not the same as user@example.com.
- Smart-card users must also have the same PIN to be considered the same user.

Configure Single Sign-On Single User Enforcement

To change how a Windows workstation or server handles multiple users, change the value of EnforceSingleLogon in the registry.

On Windows, 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}
```

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

For Windows:

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

Network Access Manager Deployment

Network Access Manager is deployed as part of AnyConnect. For information about how to install AnyConnect, along with the Network Access Manager and other modules, see the AnyConnect Deployment Overview.

Guidelines

- Confusion about the Windows network status task tray icon—Network Access Manager overrides Windows network management. Therefore, after installing the Network Access Manager, you cannot use the network status icon to connect to networks.

  Recommended Action—Remove the Windows network icon from the task tray by setting **Remove the networking icon** in a Windows group policy. This setting affects only the tray icon. The user can still create native wireless networks using the Control Panel.

- Hidden networks and network selection for Windows 7 or later—Network Access Manager tries to connect to only the networks that are configured in the Network Access Manager network scan list.

  On Windows 7 or later, the Network Access Manager probes for hidden SSIDs. When the first hidden SSID is found, it stops looking. When multiple hidden networks are configured, the 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. Cisco recommends having only one hidden corporate network at your site, since the Network Access Manager can probe only one non-broadcasting SSID at a time.

- Momentary loss of network connectivity or longer connection times—If you defined networks in Windows before the Network Access Manager was installed, the Windows connection manager may occasionally try to make a connection to that network.

  Recommended Action—When the network is in range, switch off **Connect Automatically** for all Windows-defined networks or delete all the Windows-defined networks.

- The Network Access Manager module can be configured to convert some existing Windows 7 or later wireless profiles to the Network Access Manager profile format when the module is installed on the client system for the first time. Infrastructure networks that match the following criteria can be converted:

  - Open
  - Static WEP
  - WPA/WPA2 Personal
  - Only non-GPO native Wi-Fi user network profiles are converted.
  - WLAN services must be running on the system during profile conversion.
  - Conversion will not be done if a Network Access Manager XML configuration file already exists (userConfiguration.xml).

  To enable network profile conversion, create an MSI transform that sets the PROFILE_CONVERSION property value to 1, and apply it to the MSI package. Or change the PROFILE_CONVERSION property

to 1 in the command line, and install the MSI package. For example, **msiexec /i anyconnect-nam-<version>-k9.msi PROFILE_CONVERSION=1**.

- You must install the Network Access Manager before ISE Posture starts. ISE Posture uses the Network Access Manager plugin to detect the network change events and 802.1x Wi-Fi.

Disable DHCP Connectivity Testing

When a network is configured to use dynamic IP addresses, the Windows OS service tries to establish connectivity using DHCP. However, the operating system process can take up to two minutes before it notifies the Network Access Manager that it has completed a DHCP transaction. The Network Access Manager triggers DHCP transactions, in addition to the OS DHCP transactions, to avoid long delays in establishing connectivity through the OS and to verify network connectivity.

When you want to disable the use of DHCP transactions by NAM for connectivity testing, add the following registry key as a DWORD and set the value as indicated:

- 64-bit Windows—HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP set to 1
- 32-bit Windows—HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP set to 1

Note We strongly discourage disabling the Network Access Manager DHCP connectivity test because it often results in a longer connectivity time.

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. The following sections are included:

Connection Settings

Enables 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 can also 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 logon. The default is five seconds.

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

- **After User Logon**—Connect to the network 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 Wi-Fi media and, optionally, validation of a WPA/WPA2 handshake.

  The IEEE 802.11i Wireless Networking standard specifies that the supplicant (in this case, the Network Access Manager) must validate the access point's RSN IE (Robust Secure Network Information Exchange). The IE is sent in the IEEE 801.X protocol packet's EAPOL key data during key derivation, and it should match the access point's RSN IE found in the beacon/probe response frame.

- **Enable validation of WPA/WPA2 handshake**—Validates a WPA/WPA2 handshake. If unchecked, this optional 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.

- **Enable Randomized MAC Address**—(Windows 10 and later only) Enables randomization for hardware or drivers that support it. When enabled, each unique wireless network SSID utilizes a new randomized address and uses that private address for the network. You can also change the randomized address every 24 hours, if desired. If a connection is forgotten and then reconnected, a new MAC address is assigned. Refer to Enable MAC Address Randomization, on page 15.
- **Default Association Timeout** (sec)—If you enable the WPA/WPA2 handshake, you must specify the default association timeout.
- **Manage Wired (IEEE 802.3) Media**—Enables management of wired connections.
- **Manage Mobile Broadband Media**—Enables management of Windows Mobile Broadband Adapters. This feature is disabled by default.

Note This feature is in a beta release state. Cisco TAC does not provide support for beta releases.

- **Enable Data Roaming**—Determines whether to allow data roaming.

End-user Control

Enables 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 permits users to configure a script or application for only 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**—Connects automatically to a network without a user choosing it. The default is automatic connection.
- **Select Machine Connection Type**—Enables an *Allow Connection Before Logon* choice for end users, when adding a user-defined network. The end user choice determines whether networks can connect prior to user login. Subsequently, they can choose a personal, shared WEP, or open security.

  Enable by Default—Automatically enables Allow Connection Before Logon for the end user when adding a user-defined network.

Note If you upgrade AnyConnect from an earlier version to 4.9.01095 (or later), you must open the configuration.xml file with the proper profile editor and save the file in order to get an updated xml with the new features.

Administrative Status

- **Service Operation**—If you switch off the service, clients who use this profile will not be able to connect to establish Layer 2 connections.
- **FIPS Mode**—If you enable FIPS mode, the Network Access Manager performs cryptographic operations in a way that meets the government requirements.

Federal Information Processing Standard (FIPS 140-2 Level 1) is a U.S. government standard that specifies security requirements for cryptography modules. FIPS is supported by the Network Access Manager for MACsec or Wi-Fi, depending on the type of software and hardware.

Table 1: FIPS Support by the Network Access Manager

Media/Operating System	Windows 7 or later
Wired with MACsec	FIPS compliant when an Intel HW MACsec capable NIC or any non-hardware MACsec is used
Wi-Fi	Not FIPS compliant

- **Captive Portal Detection**—You can choose to enable or disable the automatic launch of a default web browser upon captive portal detection. Refer to About Captive Portals for additional information. With captive portal detection enabled, the user is prompted to enter credentials or to acknowledge the portal page, permitting network access on the browser that is launched. When the default web browser is launched, the Network UI tile displays "Action needed, no internet. Open browser and connect." This UI tile changes to "Captive Portal Detected" and "Connected" upon authentication. If no configuration for captive portal detection exists, Network Access Manager sets the option to disabled.

Captive Portal Detection Requirements with Network Access Manager

- Within the configurable End-User Controls for Network Access Manager, captive portal remediation will not be an option.
- Captive Portal Detection is not supported on Windows 7.
- To prevent the potential for conflict, Network Access Manager Captive Portal Detection, when enabled, disables the Windows Network Location Awareness Service captive portal detection. Thw Windows service is restored only if Network Access Manager is set to disabled or uninstalled.
- The Network Access Manager probes for a connection every 10 seconds, and when it detects the completion of web authentication, it provides internet connectivity. It does not monitor when a user logs out.

Authentication Policy Window

The Authentication Policy window enables 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 required association or authentication mode, or choose **Select All**.

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 Network Access Manager supports is PAP, since challenge/response methods are not well suited for token-based authentication.
  - Certificate credentials: N/A

Networks Window

The Networks window enables you to configure predefined 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 displays a wizard that may add panes to the existing window, and enables you to 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 be a member of all groups.

Note For backward compatibility, 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 that broadcast 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 they can only be created using the profile editor.

A typical end user of an enterprise network does not need knowledge of groups 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 list of groups 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 the tray icon and choosing **Network Repair**). When the Network Access Manager is repaired or restarted, it starts using the previously active group.

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 your choice.

The following sections are included in the first dialog:

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

- 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 specify only 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. Users are 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 should increase the Connection Timeout value, especially if the smartcard may have to try several networks before making a successful connection.

Note To mitigate issues found with certain smart card middleware, the AnyConnect Network Access Manager verifies smartcard PINs by performing a signing operation on test data and verifying that signature. This test signing is done for each certificate located on a smartcard, and dependent on the number of certificates, can add significant delays to smartcard authentication. If you want to disable the test signing operation, you can add **DisableSmartcardPinVerifyBySigning** as a DWORD set to 1 in the registry entry at HKEY_LOCAL_MACHINE/SOFTWARE/Cisco/ AnyConnect Network Access Manager. Any change to enabling this key should be fully tested with all smartcards and related hardware to ensure proper operation.

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 is described in the following sections.

- Configure an Authenticating Network—Recommended for a secure enterprise.
- Configure an Open Network—Not recommended, but can be used to provide guest access through captive portal environment. Network Access Manager does not support the automatic launch of a browser when in the captive portal state.
- Configure a Shared Key Network—Recommended for wireless networks such as small offices or home offices.

Additionally, within an open, shared, or authenticating network, you can Enable MAC Address Randomization, on page 15.

Configure an 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 these panes, 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:

Note When AnyConnect ISE Posture is installed with the Network Access Manager, ISE posture uses the Network Access Manager plugin to detect the network change events and 802.1X WiFi.

- authPeriod (sec)—When authentication begins, this setting 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 setting 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 initiates authentication with the authenticator by sending an IEEE 801.X protocol packet, EAPOL key data, or EAPoL-Start before the supplicant assumes that 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 that 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, to allow data traffic only after authentication succeeds, you 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

Appears only for wired networks.

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

- Key Management—Determine which key management protocol to use with the MACsec-enabled wired network.
  - None—No key management protocols are used, and no wired encryption is performed.

- MKA—The supplicant attempts to negotiate 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.

- Encryption
  - None—Data traffic is integrity-checked but not encrypted.
  - MACsec: AES-GCM-128—This option is available only if you chose MKA for key management. It causes data traffic to be encrypted using AES-GCM-128.
  - MACsec: AES-GCM-256—This option is supported on select IOS versions with the enterprise edge (eEdge) integration and is available only if you choose MKA for key management. It must match the setting on the switch side. By enabling the MACsec 256 encryption standard, 802.1 AE encryption with MACsec Key Agreement (MKA) is supported on downlink ports for encryption between a MACsec-capable device and host devices.

See Identity-Based Networking Services: MAC Security for more information.

Port Authentication Exception Policy Pane

This pane appears only for wired networks.

The Port Authentication Exception Policy pane enables 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 opens the port only 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—Allows data traffic prior to an authentication attempt.
- Allow data traffic after authentication even if:
  - EAP fails—When selected, the supplicant attempts authentication. If authentication fails, the supplicant allows data traffic despite the 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 valid only when key management is configured. If key management is set to none, the check box is dimmed out.

Restriction 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

The pane appears only for wireless networks.

Choose the association mode:

- WEP

- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA2 Enterprise (TKIP)
- WPA2 Enterprise (AES)
- CCKM (TKIP)—(requires Cisco CB21AG Wireless NIC)
- CCKM (AES)—(requires Cisco CB21AG Wireless NIC)

Configure 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 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.

Configure a Shared Key Network

Wi-Fi networks may use a shared key to derive an encryption key for use when encrypting data between endpoints 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**.

Step 4 Click **Next**.

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 hexadecimal 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**. Then Click **OK**.

Enable MAC Address Randomization

On Windows 10 and later only, you can enable MAC address randomization for hardware or drivers that support it. Windows uses random addresses for probe requests or for connection to a network. A per-network address is calculated to ensure that the client always uses the same address when connecting to a particular network. If a connection is forgotten and then reconnected, a new MAC address is assigned.

1. If client policy allows, check the **Enable MAC Address Randomization** checkbox on the Networks, Security Level Page, on page 11. By enabling, each wireless network utilizes a random MAC address which is retained as long as the network is not deleted from the user configuration.
2. With any security level, you can check **Change Random MAC Address Daily**, if steps 1 and 2 are completed. This option allows each wireless network to utilize a random MAC address, which is retained for 24 hours. A new random MAC address is generated upon a new connection after 24 hours have passed.

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. Choose one of the following connection types:

- Machine Connection—The device's name, as stored in the Windows Active Directory, 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 on to 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 AnyConnect Start Before Login (SBL) fails if no known network is available. Network profiles allowed in SBL mode include all media types employing non-802.1X authentication modes, such as open WEP, WPA/WPA2 Personal, and static key (WEP) networks. If you configure the Network Access Manager for Before User Logon and machine connection authorization, the Network Access Manager asks the user for network information, and the VPN SBL succeeds.

- User Connection—User credentials are used for authorization.

  If Before User Logon was selected in the Client Policy pane, the Network Access Manager gathers the user's credentials after the user enters 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, the 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 machine network profiles are available, NAM reconnects 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 valid only when a user is not logged on to the device. 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 the Network Access Manager verifies that the machine and the user are known entities, and are managed by the corporation.

  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.

Networks, User or Machine Authentication Page

After selecting the network connection type, choose the authentication method(s) for those connection types. After you select an authentication method, the display is updated to the method that 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. Also, even if MACsec is not enabled, using the Network Access Manager reduces MTU from 1500 to 1468 to account for MACsec.

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 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 to the supplicant upon successful authentication.
- 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 authenticator are forwarded to the supplicant.

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 One Time Password (OTP).

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 provides 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 OTP

Note Neither the Network Access Manager, the authenticator, nor the EAP-GTC protocol can distinguish between password and token code. These options impact only 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 the token code with every authentication).

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

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 exists.
- Digital certificates provide strong authentication protection.
- Message exchange is protected with public key encryption.

- The certificates are 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 an 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.

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.

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 fails. If mutual authentication is required, 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 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 the 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 the NT-hash of the password in the authenticator's database.

Configure EAP-TTLS

- EAP—Allows use of the following 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.

Note If you enable this, make sure that the server certificate installed on your RADIUS server contains the Extended Key Usage (EKU) of *Server Authentication*. When the RADIUS server sends its configured certificate to the client during authentication, it must have this Server Authentication setting for network access and authentication.

  - 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. Available only for Wi-Fi Media Type.

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. 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 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).

Configure PEAP

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

Note If you enable this, make sure that the server certificate installed on your RADIUS server contains the Extended Key Usage (EKU) of *Server Authentication*. When the RADIUS server sends its configured certificate to the client during authentication, it must have this Server Authentication setting for network access and authentication.

  - 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—Do not use Fast Reconnect when using a smart card for authentication. Smart cards apply only 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 logon, smart card support is not available on Windows.

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 chaining is supported when both machine and user connections are configured. That means that the Network Access Manager verifies that the machine and the user are known entities and are managed by the corporation, which is useful for controlling user-owned assets that are connected to the corporate network. 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 tunneling EAP methods, EAP-FAST provides cryptobinding between inner and outer methods, preventing the special class of man-in-the-middle attacks where an attacker hijacks a valid user's connection.

Configure EAP-FAST

- 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 in to the Network Access Manager Profile Editor task list.

Note If you enable this, make sure that the server certificate installed on your RADIUS server contains the Extended Key Usage (EKU) of *Server Authentication*. When the RADIUS server sends its configured certificate to the client during authentication, it must have this Server Authentication setting for network access and authentication.

- Enable Fast Reconnect—Enables session resumption. The two mechanisms to resume the authentication sessions in EAP-FAST are user authorization PAC, which substitutes for the inner authentication, and TLS session resumption, which allows for an 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 an 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 available only 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.
  - 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 the 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 are unsuccessful.

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 expire passwords. Cisco recommends that you use EAP-FAST, PEAP, or EAP-TLS, whose authentication methods are not susceptible to dictionary attacks.

LEAP settings, which are available only for user authentication:

- Extend user connection beyond log off—Keeps the connection open when the user logs off. If the same user logs back on, the network connection is still active.

See Dictionary Attack on Cisco LEAP Vulnerability for more information.

Define Networks Credentials

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

Configure User Credentials

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.

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

- If a client certificate is used for authentication—Obtain the placeholder values for [username] and [password] 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@example.com (where username=userA and domain=example.com) for user authentication and hostA.example.com (where username=hostA and domain=example.com) for machine authentication, the following properties are analyzed:
- If user certificate based authentication:
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@eample.com
  - Subject = .../CN=userA/DC=example/DC=com/...
  - Subject = userA (no domain)
- If machine certificate based authentication:
  - SubjectAlternativeName: DNS = hostA.example.com

- Subject = .../DC=hostA.example.com/...
- Subject = .../CN=hostA.example.com/...
- Subject = hostA.example.com

- If the credential source is the end user—Obtain the placeholder's value from the information that the user enters.
- If the credentials are obtained from the operating system—Obtain the placeholder's value from the logon information.
- If the credentials are static—Use no placeholders.

On the Credentials pane, you can specify the desired credentials to use for authenticating the associated network.

Step 1 Define a user identity for the Protected Identity Pattern. 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 device.

Step 2 Specify typical unprotected identity patterns.

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.

- 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 information 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.

Step 3 Specify the protect identities patterns.

To protect the user ID from snooping, the clear text identity may provide only enough information to enable routing of the authentication request to the correct realm.

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

Step 4 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.

Note You cannot use Windows login credentials automatically with Network Access Manager and SSO. Using SSO with Network Access Manager requires that logon credentials are intercepted; therefore, you are prompted for a reboot after an installation or a log off.

- Use Static Credentials—Obtains the user credentials from the network profiles that this profile editor provides. If static credentials fail, the Network Access Manager does not use the credentials again until a new configuration is loaded.

  Note An ampersand is an invalid character in this field.

- 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. Network Access Manager prompts the user each time it needs credential information for authentication.

Step 5 Determine which certificate source to use for authentication when certificates are required:

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

Step 6 At the Remember Smart Card Pin parameter, determine how long Network Access Manager remembers the PIN used to retrieve the certificate from 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 driver, also known as the cryptographic service provider (CSP) and the key storage provider (KSP). Increasing the connection timeout may give the network enough time to perform the smart-card-based authentication.

Configure Machine Credentials

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@example.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@example.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.

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

- If a client certificate is used for authentication—Obtain the placeholder values for [username] and [password] 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:

- If user certificate based authentication:
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@example.com
  - Subject = .../CN=userA/DC=example.com/...
  - Subject = userA (no domain)
- If machine certificate based authentication:
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- If a client certificate is not used for authentication—Obtain the credentials from the operating system, and the [username] placeholder represents the assigned machine name.

With the Credentials panel you can specify the desired machine credentials.

Step 1 Define a machine identity for the Protected Identity Pattern. 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 removed.
- [raw]—Specifies the username, exactly as entered by the user.
- [domain]—Specifies the domain of the user's PC.

Step 2 Define typical unprotected machine identity patterns.

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.

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

Step 3 Define the protected machine identity patterns.

To protect the user ID from snooping, the clear text identity may provide only 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)

Step 4 Provide further machine credential information:

- Use Machine Credentials—Obtains the credentials from the operating system.
- Use Static Credentials—Specifies an actual static password to send in the deployment file. Static credentials do not apply for certificate-based authentication.

Set up Network Access Manager to Choose Correct Certificate

When there are two certificates during client authentication, the Network Access Manager automatically chooses the best certificate based on certificate attributes. Because the criteria of what is the preferred certificate varies from customer to customer, you must configure the following fields to determine certificate selection and provide any desired rules to override certificate selection.

If multiple certificates match the same rule or none matches the rule, the ACE engine runs through an algorithm to prioritize certificates and selects one based on certain criteria (such as whether it has a private key, whether it is from the machine store, and so on). If multiple certificates are of the same priority, the ACE engine chooses the first certificate it finds within that priority.

Step 1 From the AnyConnect Profile Editor, choose the **Networks** tab.

Step 2 Choose which network to edit.

Step 3 Choose the **Machine Credentials** tab.

Step 4 At the bottom of the page, choose **Use Certificate Matching Rule**.

Step 5 From the Certificate Field drop-down menu, choose what you want to use for search criteria.

Step 6 From the Match drop-down menu, determine if the search includes an exact match on the field (Equals) or a part of the field to match (Includes).

Step 7 In the Value field, enter the certificate search criteria.

Configure 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 is 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 select 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 pane, 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 **Add** to import the CA certificate into the configuration. If the certificate being used is being exported from the Windows certificate store, use the "Base 64 encoded X.509 (.cer)" option.

Network Groups Window

In the Network Groups window, you assign network connections to particular groups. 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. Enables 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 perform only sort order edits on this type of network.

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

Step 1 Choose a group by selecting it from 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, 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 scan list 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 Those 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.