Cisco Secure Services Client Administrator Guide

Software Release 5.1.1

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-15540-02

Cisco Secure Services Client Administrator Guide, Release 5.1

CONTENTS

Preface

The preface provides an overview of the *Cisco Secure Services Client Administrator Guide, Release 5.1.1*, references related publications, and explains how to obtain other documentation and technical assistance.

The following topics are covered in this section:

Audience and Scope

This publication is for system and IT administrators responsible for configuring and deploying a derived, end user version of Cisco Secure Services Client (SSC) in multiple end user machines used by your various enterprise departments/organizations. By using the information supplied in this document, you will be able to fully define and customize the following for the end user machines that you support:

- Policy—Defines the capabilities and user experience of the deployed SSC.
- Networks—Defines the configuration of all enterprise network connections that you control.

Organization

This guide contains the following sections:

Chapter 1, "802.11 Network Security Fundamentals," provides an overview of the fundamental components of network security.

Chapter 2, "Setting Up Cisco SSC," describes how to set up the SSC.

Chapter 3, "Deploying or Installing Cisco SSC," describes how to deploy and install SSC.

Chapter 4, "Using Cisco SSC," describes how to use Cisco SSC.

Chapter 5, "Troubleshooting End User Wireless Networks," describes how to troubleshoot the user's wireless network problems.

Chapter 6, "Frequently Asked Questions," provides a list of frequently asked SSC questions.

Chapter 7, "SSC FIPS 140-2 Level 1 Validation" provides a FIPS deployment example using the SSC management utility GUI.

Appendix A, "Cisco SSC 5.1 Log Messages," lists the log messages produced by the SSC Release 5.1.1 client.

Appendix B, "Notices," contains OpenSSL and SSLeay license agreements.

Appendix C, "Configuring a Single-User Account for FIPS," contains instructions for configuring a FIPS single user account.

Conventions

This publication uses the following conventions to convey instructions and information:

- For utility commands
  - Commands are in **boldface** type.
  - Variables are in *italic* type.
- For schema objects.
  - Element and attribute names when used in the text are in *italic* type.
- Notes use the following conventions and symbols:

Note Means *reader take note*. Notes contain addition information for the subject at hand or references to materials not contained in this manual.

Tip Tips contain helpful suggestions.

Related Publications

For more information about Cisco Secure Services Client, refer to these publications:

- *Cisco Secure Services Client Release Notes*—Describes new features and the open and resolved caveats in each SSC release.

You can find these Cisco SSC technical documents at this URL:

http://www.cisco.com/en/US/products/ps7034/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

802.11 Network Security Fundamentals

This chapter provides an overview of the 802.11 network security features and contains these sections:

Introduction

This section is intended for system administrators planning an enterprise wireless LAN deployment and provides an overview of the main 802.11 security features currently available. The chapter focuses on Wi-Fi Protected Access (WPA) and WPA2, but also briefly covers the older Wired Equivalent Privacy (WEP) feature.

WEP is the initial security mechanism specified in the original 802.11 standard and was superseded by the 802.11i standard update. The 802.11 standard initially had security flaws that were resolved with the introduction of the 802.11i standard update. These new security enhancements address the enterprise requirements for confidential communications through the use of authentication and encryption.

Terminology

This document uses a number of common terms for basic physical components in the wireless system. Figure 1-1 illustrates the system topology of these components: the wireless LAN client, access point, wireless LAN controller (WLC), and AAA (authorization, authentication, and accounting) server.

Figure 1-1 Secure Wireless Topology

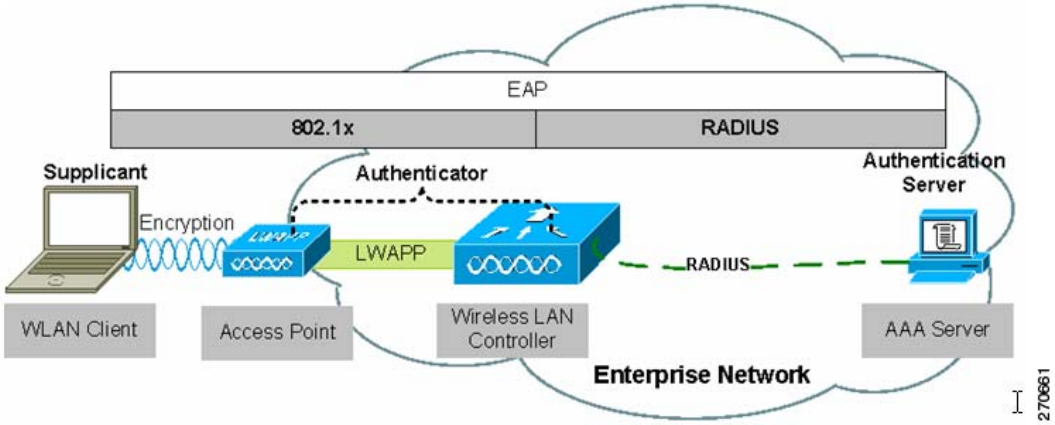


Figure 1-1 also illustrates the basic roles and relationships of the 802.1X authentication process. The 802.1X supplicant (Cisco Secure Services Client) resides on the wireless LAN client, the access point and the WLC, through the split-MAC architecture, act as the 802.1X authenticator, and the AAA server is the authentication server. This figure also illustrates the role of 802.1X and the RADIUS protocol in carrying EAP (Extensive Authentication Protocol) packets between the client and the authentication sever. For additional information on 802.1X, refer to the "IEEE 802.1X" section on page 1-6 . For additional information on EAP, refer to the "EAP" section on page 1-7.

IEEE 802.11 Fundamentals

An 802.11 wireless LAN consists of the following basic components and behaviors:

- Beacons—Used to indicate the presence of a wireless LAN network.
- Probe—Used by wireless LAN clients to find their networks.
- Authentication—A feature defined in the original 802.11 standards.
- Association—The process of establishing a link between an access point and a wireless LAN client.

Beacons are regularly broadcast by an access point, but the probe, authentication, and association frames are generally only used during the association and reassociation processes.

Beacons

The wireless LAN beacon frame contains configuration information about the access point, such as the SSID (service set identifier or the network name), the supported bit rates, and the security configuration for that wireless LAN.

The primary purpose of the beacon is to allow wireless LAN clients to know what networks are available in the area. This allows the wireless LAN clients to choose a network to try to associate with.

Many wireless LAN security documents suggest that sending beacons without the SSID is a security best practice, to help prevent potential hackers from learning the SSID. All enterprise wireless LAN solutions offer this capability as an option, but this option has little value because the SSID can be easily discovered during an association attempt. Also some wireless LAN clients rely upon the SSID

information in the beacon and do not reliably associate with wireless LANs that do not advertise the SSID information. For these reasons, it is best to allow the SSID information to be broadcast in the beacon.

Association—The Join Process

With the exception of fast roaming, an 802.11 client must go through a three-stage process before being allowed to send data over a wireless LAN network:

1. Find a suitable wireless LAN network—For an enterprise deployment, the search for a suitable network involves the sending of a probe request on multiple channels and specifying the network name (SSID), bit rate requirements, and required security configuration.
2. 802.11 authentication—802.11 supports two authentication mechanisms: open authentication and shared key authentication. Open authentication is fundamentally a NULL authentication in which the client requests to be authenticated and the access point responds positively. The 802.11 shared WEP key authentication implementation is flawed, but it must be included for compliance with the standards. Shared key authentication is not recommended and should not be used.

   Open authentication is the only mechanism used in enterprise wireless LAN deployments. As previously indicated, open authentication is fundamentally a NULL authentication, and the real authentication occurs after association through the 802.1X and EAP authentication mechanisms.
3. 802.11 associations—This stage finalizes the security and bit rate options and establishes the data link between the wireless LAN client and the access point. A secure enterprise wireless LAN access point blocks all of the wireless LAN client traffic at the access point until a successful 802.1X authentication. If a client has joined a network and roams from one access point to another network the association is called a *reassociation*. The primary difference between an association and a reassociation is that a reassociation sends the basic MAC address (BSSID) of the previous access point in the reassociation request to provide roaming information to the extended network.

Probe Request and Probe Response

SSC can be configured with the wireless LAN networks, which enables the wireless LAN client to send a probe request that contains the SSID of the desired wireless LAN network.

If the wireless LAN client is trying to discover the available wireless LAN networks, it can send out a probe request without an SSID. When this occurs, all access points that are configured to respond to this type of query send a probe response. Wireless LANs without broadcast SSID enabled do not respond.

Association

The association and association response frames provide the final agreement for the data rates and security settings. After this process is completed, 802.11 data frames can be sent between the wireless LAN client and the wireless LAN access point. In an enterprise wireless LAN deployment, these data frames are limited to 802.1X frames between the wireless LAN client and the access point until the 802.1X or EAP authentication is completed and successful.

The association process also has a related disassociation frame used to disconnect a wireless LAN client from its access point. The disassociation frame can only be a unicast frame.

Reassociation

Reassociation occurs when a wireless client temporarily moves out of range of an access point or roams to another access point. The reassociation process is similar to the association process, except that when roaming is involved, the new and old access points communicate on the wired network to move wireless client information between each other.

When the wireless client roams to a new access point, the reassociation process is used to inform the 802.11 network that the client has moved to a new location. The wireless client issues a reassociation frame to the new access point, which identifies the old access point. The new access point communicates with the old access point over the wired link to verify that the wireless client was previously associated. If the wireless client was previously associated, the new access point issues a reassociation response frame to the wireless client; otherwise, it issues a disassociation frame. After sending the reassociation response, the new access point contacts the old access point over the wired link to complete the reassociation process. Any buffered frames at the old access point are transferred to the new access point. After completing the reassociation process, the new access point begins processing frames from the wireless client.

Authentication

As previously stated, there are two 802.11 authentication modes: open-mode and shared-mode. 802.11 authentication alone provides only nominal security and is mostly used in a home wireless network in which network security is not a major concern. Home users who need to join their enterprise networks using access points that are not configured for 802.1X must establish a VPN connection using SSC. For more information on VPN, refer to the "VPN Integration" section on page 2-38.

Another frame type related to authentication frames is the deauthentication frame. When a deauthentication frame is received by a wireless LAN client, the client is disconnected from the access point. This might cause a wireless LAN client to go through the entire probe request process again or cause the client to restart the authentication association process again. Deauthentication frames can be sent to the broadcast MAC address.

Wireless Network Security Concepts

Security should be considered a network design component that needs to be integrated and not something that is added later. Security also needs to be subjected to the same cost/benefit analysis and usability considerations as the rest of the network components.

Enterprise security discussions consistently indicate that the wireless LAN's RF signals typically travel beyond the deployed building's perimeter. This allows the network to be monitored and attacked from beyond the property line. However, the range for this type of attack is very limited. To make any attack feasible an attacker with the appropriate skills needs to be in physical proximity to a wireless LAN. This requires the attacker to roam extensive areas looking for a suitable wireless LAN. An 802.1X framework for access control coupled with other wireless environment management tools can severely restrict the feasibility of such attacks. The location of an enterprise, and the type of business operated by that enterprise, will determine any recommended augmentation of the native wireless LAN security.

Physical Security

Hostile activities are equally applicable to all networks and can be broadly broken down into:

- Intelligence gathering—Normally aids in gaining unauthorized access to enterprise resources but can be for other reasons, such as to determine the location of key individuals or activity. The choice of EAP type used in authentication and the configuration of the supplicant can determine whether username information is exposed during authentication.
- Unauthorized access—The authentication and encryption in 802.11 security can protect sessions, but policies and processes do need to be in place to protect equipment and passwords. This is generally addressed in two ways:
  - End node security to protect mobile devices not directly related to the wireless LAN. This type of security needs to be assessed with a understanding of the end node's mobility.
  - WPA or WPA2 for wireless LAN clients that provides authentication of users and confidentiality of user communication over the wireless LAN.
- Denial of service—A wireless LAN network attack that prevents legitimate wireless users from accessing information or services on the network. This attack typically uses 802.11 management frames or RF interference in the same spectrum as the wireless LAN network. This type of attack is addressed through RF management and wireless IDS features (WIDS).

Regulation, Standards, and Industry Certifications

Most network system standards are typically from the Institute of Electrical and Electronic Engineers (IEEE) and the Internet Engineering Task Force (IETF). The two core standards introduced in secure wireless LAN deployment are the 802.11 standards defined by the IEEE and the EAP standards defined by the IETF.

IEEE

The IEEE owns the 802.11 group of standards. The original 802.11 standard was published in 1999 and there have been a number of amendments to the standard. These amendments have added different physical layer implementations, provided greater bit rates (802.11b, 802.11a, and 802.11g), added quality of service (QoS) enhancements (802.11e), and added security enhancements (802.11i).

The IEEE also owns the 802.1X standard for port security that is used in 802.11i for authentication of wireless LAN clients.

IETF

The main IETF Request For Comments (RFCs) and drafts associated with wireless LANs are based upon the Extensible Authentication Protocol (EAP). The advantage of EAP is that it decouples the authentication protocol from its transport mechanism. EAP can be carried in 802.1X frames, PPP frames, UDP packets, and RADIUS packets.

EAP is carried over the wireless LAN in 802.1X frames and in RADIUS packets between the access points and the AAA server. This provides an end-to-end EAP authentication between the wireless LAN client and the AAA server. See the "EAP" section on page 1-7.

Wi-Fi Organization

In wired networks it is common for devices to be from the same vendor where integration is part of product testing. When different vendor devices are combined into the same network, interoperability and integration must be managed and controlled by a group of network specialists who understand the devices and their interaction.

In wireless networks that include devices from many vendors, the wireless standards allowed different interpretations and optional features to be developed. A group of industry companies and organizations formed the Wi-Fi Alliance (www.wi-fi.org) to certify wireless LAN interoperability through WPA, WPA2, and Wi-Fi Multimedia (WMM) certification programs.

The WPA standard was developed to address the weakness in the WEP encryption process prior to the ratification of the 802.11i work group standard. One of the key development goals was to make it backward compatible with WEP hardware. This allowed the continued support of the base RC4 encryption used in WEP, but added keying enhancements and message integrity check improvements that addressed the weaknesses in WEP encryption.

WPA2 is based upon the ratified 802.11i standard and uses AES-CCMP encryption. This encryption requires new client and access point hardware. Due to the long upgrade cycles for laptops and client devices, a mixed WPA and WPA2 environment will exist for some time. In a greenfield enterprise deployment (without constraints imposed by prior implementations), it is expected that customers will be able start with WPA2.

Cisco Compatible Extensions

The Cisco Compatible Extensions (CCX) program ensures the widespread availability of wireless client devices that are compatible with a Cisco wireless LAN infrastructure and take advantage of Cisco innovations for enhanced security, mobility, quality of service, and network management.

IEEE 802.1X

IEEE 802.1X is an IEEE standard framework for port based access control that has been adopted by the 802.11i security workgroup as the means of providing authenticated access to wireless LAN networks.

- The 802.11 association process creates a virtual port for the wireless LAN client on the access point.
- The access point blocks all data frames apart from 802.1X traffic.
- The 802.1X frames carry the EAP authentication packets, which are passed through to the AAA server by the access point.
- If the EAP authentication is successful, the AAA server sends an EAP-success message to the access point. The access point then allows data traffic from the wireless LAN client to pass through the virtual port.
- Prior to opening the virtual port, data link encryption was established between the wireless LAN client and the access point. This ensures that another wireless LAN client cannot access the port that has been opened for the authenticated client.

EAP

EAP is an IEFT RFC that addresses the requirement for an authentication protocol to be decoupled from the transport protocol carrying it. This allows the EAP protocol to be carried by transport protocols, such as 802.1X, UDP, or RADIUS without changes to the authentication protocol.

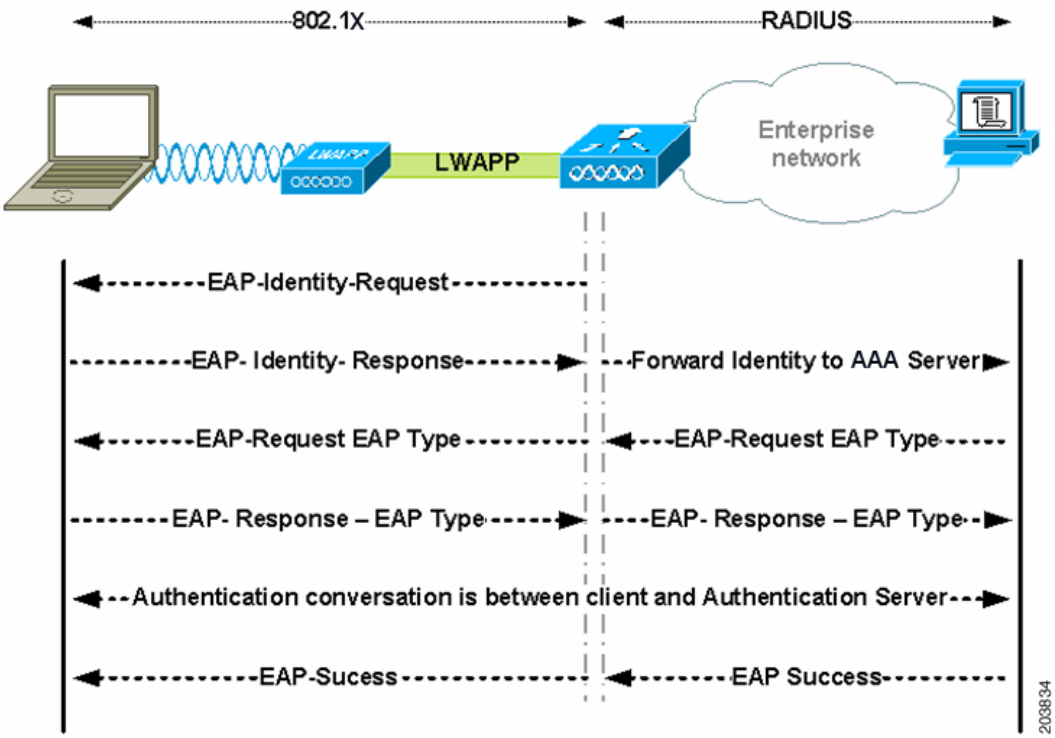
The basic EAP protocol is relatively simple and made up of four packet types:

- 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 be used. 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 unsuccessful authentication to the supplicant.

When EAP is in use in an 802.11i system, the access point is operating 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 1-2 illustrates the EAP protocol messages.

Figure 1-2 EAP Protocol Flow



EAP-FAST

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

EAP-FAST was developed for customers who want to deploy an 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).

EAP-TLS

EAP-Transport Level Security (EAP-TLS) is an 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, and private key exchange and verification between the client and the authenticating server.

The list below indicates the main reasons why using EAP-TLS client certificates provides strong authentication for wireless connections:

- Authentication occurs automatically, usually with no intervention by the user.
- Does not require dependency on a user password.
- Uses digital certificates for 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-TTLS

EAP-Tunnelled 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. The attributes tunneled during Phase 2 can be used to perform additional authentications using a number of different mechanisms.

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 establish its identity on initial link establishment.An ID/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.
- CHAP (Challenge Handshake Authentication Protocol)—Uses a three-way handshake to periodically verify the identity of the peer.

- MS-CHAP (Microsoft CHAP)—Uses a three-way handshake to periodically verify the identity of the peer.
- MS-CHAPv2—Provides mutual authentication between peers by including a peer challenge in the response packet and an authenticator response in the success packet.
- EAP—Allows use of these EAP methods:
  - EAP MD5 (EAP-Message Digest 5)—EAP-MD5 is an EAP security algorithm that uses a 128-bit generated number string, or hash, to verify the authenticity of the data packets.
  - EAP MSCHAPv2—Uses a three-way handshake to periodically verify the identity of the peer.

EAP-PEAP

EAP-PEAP is an 802.1X EAP authentication type that takes advantage of server-side EAP-TLS and supports a variety of different authentication methods, including certificates, tokens, logon passwords, and one-time passwords (OTPs).

EAP-PEAP protects the EAP methods by providing these services:

- Creates a TLS tunnel for the EAP packets
- Message authentication
- Message encryption
- Authentication of server to client
- Key exchange to establish dynamic WEP or TKIP keys

These authentication mechanisms can be used:

- Password
  - EAP MSCHAPv2—Uses a three-way handshake to periodically verify the identity of the peer.
  - EAP GTC (EAP Generic Token Card)—Defines an EAP envelope to carry the user password.
- Token
  - EAP GTC—Defines an EAP envelope to carry a user OTP generated by a token card.
- Certificate
  - EAP TLS—Defines an EAP envelope to carry the user certificate.

Authentication

Depending upon the customer requirements, different authentication mechanisms are used in a secure mobility environment, but all of the mechanisms use 802.1X, EAP, and RADIUS as their supporting protocols. These protocols allow access to be controlled based upon the successful authentication of the wireless LAN client and allows 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 performing authentication is described in more detail in the following sections, but the primary factor affecting the choice of 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.

Supplicants

The software clients used for 802.1X authentication are generally called *supplicants* and are based upon 802.1X terminology. SSC is a supplicant for wired and wireless networks. It supports a number of different EAP methods that map appropriately to different authentication system requirements of customers. Common EAP methods supported by SSC are listed below:

- Protected EAP (PEAP) MSCHAPv2—Uses a Transport Layer Security (TLS) tunnel to protect an encapsulated MSCHAPv2 exchange between the wireless LAN client and the authentication server.
- PEAP GTC (Generic Token Card)—Uses a TLS tunnel to protect a generic token card exchange.
- EAP-Flexible Authentication via Secured Tunnel (FAST)—Uses a tunnel to protect the exchange.
- EAP-TLS—Uses mutual authentication based on X.509 digital certificates.

Table 1-1 lists a summary of common EAP methods:

Table 1-1 Feature Comparison of EAP Methods with Cisco SSC

Feature	Cisco EAP-FAST	PEAP MS-CHAP v2	PEAP EAP-GTC	EAP-TLS
Single sign-on (Microsoft Active Directory only)	Yes	Yes	Yes	Yes
Login scripts (Microsoft Active Directory only)	Yes	Yes	Some	Yes
Password change (Microsoft Active Directory only)	Yes	Yes	Yes	–
Microsoft Active Directory database support	Yes	Yes	Yes	Yes
Access Control Server (ACS) local database support	Yes	Yes	Yes	Yes
Lightweight Directory Access Protocol (LDAP) database support	Yes	No	Yes	Yes
One-time-password (OTP) authentication support	Yes	No	Yes	No
RADIUS server certificate required	Yes	Yes	Yes	Yes
Client certificate required	No	No	No	Yes
Anonymity	Yes	Yes	Yes	No

Authenticator

The authenticator in the Cisco Secure Mobility Solution is the WLC that processes the incoming 802.1X frames from the wireless LAN access points, and acting in EAP pass-through mode, it relays the EAP packets to and from the 802.1X frames and the RADIUS packets.

Upon the completion of a successful authentication, the WLC receives a RADIUS packet that contains an EAP success message, an encryption key that was generated at the authentication server during the EAP authentication, and RADIUS extensions for communicating policy.

Refer to Figure 1-1 to see the location of the authenticator within the overall authentication process. The authenticator controls network access through the 802.1X mechanism and relays EAP messages between the supplicant and the authentication server.

Authentication Server

The authentication server used in the Cisco Secure Mobility Solution is the Cisco Access Control Server (ACS). Cisco ACS is available as software installable on a Windows 2000 or 2003 server or as an appliance. The authentication server can also be embedded into wireless LAN infrastructure devices; for example, it could be the local authentication services on an access point running Cisco IOS software or the AAA services included in the Cisco WLSExpress.

The authentication server performs the EAP authentication over a RADIUS tunnel.

Upon the completion of a successful EAP authentication, the authentication server sends an EAP success message to the authenticator. This message tells the authenticator that the EAP authentication process was successful and passes the Pairwise Master Key to the authenticator. The master key is used to create the encrypted stream between the wireless LAN client and the access point.

Encryption

There are two enterprise level encryption mechanisms specified in 802.11i: WPA and WPA2. These encryption types are Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

TKIP, the encryption certified in WPA, provides support for legacy wireless LAN equipment by addressing the flaws in WEP while still supporting the core encryption algorithm (RC4). The hardware refresh cycle of the client devices is such that TKIP is likely to be a common encryption mechanism for a number of years. While TKIP addresses all the known weaknesses of WEP, the AES encryption of WPA2 is the recommended encryption mechanism because it brings the wireless LAN encryption into alignment with current encryption best practice.

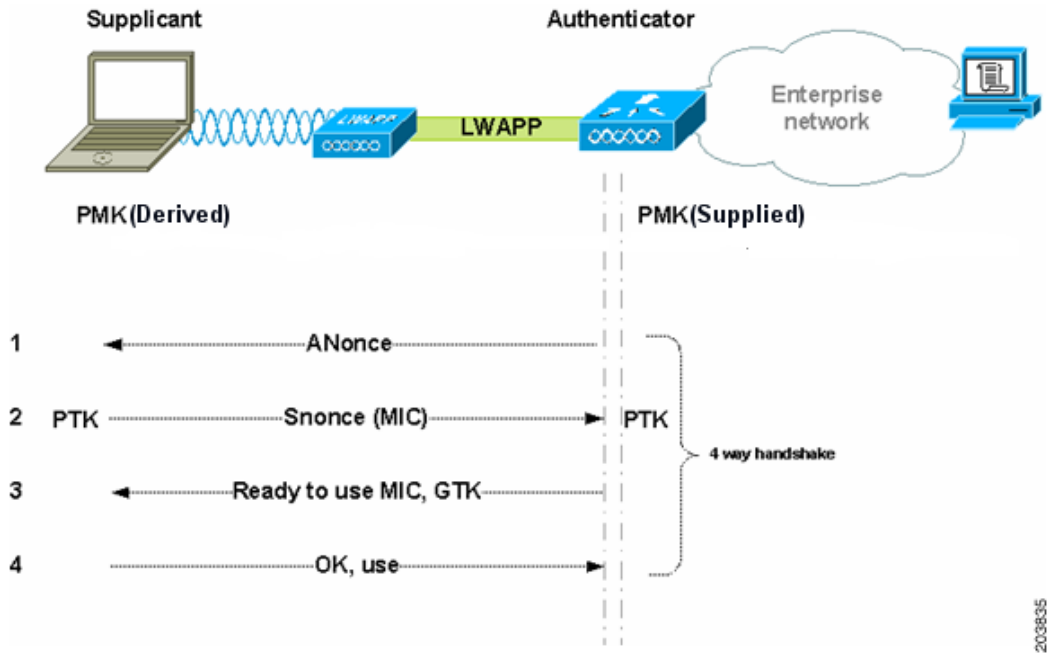
The two primary mechanisms in TKIP are the generation of a per packet key for RC4 encryption of the MSDU (MAC Service Data Unit) and an additional Message Integrity Check (MIC) for the encrypted packet.

AES Counter Mode/CBC MAC Protocol (CCMP) is the AES encryption mode used in 802.11i in which the counter mode provides confidentially and CBC MAC provides message integrity.

Four-Way Handshake

The four-way handshake describes the mechanism used to derive the encryption keys used to encrypt wireless data frames. Figure 1-3 shows a schematic of the frame exchanges used to generate the encryption keys. These keys are referred to as *temporal keys*.

Figure 1-3 Four-Way Handshake



The keys used for encryption are derived from the Pairwise Master Key (PMK) that has been mutually derived during the EAP authentication section. This PMK is sent to the authenticator. The PMK is not forwarded to the supplicant because the supplicant has derived its own copy of the PMK.

The four-way handshake consists of these events:

1. The authenticator sends an EAPOL-Key frame containing an ANonce (Authenticator Nonce—a random number generated by the authenticator).
   - The Supplicant derives a Pairwise Temporal Key (PTK) from ANonce and SNonce (Supplicant Nonce—a random number generated by the supplicant).
2. The supplicant sends an EAPOL-Key frame containing SNonce, the RSN information element from the reassociation request frame, and a Message Integrity Check (MIC).
   - The authenticator derives PTK from ANonce and SNonce and validates the MIC in the EAPOLKey frame.
3. The authenticator sends an EAPOL-Key frame containing ANonce, the RSN information element from its beacon or probe response messages, MIC, whether to install the temporal keys, and the encapsulated Group Temporal Key (GTK—the multicast encryption key).
4. The supplicant sends an EAPOL-Key frame to confirm that the temporal keys are installed.

Seamless Connectivity

To achieve wireless mobility, the network administrator needs to perform a site survey to ensure that the enterprise premise has adequate wireless coverage. Cisco provides wireless spectrum analysis tools and applications that help achieve a balanced and well-designed wireless infrastructure.

Enterprise network infrastructures are based on both wired and wireless media in which wireless media provide better mobility and wired media often provide much greater speeds and throughput. Both wired and wireless connections should be able to restore mapped network drives, run log-on scripts, execute computer group policy objects (GPOs) and user GPOs, and perform tasks that require network connections when a user logs in to a wireless LAN client PC or reboots. In addition, the wireless LAN client should be able to restore connectivity after resuming from a client suspension or hibernation.

Most enterprise environments require that end users be able to have connectivity when they undock their workstations or detach the Ethernet cable and move to another location, such as a conference room. In a typical enterprise, a lack of connection is acceptable while the user is in transit. However, when he arrives at the new location, he should be able to easily regain connectivity. Other enterprises may require connectivity while in transit as they may have application that may require continuous connectivity such as Voice-over-IP (VoIP) applications. Wireless roaming addresses these concerns in a wireless network infrastructure.

Roaming

The end user should be able to:

- Easily switch from a wired connection to a wireless connection and back again.
- Roam from one access point with a lower signal strength to another access point with a better signal strength that has the same SSID.

Roaming from one access point to another requires a disassociation with the previous access point and an association with the new access point. This process leads to a termination of existing network connections, especially in an enterprise environment that requires 802.1X. Roaming is followed by an 802.1X authentication. This whole process may take 30 seconds or more.

Session resumption reduces the reconnection time during an 802.1X reauthentication provided that EAP-TLS, EAP-FAST, or EAP-PEAP is the deployed authentication method.

Session Resumption

A typical EAP-TLS handshake takes many packet exchanges before an EAP success message is generated, which is followed by a four-way handshake to establish the encryption keys. When using a centralized backend authentication server, session resumption provides a simpler authentication handshake when roaming to a new access point by leveraging session state information from the user's previous authentication session. This reduces the number of the handshake packet exchanges.

Although this action reduces the time for reconnection, it still does not suffice for real-time applications such as Voice-over-IP (VoIP) running on the wireless LAN client that require the reconnection time to be between 50 and 200 ms.

The wireless network framework supports fast secure roaming where authenticated client devices can roam securely from one access point to another without any perceptible delay during reassociation. Fast secure roaming also supports latency-sensitive applications such as wireless VoIP.

Fast Secure Roaming

Fast roaming is most pertinent for hand-held devices using Wi-Fi applications dealing with real-time data. There are two main techniques that help achieve fast roaming: Cisco's CCKM and 802.11i PMKID caching.

In both the approaches, the wireless infrastructure pre-establishes the needed key material that was previously derived from 802.1X authentication for the neighboring access points.

Once connected to an access point, 802.11i PMKID caching allows the list of neighboring access points to be shared with the wireless LAN client, and then 802.11i PMKID tunnels the 802.1X authentication (referred to as pre-authentication) between other access points and the wireless LAN client over the existing wireless connection. When the wireless LAN client actually roams from one access point to another, it looks up its neighboring access point and uses the applicable PMK to perform just the four-way handshake to establish connectivity after association.

CCKM uses a different method. If the wireless network infrastructure is based on Cisco access points, the wireless LAN client can avoid a pre-authentication and a four-way handshake so that fast roaming is achieved during reassociation to another Cisco access point.

CHAPTER 2

Setting Up Cisco SSC

This chapter provides an overview of the Cisco Secure Services Client and provides instructions for adding, configuring, and testing the user profiles. This chapter contains these sections:

Introduction

The Cisco Secure Services Client (SSC) is client software that provides 802.1X (Layer 2) and device authentication for access to both wired and wireless networks. SSC manages user and device identity and the network access protocols required for secure access. It works intelligently to make it simple for employees and guests to connect to an enterprise wired or wireless network.

SSC supports these main features:

- Wired (802.3) and wireless (802.11) network adapters
  - SSC is single-homed—only one network adapter can be used
  - SSC prioritizes wired network adapters over wireless network adapters
- Integrated VPN support
- Authentication using Windows machine credentials (when using Windows Vista, see the "SSC Differences with Windows Vista" section on page 2-3)
- Single sign-on user authentication using Windows logon credentials
- Simplified and easy-to-use 802.1X configuration

- EAP methods (when using Windows Vista (see the "SSC Differences with Windows Vista" section on page 2-3):
  - EAP-FAST, EAP-PEAP, EAP-TTLS, EAP-TLS, and LEAP (EAP-MD5, EAP-GTC and EAP-MSCHAPv2 for 802.3 wired only).
- Inner EAP methods (when using Windows Vista (see the "SSC Differences with Windows Vista" section on page 2-3):
  - PEAP—EAP-GTC, EAP-TLS, and EAP-MSCHAPv2
  - EAP-FAST—EAP-GTC, EAP-TLS, and EAP-MSCHAPv2
  - EAP-TTLS—EAP-MD5 and EAP-MSCHAPv2 (also legacy protocols—PAP, CHAP, MSCHAP, and MSCHAPv2)
- Encryption modes:
  - Static WEP (Open or Shared), dynamic WEP (generated with 802.1X), TKIP and AES
- Key establishment protocols:
  - WPA, WPA2/802.11i and CCKM (selectively, depending on the 802.11 NIC adapter)
- Smartcard-provided credentials (see the "SSC Differences with Windows Vista" section on page 2-3)

Supported Operating Systems

The supported operating systems are:

- Windows Vista Business, Enterprise and Ultimate Editions—32-bit and 64-bit
  - Required Windows Hot Fixes:

    KB952613
    KB935222 or SP1
    KB932063 or SP1
- Windows XP Professional (SP2)—32-bit
- Windows 2000 (SP4)—32-bit
- Windows 2003 Server Enterprise Edition (SP2)—32-bit

Note Other Windows XP versions, such as Media Center, Tablet PC, and Professional x64 are not supported. Other Windows Vista versions, such as Home Premium and Home Basic are not supported.

Note The latest drivers should be loaded on the user's PC prior to installing SSC.

Note Cisco strongly recommends that you install Windows Vista Service Pack 1. However, SP1 is required if wired network connections are to be attempted before user logon.

SSC Differences with Windows Vista

When using Windows Vista, SSC has these differences when compared to Windows XP:

- Wired Networks—SSC supports a single wired network per group.
- These EAP methods are not supported:
  - EAP-MD5
  - EAP-MSCHAPv2
  - EAP-GTC
  - EAP-TLS
  - EAP-TTLS
  - PEAP-TLS
- Machine Authentication
  - SSC ignores all static machine credentials stored in the configuration; SSC uses the machine's password or certificate instead.
  - The [username] identity patterns specified in the configuration is always expanded to *host/(fully qualified domain name)*.
  - For EAP-FAST and PEAP, the inner EAP method specified in the configuration might be ignored; the EAP method negotiates the best inner method with the AAA server.
  - Configurations that specify a different EAP method for machine authentication from what is specified for user authentication are translated to use the same EAP method specified for user authentication.
- Credential Caching
  - The *forever* credential caching option is not supported. For configurations with the *forever* credential cashing setting, the credentials are cached until the user logs off.
- Single Sign On—When configured to use single sign on credentials with an inner method of GTC, it is possible that at some point, such as when authentication fails, the user will be prompted for their password.
- Server Validation
  - The Personal stores are not used for server validation.
  - When the configuration specifies *validateChainWithAnyCaFromOs*, the certificate must be installed in the Local Computer\Trusted Root store.
  - Any Root CA certificate included in the configuration is ignored and the configuration is translated to *validateChainWithAnyCaFromOs*. The Root CA certification must be installed by some other means.
  - The certificate store is limited to *Local Computer* during machine authentication and user authentications when the connection is attempted before Windows logon.
- EAP-LEAP
  - EAP-LEAP does not work with all versions of ACS. ACS versions which are known to not work include: 3.2.3 and 3.3.1.11. Versions which have been tested and work include 3.3.1.16, 3.3.2.2, and 3.3.4.12.

- EAP-FAST
  - Supports anonymous TLS renegotiation.
  - All PACs contained in the configuration are ignored.
  - To use authenticated provisioning, the configuration must specify server validation. When server validation is not used, the authentication fails and the ACS server reports an *EAP type not configured error.*
  - When using TLS, the protected identity pattern is ignored.
  - Unless the radius server is configured to allow anonymous TLS renegotiation, when a PAC is received using un-authenticated provisioning, a user must wait for the connection timer to expire before an authentication attempt can be made.
- Smart Card Support—Smart cards are not supported.
- SofToken II—Not supported on Windows Vista. For configurations specifying SofToken II, SSC prompts the user for the username and the unique one-time password (OTP) rather than the username and password for the soft token account.
- Logging—The EAP log entries may appear out of order in the log file, but the time and date stamps are correct.
- Group Policy Object (GPO)—-SSC does not support working with wired and wireless group policy objects; all other types of group policy objects are supported.
- Automatic connection mode—SSC actively scans for the networks defined in the configuration file rather than attempting to sequentially connect to each configured network connect until a connection is established (called walk-the-list). Consequently, it may appear that SSC skips over networks without attempting to connect.

Obtaining SSC Software

SSC software packages are available for the Windows Vista and the Windows XP operating systems.

SSC Software for the Windows Vista Operating System

SSC 5.1.1 software is available from the Cisco Software Center:

- SSCMgmtToolKit_5.1.1.zip—Contains the sscManagementUtility and support files.
- Cisco_SSC-Vista_5.1.0.zip—Contains the SSC files. For license information, see the "SSC License Information" section on page 2-5.
- CiscoClientUtilities_5.1.0.zip—Contains the Log Packager.

The SSC software can be obtained from the Cisco Software Center at this URL

http://www.cisco.com/public/sw-center/index.shtml

Click **Wireless Software** > **Client Adapters and Client Software** > **Cisco Secure Services Client** > **Windows Vista** and follow the prompts to 5.1.0 under Latest Releases.

Note You must register with Cisco.com or be a registered user to download software.

SSC Software for the Windows XP Operating System

SSC 5.1.0 software is available from the Cisco Software Center:

- SSCMgmtToolKit_5.1.0.zip—Contains the sscManagementUtility and support files.
- Cisco_SSC-XP2K_5.1.0.zip—Contains the SSC files. For license information, see the "SSC License Information" section on page 2-5.
- CiscoClientUtilities_5.1.0.zip—Contains the Log Packager.

The SSC software can be obtained from the Cisco Software Center at this URL

http://www.cisco.com/public/sw-center/index.shtml

Click **Wireless Software** > **Client Adapters and Client Software** > **Cisco Secure Services Client** > **Windows XP** or **Windows 2000** and follow the prompts to 5.1.0 under Latest Releases.

Note You must register with Cisco.com or be a registered user to download software.

SSC License Information

The SSC software obtained from the Cisco Software Center on Cisco.com contains two special licenses and their associated limitations:

- A 90-day trial license for both wired and wireless functions. This license is a full-featured SSC license, but is limited to an evaluation period of 90 days (see http://www.cisco.com/en/US/docs/wireless/wlan_adapter/secure_client/product/notes/sscLicense.html). After 90 days, to use the full features, you are expected to purchase a permanent license from Cisco.
- Permanent wired-only license. This license allows a limited subset of the full-featured 90-day trial SSC license. To obtain full functionality, you are expected to purchase a permanent license from Cisco.

To obtain additional information on the features supported in these special licenses, refer to the *Cisco Secure Services Client Version 5.1 Bulletin* available on Cisco.com an this URL:

http://www.cisco.com/en/US/products/ps7034/prod_bulletins_list.html

Note When the trial license period has expired and the user attempts to use a non-supported feature, SSC displays a pop-up message that instructs the user to contact their system administrator. If the license has expired, this message can occur each time SSC starts. The message continues until the user obtains a non-expiring license.

The SSC 5.1 non-expiring license can be ordered from Cisco using these product numbers for your operating system:

- AIR-SC5.0-XP2K—For Windows 2000 and Windows XP
- AIR-SC5.0-VISTA—For Windows Vista

Network Administrator and End User Experience

A typical enterprise user does not know about 802.1X or EAP methods. The user's primary concern is to get easily connected to wired and wireless connections using simple mouse clicks. SSC is designed to provide a simple user experience by hiding as much complexity as possible.

As the network administrator, however, you need the flexibility to configure and customize SSC for the enterprise deployment requirements. The SSC management utility is designed to support your administrator configuration needs. The following sections describe how to use the SSC management utility.

SSC Management Utility

The SSC management utility is designed for system administrators as a standalone application enabling you to create and edit SSC configuration profiles and create pre-configured client packages. The pre-configured client packages are deployed to end user PCs.

The management utility has two modes of operation: A graphical user interface (GUI) and a command line interface (CLI) that allows system administrators to perform certain operations through the command line.

Note For Windows Vista, the SSC management utility (by default) must be run with administrator privileges. Other users can be given permission to run the management utility by changing the permissions in the *C:\ProgramData\Cisco\Cisco Secure Services Client\newConfigFiles* directory.

In instances where the user does not have sufficient privileges to save the file in the newConfigFiles directory and User Access Control is enabled, the management utility does not display an error and appears to work normally. However, the changes do not have an effect on the running system because Windows Vista redirects the changed configuration file to the virtual store located in the folder: *C:\Users\%username%\AppData\Local\VirtualStore\ProgramData\Cisco\Cisco Secure Services Client\newConfigFiles*.

Command-Line Operation

The syntax of the command-line version of the management utility (sscManagementUtility) is described below:

sscManagementUtility { **validate** | **sign** | **help** | **package** } [*command specific options*]

sscManagementUtility help

sscManagementUtility validate {**–i** *input-file* | **--in=***input-file*}

sscManagementUtility sign {**–i** *input-file* | **--in=***input-file*} {**–o** *output-file* | **--out=***output-file*}

sscManagementUtility package {**–p** *srcMsi-file* | **--package=***srcMsi-file*}
{**-i** *xml-file* | **--in=***xml-file*} {**–o** *dstMsi-file* | **--out=***dstMsi-file*}

Table 2-1 lists the sscManagementUtility CLI commands and command-line options.

Table 2-1 sscManagementUtility Commands and Command-Line Options

Command Elements	Meaning
validate	Validate a destination package xml file only.
sign	Postprocess (validate, encrypt, and sign) a destination package xml file.
help	Displays utility release and command usage information.
package	Creates a client destination package.
–i *input-file* **--in=***input-file*	Path and filename of the destination package xml file to be processed.
–o *output-file* **--out=***output-file*	Path and filename of the processed destination package xml file ready for deployment.
–p *srcMsi-file* **--package=***srcMsi-file*	Path and filename of the original client source package .msi file. **Note** For SSC 5.0, the sscPackageGen utility must be used to generate the destination package file.
–i *xml-file* **--in=***xml-file*	Path and filename of the processed and signed configuration .xml file.
–o *dstMsi-file* **--out=***dstMsi-file*	Path and filename of the destination package .msi file.

Return codes sent to the standard error output (stderr) include:

- 0—Successful operation
- 1—Wrong arguments
- 2—Unknown configuration file version
- 3—Schema validation failed
- 4—Business rules validation failed
- 5—Referenced files cannot be found
- –1—Unexpected error (see stderr for details)

Note When extracting files from the SSCMgmtTookkit.zip file, ensure that the original folder structure and file locations are maintained. The management utility uses support files located in data folders in the same folder as the utility. Do not move files or folders from their original installed locations.

GUI Operation

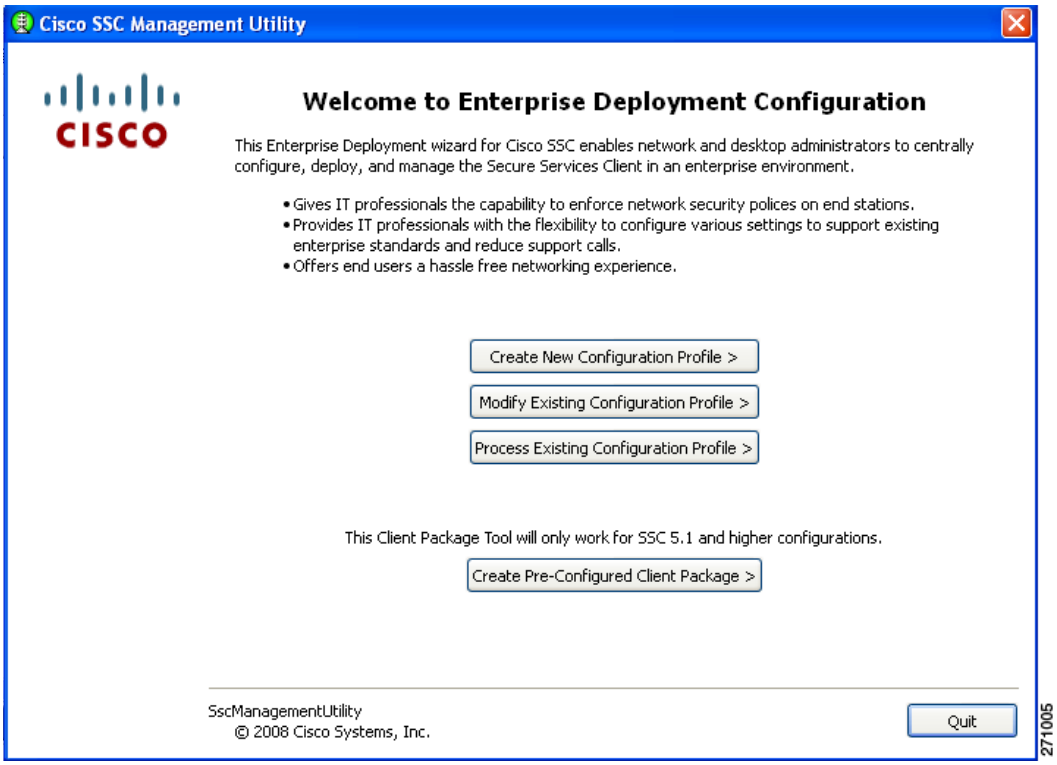
The management utility GUI guides the administrator through a series of windows and menu options to specify and configure the wired and wireless network security profiles.

Points to remember when using the management utility GUI:

- If an entry has a ? next to it, you can click the ? to obtain context-sensitive help.
- The window that appears when you click **Next** is determined by the choices you made on the current window.

To activate the SSC management utility GUI, double-click **sscManagementUtility.exe**. The welcome window appears (see Figure 2-1).

Figure 2-1 Cisco SSC Management Utility Welcome Window



There are four choices on this window:

- Create New Configuration Profile—Used to create a new deployment profile. The management utility guides the system administrator through the process of specifying client policies and security authentication policies for single or multiple networks. The management utility validates the configuration file against the configuration schema and the business rules.
- Modify Existing Configuration Profile—Used to revise the policy settings of an already created (unprocessed or processed) configuration file. Processed profiles are valid, signed, encrypted (shared keys and passwords are encrypted), and contain embedded certificate and Proxy Auto-Configuration (PAC) files.

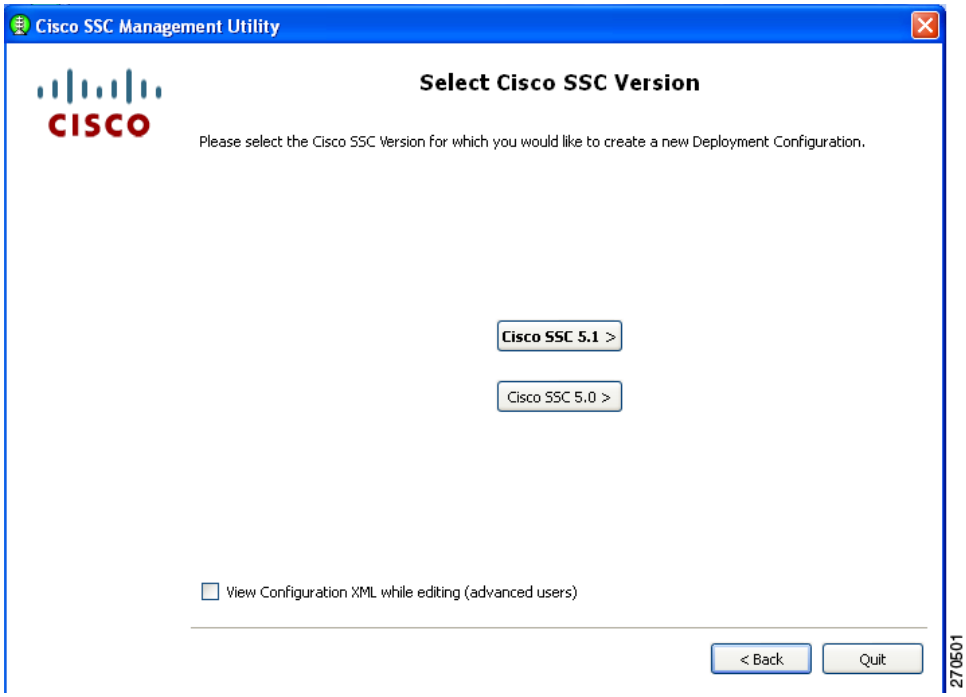
- Process Existing Configuration Profile—Used to process and validate an existing configuration profile (processed or unprocessed) against the configuration schema and business rules. The processing involves these operations:
  - Verifying the validity of the created file
  - Embedding any referenced certificate or PAC files
  - Encrypting any passwords or shared keys
  - Signing the final configuration file, so that end users cannot tamper with the administrator-deployed configuration file.
- Create Pre-Configured Client Package—The management utility combines the client source package file with the processed and signed configuration file to produce the client destination package file. The client destination package file is used to configure the user's PC with SSC and the defined profiles.

Note For SSC 5.0, the sscPackageGen utility must be used to generate the destination package file.

Creating a New Configuration File

To create a new configuration file, click **Create New Configuration Profile** and the window shown in Figure 2-2 appears.

Figure 2-2 Select Cisco SCS Version Window



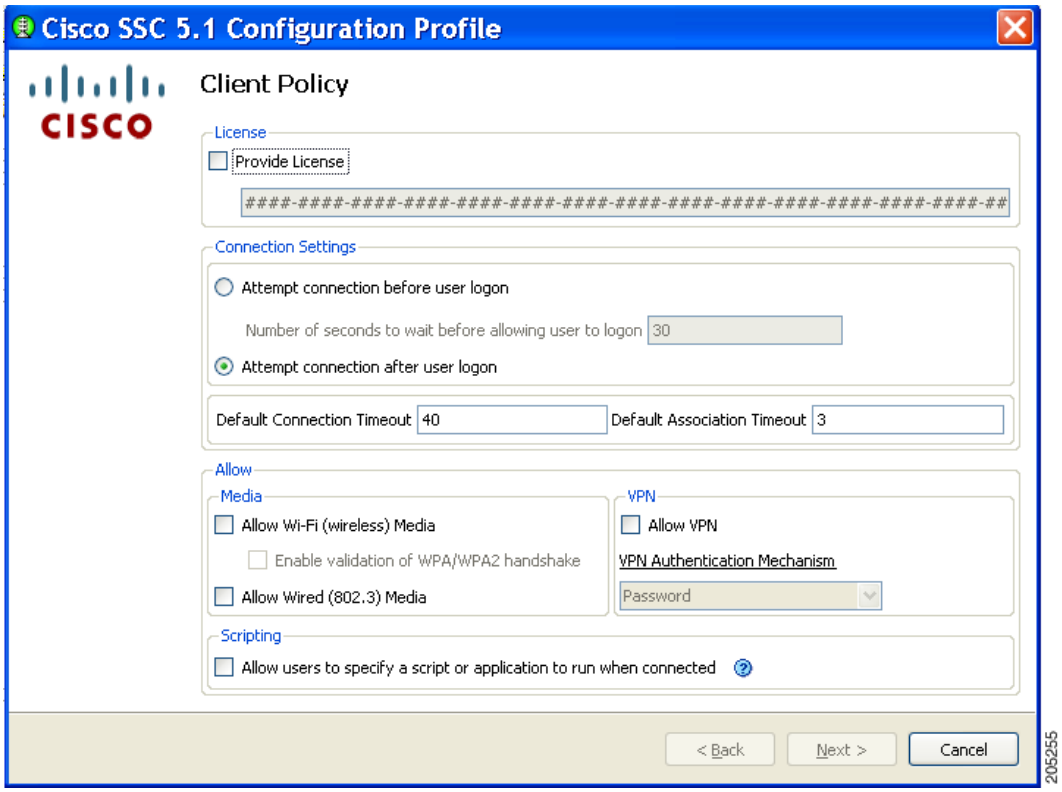
The SSC management utility enables you to create a configuration file for SSC 5.1 or 5.0.

When you click **Cisco SSC 5.1**, the Client Policy window appears (Figure 2-3).

Configuring Client Policy

The Client Policy window enables you to configure the client policy options (Figure 2-3).

Figure 2-3 Client Policy Window



Note SSC releases 5.0 and later do not allow end users to enter license numbers using the SSC GUI. It is the responsibility of the network administrator to enter a valid license in the destination package using the SSC management utility so that all end users have the appropriate license.

There are three sections on this window:

- License section—allows you to specify a new unlimited SSC license key that you purchased from Cisco.

  Note The SSC software downloaded from the Cisco.com download center supports a limited 90-day trial license.

- Connection Settings section—allows you to define whether 802.1X authentication must be attempted after user logon or before Windows domain authentication (pre-logon). If you choose pre-logon, you can also specify the maximum (worst case) number of seconds to wait before allowing the user to logon (default 30 seconds). If a network connection cannot be established within this time, the Windows logon process continues with user logon.

- Allow section—enables the types of media controlled by the SSC client.
  - Media section—enables wired and Wi-Fi media.

    Note SSC releases 5.0 and later are single-homed allowing only one network connection to be operating at a time. Also, wired connections have higher priority than wireless connections.

  - VPN section—enables VPN and specifies the VPN authentication mechanism.
  - Scripting section—Allows users to specify a script or application to run when the network connects. Because this presents some security risks, a warning message similar to that shown in Figure 2-4 appears when you check this box.

    Note The scripting feature is supported in Windows 2000, Windows 2000/2003 Server, and Windows XP. It is not supported in Windows Vista.

Figure 2-4 Scripting Security Warning Message

Note The scripting settings are specific to one network and allow the user to specify a local file (.exe,.bat, or.cmd) to run when the that network gets to a connected state for user-configured networks only. To avoid conflicts, the scripting feature only allows 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 the administrator does not allow users to configure a running script, the feature is not seen on the user's SSC GUI.

If you enable VPN for a wireless connection, you can specify the authentication mechanism VPN will use:

- Soft token authentication—Prompts for username and password for the soft token account. SSC automatically obtains the soft token from the Secure Computing SofToken-II program and passes the soft token to the IPSec VPN client.

Note For Windows Vista, Secure Computing SofToken II is not supported. When SofToken II authentication is specified in the network configuration and SSC prompts for the username and password, the username and the unique one-time password must be entered. This is different from Windows 2000 and Windows XP where the SofToken II application password is entered.

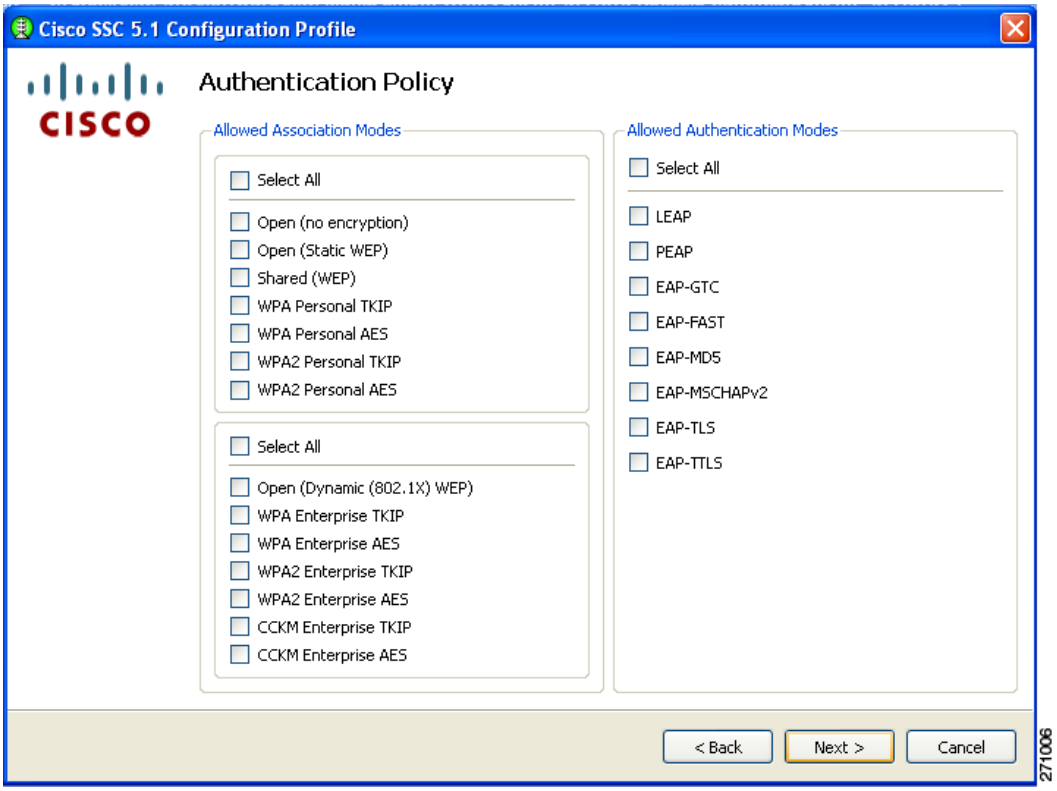
- Password authentication—Prompts for the VPN password. SSC automatically activates the IPSec VPN client and passes the password.
- Certificate authentication—No prompt is required. SSC automatically activates the IPSec VPN client, and the VPN server obtains the certificate.

When you complete your selections and click **Next**, the Authentication Policy window appears (Figure 2-5).

Configuring Authentication Policy

This window allows you to define global association and authentication network policies. Global policies apply to all networks that you, the administrator, or the user can create.

Figure 2-5 Authentication Policy Window

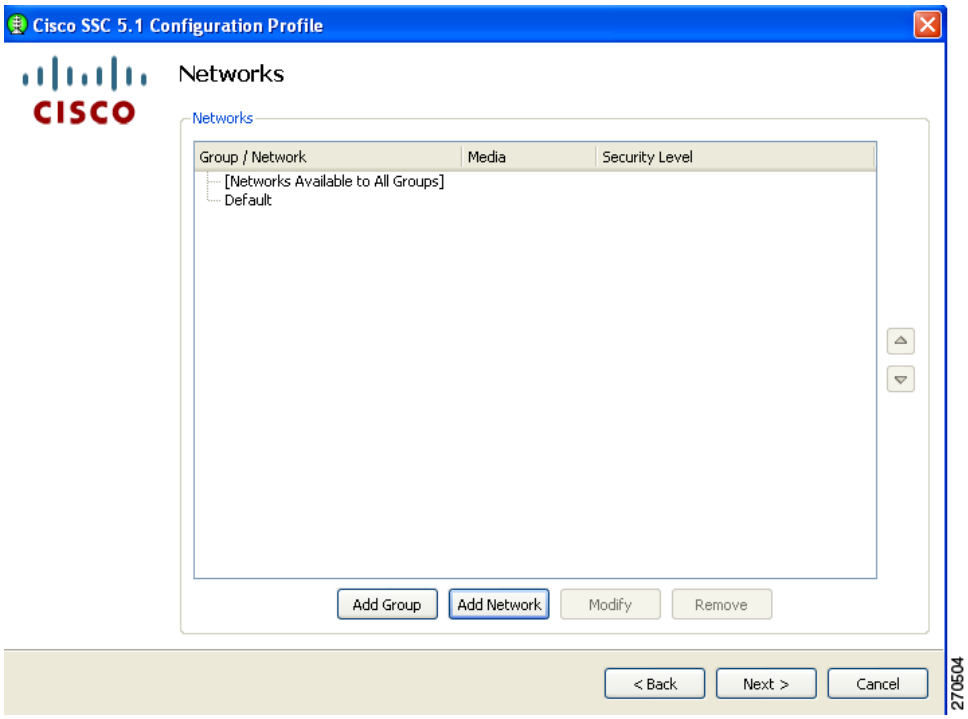


When you complete your selections and click **Next**, the Networks window appears (Figure 2-6).

Configuring Networks

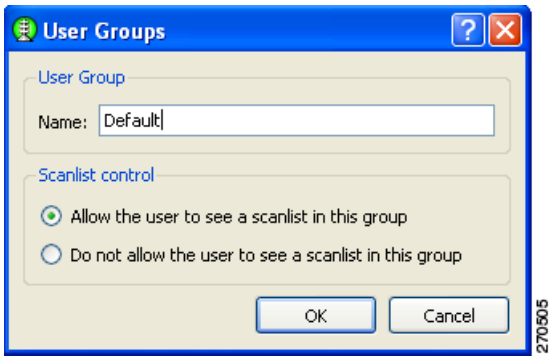
The Networks window allows you to configure networks that are pre-defined for your enterprise user. You can either configure networks that are available to all groups or create groups with specific networks. For additional information on groups, see the "Groups in SSC" section on page 2-37.

Figure 2-6 Networks Window



When you click **Add Group**, the User Groups window appears (Figure 2-7).

Figure 2-7 User Groups Window

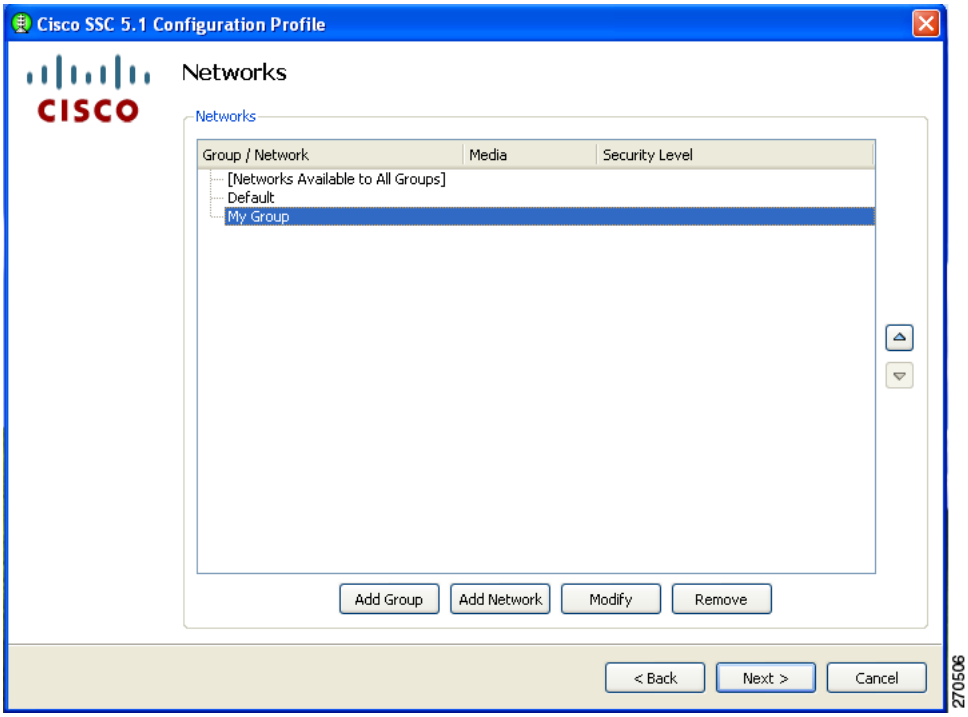


The Scanlist control section enables you to control whether users can see the scanlist when this group is active. It may be necessary to restrict viewing of the scanlist; for example, in order to prevent users from accidentally connecting to nearby devices.

Note This is a per-group setting. For groups created by the end user using the SSC GUI, the scanlist control is set to *Allow the user to see a scanlist in this group*.

Click **OK.** The Networks window reappears with the new group just created visible (*My Group* in Figure 2-7).

Figure 2-8 Networks Window with New Group Visible



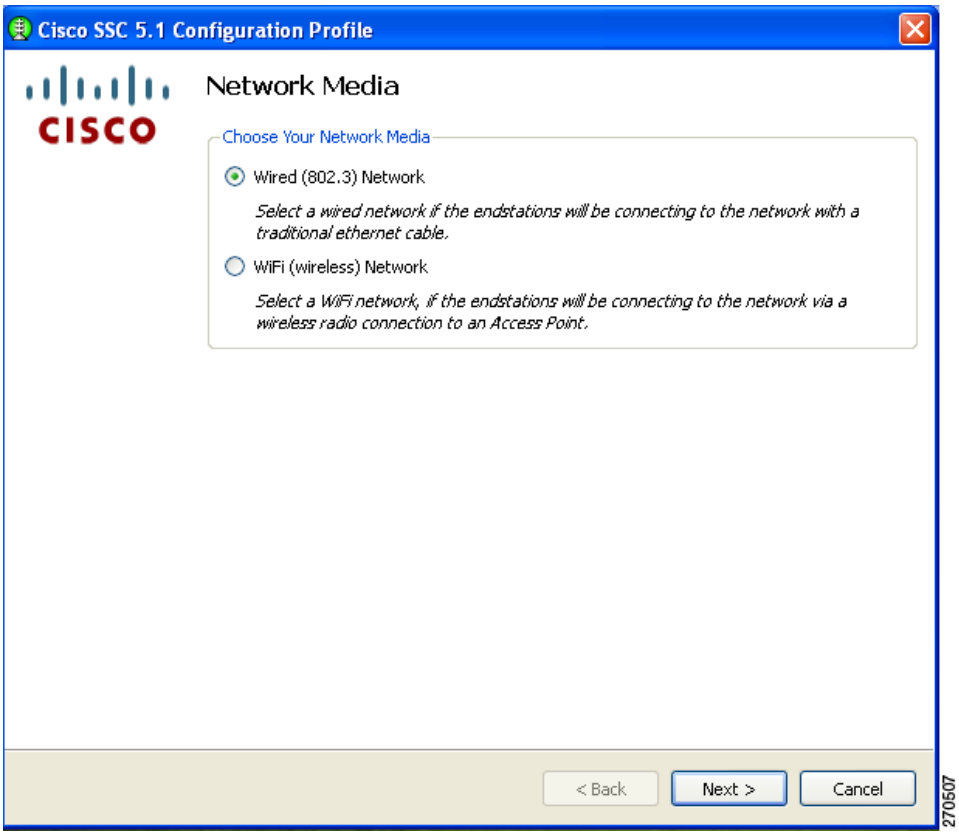
Network groups contain single or multiple network profile descriptions. A network profile defines the specific properties and operational behavior of a single network. The profile includes the following characteristics:

- The user-friendly name of the network.
- Network access media (wired, Wi-Fi) and adapter details used for the network connection.
- Definition of the security class (open, shared key, authenticating) of the network.
- Definition of the connection context (machine only, user only, machine and user) for the network.
- Wi-Fi association and encryption method (Wi-Fi network).
- Authentication methods supported and properties (authenticating network).
- Static keys, if applicable (non-authenticating network).
- Definition of types and source of credentials (authenticating network).
- Definition of trusted servers (authenticating network) and support for deploying Certificate Authority (CA) certificates and manual provisioning of EAP-FAST Protected Access Credentials (PACs).

Networks defined as part of the distribution package are locked; therefore, the end user is not able to edit the configuration settings or delete the profiles.

On the Networks window (Figure 2-8), you can add a network to a newly created group, such as My Group, by highlighting it and clicking **Add Network**. The Network Media window appears (Figure 2-9).

Figure 2-9 Network Media Window



This window enables you to choose a wired or a wireless network.

If you choose **Wired (802.3) Network** and then click **Next**, the Wired Network Setting window appears (Figure 2-10).

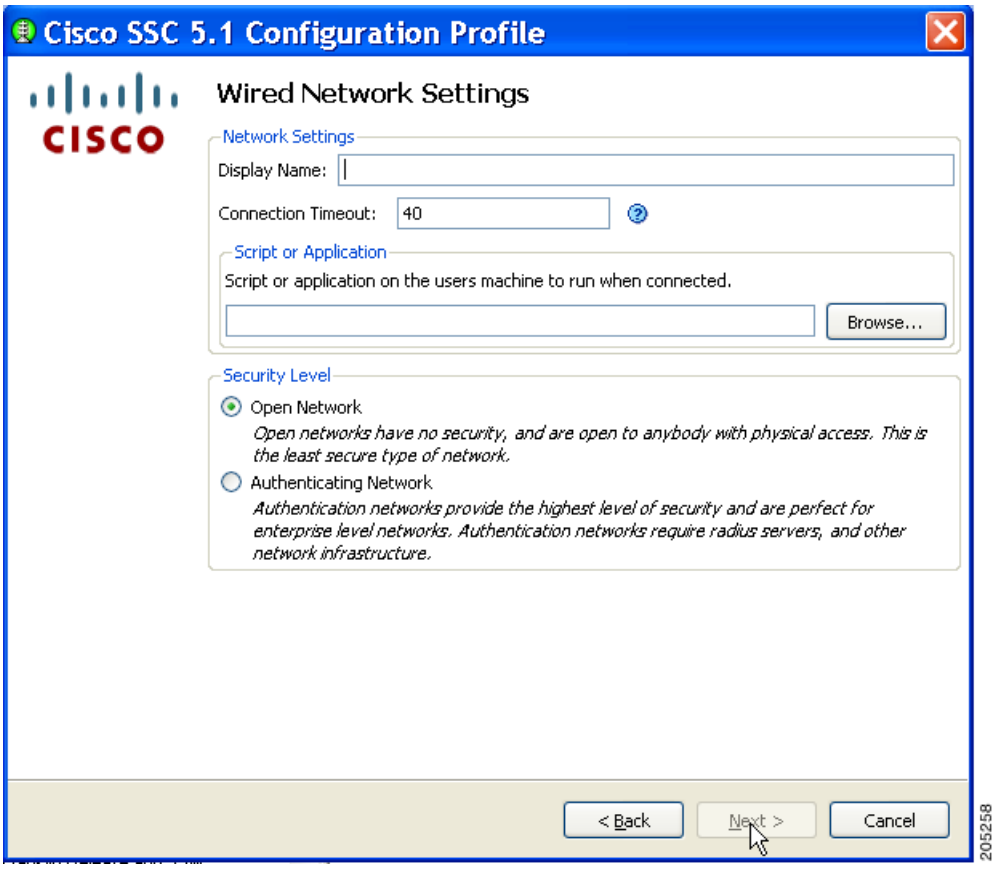
If you choose **Wifi (wireless) Network** and then click **Next**, the WiFi Network Setting window appears (Figure 2-13).

When you have finished adding all your groups and networks, click the **Next** button and Figure 2-27 appears (see the "Validating the Configuration File" section on page 2-35).

Configuring Wired Network Settings

The Wired Network Settings window enables you to create an open (non-secure) network or an 802.1X authentication wired network (Figure 2-10).

Figure 2-10 Wired Network Settings Window



In the Display Name field, you can enter the name that is displayed for this wired network.

The Connection Timeout value is the length of time that SSC waits for a network connection to be established before it tries another network.

Note When using Windows 2000 or Windows XP, some smartcard authentication systems require almost 60 seconds to complete an authentication. When using a smartcard, you might need to increase the Connection Timeout value. Windows Vista does not support smartcard authentication systems.

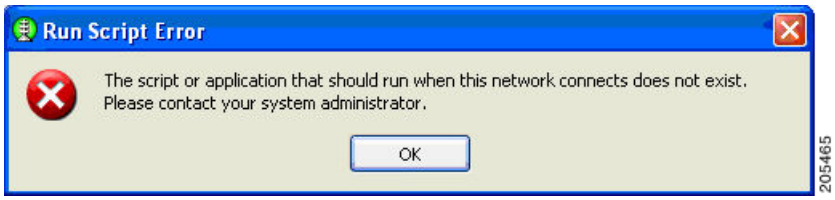
In the Script or Application section, you can enter the path and filename of the file you desire to run or you can browse to the location and select the file to run.

The following applies to scripts and applications:

- Allowable files are .exe, .bat, or .cmd.
- The administrator has the ability to allow or not allow a user to run a script when connected. See page 11 for additional information.

- User specified scripts or applications are allowed only on user created networks. They are not allowed on administrator created networks.
- The path and script or application filename must be specified by the administrator using the management utility only. If the script or application does not exist on a user's machine, an error message appears similar to that shown in Figure 2-11. The message informs the user that the script or application does not exist on their machine and they need to contact their system administrator.
- On execution of the script or application the user's path is checked. If the application to be run exists on the user's path, only the application or script name needs to be specified and the user's path search rules will be followed.

Figure 2-11 Run Script Error Message



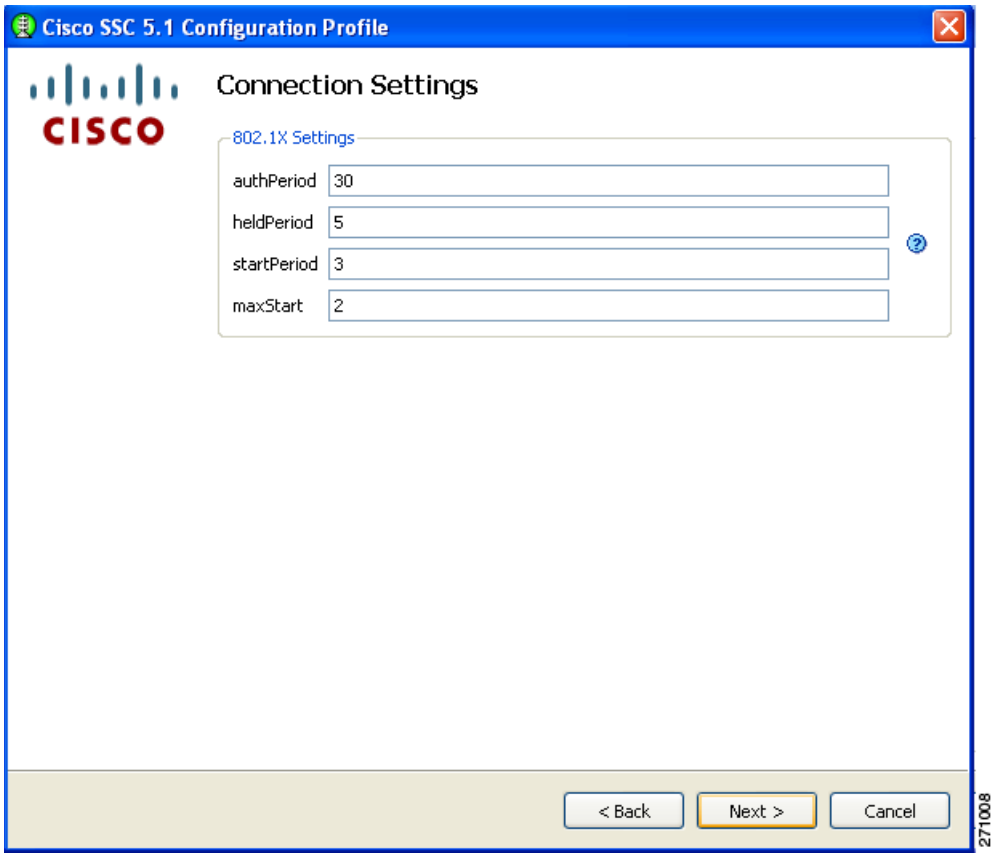
In the Security Level area, choose the desired network type:

- Open Network—This setting is recommended for guest access on the wired network.
- Authenticating Network—This setting is recommended for secure enterprise wired networks.

When you choose **Open Network** and click **Next**, the 802.1X Connection Setting window appears (Figure 2-15).

When you choose **Authenticating Network** and click **Next**, the 802.1X Connection Settings window appears (Figure 2-12). This window enables you to enter your 802.1X timer values. The default values should work for most wired networks; however, you have the option to configure the settings to suit your environment.

Figure 2-12 Connection Settings Window for a Wired Network

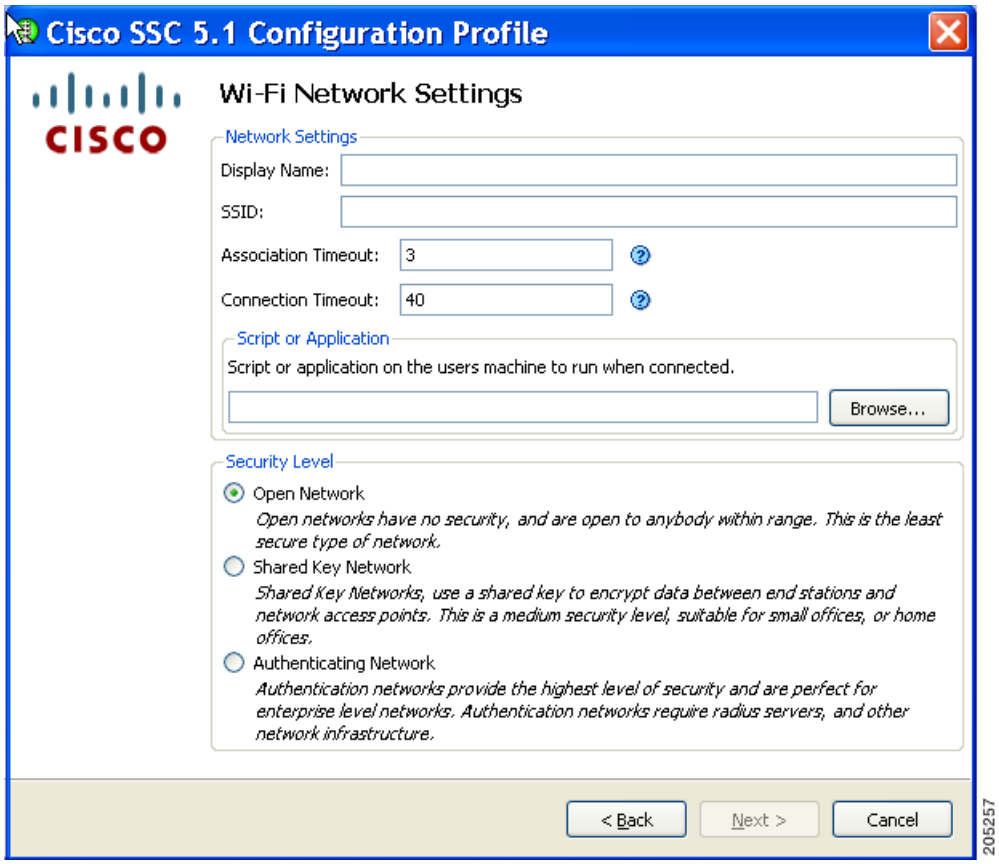


When complete and you can click **Next,** the Network Connection Type window appears (Figure 2-16).

Configuring WiFi Network Settings

The WiFi Network Settings window enables you to create an open (non-secure) network, a shared key network, or an 802.1X authentication wireless network (Figure 2-13).

Figure 2-13 WiFi Network Settings Window



In the Display Name field, you can enter the name that is displayed for this wireless network.

In the SSID field, you should enter the SSID (or network name) for this wireless network.

The Association Timeout value is the length of time that the SSC waits for association to the SSID before it tries another network.

The Connection Timeout value is the length of time that the SSC waits for a network connection to be established, before it tries another network.

Note When using Windows 2000 or Windows XP, some smartcard authentication systems require almost 60 seconds to complete an authentication. When using a smartcard, you might need to increase the Connection Timeout value. Windows Vista does not support smartcard authentication systems.

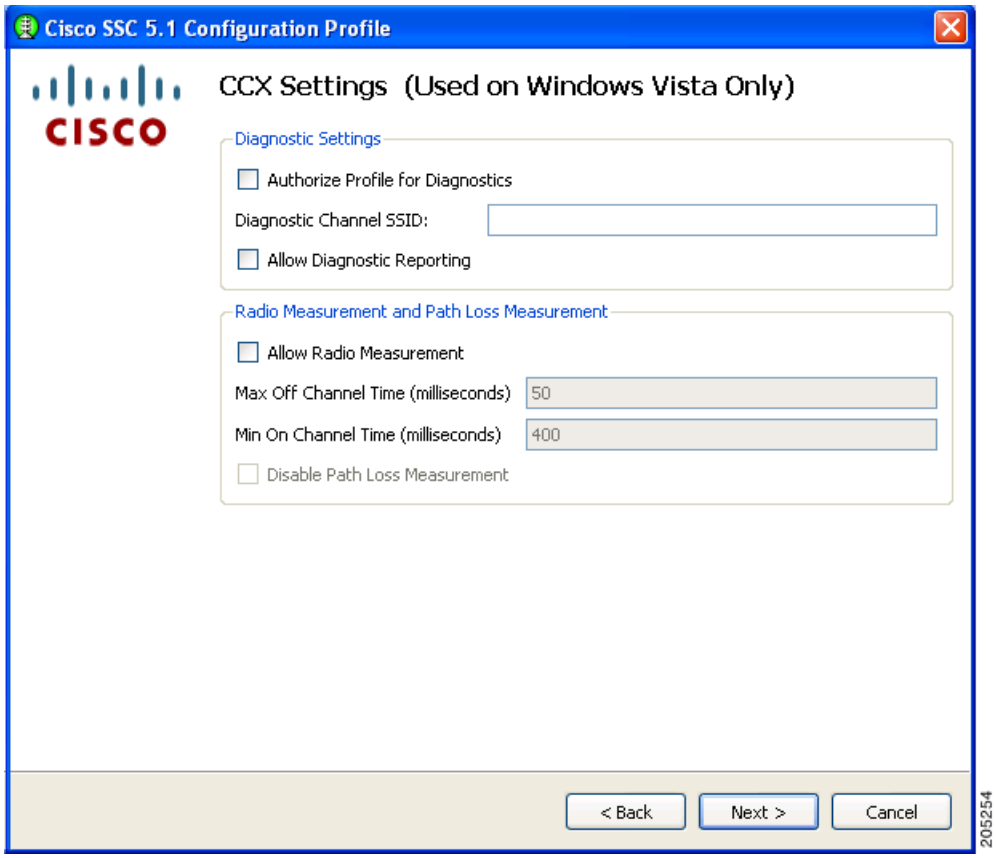
Note The Script or Application section is not currently supported.

In the Security Level area, choose the desired network type:

- Open Network—This setting is recommended for guest access wireless networks.
- Shared Key Network—This setting is not recommended for enterprise wireless networks.
- Authenticating Network—This setting is recommended for secure enterprise wireless networks.

When you complete your selections and click **Next**, the CCX Settings window appears (Figure 2-14).

Figure 2-14 CCX Settings Window



For a Windows XP or Windows 2000 environment, ignore the CCX settings window and click **Next**. The 802.1X Connection Settings window appears (Figure 2-15).

For a Windows Vista environment, the CCX Settings screen contains two sections:

- Diagnostic Settings
  - Authorize Profile for Diagnostics—Authorizes the user to diagnose this network using CCXv5 diagnostic capable infrastructures.
  - Diagnostics Channel SSID—Specifies the SSID of the diagnostics channel. A blank SSID field indicates to use the default SSID (Diagnostic Channel).'
  - Allow Diagnostics Reporting—Allows CCX diagnostics reports, profile configuration information, and logs to be sent when connected on this network.
- Radio Measurement and Path Loss Measurement
  - Allow Radio Measurements—Allows or prevents the client from participating in CCX radio measurement requests.
  - Max Off Channel—Specifies the maximum amount of time the client can operate off-channel to process a CCX radio measurement request.
  - Min on Channel—Specifies the minimum amount of time the client must operate on the service channel in between off-channel CCX radio measurement requests.
  - Disable Path Loss Measurement—Allows or prevents the client from participating in CCX path loss measurement requests.

Note The CCX settings apply only in a Windows Vista environment.

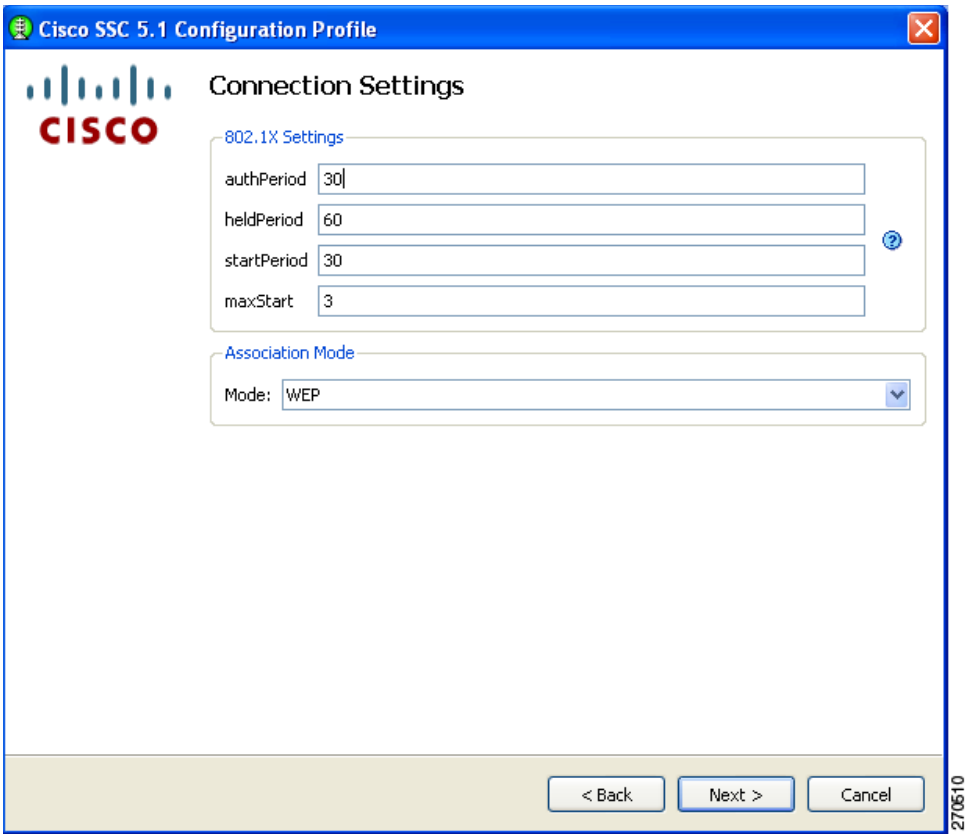
Note SSC management utility version 5.1.1 is required to configure these CCX settings.

Note These CCX settings only work with CCXv5 capable clients that use the CCX SDK, which Cisco makes available to Cisco CCX partners.

When complete, click **Next**. The 802.1X Connection Settings window appears (Figure 2-15).

This window enables you to enter your 802.1X timer values. The default values should work for most networks; however, you may set it to suit your environment.

Figure 2-15 802.1X Connection Settings Window for a Wireless Network



In the Association Mode field, click the drop-down arrow to select the association mode for this network:

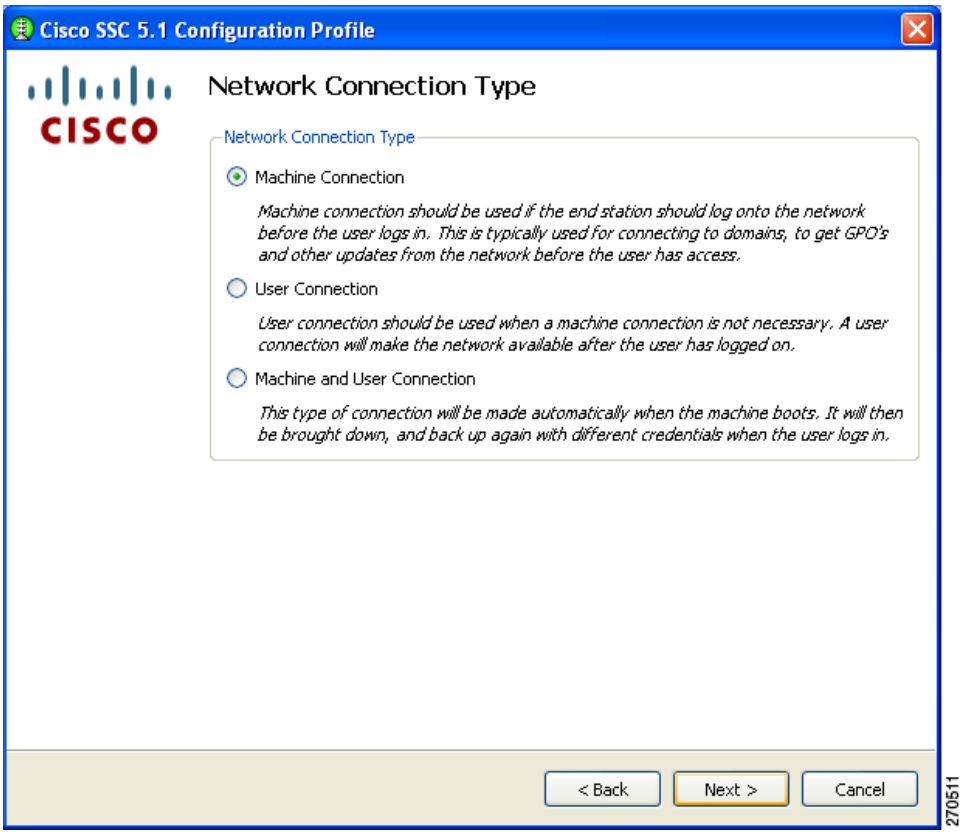
- WEP
- WPA Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA2 Enterprise (TKIP)
- WPA2 Enterprise (AES)
- CCKM (TKIP)
- CCKM (AES)

Note The chosen association mode must be enabled from the Authentication Policy window (see the "Configuring Authentication Policy" section on page 2-12).

When finished, click **Next** and the Network Connection Type window appears (Figure 2-16).

Configuring the Network Connection Type

Figure 2-16 Network Connection Type Window



This window enables you to choose the type of network connection. SSC defaults to Machine Connection. The User Connection option defines the connection as a user connection type. User connections are attempted after the user has logged onto the PC.

A machine and user network contains a machine part and a user part. The SSID is the same for the two parts, but the credential type for machine connection can be different from the credential type for user connection.

Note For an open network, the Machine and User Connection option is not available.

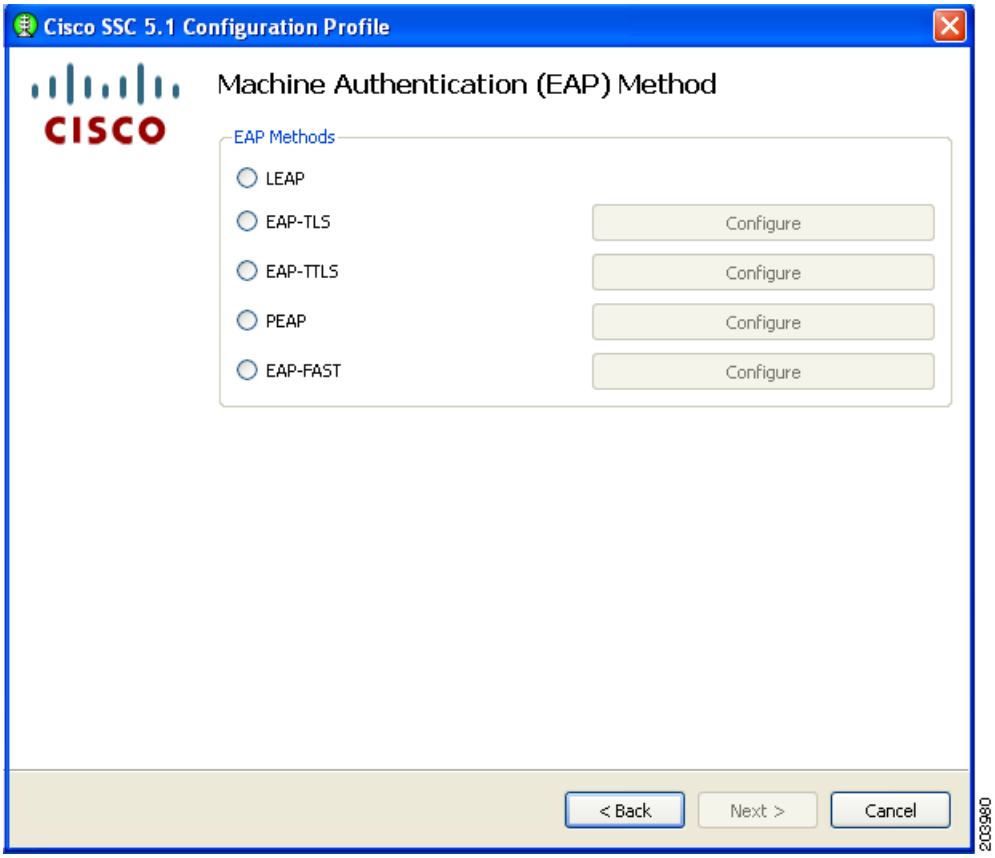
When finished, click **Next** and the Machine Authentication (EAP) Method window appears (Figure 2-17).

Configuring EAP Authentication

The Machine Authentication (EAP) Method and the User Authentication (EAP) Method windows enable you to choose the authentication method for the machine and the user, respectively. Both windows contain the same authentication method options.

Figure 2-17 lists the EAP methods for a wireless network connection.

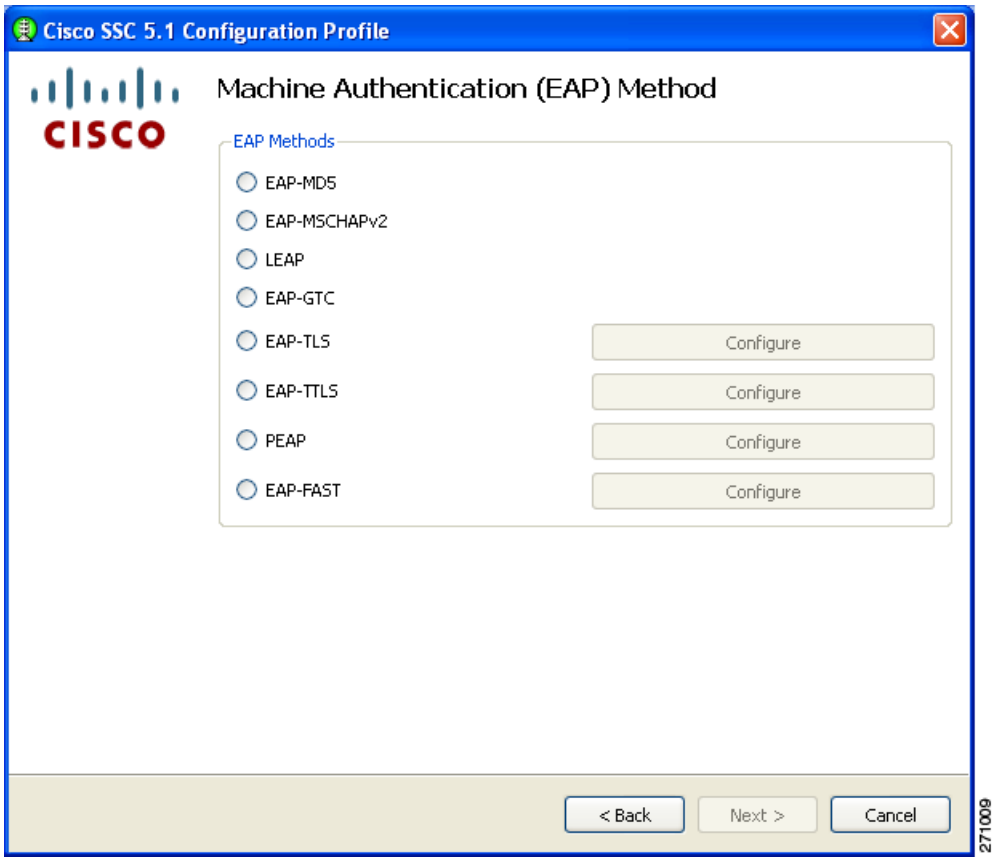
Figure 2-17 Machine Authentication (EAP) Method Window for a Wireless Network Connection



Note The Windows Vista version of SSC does not support these authentication methods: EAP-TLS and EAP-TTLS.

Figure 2-18 lists the EAP methods for a wired network connection.

Figure 2-18 Machine Authentication Method Window for a Wired Network Connection



Note The Windows Vista version of SSC does not support these authentication methods: EAP-MD5, EAP-MSCHAPv2, EAP-GTC, EAP-TLS, and EAP-TTLS.

Note The chosen authentication mode must be enabled from the Authentication Policy window (see the "Configuring Authentication Policy" section on page 2-12).

If you choose any of the EAP options with a configure button, you must click the corresponding Configure button to configure the EAP method:

- EAP TLS—See the "Configuring EAP TLS" section on page 2-26.
- EAP TTLS—See the "Configuring EAP TTLS" section on page 2-27.
- PEAP—See the "Configuring PEAP Options" section on page 2-28.
- EAP Fast—See the "Configuring EAP Fast Settings" section on page 2-29.

If you chose the Validate Server Identity option on the EAP TLS, EAP TTLS, PEAP, or EAP Fast settings window, the window in Figure 2-23 appears after you click **Next** (see the "Configuring Trusted Server Validation Rules" section on page 2-31).

If you do not choose the Validate Server Identity option, Figure 2-25 appears when you click **Next** (see the "Configuring Trusted Certificate Authority" section on page 2-32).

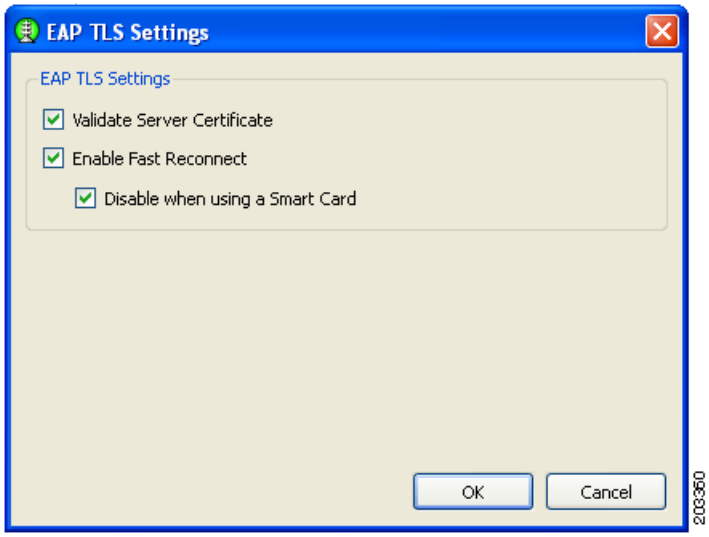
Configuring EAP TLS

The EAP TLS Settings window contains two options (Figure 2-19):

- Validate Server Certificate—enables server certificate validation.
- Enable Fast Reconnect—enables session resumption.

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

Figure 2-19 EAP TLS Settings Window



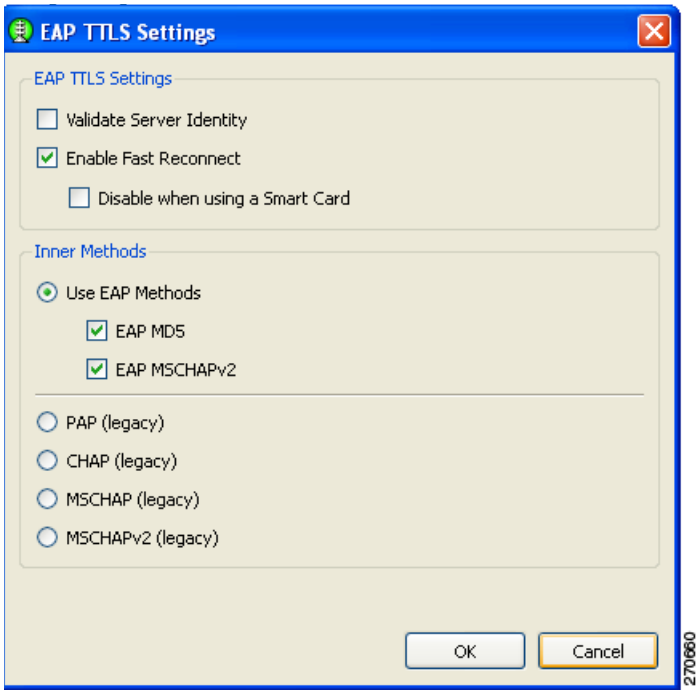
Note The Windows Vista version of SSC does not support EAP-TLS.

When you click **OK**, the Machine or User Authentication (EAP) Method window reappears (see the "Configuring EAP Authentication" section on page 2-24).

Configuring EAP TTLS

The EAP TTLS Settings window enables you to configure EAP TTLS settings (Figure 2-20).

Figure 2-20 EAP TTLS Settings Window



Note The Windows Vista version of SSC does not support EAP-TTLS.

The EAP TTLS Settings window contains two sections:

- EAP TTLS Settings
  - Validate Server Identity—enables server certificate validation.
  - Enable Fast Reconnect—enables session resumption.

    Note The *Disable when using a Smart Card* option is not available on machine authentication EAP method setting windows.

    Note Smart cards are not supported on Windows Vista.

- Inner Methods—Specifies the EAP methods.

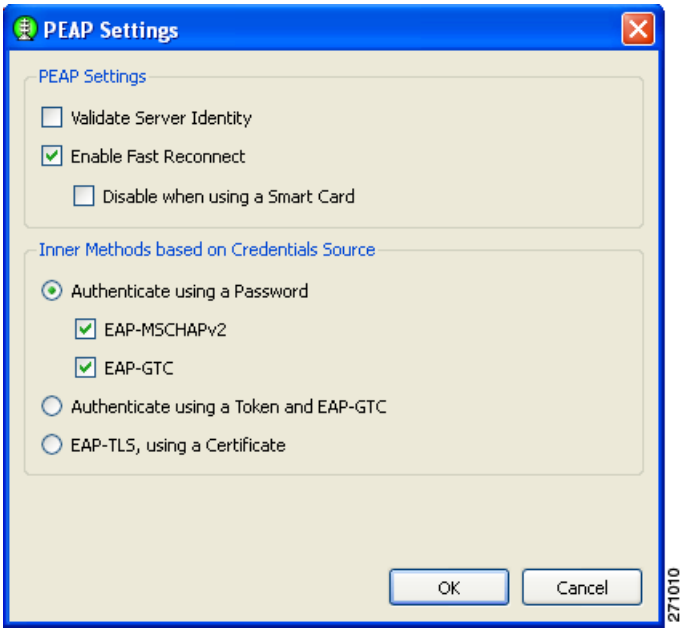
  Note Prior to choosing the EAP MD5 or EAP MSCHAPv2, the option needs to be enabled on the Authentication Policy window (see the "Configuring Authentication Policy" section on page 2-12).

When you are finished, click **OK**. The Machine or User Authentication (EAP) Method window reappears (see the "Configuring EAP Authentication" section on page 2-24).

Configuring PEAP Options

The PEAP Settings window enables you to configure PEAP settings (Figure 2-21).

Figure 2-21 PEAP Setting Window



Note The Windows Vista version of SSC does not support the EAP-TLS option with PEAP.

There are two sections on this window:

- PEAP settings
  - Validate Server Identity—enables server certificate validation.
  - Enable Fast Reconnect—enables session resumption.

    Note 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.

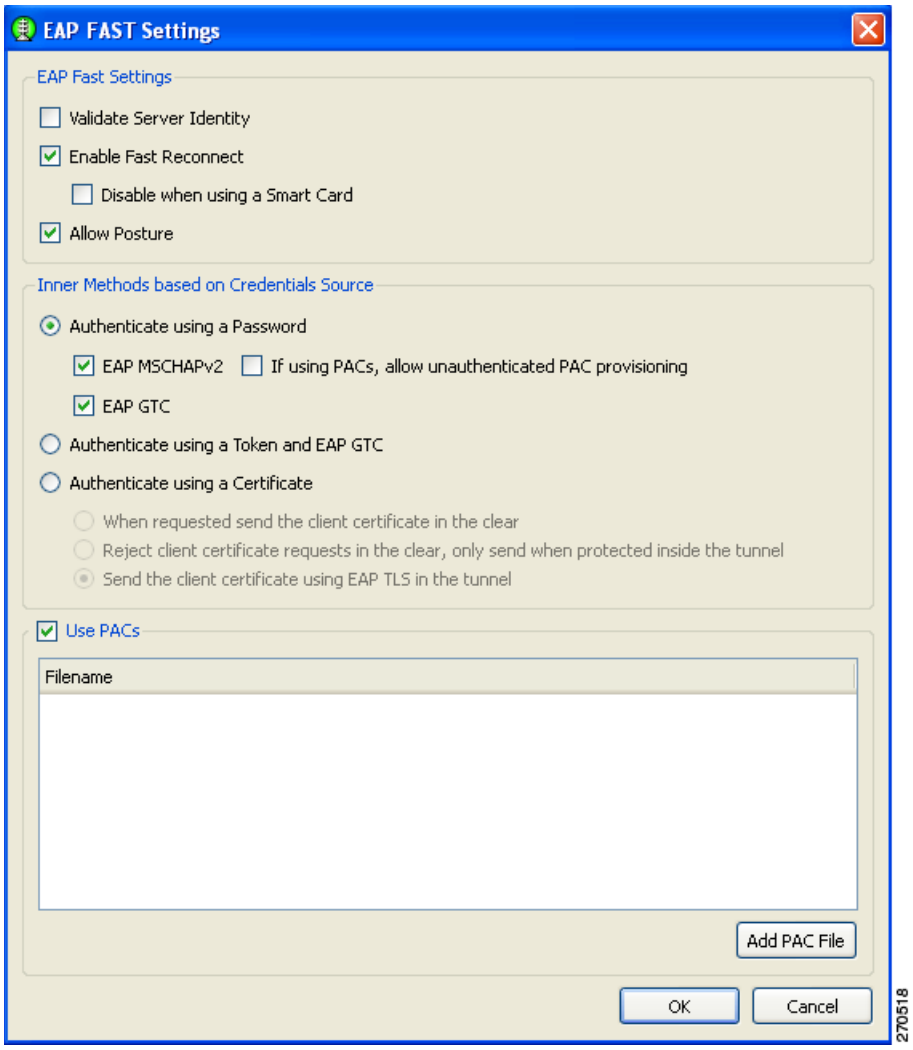
  Note Prior to choosing EAP MSCHAPv2 or EAP GTC, the option needs to be enabled on the Authentication Policy window (see the "Configuring Authentication Policy" section on page 2-12).

When you complete your selections and click **OK**, the Machine or User Authentication Method window reappears (see the "Configuring EAP Authentication" section on page 24).

Configuring EAP Fast Settings

The EAP FAST Settings window enables you to configure the EAP Fast settings (Figure 2-22):

Figure 2-22 EAP FAST Settings Window



This window contains three sections:

- EAP Fast Settings
  - Validate Server Identity—enables server certificate validation.
  - Enable Fast Reconnect—enables session resumption.

Note The *Disable when using a Smart Card* and the *Authenticate using a Token and EAP GTC* options are not available for machine authentication.

– Allow Posture—The term *posture* refers to a collection of attributes that can be use to identify the status of the endpoint device that is seeking access to the network. Some of these attributes relate to the endpoint device type and operating system; other attributes support various security applications that might be present on the endpoint, such as antivirus (AV) scanning software.

  Validating or assessing posture applies to a set of rules for the posture data to assess the level of trust that can be placed in that endpoint. The assessment, or **posture token**, can be used as one of the conditions for authorizing network access. Posture validation, together with the traditional user authentication, provide a complete security assessment of the endpoint device and the user.

Note Allow Posture is only supported in a Windows Vista environment.

- Inner methods based on Credentials Source—Enables you to authenticate using a password, certificate, token, or EAP GTC.

Note Prior to choosing EAP MSCHAPv2 or EAP GTC, the option needs to be enabled on the Authentication Policy window (see the "Configuring Authentication Policy" section on page 2-12).

- Use PACs—Specifies the use of PACs for EAP-FAST authentication.

Note Typically, the Use PACs option must be checked because most authentication servers use PACS for EAP FAST. Before unchecking this option, verify that your authentication server does not use PACs for EAP FAST; otherwise, the clients authentication attempts will be unsuccessful.

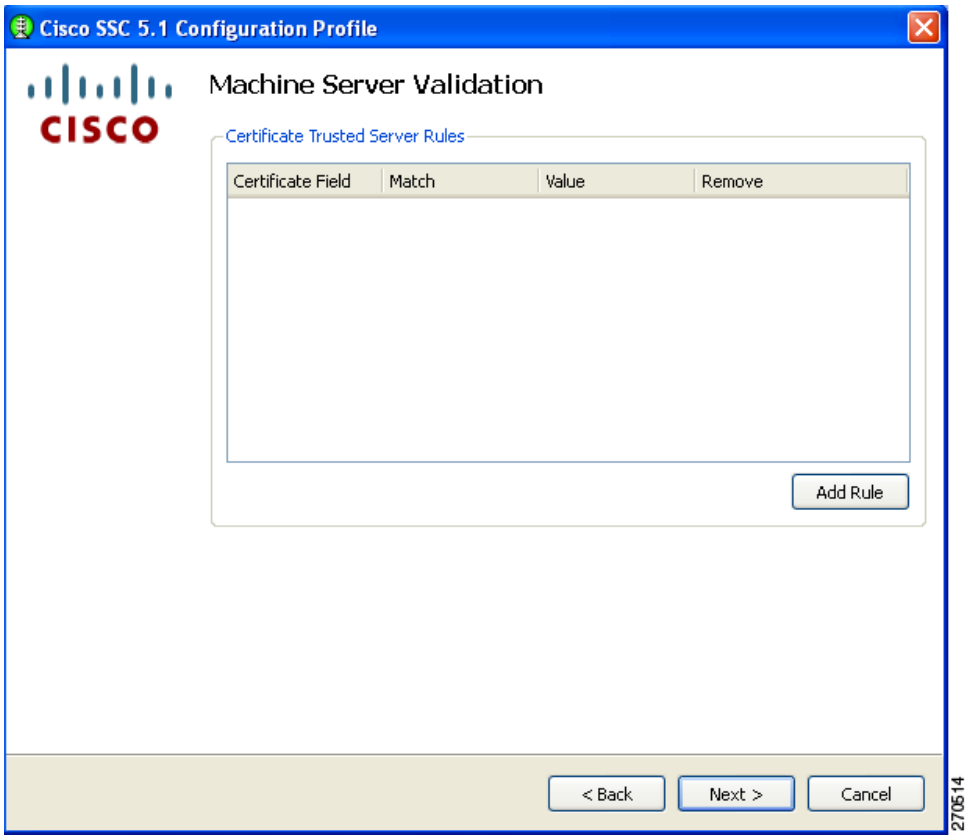
On this window, you can manually provide one or more specific PAC files or authentication by clicking **Add PAC File**.

When you complete your selections and click **OK**, the Machine or User Authentication (EAP) Method window reappears (see the "Configuring EAP Authentication" section on page 24).

Configuring Trusted Server Validation Rules

When the Validate Server Identity option is configured for the EAP method, the Machine Server Validation window enables you to configure certificate trusted server rules (Figure 2-23).

Figure 2-23 Certificate Trusted Server Validation Rules Window



To define server validation rules, follow these steps:

a. Click **Add Rule**.

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

c. Enter a value in the Value field.

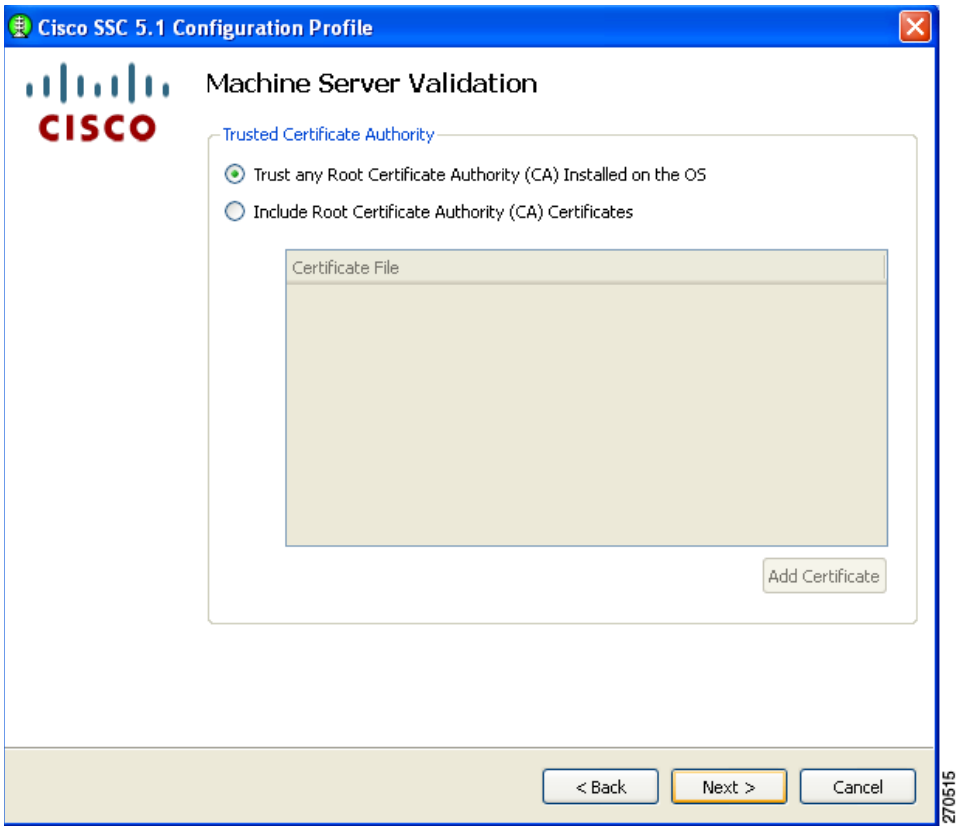
Note Click **Remove** to remove the rule.

When finished, click **Next** and Figure 2-24 appears.

Configuring Trusted Certificate Authority

The Trusted Certificate Authority window enables you to configure authority options.

Figure 2-24 Trusted Certificate Authority Window



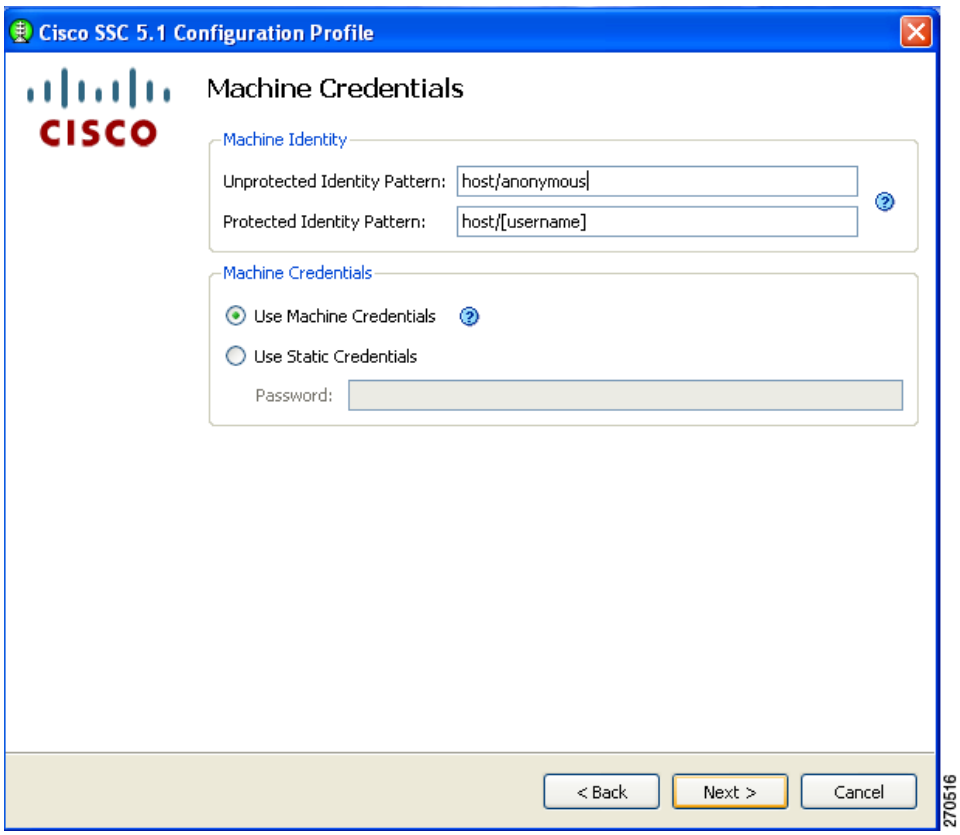
When you check the Include Root Certificate Authority (CA) Certificate option, you must click **Add Certificate** to add a certificate file.

When you are finished, click **Next**. The Machine Credentials window appears (Figure 2-25).

Configuring Machine Credentials

The Machine Credentials window enables you to specify the machine credentials (Figure 2-25).

Figure 2-25 Machine Credentials Window



Note The Protected Identity Pattern option is not available when the EAP-TLS authentication method is chosen.

SSC releases 5.0 and later support these placeholder patterns when you specify identities:

- [username]—Specifies the username.
- [domain]—Specifies the domain of the user's PC.

When the [username] and [domain] placeholders are used, one of these conditions applies:

- If a client certificate is used for authentication, the placeholder's value is obtained from the CN field of the client certificate.
- 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.

A typical pattern for machine unprotected identity is *host/anonymous.[domain]*.

- If password source is configured for this profile, the pattern would be the actual string to send as the username with no placeholders.

A typical pattern for machine protected identity is *host/[username].[domain]*.

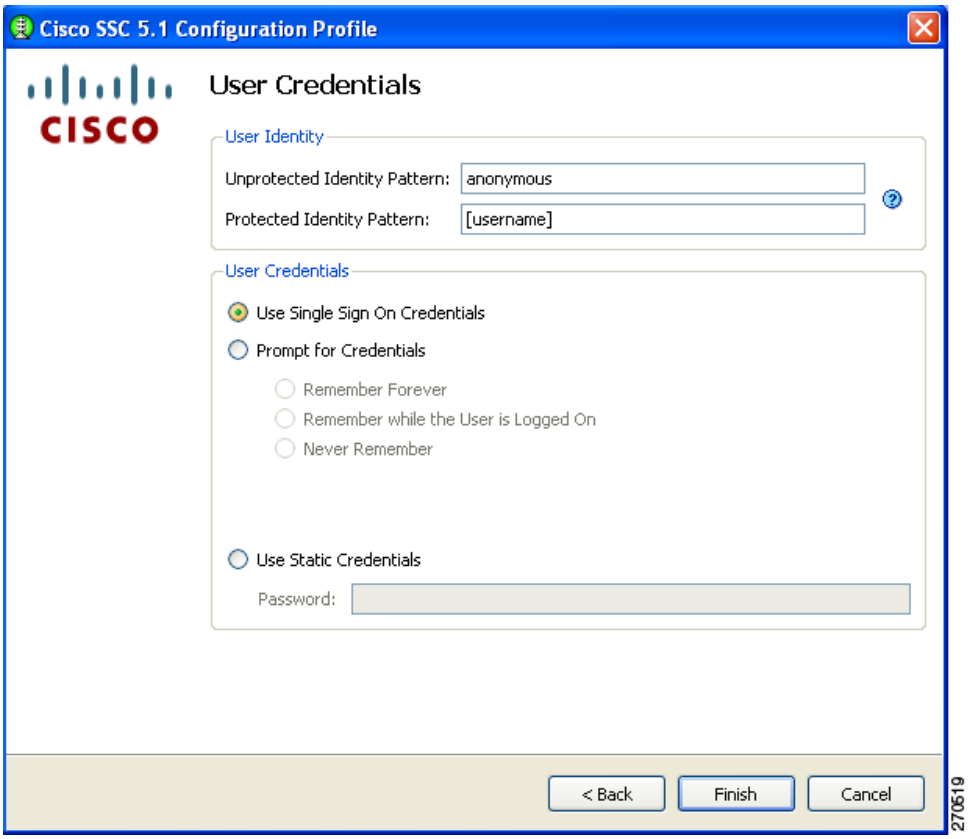
- If password source is configured for this profile, the pattern would be the actual string to send as the username.

When finished, click **Finish** and the Networks window reappears (Figure 2-8).

Configuring User Credentials

When you have configured a user connection, the User Credentials window enables you to configure the user credentials (Figure 2-26).

Figure 2-26 User Credentials Window



Note The Protected Identity Pattern option is not available when the EAP-TLS authentication method is chosen.

SSC releases 5.0 and later support these placeholder patterns when you specify user identities:

- [username]—Specifies the username.
- [domain]—Specifies the domain of the user's PC.

When the [username] and [domain] placeholders are used, these conditions apply:

- If a client certificate is used for authentication, the placeholder's value is obtained from the CN field of the client certificate.
  - 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.

  A typical pattern for user unprotected identity is *anonymous@[domain]* for tunneled methods or *[username]@[domain]* for non-tunneled methods.

If a client certificate is not used, the user identity pattern would be the actual string to send as the username (no placeholders). A typical pattern for user protected identity is *[username]@[domain]*.

If the password source is this profile, the pattern would be the actual string to send as the password (no placeholders).

You can specify the user credentials by choosing to use single signon credentials (SSC obtains the credentials from the operating system), prompting the user for credentials, or specifying an actual static password credential to be sent in the deployment file.

When finished, click **Finish** and the window in Figure 2-8 reappears with the group and network configurations you have specified. When you click **Next**, the Validation window appears.

Validating the Configuration File

At this point, the management utility validates the networks you have defined against your policy settings. Any policy violations are displayed. You must correct any errors before you save the file. For example, errors might appear in the Validation window (Figure 2-27).

Figure 2-27 Validation Window with Validation Errors

When there are no validation errors, you can save the deployment file in any location you choose or accept the default location. The processed file (signed with encrypted credentials, PACs, and CA certificates) is stored by default in this file location:

- For Windows 2000 and Windows XP:

  C:\Documents and Settings\All Users\Application Data\Cisco\Cisco Secure ServicesClient \newConfigFiles\configuration.xml

- For Windows Vista:

  C:\ProgramData\Cisco\Cisco Secure ServicesClient\newConfigFiles\configuration.xml

The Cisco SSC client looks in this location for any new destination package. If you have the client installed on your system, you can automatically test and verify the configuration that you just created before deploying it.

Click **Finish** to save the configuration file.

If you need to make changes to the deployment package you just created, you can reopen the management utility, click **Modify Existing Configuration** on the welcome window (Figure 2-1), and choose the configuration file that you just saved.

Creating the Pre-Configured Client Destination Package File

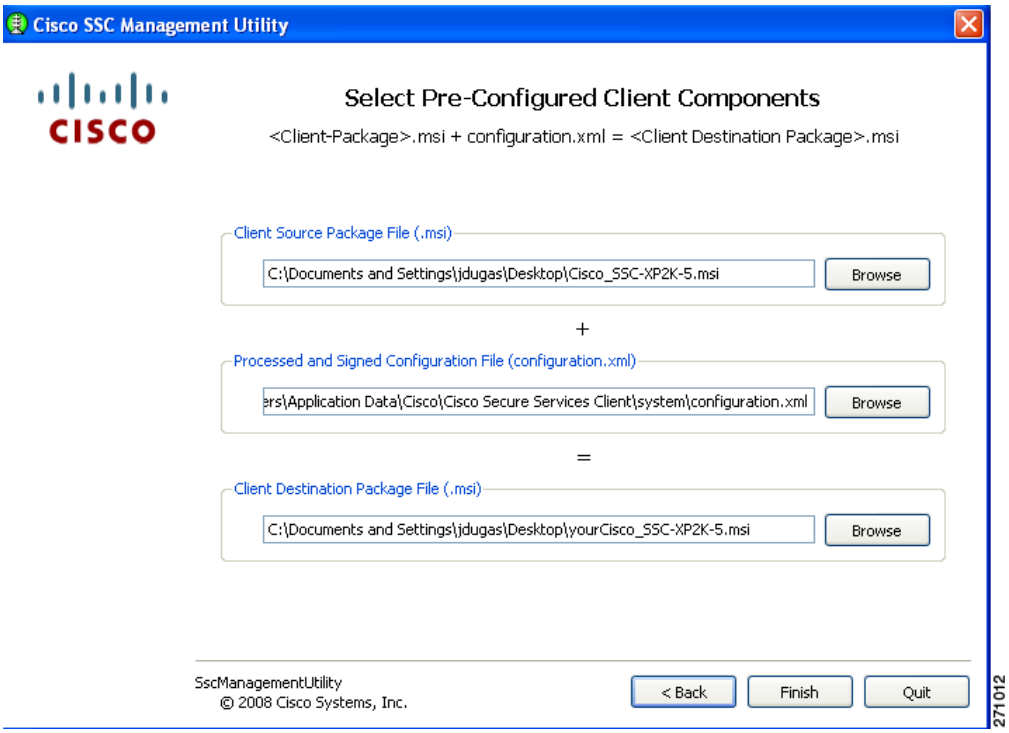
The sscManagement Utility can be used to create the client destination packages with network administrator configured profiles.

Note For SSC 5.0, the sscPackageGen utility must be used to generate the destination package file.

Using the Management Utility GUI

To create a pre-configured client package, the administrator clicks the Create Pre-Configured Client Package button on the management utility GUI window (Figure 2-28).

Figure 2-28 Select Pre-Configured Client Components Window



The management utility combines the client source package file (Cisco_SSC-SP2K-5.msi) with the processed and signed configuration file (configuration.xml) to produce the final client destination package file (yourCisco_SSC-XP2K-5.msi).

Accept the default file locations or click **Browse** to locate the files. Click **Finish**.

You can distribute the pre-configured client destination file (yourCisco_SSC-SP2K-5.msi) to the desired user PCs using your preferred distribution methods.

Groups in SSC

A group, fundamentally, is a collection of configured connections (networks). Every configured connection must belong to some group or be defined under the *globalNetworks* section in the distribution package.

Note End users can add networks only to groups and not to the *globalNetworks* section (because they typically do not have access to the management tool that would allow them to sign the distribution package).

Classifying connections into groups provides multiple benefits:

- Improved user experience when attempting to make a connection. It is important to understand how the client establishes a network connection in order to illustrate this point. The client works through the list of available networks in the order in which they are defined until a successful connection is made.

  For example, an enterprise end user who often travels outside the business campus might configure connections for public WiFi networks or hotspots. Without groups, a newly configured home network is added to the end of this list, which could be quite large. The client works through the list from the beginning, including all the public networks, before establishing a connection to the home network. This greatly increases the time to get connected to the last added network.
- Easier management of configured connections. In the previous example, an end user might attempt to delete some connections to connect more quickly, but the deleted connections might be needed at a later time. However, if the connection list is divided into groups, each group list would be much smaller. It is easy to switch between the groups to obtain faster connectivity.

A group may be created by an administrator or an end user. At least one group must be defined in the configuration. If there are multiple groups, one group must be chosen as the *active* group. The client attempts to make a network connection using the connections defined in the active group. End users can add or delete networks only from the active group. Groups can be added or deleted by clicking on the Configure Groups button on the main window of the client GUI.

Networks that are defined in the *globalNetworks* section of the distribution package are available in every group at the top of the list. Because only enterprise administrators can create *globalNetworks*, administrators can control the enterprise networks that an end user can connect to, even in the presence of user-defined networks. An end user cannot delete administrator-configured networks.

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. It is the responsibility of the administrator to always specify a default group in the created distribution package. If there is just one group available, the client selects that as the active group. The end user can add or delete their own networks without using groups.

Note A group selection is not maintained across reboots or SSC repairs. When SSC is repaired or restarted, SSC always goes back to the first configured group in the configuration.xml file.

VPN Integration

SSC 5.1 integrates an automatic VPN connection feature but requires a specific version of the Cisco IPSec VPN client to be installed on the user's PC:

- Windows 2000 and Windows XP—requires Cisco IPSec VPN client (4.8 or later)
- Windows Vista—requires Cisco IPSec VPN client (5.0.03.0560 or later)

SSC minimizes user intervention when establishing a VPN connection. SSC supports these IPSec VPN authentication options:

- Password—Specifies a simple password authentication.
- Secure Computing SofToken II—Specifies a soft token from Secure Computing SofToken II for authentication. This option requires that Secure Computing SofToken II be installed on the user's PC. SSC uses the Secure Computing SofToken II APIs to get a password that is automatically passed to the VPN daemon as a credential.

  Note For Windows Vista, Secure Computing SofToken II is not supported. When SofToken II authentication is specified in the network configuration and SSC prompts for the username and password, the username and the unique one-time password must be entered. This is different from Windows 2000 and Windows XP where the SoftToken II application password is entered.

- Certificate—Specifies certificate authentication and uses the connection to specify the certificate to use. Using this option, SSC does not prompt the end user for anything.

If the VPN concentrator does not require user authentication, such as in group authentication, SSC does not prompt the user for information.

When authentication is required by the VPN concentrator, SSC prompts the user for VPN logon information:

- Soft token authentication—Prompts for username and pin for the soft token account.

  Note For Windows Vista, Secure Computing SofToken II is not supported. When SofToken II authentication is specified in the network configuration and SSC prompts for the username and password, the username and the unique one-time password must be entered. This is different from Windows 2000 and Windows XP where the SoftToken II application password is entered.

- Password authentication—Prompts for username and password.
- Certificate authentication—No prompt is required.

When the VPN connection is successful, SSC maintains the user-entered information for possible future VPN connection attempts while the user is logged on to the PC. If the VPN connection fails, SSC re-prompts the user for VPN logon information.

SSC deletes the user's VPN information when the user logs off, shuts down the PC, or repairs SSC.

Supported VPN Features

SSC supports these VPN features:

- A single set of credentials for VPN access through all networks and VPN connections, which is maintained until the user logs off or the service is restarted (repair or reboot).
- Each individual profile has a setting to enable or disable automatic VPN connection and a choice of the VPN connection entry.
- An edit networks option is provided to allow the user to change the automatic VPN connection setting.
- SSC loads the .dll files for IPSec VPN and Secure Computing SofToken. If the .dll files cannot be loaded the VPN feature is disabled.
- SSC provides a new icon to indicate the VPN connection status.
  - Right clicking the tray icon provides options to Connect VPN or Disconnect VPN.
- Prompt for soft token credentials.

Unsupported VPN Features

SSC does not support these VPN features:

- Use of static credentials in the schema as soft token credentials.
- Use of single sign-on credentials in the schema as soft token credentials.
- Use of hardware tokens.
- Changing the password for the soft tokens from Secure Computing SofToken II.

Remote Desktop

There are two methods to access a network computer remotely while the connection is being managed by SSC on that network computer.

The first method, which was supported in previous versions, involves network profiles with machine authentication (machine-only or machine+user). This method is configured as follows:

- SSC must be configured for machine authentication.
- When a user logs in remotely, SSC remains authenticated with the machine's credentials.
- If a local user is logged in and SSC is authenticated to the network with the local user's credentials and a remote user logs in via remote desktop, the local user is logged off and SSC reverts to machine authentication.

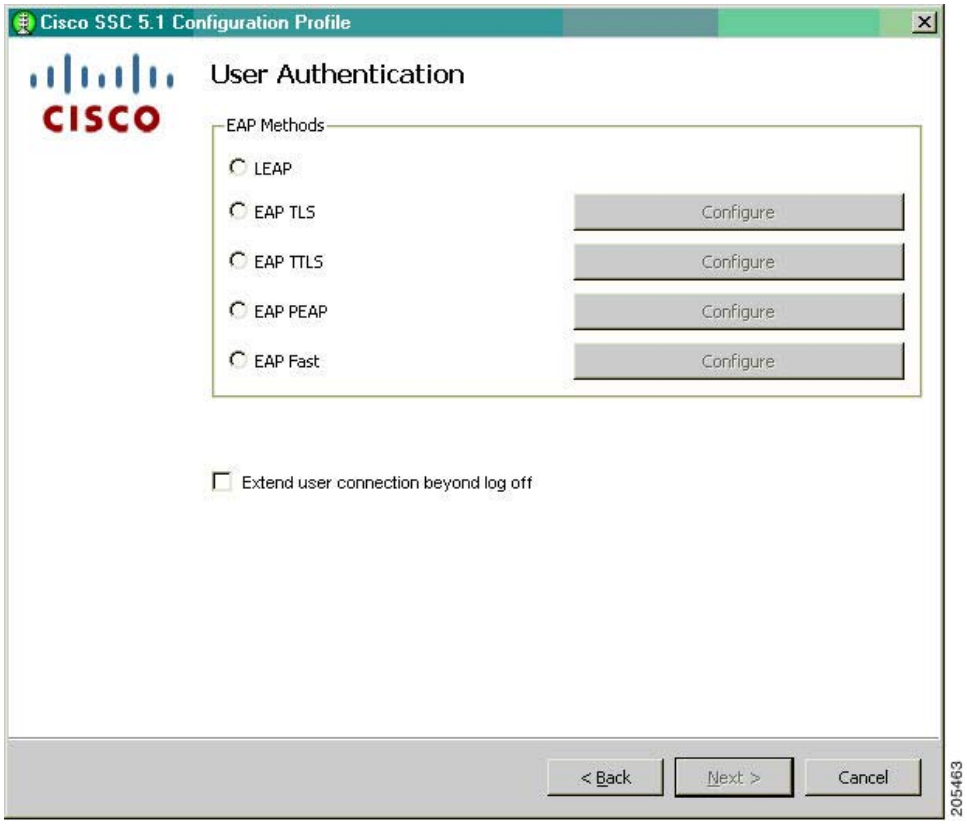
There may be complications with this method. For example, depending on the configuration, the machine and the user sub-profiles may put the computer on different networks (usually VLANs, and for the purpose of this discussion, we will call them *user VLAN* and *machine VLAN*). Therefore, if the network computer is left connected as a user on the user VLAN (user is not logged off) and later it is accessed remotely, the computer will be reconnected as a *machine-to-machine VLAN*. Thus the remote desktop session may need to be reestablished to a different IP address on a different VLAN (the *machine VLAN*).

The second method is a new parameter introduced in CSSC version 5.1.1. The *extendUserConnectionBeyondLogoff* parameter makes it possible to configure a user authentication in such way that it remains active (connected) even after the local user has logged off (voluntarily or due to an incoming remote desktop session). Therefore, there is no need to have a machine authentication solely to support remote desktop functionality. This method is configured as follows:

- In the management utility, a user authentication network must be configured.
- When specifying the user authentication method, the *Extend user connection beyond logoff* checkbox appears on the GUI page. Checking this parameter extends the user connection beyond a voluntarily or forced logoff.

The parameter is enabled by creating a new configuration or modifying an existing one. The parameter is shown on Figure 2-29.

***Figure 2-29 Configuring the extendUserConnectionBeyondLogoff* Feature**



Windows 2000

No native remote desktop functionality is available on Windows 2000 Professional, therefore the *extendUserConnectionBeyondLogoff* parameter affects the behavior only on an explicit local logoff.

Windows 2000/2003 Server

Windows 2000/2003 Server remote desktop sessions do not force the termination of other existing user sessions. Therefore, the *extendUserConnectionBeyondLogoff* parameter affects the behavior of explicit local logoff only, so there should be no need to use the parameter for remote desktop operations. There can be only one or no local session. If there is a local session, then that session's connection is used. If if there is no local user session, then the machine connection is used unless the user connection from the previous local user session was extended beyond logoff by enabling the *extendUserConnectionBeyondLogoff* parameter in the administrator's SSC configuration.

Note Keep in mind that even without the *extendUserConnectionBeyondLogoff* parameter, SSC continues to use the existing local user session for the network connectivity. However, the new parameter provides the ability to extend the user connection beyond explicit local logoff if needed. In all other aspects, the solution for Windows Server 2000/2003 is the same as for Windows XP.

Windows Vista

Windows Vista remote desktop sessions do not force termination of the other existing user sessions. Therefore, like Windows Server 2000/2003, there is no need to use the *extendUserConnectionBeyondLogoff* parameter for remote desktop operations. However, due to other circumstances, Vista ignores the *extendUserConnectionBeyondLogoff* parameter altogether and does not extend the local user session for explicit local logoffs. In such instances, the machine connection is used instead of the local user session. Therefore, Vista's behavior is different than that for other supported versions of Windows.

Configuration and Restrictions

RADIUS Accounting

RADIUS accounting will not work as usually expected. The only way the network distinguishes a user and a machine is by their credentials. The operating system distinguishes the difference between user- and machine-based on whether the user is logged on or off. Without the *extendUserConnectionBeyondLogoff* parameter, both party's states and views are always synchronized. But when the parameter is enabled, there will be cases when the operating system's and network's views differ (the operating system “thinks” machine while the network “thinks” user). This is expected behavior and you should consider it before deploying the remote desktop feature.

Smart Card Authentication

A smart card-based user authentication during a user connection extended beyond logoff requires all of the following:

- The smart card must be kept in the reader since the last user session. The card must not be removed.
- The CA certificates for the user's certificate chain should be available in the machine certificate store and/or on the AAA server.
- <*certificateSource*> must be either <*certificateFromLogon*> or <*certificateFromUser*>.

- If *<certificateSource>* is *<certificateFromUser>*, then *<allowedCertSourceFromUser>* must be *<smartCardOnlyCertificate>* and both *<cacheCertificateFromUser>* and *<cachPinForSmartcard>* must be either *<tilLogout>* or *<forever>*. However, they do not have to be the same.

Other Restrictions

- If re-authentication occurs while the user connection is extended beyond logoff and a user interaction is required, then the re-authentication fails and the connection is lost. If there are other profiles with machine authentication then the connection via such profiles may still be established (perhaps with a different IP address). Otherwise, the user must login to the network computer locally in order to re-establish the connection. Therefore, we recommend that the user enable fast re-authentication (which does not require a user interaction) for user profiles that may extend beyond logoff.
- The SSC user interface does not support the *extendUserConnectionBeyondLogoff* parameter setting for user created connections unless the parameter is added to the *userConnection.xml* file.
- There is no administrative setting in the policy which allows or prohibits using the parameter in networks configured by a user.
- There may be a case when authentication fails due to authorization failure on the AAA server (e.g., users may be allowed to connect only during business hours). In EAP there is no definitive way to distinguish such failures from authentication failures due to incorrect credentials. In such cases, you may want to retry the same credentials later. But in case of an actual authentication failure, the same credentials should not be tried again in order to prevent the user's account from being locked. SSC version 5.1 flushes all credentials when an EAP failure is received after the credentials were sent.

CHAPTER 3

Deploying or Installing Cisco SSC

This chapter lists SSC installation requirements and describes how to deploy, install, and upgrade SSC. The chapter contains these sections:

Before You Begin

To install SSC 5.1.1, you must have administrative privileges on the PC running Windows 2000, Windows XP, or Windows Vista. Before beginning the installation, please observe these guidelines:

- Review your authentication server requirements:
  - Identify and prioritize the needed authentication protocols.
  - Ensure that the authentication policies are configured in the user and machine profiles of the SSC distribution package.
  - If necessary, configure the server certificate on the authentication server.
  - If personal certificates are required for user authentication, ensure that the certificate infrastructure is configured and operational.
- Ensure that the access points and switches in your network are properly configured for 802.1X authentication.
- Ensure that your user PCs are configured with the required wired and wireless network cards and drivers.
- Prior to actual user deployments:
  - Test your client distribution package on a lab PC and ensure the user and machine profiles are working properly.
  - Uninstall other client management software, such as the Odyssey Client Manager. The Cisco Aironet Client Utility (ACU) and the Cisco Aironet Desktop Utility (ADU) can coexist with SSC and do not need to be uninstalled.
  - Ensure that Microsoft Internet Explorer 5.0 or later is installed on the user's PC.

Requirements

The supported operating systems are:

- Windows Vista Business, Enterprise and Ultimate Editions—32-bit and 64-bit
  - Required Windows Hot Fixes:

    KB952613
    KB935222 or SP1
    KB932063 or SP1
- Windows XP Professional (SP2)—32-bit
- Windows 2000 (SP4)—32-bit
- Windows 2003 Server Enterprise Edition (SP2)—32-bit

Note Other Windows XP versions, such as Media Center, Tablet PC, and Professional x64 are not supported. Other Windows Vista versions, such as Home Premium and Home Basic are not supported.

Note The latest drivers should be loaded on the user's PC prior to installing SSC.

Note Cisco strongly recommends that you install Windows Vista Service Pack 1. However, SP1 is required if wired network connections are to be attempted before user logon.

Installing SSC

The system administrator normally deploys the SSC client destination package to the end user PC, and SSC is automatically installed without user intervention. Typically, the system administrator provides pre-configured enterprise network connections in the destination package.

Prior to distributing the destination package to end users, the system administrator should manually install SSC and test the configured profiles to ensure that they operate correctly.

Manually Installing an SSC Test Package

To manually install SSC on a PC, follow these instructions:

Step 1 Obtain the client destination package .msi file produced by the SSC management utility

Step 2 Place the file in a folder on a test PC.

Step 3 Double-click the client destination package .msi file.

Step 4 Click **Next** and the license agreement window appears.

Step 5 Read and accept the terms in the license agreement, then click **Next**.

Step 6 Accept the default destination folder or click **Change** and follow the prompts to the desired folder. When complete, click **Next**.

Step 7 Click **Install** and a bar appears indicating the progress of the installation.

Step 8 When the installation is complete, click **Finish** and a pop-up message appears indicating that your PC must be restarted and asks if you want to restart now.

Step 9 Click **Yes** and your PC reboots.

When you log in to the PC, the SSC icon appears in the system tray.

Deploying to a User PC

SSC does not provide mechanisms for moving files to user PCs; however, there are numerous third-party methods available for use by the system administrator. Cisco assumes that the IT Administrators already have a preferred method of moving files to user PCs, such as Microsoft's System Management Server (SMS) method.

When the SSC destination package file is placed on the user's PC, the standard Microsoft installer mechanism can be used by the system administrator to silently install the SSC destination package file. For this example, execute this command:

msiexec /i yourCisco-SSC-XP2K-5.msi /quiet

The **/quiet** parameter prevents the installation process from being visible to the user and prevents user interaction.

Note When you are upgrading or reinstalling SSC, the new SSC destination file must have the same fileneme as the previous installation.

Upgrading SSC Running Windows 2000 or Windows XP

Migrating From SSC 5.0 to SSC 5.1.1

Previously installed SSC 5.0 software with administrator pre-deployed configurations must be uninstalled and the PC rebooted prior to installing SSC 5.1.1. The SSC 5.1.1 installation process automatically detects a previous SSC 5.0 pre-deployed package installation and displays an error message indicating *Internal error 2771 Core* and fails to install. After SSC 5.0 software is uninstalled from the user's PC and the PC rebooted, SSC 5.1.1 can be successfully installed.

Note The installation error occurs because the SSC 5.0 pre-deployed installation package functionality is not in compliance with the Windows Installer Component Rules. This prevents backwards compatibility and the normal SSC upgrade procedure, which does not require an explicit uninstall-reboot and install-reboot sequence.

If the SSC 5.0 software does not contain a pre-deployed configuration, there is no need to uninstall the SSC software prior to installing SSC 5.1.1.

After the SSC 5.1.1 installation, the PC must be rebooted for the SSC software changes to take effect.

Migrating From SSC 4.x to 5.x

The SSC installation process uninstalls SSC releases 4.1.1 to 4.2.x and converts the user configurations from the SSC 4 product to SSC 5.1.1 configuration settings.

SSC releases earlier than 4.1.1 are not converted or uninstalled. The earlier SSC release must be manually installed before you install SSC 5.1.1. Also, the SSC 5.1.1 installation process will indicate that the previous SSC release must be manually uninstalled.

Note For some configurations, it might be easier and faster to create a new destination package file using the SSC management utility.

Upgrading Administrator-Deployed Networks from SSC 4.1.x to 5.x

An administrator must have the following SSC 5.x client elements on his PC:

- SSC 5.x installation msi file (Cisco_SSC-XP2K-5.msi)
- Configuration management utility (sscMgmtToolkit_5.x.0.xxxx.zip)
- Configuration combining tool (ConfigCombiner.exe)
- Configuration conversion tool (ConfigConverter.exe)
- Administrator xslt file (configConvert_3_1_admin.xslt)—used to translate administrator-configured SSC 4.1 networks to SSC 5.x schema.
- sscPackageGen utility that generates a custom client destination package file.

Note The ConfigCombiner.exe, ConfigConverter.exe, and Convert_3_1_admin.xslt files are only available after the SSC 5.1.1 installation completes. The files are located in the C:\Documents and Settings\All Users\Application Data\Cisco Secure Services Client\Conversion Tools folder.

The administrator also must have the current SSC 4.x deployment package translated into SSC 4.1.2 internal configuration. This is the *profiles* folder found in the *Program Files\Cisco Systems\Cisco Secure Services Client* folder.

In order to deploy an SSC 5.1.1 client that is equivalently configured to your SSC 4.x destination, you must perform these operations:

1. Use the combining tool (ConfigCombiner.exe) to combine SSC 4.1 configuration files into a single file:

   Usage: ConfigCombiner.exe [options]

   Options include:

   --source *directory* or -s *directory*—specifies the source directory path. If the source directory option is not specified, the default value for the source directory is *C:\Program Files\Cisco Systems\Cisco Secure Services Client\profiles*.

   --quiet or -q—do not display the results

   --help—gives the usage of the tool

The following illustrates a combining tool example:

```
ConfigCombiner.exe -q
```

The output of this operation produces a file called *configuration.xml*. The file is located in the folder where the tool was executed. The file contains the information in the multiple folders under *c:\Program Files\Cisco Systems\Cisco Secure Client Services\profiles*.

Note SSC 4.1.x files are not modified in any way as a result of this operation.

2. Use the conversion tool (ConfigConverter.exe) with the administrator XSLT file (configConvert_3_1_admin.xslt) to convert the output of the combining tool into an SSC 5.1.1 configuration.xml file:

   Usage: ConfigConverter.exe [options]

   Options include these values:

   --quiet or -q—specifies to not display the results

   --output *filename* or -o *filename*—specifies the output XML file

   --input *filename* or -i *filename*—specifies the input XML file

   --xslt *filename* or -xslt *filename*—specifies the XSLT file

   You should specify the *--xslt* file option with the XSLT file name set to *configConvert_3_1_admin.xslt* when you are converting the administrator-deployed networks using the ConfigConverter tool. This is the same tool used with a different default xslt file to translate the end user created networks on end user systems.

   The following illustrates a conversion tool example:

```
ConfigConverter.exe -i configuration.xml -o configuration.xml
--xslt configConvert_3_1_admin.xslt
```

   The output of this operation is an SSC 5.1.1 schema compatible destination package with an equivalent configuration of your SSC 4.1.x deployed networks.

3. You can now use the management utility to perform these operations:
   - Read in the SSC 5.1.1 configuration.xml (which contains the administrator-deployed SSC 4.1 networks).
   - If needed, modify the SSC 5.1.1 configuration.xml file.
   - Sign the SSC 5.1.1 configuration.xml file.
4. Run the sscPackageGen tool to bundle the signed configuration.xml file along with the SSC 5.1.1 msi file and then deploy the package.

Upgrading End User Created SSC 4.1.x Networks to 5.x

When SSC 5.1.1 is installed on a PC as an upgrade, it automatically upgrades the SSC Release 4.1.x end user created networks to SSC 5.1.1 networks. There is nothing that you, the administrator, or the end user need to do. The results of the upgrade are as follows:

- SSC 5.1.1 starts running with the deployed administrator configuration file.
- All the end user created profiles from SSC 4.1 are imported into SSC 5.1.1.
- This conversion is done once only during the upgrade.

- SSC 4.1 has multiple user xml files on an end-station, but SSC 5.1.1 has only one user XML file. The conversion tool places the contents of multiple SSC 4.1 user profile files into the single SSC 5.1.1 user XML file. Each user XML file in SSC 4.1 corresponds to a group in SSC 5.1.1. The group name is the user xml file name prefixed with *SSC 4_*. The profiles in the *allusers* file are placed in the *SSC4_allusers* group. It is the responsibility of the end user to later go through the list of available networks using the GUI and delete any networks they do not want.
- There may be multiple networks created in SSC 5.1.1 for a single network in SSC Release 4.1. This is because the SSC 5.1.1 schema allows only one EAP-method per network, whereas the SSC 4.1 schema allows multiple EAP methods per network. This means that a user network from SSC 4.1, after conversion to SSC 5.1.1, has a network name that includes both the SSC 4.1 network name and the EAP method. This is done to help avoid confusion.
- On an upgrade from SSC 4.1 to SSC 5.1.1, all static user credentials are imported into SSC 5.1.1. Also, the WEP and PSK credentials entered by the user are also imported into SSC 5.1.1. However, any 802.1X credentials are not imported, they need to be re-entered if required.

Pre-Installation of Client Certificates

If the end user SSC file uses a client-certificate-based EAP method, the client certificate used to supply the user's credentials must be independently deployed and placed in the proper Windows Certificate Store (User-Personal Store). The destination package file can be used to deploy a server certificate, an intermediate CA certificate, and/or the trusted root certificate on the user’s PC.

Upgrading SSC from Windows XP to Windows Vista

After upgrading your operating system from Windows XP to Windows Vista, the previously installed SSC software must be uninstalled. After the SSC software is uninstalled from the user’s PC and the PC rebooted, SSC 5.1.1 for Windows Vista can be successfully installed.

After the SSC 5.1.1 installation, the PC must be rebooted for the SSC software changes to take effect.

Upgrading SSC Running on Windows Vista

A previous version of SSC 5.1.1 software for Windows Vista can be upgraded to a later version by reinstalling SSC using the procedures define in the “Installing SSC” section on page 3-2. The SSC 5.1.1 installation process automatically detects a previous SSC 5.1.1 installation and maintains any existing connection profiles.

After the SSC 5.1.1 installation, the PC must be rebooted for the SSC software changes to take effect.

Upgrading Only SSC Profiles in all Supported Operating Systems

After the administrator has successfully deployed SSC on the user’s PC, it might become necessary from time to time to modify the deployed connection settings or policies due to an infrastructure improvement, new security policies, and so on. The administrator can modify these settings and profiles by generating an updated configuration.xml file using the SSC management utility. The administrator only needs to deploy the configuration.xml file on the user’s PC and does not need to reinstall SSC.

The revised configuration.xml file must be installed in this directory location on the user's PC:

- Windows 2000 and Windows XP:

  C:\Documents and Settings\All Users\Application Data\Cisco\Cisco Secure Services Client\system

- Windows Vista:

  C:\ProgramData\Cisco\Cisco Secure Services Client\system

SSC switches to the new configuration when any one of these events occurs:

- The PC reboots.
- The current network connection is lost. Before attempting to establish the connection again, SSC switches to the new configuration.
- The user explicitly initiates the configuration switch by right-clicking the SSC tray icon and choosing **Repair**.

CHAPTER 4

Using Cisco SSC

This chapter provides an overview of SSC and the main SSC GUI features available to the user. The chapter contains these sections:

Note The illustration colors might be different in some of the figures.

Overview

SSC runs from two logical interfaces:

- SSC tray icon—A minimal user interface designed for quick access to primary SSC functions and information.
- Main SSC GUI window—The primary user interface designed to provide complete SSC functionality.

The SSC tray icon interface simplifies the user interface similarly to a Windows wired connection icon. The SSC tray icon allows the user to manage wireless connections using a few simple clicks.

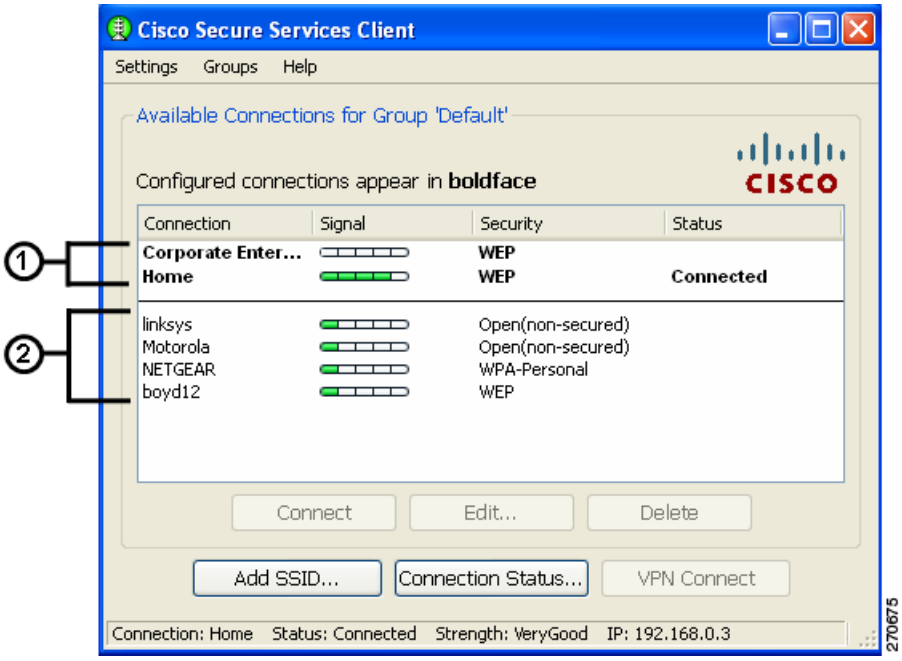
The main SSC GUI interface adds functionality for configuring networks, enabling or disabling the client, configuring VPN, and viewing network information such as signal strength and the complete network scan list.

Using the Main SSC GUI Window

The main SSC GUI window contains three main areas to help the user configure, control, and manage networks (see Figure 4-1):

- Menu area—Enables and disables SSC and the Wi-Fi radio, views and configures groups, and obtains helpful information.
- Graphical area—Displays a listing of configured network connections and a list of detected neighboring networks.
- Button area—Allows the user to add, edit, delete, and connect to network connections. The user can also view connection status information and connect using a VPN tunnel.

Figure 4-1 Main SSC GUI Window



1	Configured connections are listed in the following order: First—By administrator-created connections in the order they were deployed, with global networks always listed first. Second—By user-created connections in the order they were created.	**2**	Discovered scan-list connections are neighboring networks that might be available for user connections. They are identified by the SSID of the wireless access point. These connections are listed by security level groupings.

Table 4-1 describes the main SSC GUI window components.

Table 4-1 Main SSC GUI Window Components

Component		Description
Column	Connection	Identifies a list of configured network connections and a scan-list of detected neighboring networks.
	Signal	When the connection is wireless, this column displays a relative signal strength bar of the received radio signal. If the wireless connection is not detected or hidden (non-beaconing), then an empty bar is displayed. If the connection is wired, a static placeholder icon is displayed.
	Security	Identifies the security level: Open (non-secured)—Specifies no authentication and no encryption. WEP—Legacy open association with static WEP encryption or shared association with WEP-shared keys. WPA/WPA2-Personal—A Wi-Fi standard that uses a pass-phase pre-shared key (PSK). WPA2 is a recent upgrade to WPA based on the full 802.11i standard. WPA/WPA2-Enterprise—A Wi-Fi standard that uses an authentication server. WPA2 is a recent upgrade to WPA based on the full 802.11i standard. CCKM-Enterprise—Cisco Central Key Management (CCKM) security protocol enables an 802.11 station to quickly re-authenticate and establish a new session between a client and a new parent access point. **Note** For the configured networks, the security level displayed is the setting configured by the administrator and the user. For the scan-list detected networks, the security level is the most secure level when multiple security levels are available.
	Status	Displays the current connection status: Searching for adapter—Specifies an adapter is not available or the adapter is disabled. Associating—The connection is currently associating using the 802.11 association protocol. Authenticating—The connection is currently authenticating using the 802.1X authentication protocol. Acquiring IP address—The connection is obtaining an IP address. Connected—A connection has been established. Scanning for a Network—SSC is currently searching for an available network. VPN Connecting—SSC is attempting to establish a VPN connection. VPN Connected—The VPN connection has been successfully established.

Table 4-1 Main SSC GUI Window Components

Component		Description
Button	Connect	Used to connect to a highlighted configured connection or a neighboring network from the scan list.
	Edit	Used to edit the highlighted user-configured connection. The user cannot edit a pre-configured network connection or neighboring networks in the scan list.
	Delete	Used to delete the highlighted user-configured connection. The user cannot delete a pre-configured network connection or a neighboring network in the scan list.
	Add SSID	Used to add and configure a new connection.
	Connection Status	Displays status information for the current connection being used.
	VPN Connect	Used to activate a VPN connection. VPN must be specified in the administrator's client policy settings in the configuration.xml file.
Menu	Settings	Enable Client—Allows the user to enable or disable SSC. Enable Wi-Fi Radio—Allows the user to enable or disable the radio. A checkmark indicates that the option is enabled.
	Groups	Contains a lists the configured groups and a group configuration option. Configure Groups—Allows the user to configure a new group of configured connections.
	Help	Allows the user to obtain helpful information. Help—Provides SSC help information. Repair—Allows the user to repair the SSC. About—Provides SSC version information.

Connecting with Configured Connections

The main SSC GUI window contains a list of network administrator-deployed pre-configured connection profiles and a list of user-created configured connection profiles. SSC supports two modes for making connections:

- Automatic connection mode
- Exclusive connection mode

Automatic Connections

In the normally preferred automatic connection mode, SSC automatically chooses the best available configured connection. If the group contains both wired and wireless connections, the wired connection has higher priority.

Note SSC allows only one connection at a time.

The SSC automatic connection mode is described in the following operating system sections.

Windows 2000 or Windows XP

In automatic connection mode, SSC starts at the top of the configured connection list and attempts to associate with the first network. When a connection is unsuccessful or broken, SSC attempts to associate with the next entry in the list. This operation (sometimes called walking-the-list) continues until a successful connection is established.

These conditions cause SSC to restart at the top of the configured network connection list:

- The user restarts the PC or a power interruption occurs.
- The user switching to a different connection group.
- The user clicks the Repair option to restart SSC.

In automatic connection mode, the user can override the SSC connection criteria by performing one of these operations:

- Highlighting a configured connection and clicking the Connect button.
- Right-clicking a configured connection and choosing the Connect option.
- Double-clicking a configured connection.

These operations cause SSC to break the current connection and attempt to initiate a connection with the selected configured connection. SSC remains in the automatic connection mode. If the connection attempt is unsuccessful, SSC attempts to connect to the first configured connection in the configured network connection list.

Windows Vista

In automatic connection mode, SSC starts scanning for available networks and attempts to connect to the first configured network that matches a network found in the scan list.. When a connection is unsuccessful, SSC attempts to connect to the next configured network connection found in the scan list. SSC continues moving through the configured network connections found in the scan list until a successful connection is established or an SSC timer expires. When the SSC timer expires, SSC begins scanning for active networks again.

When SSC is scanning for active configured networks, SSC displays *Scanning for a Network* in the main SSC GUI window and the Connection Status window.

These conditions cause SSC to restart scanning for active networks:

- The user restarts the PC or a power interruption occurs.
- The user switches to a different connection group.
- The user clicks the Repair option to restart SSC.
- The current network connection fails and cannot be reactivated.

In automatic connection mode, the user can override the SSC connection criteria by performing one of these operations:

- Highlighting a configured connection and clicking the Connect button.
- Right-clicking a configured connection and choosing the Connect option.
- Double-clicking a configured connection.

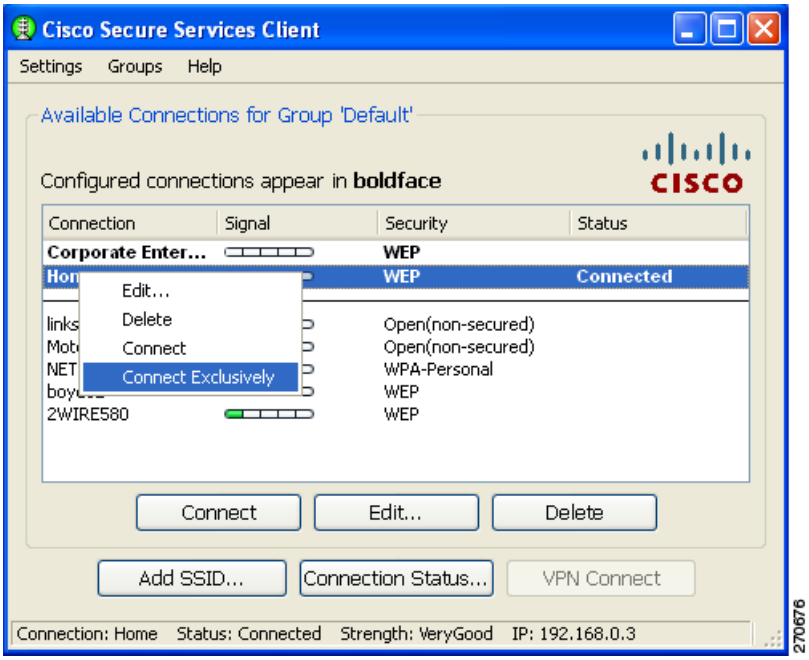
These operations cause SSC to break the current connection and attempt to initiate a new connection with the selected configured connection. SSC remains in the automatic connection mode.

If the connection attempt is unsuccessful, SSC starts scanning for an active networks.

Exclusive Connections Mode

SSC allows the user to specify an exclusive connection (see Figure 4-2). This causes SSC to break an existing connection and forces SSC to exclusively attempt to connect to the new specified selection. If the connection fails or is broken, SSC does not attempt to switch to an alternate connection.

Figure 4-2 Connect Exclusively Option



The user can activate the exclusive connection option by right-clicking a configured connection and choosing the Connect Exclusively option.

To exit the exclusive connection mode and revert to automatic connection mode, the user must right-click the connection and choose the Connect Exclusively option again.

The typical reason for using the exclusive connection mode is to force SSC to drop an existing wired connection and to connect only to the specified wireless connection.

Creating New Connections

The user can manually configure a new connection several ways:

- Double-clicking a detected network from the scan-list.
- Right-clicking a detected network from the scan-list and choose the Connect option.
- Highlighting a detected network from the scan-list and click the Connect button.
- Clicking the Add SSID button. The Add SSID button should be used in these wireless situations:
  - Scanable access point—Transmits beacons or responses to active probes to allow detection but is known not to be available (not physically within detection range).
  - Non Scanable access point—Not configured to be detectable in a wireless scan (not-beaconing or hidden) and might not be physically within detection range.

SSC Security Options

Using the SSC GUI, the user can create new connection profiles using these security options:

- Open(non-secured)
- WEP
- Shared WEP
- WPA Personal AES
- WPA Personal TKIP
- WPA2 Personal AES
- WPA2 Personal TKIP
- WPA Enterprise AES
- WPA Enterprise TKIP
- WPA2 Enterprise AES
- WPA2 Enterprise TKIP
- CCKM Enterprise AES
- CCKM Enterprise TKIP

Note The security options that are available to a user depend upon the administrator-enabled options in the deployed SSC configuration file.

Configuring VPN Connection Options

The bottom section of all the connection security configuration windows allows the user to configure VPN connection options. To configure the VPN options, the user performs these operations:

- Check the Automatically connect to VPN option.
- Click the drop-down arrow and choose one of the VPN authentication options.

Note The VPN connection option is only available when Cisco IPSec VPN is installed on the user's PC.

- For Windows 2000 and Windows XP, Cisco IPSec VPN must be version 4.8 or later.
- For Windows Vista, Cisco IPSec VPN must be version 5.0.03.0560 or later.

Note For Windows 2000 and Windows XP, when using VPN with SofToken-II and SSC prompts for the username and PIN, the user must provide to SSC the PIN normally intended for the SofToken application. The user must not enter the one-time password that is generated by the SofToken-II application rather than the username and pin.

Note For Windows Vista, Secure Computing SofToken II is not supported. When SofToken II authentication is specified in the network configuration, SSC prompts for the username and the actual one-time password rather than the username and password for the soft token account.

Note SSC maintains the user's VPN credentials only until the user logs off or SSC shuts down.

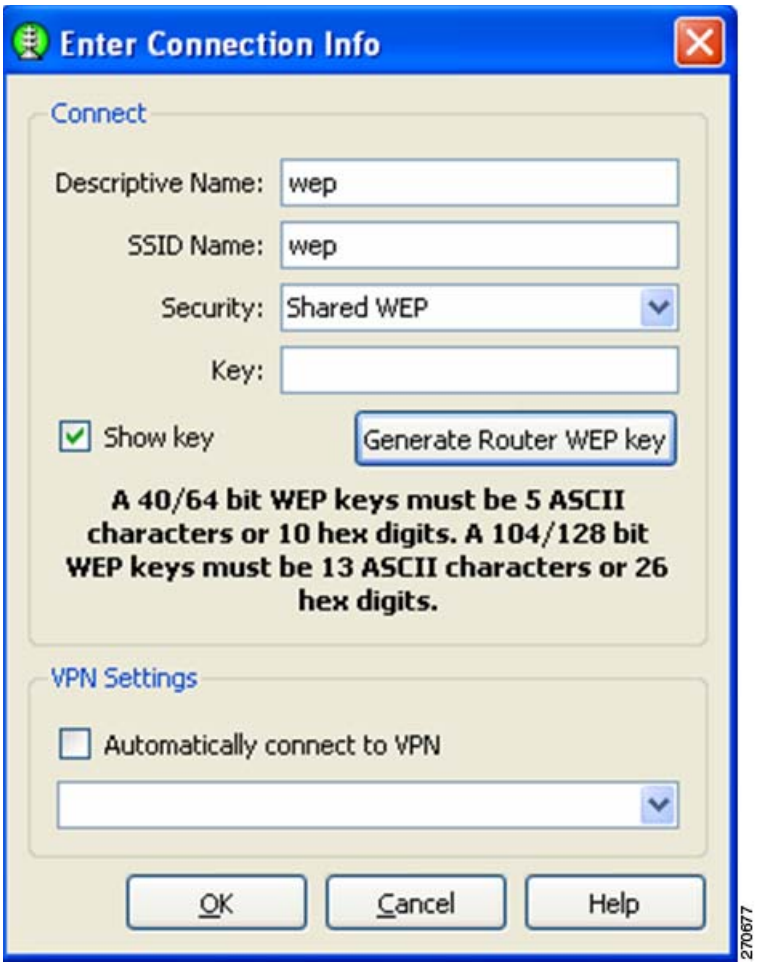
Using an Open Non-Secured Network Connection

When the user selects an Open(non-secured) network from the scan-list, SSC automatically reassigns the connection as a configured connection, moves the connection to the bottom of the configured connections list, and initiates the connection (unless a higher priority wired connection is available).

Configuring a WEP or Shared WEP Connection

When a user selects a WEP or Shared-WEP network from the scan-list, the Enter Connection Info window appears (Figure 4-3). The user needs to enter a descriptive name for the profile, the SSID name, and the WEP key information. When the Show key option is checked, the actual characters entered are displayed to allow the user to visually verify the key information.

Figure 4-3 WEP or Shared WEP Information



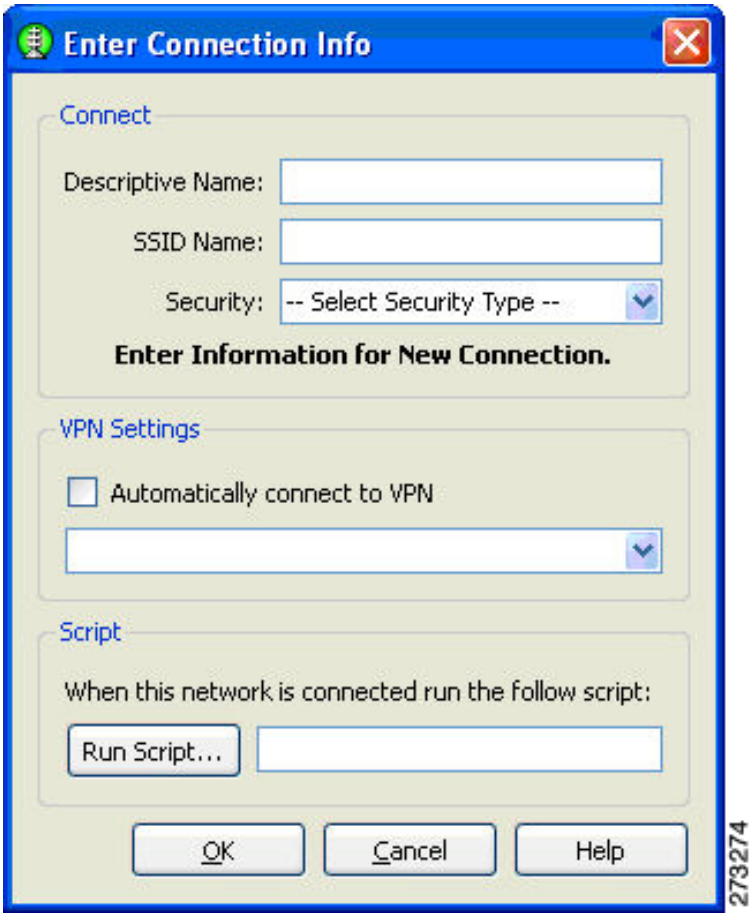
Some routers use a pass-phrase to create a unique WEP key. The Generate Router WEP key button can be used to enter a router pass-phrase of 64 bits (10 hexadecimal digits) or 126 bits (26 hexadecimal digits) that SSC uses to create a WEP key.

The VPN Settings option enables the user to choose if an automatic VPN connection is used and to choose the VPN server location by clicking the drop down arrows.

If the administrator enables the scripting feature allowing users to specify a local file (.exe, .bat, or .cmd) to run when the network gets to a connected state, the user's GUI runs the file when the network state is connected. Figure 4-6 shows the Enter Connection Info dialog box that appears on the user's screen for a user created network when the user selects **Add SSID** with scripting enabled.

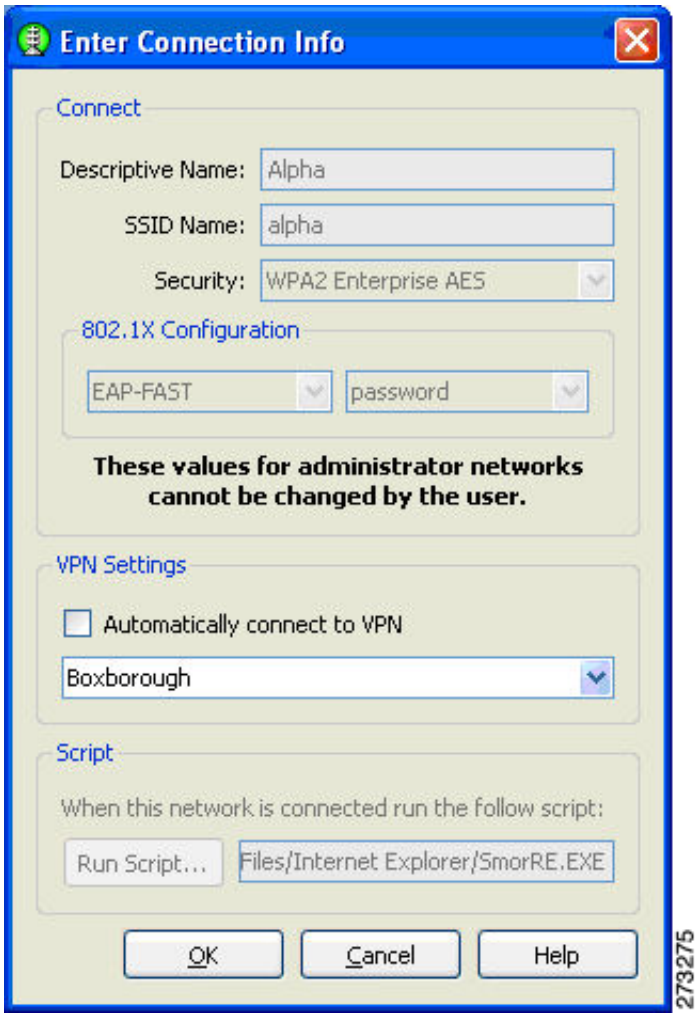
Note The scripting feature is supported in Windows 2000 and Windows XP. It is not supported in Windows Vista.

Figure 4-4 User Created Network - Enter Connection Info Dialog Box When Add SSID is Selected



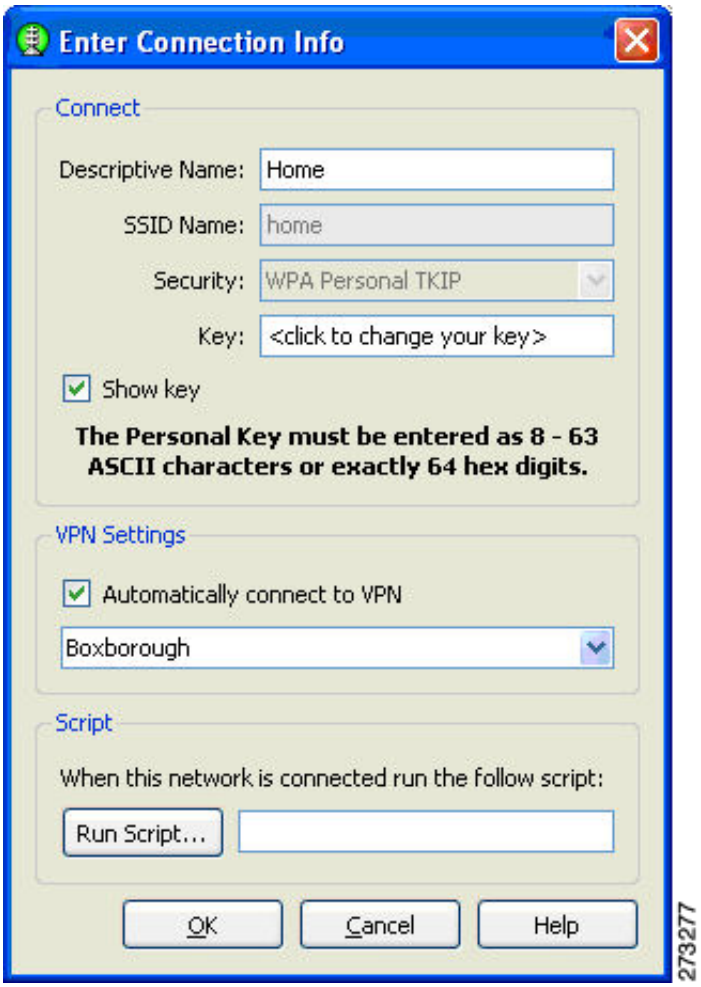
The Script group box is disabled for administrator created networks. Figure 4-5 shows the dialog box that appears on the user's screen for an administrator created network when the user selects **Edit**.

Figure 4-5 Administrator Created Network - Enter Connection Info Dialog Box When Edit is Selected



If the user selects a user created network with scripting enabled, shows the dialog box that appears when the user selects **Edit**.

Figure 4-6 User Created Network - Enter Connection Info Dialog Box When Edit is Selected



When complete, the user clicks the OK button.

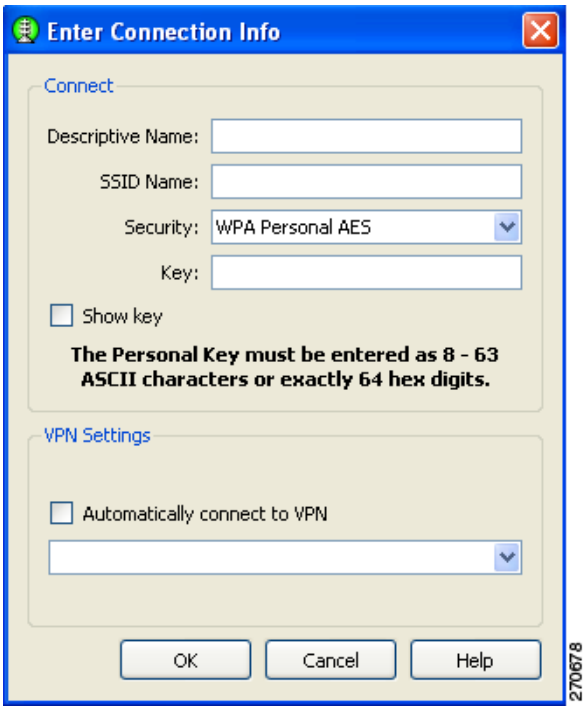
Configuring a WPA Personal or a WPA2 Personal Connection

When the user selects a network with WPA Personal or WPA2-Personal security options, Figure 4-7 appears. The user needs to enter a descriptive name and the SSID name for the profile.,and the key information. When the Show key option is checked, the actual characters entered are displayed to allow the user to visually verify the key information.

SSC supports these WPA Personal and WPA2 Personal security types:

- WPA Personal AES or WPA Personal TKIP
- WPA2 Personal AES or WPA2 Personal TKIP

Figure 4-7 WPA Personal or WPA2 Personal Information



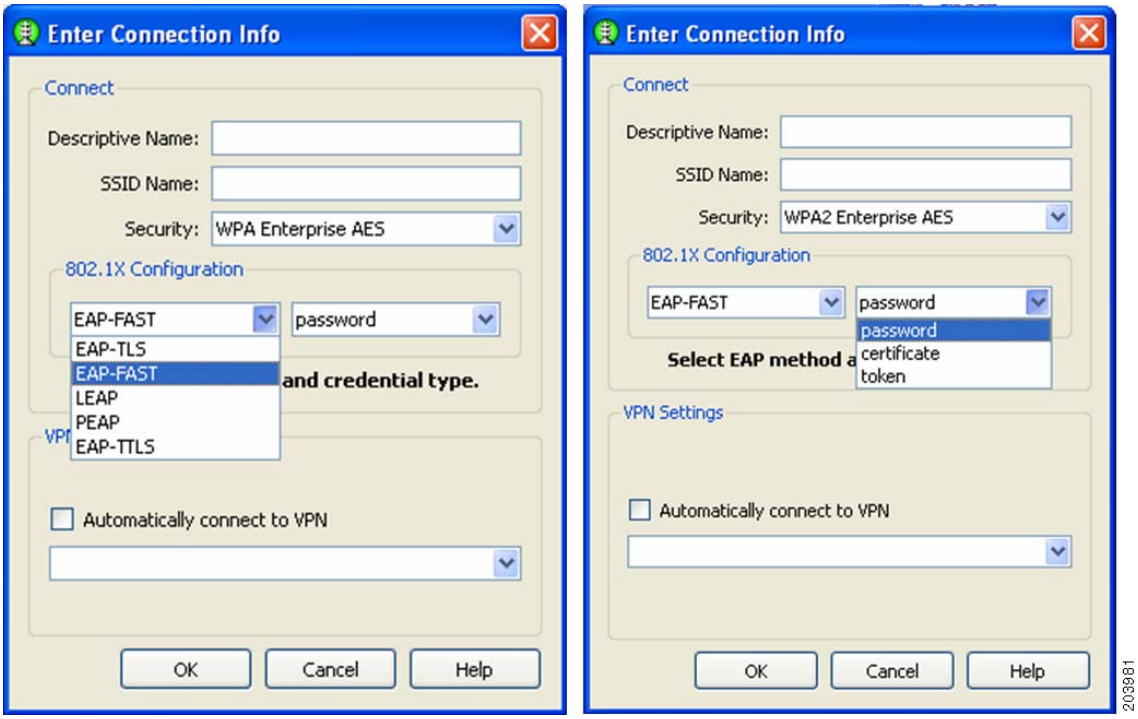
The VPN Settings option enables the user to choose if an automatic VPN connection is used and to choose the VPN server location by clicking the drop down arrow.

When complete, the user clicks the OK button.

Configuring an 802.1X Connection

When the user selects a network with 802.1X security from the scan list, the user needs to enter a descriptive name for the profile, the SSID name, and choose the EAP method and credential type that are used (see Figure 4-8).

Figure 4-8 802.1X Security Information



Note The SSC GUI provides a limited subset of 802.1X options. For deployment purposes, 802.1X profiles should be created by the network administrator using the SSC management utility.

SSC supports these 802.1X security types:

- WPA Enterprise AES
- WPA Enterprise TKIP
- WPA2 Enterprise AES
- WPA2 Enterprise TKIP
- CCKM Enterprise AES
- CCKM Enterprise TKIP

Note The specific options available to a user depends upon the administrator-enabled options in the deployed SSC configuration file.

The user clicks the EAP method drop-down arrow and chooses one of these SSC supported EAP methods:

- LEAP
- PEAP
- EAP-TLS
- EAP-TTLS
- EAP-FAST

Note The Windows Vista version of SSC does not support EAP-TLS, and EAP-TTLS. These options are not available on the EAP method drop-down list.

The user clicks the certificate type drop-down arrow and chooses one of these SSC supported certificate types:

- Static password, Certificate, or Token

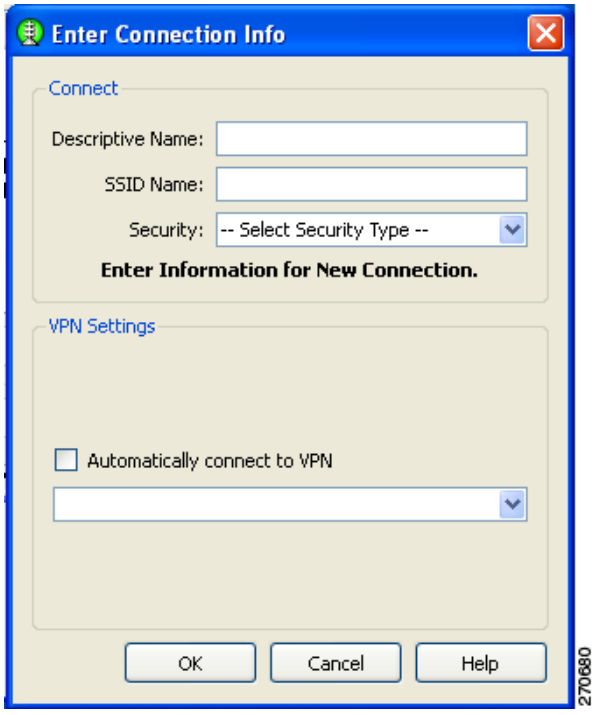
The VPN Settings option enables the user to choose if an automatic VPN connection is used and to choose the VPN server location by clicking the drop down arrow.

When complete, the user clicks the OK button.

Configuring a New Connection Using the Add SSID Button

When the user clicks the Add SSID button, Figure 4-9 appears.

Figure 4-9 New Connection Information



The user needs to configure these connection options:

1. Descriptive Name—A name that is displayed to identify the connection.
2. SSID Name—The network name that is used to establish the connection and is broadcast by the access point in its beacon.
3. Security—Specifies the type of security authentication used by the connection (see the "SSC Security Options" section on page 4-7).
4. VPN Settings—Enables the user to choose if an automatic VPN connection is used and to choose the VPN server location by clicking the drop down arrow.
5. When complete, the user clicks the OK button.

Managing Configured Connections

From the main SSC GUI window, the user can edit or delete user-created configured connections.

Note Administrator-deployed pre-configured connections cannot be edited or deleted by the user, but the settings can be viewed.

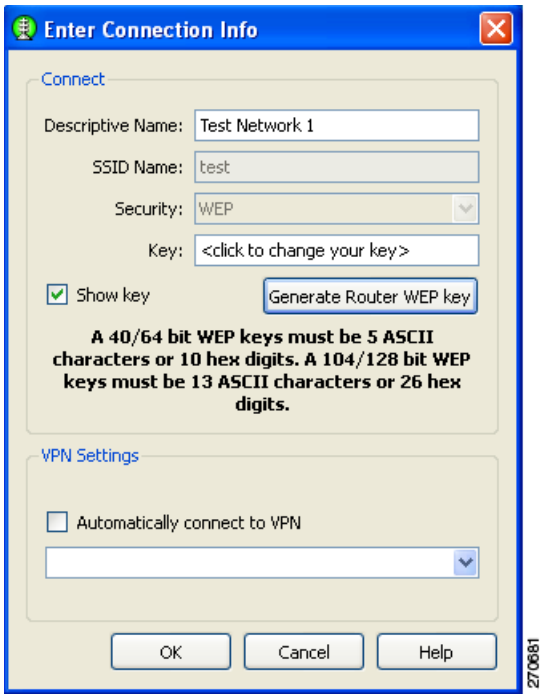
To delete a user-created configuration connection, the user needs to right-click the desired configuration connection and choose the Delete option.

Editing a User-Created Configured Connection

The main SSC GUI window provides these edit options for user-created configured connections:

- Right-click the desired configured connection and choose the Edit option. Figure 4-10 appears.
- Highlight the desired configured connection and click the Edit button. Figure 4-10 appears.

Figure 4-10 Configured Connection Profile Fields



The user can edit these connection profile fields:

- Descriptive Name
- Key (when applicable)
- VPN Settings

Note To change the security mode of the connection, the user must first delete the connection and then recreate the connection using a new security option.

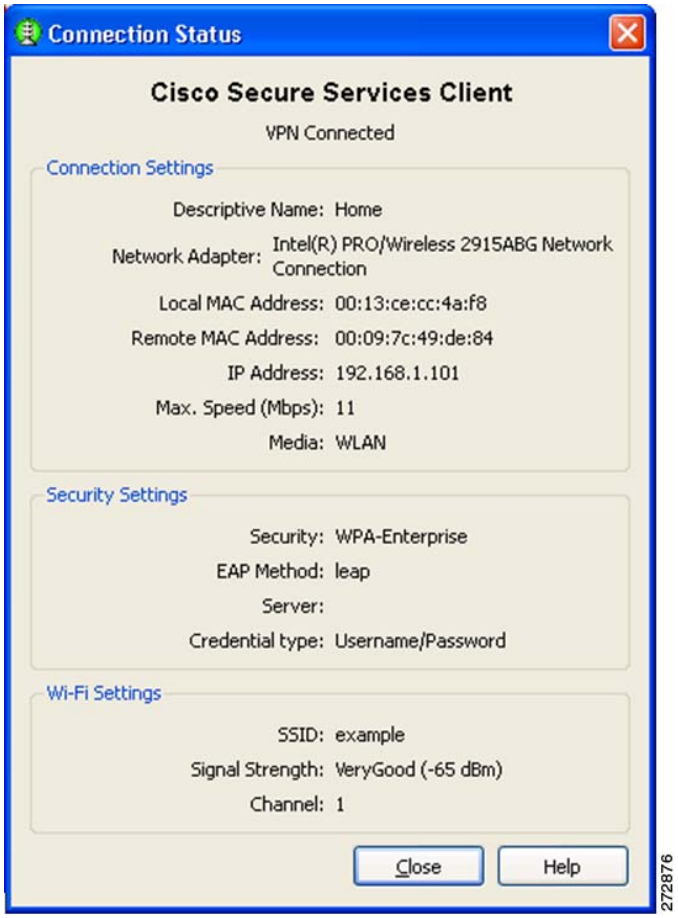
When complete, the user clicks the OK button.

Obtaining Connection Status Information

You can obtain current connection status information by performing one of these operations:

- On the SSC GUI window, click **Connection Status** and Figure 4-11 appears.
- Right-click the SSC tray icon and choose **Connection Status**. Figure 4-11 appears.

Figure 4-11 SSC Connection Status Window



The Connection Status window contains these informational sections:

- Connection status
- Connection Settings
- Security Settings
- Wi-Fi Settings

Connection Status

The connection status area indicates the state of the active connection (same as the Status field of the main SSC window). These are the supported connection states:

- Searching for adapter—SSC is searching for an active adapter. An active adapter is not currently available or the adapter is disabled.
- Associating—SSC is performing the 802.11 association protocol.
- Authenticating—SSC is performing the 802.1X authentication protocol.
- Acquiring IP address—SSC is attempting to obtain your IP assignment from a DHCP server.
- Connected—The adapter is successfully connected to an access point.
- Scanning for a Network—SSC is currently searching for an available network.

- VPN Connecting—SSC is attempting to establish a VPN connection.
- VPN Connected—The VPN connection has been successfully established.

Connection Settings

This section indicates the current connection settings. These are the fields supported:

- Network Adapter—Identifies the friendly name for the associated network adapter used for the network connection.
- Local MAC Address—The local MAC address of the network adapter.
- Remote MAC Address—Identifies the MAC address of the access point.
- IP Address—Identifies the address currently assigned to the adapter (shown in standard x.x.x.x format).
- Max. Speed (Mbps)—Indicates the maxumum data rate supported by the adapter.
- Media—Identifies the physical type of the connection as follows:
  - WLAN— Indicates a wireless Wi-Fi connection.
  - Ethernet—Indicates a wired connection.

Security Settings

This section indicates the current security settings for the connection. These are the supported fields:

- Security—Indicates the current security type being used on the connection. These are the supported options:
  - Open—No authentication and no encryption is being used.
  - WEP—Legacy open association with static WEP encryption (staticWep) or shared association with WEP shared keys (shared)
  - WPA–Personal or WPA2–Personal—This security type uses a pass-phase preshared key (PSK). WPA2 is a recent upgrade to WPA based on the full IEEE 802.11i standard.
  - WPA–Enterprise or WPA2-Enterprise—This security type uses an authentication server. WPA2 is a recent upgrade to WPA based on the full IEEE 802.11i standard.
  - CCKM–Enterprise—Cisco's Centralized Key Management (CCKM) is the basis of Cisco Fast reassociation and reauthentication solution, which utilizes an access point, as the key distributor to enable protected communications between the access point and the wireless clients.
- EAP Method—For an authenticating connection, this field indicates the outer EAP method used for authentication.
- Server—For an authenticating connection, indicates the following:
  - The server certificate's name (for mutually authenticating EAP methods)
  - The server's FAST A-ID (for EAP-FAST)
  - Unknown (for non-mutually authenticating EAP methods)
  - Blank when not performing 802.1x authentication
- Credential type—For an authenticating connection, indicates the type of user credentials used for authentication:
  - Username/Password
  - Client Certificate

- Token
- Key

WiFi Settings

This section indicates the connections Wi-Fi settings and contains these fields:

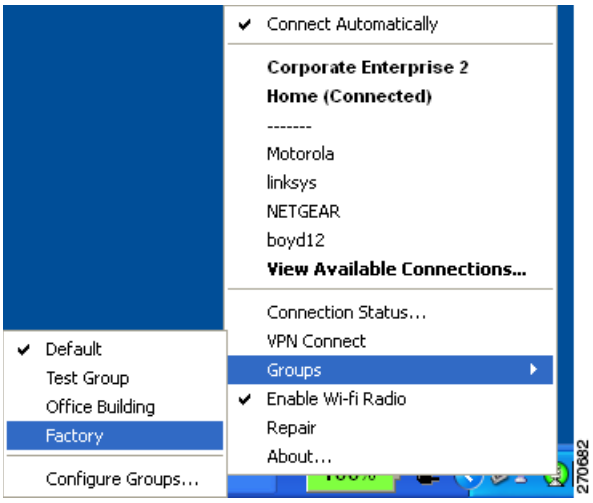
- SSID—The service set identifier for the WiFi connection.
- Friendly Name—The name assigned to a connection for display purposes
- Signal Strength—For wireless connections, five relative received radio signal levels are supported: very poor, poor, good, very good, excellent
- Channel—The 802.11 radio channel on which the network is communicating

Selecting Network Groups

SSC supports a group feature that allows the user to partition network connections into convenient groups. SSC provides two ways for the user to select and activate a configured connection group:

- Use the SSC tray icon (see Figure 4-12).
  - Right-click the SSC tray icon, scroll to Groups, and choose the desired group from the list.
- Use the Group menu on the main SSC GUI window (see Figure 4-13).
  - On the main SSC GUI window, click Groups and choose the desired group.

Figure 4-12 SSC Tray Icon Right-Click Menu



Changing the active group causes SSC to perform these operations:

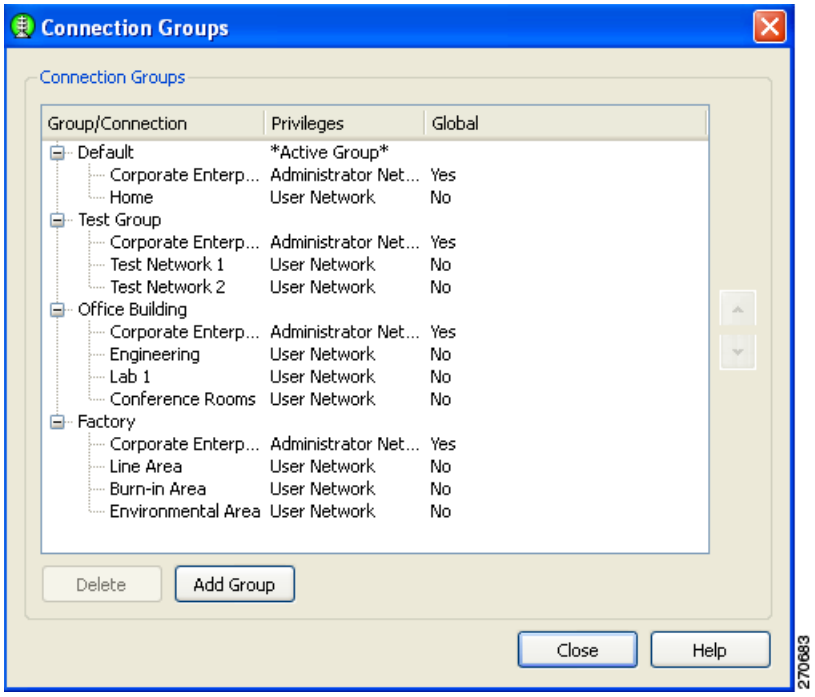
- Drops any active connection from the current group.
- Cancels exclusive connect mode if active.
- Starts the automatic connection process from the top of new group's connection list.

Managing Network Connection Groups

The user can manage network connection groups by using the Connection Groups window. To open the Connection Groups window, the user can perform one of these operations:

- From the main SSC GUI window, click ***Groups*** > **Configure Groups** and Figure 4-13 appears.
- Right-click the SSC tray icon, scroll to Groups, and choose **Configure Groups**. Figure 4-13 appears.

Figure 4-13 Connection Groups Window



From the Connection Groups window, the user can add new groups or delete user-created network connections or groups.

Note Pre-configured connections cannot be deleted by the user.

Tip Groups should be limited to a maximum of 8-10 profiles. Creating large groups can result in connection delays due to the time used scanning for unavailable network connections.

When complete, the user clicks the Close button.

Menu Controls

The main SSC GUI menu contains three menu selections:

- Settings—Used to enable or disable SSC or the radio.
- Group—Used to select, add, or delete groups.
- Help—Used to obtain helpful information, repair SSC, enable packet capture, or obtain SSC version information.

Settings Menu

When the user clicks **Settings**, a drop-down list appears (see Figure 4-14).

Figure 4-14 Settings Menu Options

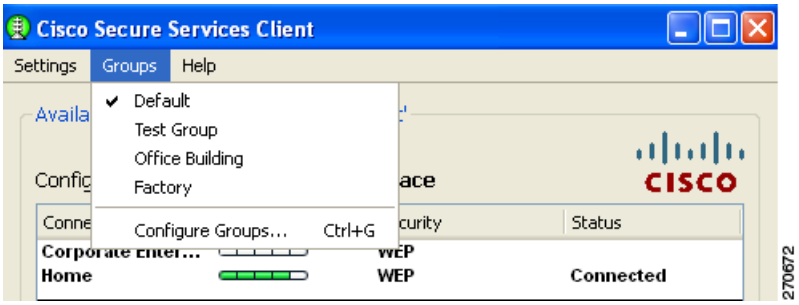
The Settings menu contains these options:

- Enable Client—Controls whether SSC is managing the network adapters.
  - When checked, the SSC is managing all wired and wireless adapters according to the allowed media policy setting of the deployed configuration file.
  - When unchecked, SSC is disabled and has relinquished control of all network adapters.
- Enable Wi-Fi Radio—Controls the state of the radio in all managed wireless adapters.
  - When checked, all wireless adapters radios are enabled and active.
  - When unchecked, all wireless adapter radios are disable and turned off.

Groups Menu

When the user clicks **Groups**, a drop-down list appears (see Figure 4-15).

Figure 4-15 Main SSC GUI Groups



The Groups menu provides these features:

- Displays a list of configured groups.
  - A checkmark indicates the active group.
  - The user can click on a listed group to activate the selected group.
- Configure Groups—Allows the user to create new groups and to delete user-created groups and configured connections. For additional information, see the "Managing Network Connection Groups" section on page 4-21.

Help Menu

When the user clicks **Help**, a drop-down menu appears with these options:

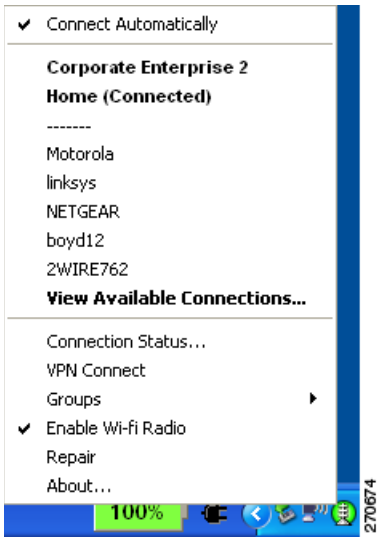
- Help—Opens the Help interface and provides helpful information.
- Repair—Forces a restart of the SSC service and causes the following actions:
  - The SSC tray icon displays a red x while the SSC service is restarting.
  - SSC detects and processes any new configuration settings.
  - SSC restarts in automatic connection mode from the top of the connection list for the previously active group.
- About—Displays the product name and version number.

Using the SSC Tray Icon

The SSC tray icon provides two convenient ways for the user to activate a desired connection:

- Double-click the SSC tray icon to activate the main SSC GUI window (see Figure 4-1).
- Right-click the SSC tray icon to activate the icon menu (see Figure 4-16).

Figure 4-16 SSC Icon Right-Click Menu



The SSC icon right-click menu provides shortcuts to many of the controls available on the main SSC GUI window:

- Connect Automatically—Indicates the operating mode of SSC.
  - When checked, SSC automatically chooses the best available configured connection.
  - When unchecked, SSC will only connect to the checked configured connection in the list below.
- Configured connections are indicated in bold.
  - When a connection in this list is checked, the SSC Connect Automatically feature is turned off and an exclusive connection is being attempted on this connection.
  - When a connection in this list is followed by (connected), SSC is currently connected to the indicated configured connection.
  - When the user clicks a connection in this list, SSC attempts to connect to the specified configured connection. If the connection fails, SSC continues to search for the next best connection from the configured connections list.
- Detected scan-list networks are listed directly below the dotted line.
  - When the user clicks a network in the scan-list, SSC attempts to connect to the specified network. If the network has security enabled, SSC prompts the user to enter the needed Key information.

    After the user enters the needed security information, if the connection attempt fails, SSC continues to search for the next best connection from the configured connection list. The new network connection remains in the configured connection list.
- Connection Status—Provides the user with valuable connection information.
  - When Connection Status is clicked, the Connection Status window appears and provides connection, security, and Wi-Fi setting information.The user can click the Help button on the Connection Status window to obtain information about the window elements and values.
- Connect VPN—Allows the user to enable an automatic VPN connection.
  - When Connect VPN is clicked, the VPN Settings window appears and allows the user to enable automatic VPN connection on the currently active connection and to select a VPN connection entry.
- Groups—Displays a list of configured connection groups and allows the user to add or delete connection groups.
  - Configure Groups—When Configure Groups is clicked, the Connection Groups window appears and displays a list of configured connection groups. The user can click the Help button on the Connection Groups window to obtain information about the window elements and values.
- Enable Wi-Fi Radio—Allows the user to turn the radio on and off.
- Repair—Allows the user to restart SSC and enable its repair procedure.
- About—Displays the product name and version information.

SSC Tray Icon

The SSC system notification tray icons are explained in Table 4-2.

Table 4-2 System Notification Tray Icons

Tray Icon	Description
	Wireless—Secured connection.
	Wireless—Secured, VPN connected state.
	Wireless—Unsecured, open connection.
	Wireless—Unsecured, VPN connected state.
	Wired—Secured connection.
	Wired—Secured, VPN connected state.
	Wired—Unsecured, open connection.
	Wired—Unsecured, VPN connected state.
	Serious error. Contact your administrator.

Note A blue background with a dashed line indicates an unsecured, open connection. A green background with a solid border indicates a secured connection. The lock indicates a VPN connected state. An animated state (pulsing lines radiating out from center) indicates SSC is trying to make a connection.

CHAPTER 5

Troubleshooting End User Wireless Networks

This chapter provides troubleshooting suggestions for typical user problems and contains these sections:

Using the Cisco SSC Simplified User Interface

SSC is designed to eliminate the chances of an end user corrupting the 802.1X configurations that have been deployed by an administrator. Users cannot edit the deployed configuration profiles. Also, the 802.1X wireless configurations are validated and tested prior to deployment mis-configured 802.1X settings are unlikely.

The SSC GUI also helps to minimize the possibility of end user errors with manual entries. Home networks can be created by simply double-clicking the detected home SSID (network name) or by selecting it from the SSC tray icon. Where the user is required to provide a WEP key for home networks, the key entry can be unmasked to allow easy visual verification.

By minimizing the user interface and hiding unneeded 802.1X information from the end user, SSC helps the user to easily diagnose wireless connection settings:

- The signal strength can quickly indicate if the user's PC is located within range of the wireless network (if the SSID is not hidden).
- The user can quickly connect to a specific network profile by right-clicking the profile and choosing **Connect Exclusively**.
- The user can determine if the error is caused by incorrect credentials.
- If authentication fails, the user can right-click on the SSC system tray icon and choose **Connection Status** to view connection information to verify the settings.
- To fix a wireless association that was previously working, the user can right-click the SSC system tray icon and choose **Repair**.
- The user can click the Microsoft wireless network connection icon in the system tray, then right-click the desired wireless network connection, and choose **Repair** to have Windows attempt to fix a wireless association that was previously working.

- The user can turn the Wi-Fi radio off and on by right-clicking the SSC system tray icon and choosing **Enable Wi-Fi Radio**. The check mark indicates the radio is turned on.
- The user can use the SSC Help menu to obtain usage information.
- The user should ensure that the latest wireless NIC (radio) driver for the operating system is loaded on the PC.

When the user is unable to resolve the network problem after following the self-help options listed above, it might be necessary to contact the support help desk to resolve the problem.

When a help desk call is generated the user might report one of the following problems:

- Association Failure—See the "Association Failure" section on page 5-2.
- Authentication Failure—See the "Authentication Failure" section on page 5-4.
- IP Connectivity Failure—See the "IP Connectivity Failure" section on page 5-5.

Association Failure

This section describes two association problems that might be experienced by a typical user.

Example 1 - Unable to Connect to the Home Access Point

The user cannot configure SSC to use his home access point. In a home environment, the user might be using one of these association modes:

- Open with no security
- Open with static WEP key
- Shared with static WEP key
- WPA Personal (PSK) with TKIP (passphrase based)
- WPA Personal (PSK) with AES (passphrase based)
- WPA2 Personal (PSK) with TKIP (passphrase based)
- WPA2 Personal (PSK) with AES (passphrase based)

The support help desk should be able to assist in correcting the problem and might ask the user to follow these operations:

1. Power off all wireless network components and wait for 3 minutes. Power up each network component in the sequence shown below but wait for the component to completely power up before powering up the next component:
   a. Modem (cable, DSL, or satellite)
   b. Router
   c. Access point
   d. PC

Note The user's home network might contain a wireless router instead of a separate access point. The wireless router is a router with an integrated access point.

2. Verify that the wireless connection can be established.

3. If the wireless connection is unsuccessful and the user knows the access point IP address, verify that the client profile settings match the access point's settings. This might be accomplished by one of these methods:
   a. Directly connect to the Ethernet port of the access point and browse to the access point's GUI.
   b. If the user has a wired or wireless router with Ethernet ports, connect to an Ethernet port and browse to the access point's web window to verify the access point's settings.
4. If the wireless connection is unsuccessful and the user doesn't know the access point IP address, verify that the client profile's settings match the access point's settings using this method:
   a. Disable the SSC by clicking **Settings > Enable Client**. A check mark indicates that SSC is enabled.
   b. Use the previously configured client (in most cases it is the Windows native client).
   c. If the access point connection is successful, the user can access the access point's web window to verify the access point's settings.
5. If the user has documented the access point configuration, the user might be experiencing one of these common problems:
   - Open or Shared mode of 802.11 authentication with WEP keys.

     The user might have mis-configured the client using *Open WEP* instead of *Shared WEP* or vice versa. The user can toggle the settings using SSC to try the other mode.
   - Incorrect WEP key generation or incorrect manual input.

     Some access points use a passphrase to generate a WEP key. The user should highlight the connection and click **Edit > Generate Router WEP key** and provide the passphrase to generate the correct WEP key.

     If a passphrase is not used, the user should highlight the connection in the SSC GUI, click **Edit,** and check **Show password** to visually verify the password entered.
   - Incorrect WPA/WPA2 passphrase manual input.

     The user might have forgotten the password because the previously used client application was caching the credentials. The user might need to reconfigure the access point's settings with a new password (see Steps 3 and 4 above).
   - Mismatching WEP key index.

     Some access points provide multiple key indices in which the WEP key can be configured. Cisco recommends that the first key index be configured with the static WEP key. The user might need to reconfigure the access point's WEP key setting (see Steps 3 and 4 above).
   - MAC filtering enabled on access point.

     If the user's PC has multiple wireless network adapters installed and enabled, SSC might be using a wireless network adapter that is being blocked by the MAC filter settings on the access point. The user might need to reconfigure the access point's settings (see Steps 3 and 4 above).

If the user is still unable to successfully connect to the access point, the user should reset the access point to factory defaults and then re-configure the access point's settings.

Example 2 - Unable to Connect to the Enterprise Network

The user cannot connect to the enterprise network using a wireless connection in a cube, conference room, or office building.

The network administrator deploys pre-configured configuration profiles within an enterprise. There are two main reasons for an 802.11 association failure in an enterprise environment:

1. Lack of wireless coverage or excessive wireless noise.

   This may happen when the wireless deployment is not well designed or because of noisy spectrum due to other devices in the environment that may even include microwave ovens.

2. Use of obsolete wireless NIC drivers.

   Wireless networks have been around for a long time and it is very likely that the user's PC has an old version of the wireless NIC driver. It is recommended that the network administrator redistribute known good NIC drivers for the NIC driver chipsets within his enterprise environment to all users.

Authentication Failure

In an enterprise environment in which the 802.1X configuration is correctly deployed with SSC and the network infrastructure components (including the access points, controllers, and the RADIUS server) are correctly configured, these problems might cause an authentication failure:

- The user provided incorrect credentials.
- The user unknowingly provided incorrect credentials a set number of times, locking his account and making it unable to work with the correct credentials.
- The user credentials have expired.
- The network infrastructure, public key infrastructure (PKI), or the user database has a problem: an access point cannot communicate to the authentication server, the authentication server is not functioning, or its configuration has changed.
- The device involved in the authentication process is not functioning properly, such as the smart card, smart card reader, or token, etc.
- The user's PC does not have Windows Internet Explorer 5.0 or later installed.

If the problem continues, the support help desk should request that the user provide a Cisco Support Report with packet capturing enabled. For instructions on creating the support report, see the "Gathering Logs and Packet Traces" section on page 5-8.

IP Connectivity Failure

When the 802.1X authentication is successful, SSC tries to get a valid IP address. In some networks, it might take up to 40 seconds to renew the IP address. If the wireless LAN adapter fails to receive a valid IP address, these actions might help to resolve the problem or identify the cause:

- Disable and then enable the wireless NIC adapter.
- Repair the connection by right-clicking the SSC system tray icon and choosing **Repair**.
- Right-click the network connection in the SSC GUI and choose **Connect Exclusively**.
- Use network tools, such as ARP, ping, and ipconfig to check Layer 2 or Layer 3 connection status, and availability of an IP address.

The root cause of the problem might be as simple as a DHCP server running out of available IP addresses.

Integrated VPN Connection Failure

SSC allows the user to automatically establish a VPN connection after connecting to a wireless profile, if the profile is configured to do so.

The end user might be unable to establish a VPN tunnel to his enterprise network using SSC. VPN problems might be indicated as follows:

- The SSC VPN Connect button is not visible on the SSC main window.

  This might happen if the administrator did not deploy a profile with the *Allow VPN* option checked to the user.

- The SSC VPN Connect button is visible but dimmed.

  This might happen if the Cisco VPN client version is older than 4.8. The user must upgrade the VPN client on his PC.

- The user cannot access the VPN service.

  This may happen if the user is using the stand-alone Cisco VPN client interface to establish VPN connections. If the Cisco VPN client interface is being used to connect and disconnect VPN connections, SSC gives up control over VPN functionality.

  To resolve this problem, the user should not use the standalone Cisco VPN client interface to establish a connection. He should allow SSC to establish the VPN connection. However, if desired, he can use the Cisco VPN client interface to see the connection status.

- SSC displays a VPN connection failed error.

  This might happen when the user credentials provided to SSC are incorrect. When using SSC with the Soft Token option, the user credentials to be provided to SSC must be the username and the user PIN that were previously provided to the SofToken-II application.

Note For Windows 2000 and Windows XP, the unique soft-token password generated by the SofToken II application must NOT be provided to SSC when prompted for the VPN username and PIN.

Note For Windows Vista, Secure Computing SofToken II is not supported. When SofToken II authentication is specified in the network configuration and SSC prompts for the username and password, the username and the unique one-time password must be entered. This is different from Windows 2000 and Windows XP where the SoftToken II application password is entered.

If the VPN problem continues, a Cisco support report should be provided to the support help desk to analyze the problem and determine the root cause of the problem (see the "Gathering Logs and Packet Traces" section on page 5-8).

Co-Existence with Other Wireless Client Managers

To enable the Cisco Aironet Client Utility (ACU) to coexist with SSC, the user must configure the wireless network adapter to allow Windows to configure the adapter. The user must follow these steps to configure the wireless network adapter:

Step 1 Right-click **My Networks** on the desktop.

Step 2 Right-click the wireless network adapter and choose **Properties**.

Step 3 Click **Wireless Networks** and check **Use Windows to configure my wireless network settings**.

Step 4 Click **OK** and close the Network Connections window.

To enable the Cisco Aironet Desktop Utility (ADU) to coexist with SSC, the user must configure the ADU to allow SSC to control the adapter.

Note It might be necessary for the user to download the latest ADU version from the Cisco Software Center at this URL: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=278875243

The user must click **Client Adapters and Client Software** and follow the prompts. The user must register or be a registered user of Cisco.com to download software.

The user must follow these steps to configure the ADU:

Step 1 Open the ADU by double-clicking the ADU task bar icon.

Step 2 Click **Options** > **Select Client Software** and the Select Client Software pop-up window appears.

Step 3 Check **Third-Party Tool** and click **OK** on the pop-up window.

Step 4 When the Client Software selection pop-up indicates successful, click **OK**.

Step 5 Close the ADU.

When SSC is active, it takes control from the Microsoft Windows native wireless client. In other words, the Windows native client can display SSID's but cannot configure or set wireless connection settings. To stop SSC from controlling the wireless adapter, the user must disable SSC by clicking **Settings** and choosing **Enable Client** (a check indicates SSC is enabled). Disabling SSC gives control of the wireless adapter to any other wireless client management application that can manage the wireless connections.

Note SSC and the Odyssey Access Client Manager application must not be installed at the same time on a user's PC.

The iPassConnect client software and SSC can co-exist if the following instructions are carried out when the user is using a public Wi-Fi hotspot (such as an airport).

Step 1 Right-click the SSC tray icon and choose the name of the Wi-Fi connection.

Step 2 When the SSC icon turns blue and is no longer animated, you need to activate the iPassConnect application and use it to authenticate yourself and to successfully establish a VPN connection.

Step 3 In iPassConnect choose **Available Connections** and then choose the name of the connection that you are already connected to with SSC.

Step 4 iPassConnect prompts you for your username and password. Enter your corporate network username and then use your soft token application to generate the password.

Step 5 iPassConnect finishes authenticating and launches the Cisco VPN application. At this point you should exit the Cisco VPN application, right-click the SSC icon, and choose **Connect VPN**.

Note Typically the webauth systems available at most hot spots keep you authenticated for over an hour. If you lose your connection, you must connect again. Right-click the SSC icon and choose **Connect VPN** when available. If you don't succeed the first time, try choosing **Connect VPN** again another couple of times. If that doesn't work, launch a web window and see if you have connectivity to the internet or if the web window requests that you authenticate yourself. If the web window is asking for authentication information, you need to repeat the iPassConnect steps starting with Step 4.

Gathering Logs and Packet Traces

SSC provides a diagnostic utility called the *Log Packager,* which is part of the Cisco Client Utilities. Installed separately, this utility is available from the Windows Start > Programs menu. The utility provides SSC's current status, interface and driver details, FIPS status, and wireless LAN information (SSIDs detected, association status, etc.). This information can be useful in diagnosing connectivity problems when using SSC and the NIC adapter.

Note When using Windows Vista, the Log Packager does not include a scan list in the report.

Creating the Cisco Support Report for SSC

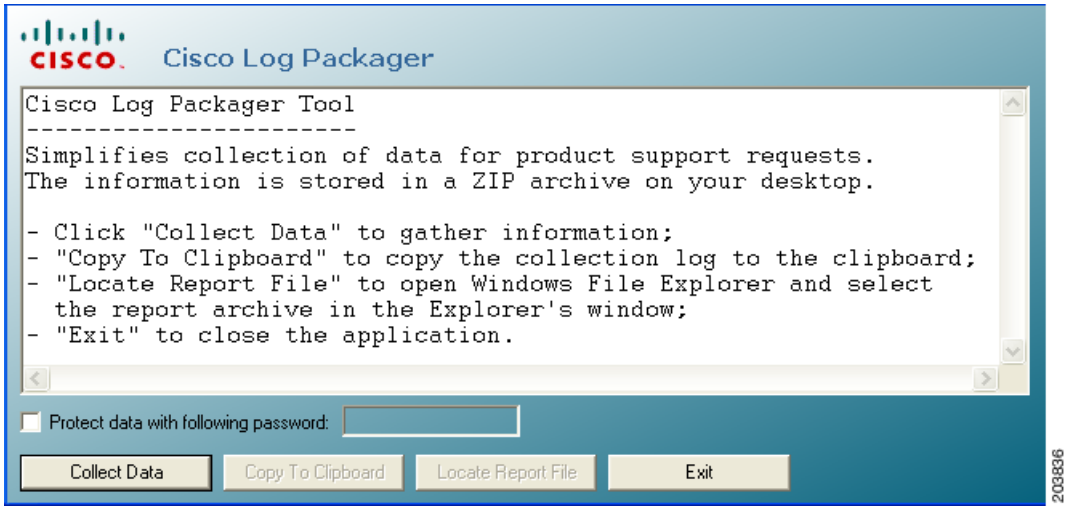
To create the Cisco support report, follow these steps:

Step 1 Click **Start** > **All Programs** > **Cisco** > **Client Utilities** > **Log Packager** (see Figure 5-1).

Figure 5-1 Accessing the Client Utility Using Windows Program Menu

When the Log Packager program opens, Figure 5-2 appears.

Figure 5-2 Log Packager Window



Step 2 Click **Collect Data**.

Step 3 When the buttons are visible again, click **Locate Report File**. A Microsoft Explorer window opens in the directory with the zipped report file. The filename is CiscoSupportReport.zip and is located on your PC desktop. The zip file contains a number of log files, capture files, several .xslt files, and several configuration .xml files.

If you click **Copy to Clipboard**, the contents of the CiscoSupportReportLog.txt file is copied to the Windows clipboard.

Step 4 Close Windows Explorer and the Cisco Log Packager.

CHAPTER 6

Frequently Asked Questions

This chapter contains these SSC frequently asked questions (FAQs):

Questions and Answers

Q. Does SSC 5.1.1 support the SSL-based VPN (Cisco AnyConnect VPN) client?

A. No, currently SSC 5.1.1 supports Cisco's IPSec VPN client 4.8.0.1 or later on Windows 2000 and Windows XP or 5.0.03.0560 or later on Windows Vista.

Q. How do I configure an 802.1X network?

A. You have two choices.

1. Download the SSC management utility, unzip the file, and run the sscManagementUtility.exe that's included in the package to create comprehensive 802.1X profiles.
2. The SSC GUI can be used to configure basic 802.1X profiles.

Q. When I click Connect, why doesn't it connect to the network I have selected?

A. SSC should always try to connect to the network you have selected. However, if SSC fails to connect to the network, instead of continuing to try, it simply moves on to the next network in the list, until a network is connected. If you want SSC to connect to one specific network, right-click on the network connection, and choose **Connect Exclusively**.

Q. I have a wired connection but I want to use a wireless connection, what should I do?

A. SSC prioritizes a wired connection over a wireless connection. If you want to use a wireless connection without disconnecting the Ethernet cable, you can manually over-ride the SSC setting. Right-click the desired wireless connection and choose **Connect Exclusively**. To return to the auto-connect mode where SSC determines the best connection, click **Connect** to resume the auto-connect setting.

Q. Hey, where are my log and configuration files?

A. Cisco has standardized the location for all log and configuration files. The new location is:

- Windows 2000 and Windows XP:

  C:\Documents And Settings\All Users\Application Data\Cisco\Cisco Secure Services Client

- Windows Vista:

  C:\ProgramData\Cisco\Cisco Secure Services Client

Q. How do I keep wired and wireless connections simultaneously connected?

A. SSC is designed to provide one network connection at a time (single-homed).

Q. When I use SSC to configure a new profile with a VPN connection, why is the VPN drop-down option field blank?

A. For you to use the VPN option in a new connection profile, SSC requires the Cisco IPSec VPN client to be installed and configured on the user's PC.

CHAPTER 7

SSC FIPS 140-2 Level 1 Validation

This chapter contains these sections:

Overview

U.S. Federal agencies as well as Canadian government agencies are required to comply with the Federal Information Processing Standards Publication (FIPS) 140-2 when purchasing IT products that contain cryptographic modules. This release of SSC supports a FIPS 140-2 Level 1 module (currently in process for validation with the National Institute of Standards and Technology (NIST) and provides FIPS-compliant IEEE 802.11i (WPA2) security support.

Note FIPS functionality is not supported by the Windows Vista version of SSC.

An administrator can choose to allow enterprise employees to perform one of these operations:

- Connect to only FIPS-compliant networks.
- Connect to other non-FIPS-compliant networks.

This can be achieved by restricting the allowed association and encryption modes and the authentication methods in the policy section of the SSC schema.

The SSC FIPS module supports FIPS approved AES encryption modes including WPA2 Personal (WPA2-PSK) and WPA2 Enterprise (802.1X). The SSC FIPS module also supports EAP methods including EAP-TLS, EAP-PEAP, and EAP-FAST. SSC 5.1.1 enables administrators to support both FIPS-compliant WLAN profiles as well as optional non-compliant configurations such as access to Wi-Fi hotspots with client VPN security enabled.

The administrator is responsible for naming the profile appropriately to indicate whether the network is FIPS enabled.

A fully FIPS-compliant solution requires three components:

- SSC 5.1.1 with the FIPS module
- 3eTI FIPS certified Crypto Kernel Library (CKL) with supported NIC adapter drivers
- A FIPS-compliant network profile configuration created by the network administrator

3eTI FIPS Certified Crypto Kernel Library (CKL)

These NIC adapter chipsets are supported by the 3eTI FIPS certified CKL:

- Intel 2100, 2200, 2915, and 3945 chipsets
- Broadcom: All BCM 43xx chipsets that support driver version 4.100.27.0 or later
- Atheros PCI chipset based NIC adapters, including Cisco AIR-CB21 wireless client adapter cards
- Atheros: 5001, 5004, 5005, AR5211, and AR5212 chipsets

FIPS Integration

To ensure a FIPS-compliant solution, the network administrator is required to set up network profiles that allow only WPA2 handshakes with AES encryption with FIPS-compliant EAP types or WPA2-Personal (Pre-shared key).

The SSC Log Packager utility collects logs of the 3eTI packets.

3eTI CKL Driver Installer

For instructions on how to install the 3eTI FIPS validated CKL with supported drivers, see the "Installing the 3eTI Driver" section on page 7-3.

Additional FIPS Information

For additional FIPS information, refer to the "FIPS 140-2 Level I Compliant Deployment Example" section on page 7-14 and the "Configuring a Single-User Account for FIPS" section on page C-1.

Installing the 3eTI Driver

This section provides instructions for installing the 3eTI FIPS validated Cryptographic Kernel Library (CKL) with supported drivers that integrate with SSC to provide a complete FIPS solution.

Important Notes

1. The 3eTI CKL driver installer is designed to allow only one 3eTI wireless driver to be installed on a system at any given time. A previous driver must be un-installed prior to installing a different type of driver. For a driver of the same type, uninstalling the previous driver is not necessary because the next installation just updates the existing driver.
2. When the hardware is present and installed in the system, the installer updates the corresponding OEM wireless NIC adapter driver with the 3eTI modified driver that supports the 3eTI CKL.

3eTI CKL Driver Installer Overview

The 3eTI CKL driver installer can be started using one of these methods:

- Double-clicking the .exe file—can only be used for normal driver installations in which the NIC adapter is installed in the PC before the installer is run.
- Using the installer command without command-line options—can be used only for normal driver installations.
- Using the installer command with command- line options—can be used for normal and pre-installed driver installations.

When you start the driver installer by double-clicking the .exe file or using the run command without command-line options, the installer performs these operations:

- Detects and installs the 3eTI CKL with a supported NIC adapter driver for FIPS operation.
- If multiple NIC adapters are detected that support the 3eTI CKL, the installer prompts the user for adapter selection.
- If a compatible NIC adapter is not found on the PC, the installer aborts the installation and displays this error message:

  The installer cannot auto-detect a NIC chipset to provide FIPS support. To enforce a pre-installation, you are required to run the installer using the command line. For instructions or further assistance, please contact your network administrator.

Note Pre-installation scenarios are best supported with command-line options that allow the network administrator to specify specific installation options. Pre-installations are typically preformed by a network administrator and not a novice user.

Installer Command and Command-Line Options

The installer supports the following command and command-line options:

3eTI-drv-installer.exe –s –auto Type= XXXX

–s	Used to perform a silent installation without prompting the user.
–auto	Used to perform an intelligent installation, where the installer determines the supported NIC adapter in the PC and installs the appropriate driver. This causes the installer to perform the same operations as entering the command without command line options.
Type=*XXXX*	Used to specify the NIC adapter chipset for a pre-installation or a normal installation. *Pre-installation* means that the driver is installed before the specified NIC adapter is installed in the PC. *Normal installation* means that the NIC adapter is installed before the driver is installed.

XXXX Value	Description
Intel3945	Specifies drivers for the Intel3945 chipset.
Centrino	Specifies drivers for Intel 2100, l2200, and 2915 chipsets.
Broadcom	Specifies drivers for Broadcom chipsets supported by the Installer.
Atheros	Specifies drivers for the Atheros 5001, 5004, 5005, AR5211, and AR5212 chipsets.
Cisco	Specifies drivers for the Cisco AIR-CB21 card with an Atheros chipset.

Note When using –s for silent installation, you must also specify –auto or Type=XXXX or both –auto and Type=XXXX.

Examples:

- Using *–auto* in conjunction with *–s*:
  - Performs an intelligent installation by automatically detecting the NIC adapter that is installed.
  - Performs a silent installation without prompting the user.
  - If multiple NIC adapters are detected, selects any supported chipset.
- Using *–auto* in conjunction with *Type=XXXX*:
  - Attempts to Install the driver for the NIC adapter chipset specified by Type=XXXX.
  - If the detected NIC adapters do not support the specified chipset, installs a driver for any NIC adapter with a supported chipset.
- Using *3eTI-drv-installer.exe Type=Intel3945 –auto –s*:
  - Attempts to install a driver for the Intel3945 chipset without prompting the user.
  - If a NIC adapter with the Intel3945 chipset is not detected, silently installs a driver for any other detected NIC adapter with a supported chipset.
  - If a NIC adapter with a supported chipset is not detected, does not pre-install any driver.

- Using *3eTI-drv-installer.exe Type=Intel3945 –s*:
  - Attempts to install a driver for the Intel3945 chipset without prompting the user.
  - If a supported NIC adapter chipset is not detected, performs a pre-install by installing the specified chipset driver.

Running the Installer without Using Command-Line Options

To perform a normal installation with the NIC adapter installed in the PC, follow these instructions:

Step 1 Start the installer by following one of these steps:

a. Use Windows Explorer to locate the **3eTI-drv-installer.exe** file on your PC and double-click the filename.

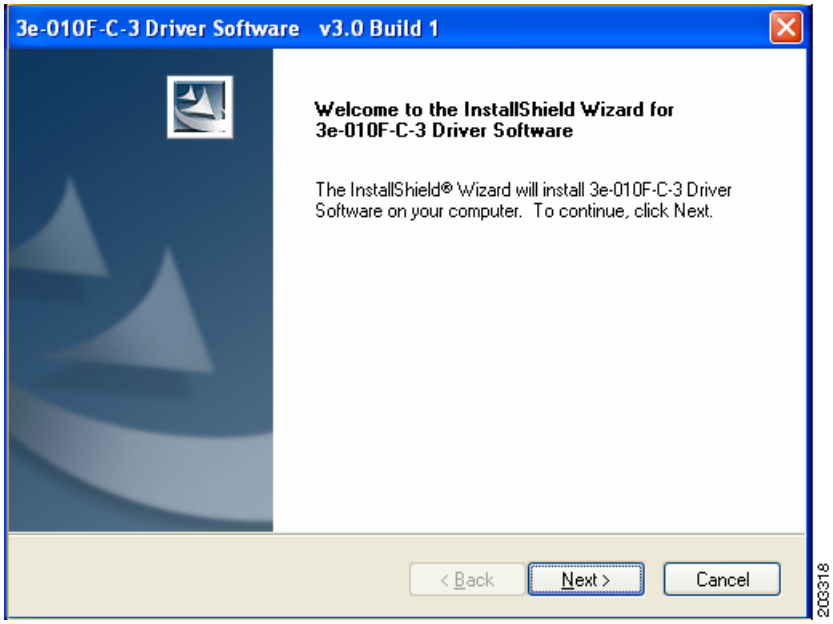
b. Click **Start** > **Run** and enter this installer run command:

path **/ 3eTI-drv-installer.exe**

Where *path* is the directory path to the installer file.

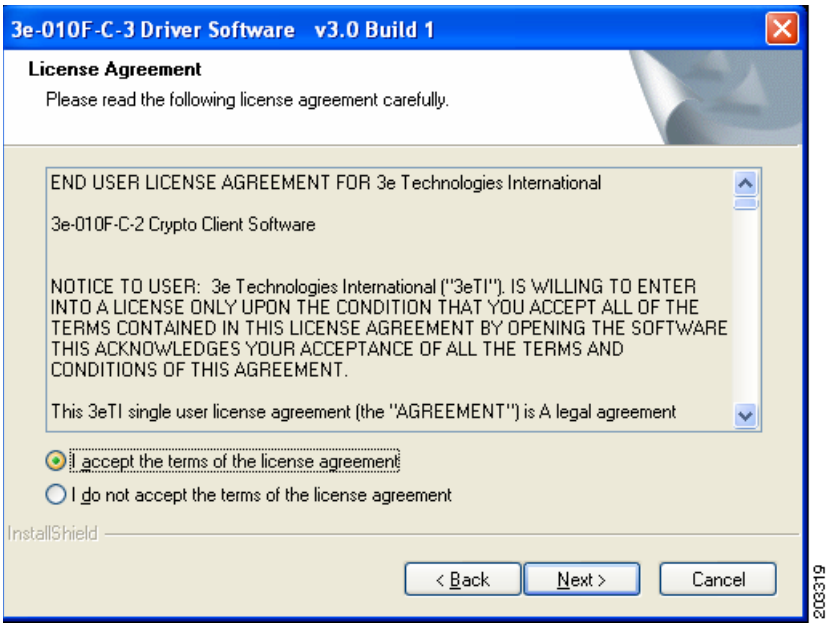
The Driver Welcome window appears (Figure 7-1).

Figure 7-1 Driver Welcome Window



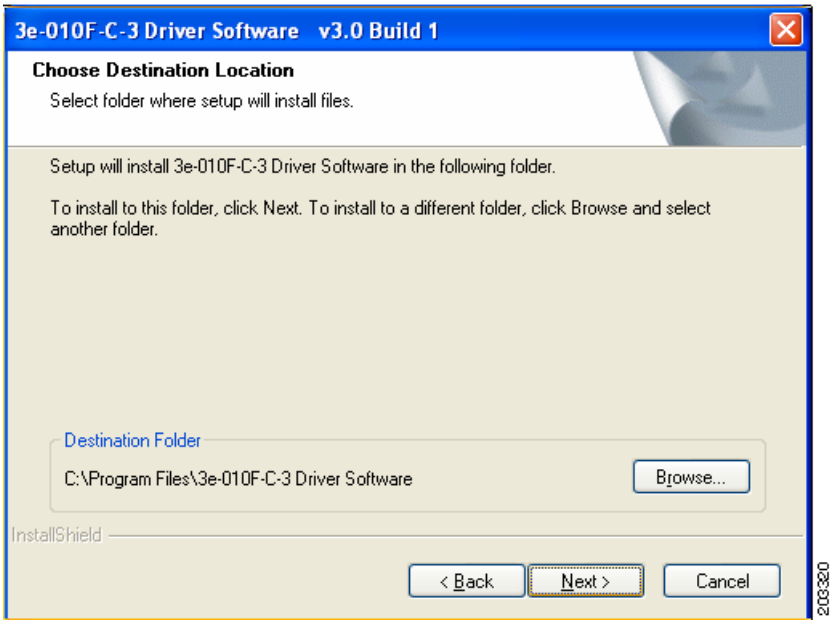
Step 2 Click **Next** and the license agreement appears (see Figure 7-2).

Figure 7-2 License Agreement



Step 3 Read and accept the license agreement and click **Next**. Figure 7-3 appears.

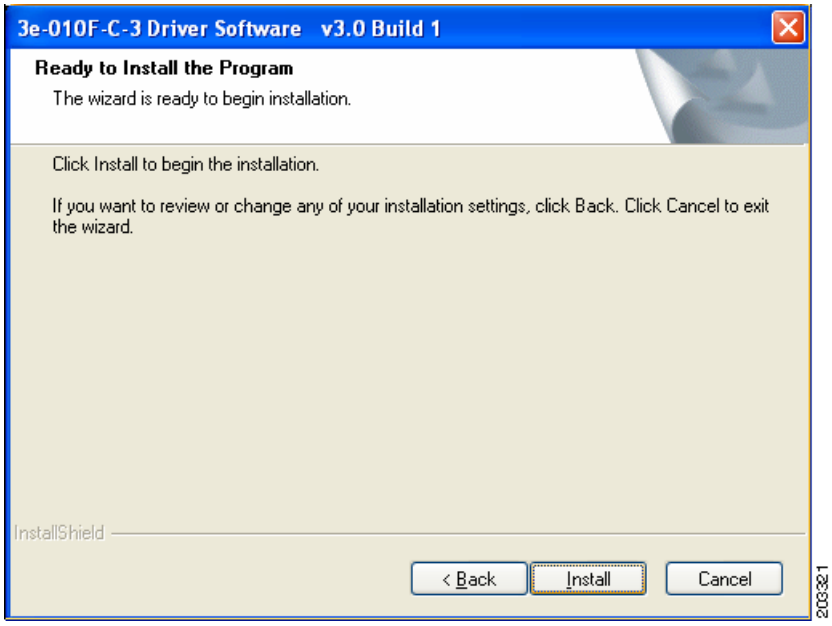
Figure 7-3 Destination Location Window



Step 4 Accept the driver software default destination folder or click **Browse** to locate the desired folder.

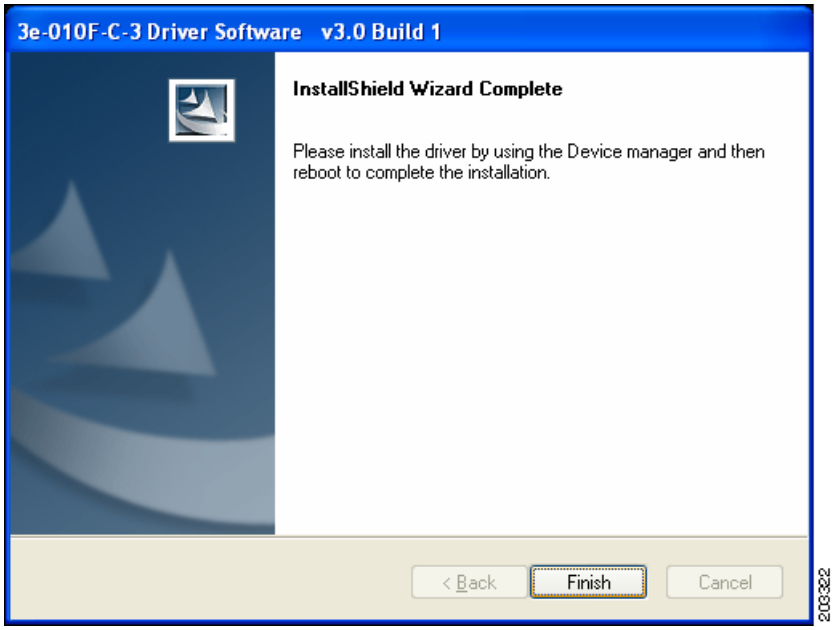
Step 5 Click **Next** and Figure 7-4 appears.

Figure 7-4 Ready to Install Window



Step 6 Click **Install** to start the installation process. When the installation completes, Figure 7-5 appears.

Figure 7-5 Wizard Complete Window



Step 7 Click **Finish**.

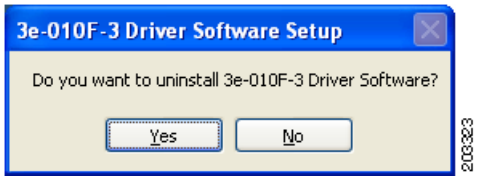
Uninstalling Previous 3eTI Driver Software

To uninstall previous 3eTI driver software, follow these steps:

Step 1 To uninstall the previous 3eTI driver software, click **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.

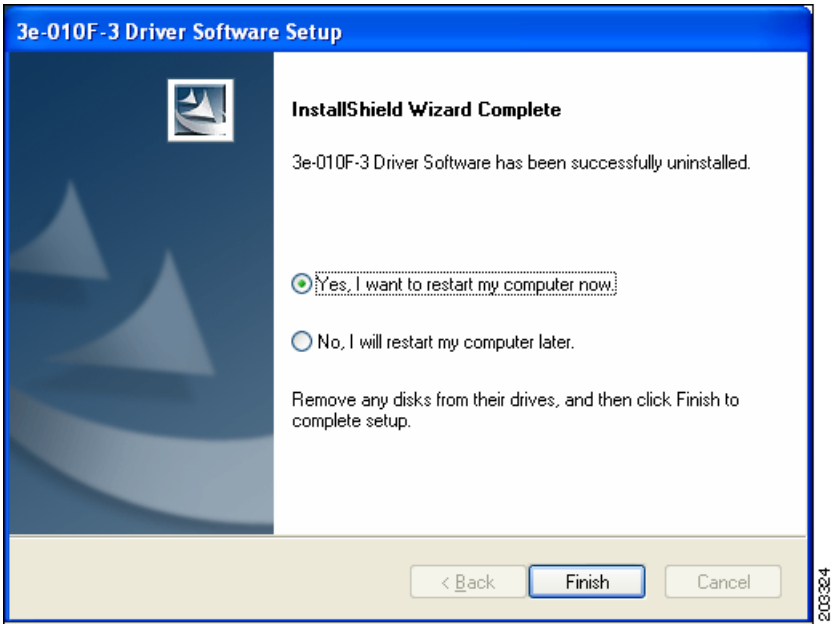
Step 2 Choose the 3eTI driver software, such as 3e-010F-3 and click **Remove**. A pop-up window appears (see Figure 7-6).

Figure 7-6 Uninstall Driver Software Pop-Up



Step 3 Click **Yes** to uninstall the driver software. Figure 7-7 appears.

Figure 7-7 Restart Computer Now Window



Step 4 Check **Yes** to restart your computer.

Step 5 Click **Finish**. Your PC reboots to completely remove the driver software.

Silent Driver Installation for Enterprise Deployment

To run the installer using a silent mode, follow these steps:

Step 1 Run the installer by entering this command:

path **/ 3eTI-drv-installer.exe -s Type=***XXXX*

Where:

path is the directory path to the installer file.

-s indicates silent installation.

Type= *XXXX* specifies the chipset, such as Centrino, Intel3945, or Cisco (see the "Installer Command and Command-Line Options" section on page 7-4).

A pop-up status window appears indicating that the driver installation is in progress and then disappears when the installation completes.

Installing the Driver without a Previously Installed Network Adapter

To install the 3eTI driver on a PC without an installed NIC adapter, follow these steps:

Step 1 Start the installer by clicking **Start** > **Run** and enter this installer run command:

path **/ 3eTI-drv-installer.exe Type =** *XXXX*

Where:

path is the directory path to the installer file.

Type=*XXXX* specifies the chipset, such as Centrino, Intel3945, or Cisco (see the "Installer Command and Command-Line Options" section on page 7-4).

Figure 7-1 appears.

Step 2 Perform Step 2 through Step 7 in the "Running the Installer without Using Command-Line Options" section on page 7-5.

Step 3 When the driver installation is complete, insert or install the NIC adapter in the PC.

Manually Upgrading the 3eTI Driver Software

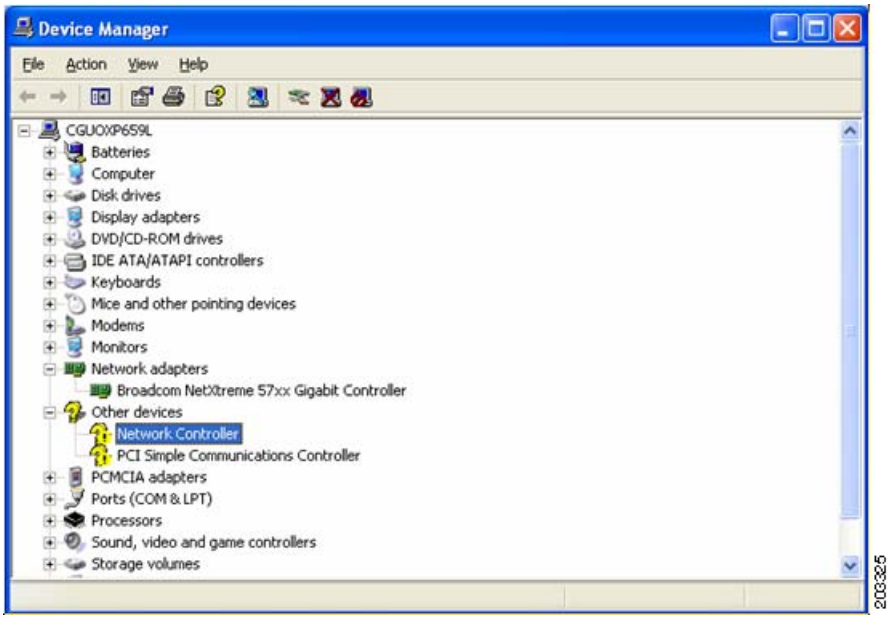
Manual upgrade instructions are provided to help troubleshoot driver installation problems. This is not expected to be a part of an enterprise-wide deployment.

Follow these steps to manually upgrade the 3eTI driver software using the Windows Device Manager:

Step 1 Right-click the **My Computer** icon on your desktop and choose **Properties**.

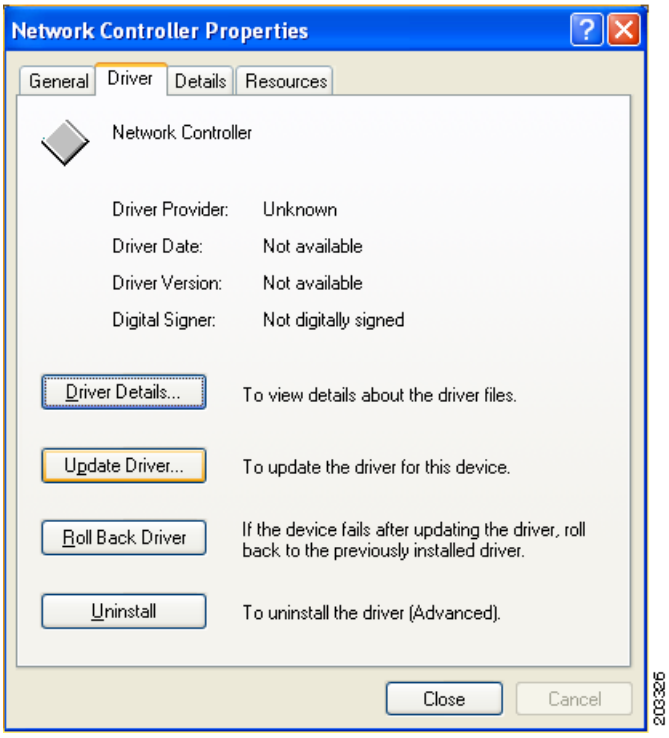
Step 2 Click **Hardware** on the System Properties window, click **Device Manager**. Figure 7-8 appears.

Figure 7-8 Windows Device Manager Window



Step 3 If your Network Adapter is installed or inserted and the driver software is not installed, the device will be listed under Other devices and shown with a yellow question mark. Right-click on your network adapter and choose **Properties**. The Network Controller Properties window appears (see Figure 7-9).

Figure 7-9 Network Controller Properties Window

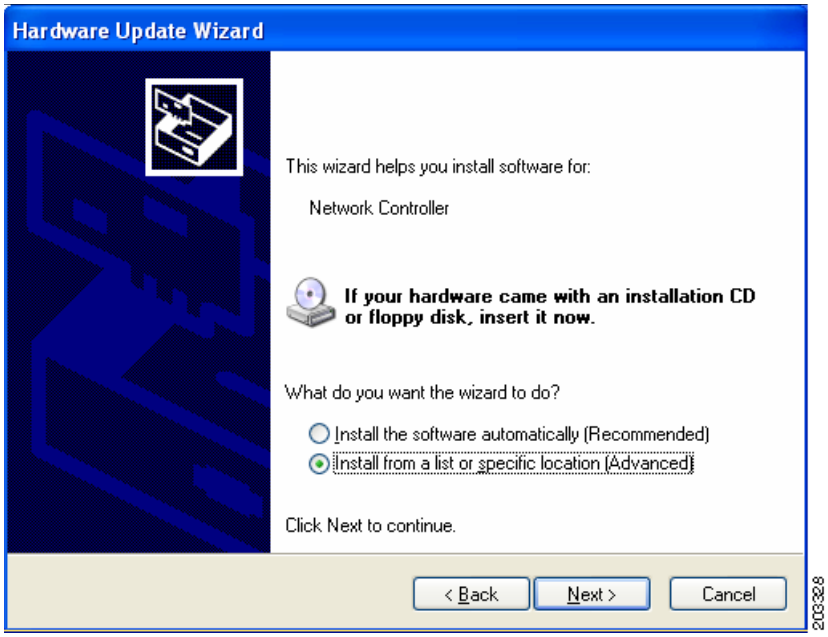


Step 4 Click **Driver** > **Update Driver** and Figure 7-10 appears.

Figure 7-10 Windows Hardware Update Wizard Window

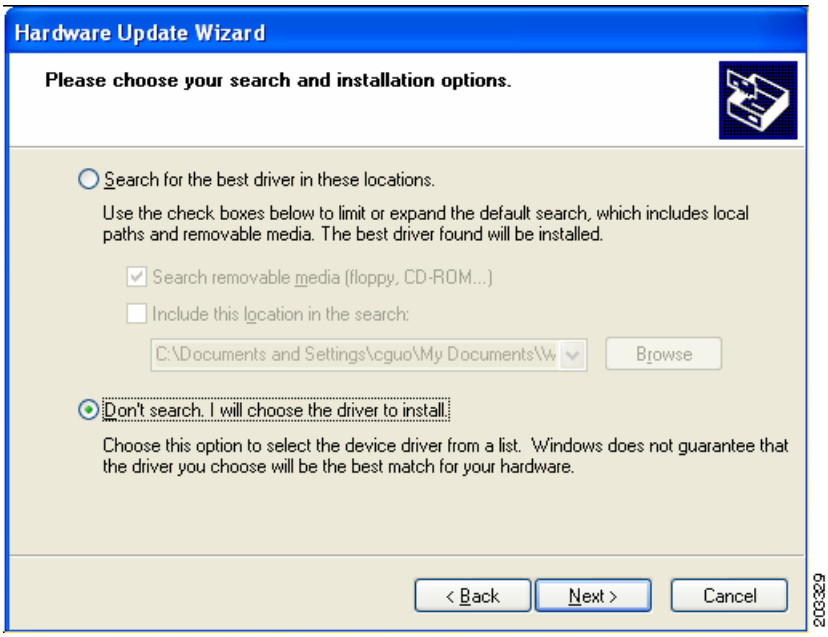
Step 5 Click **No** to prevent Windows from searching for the driver software and click **Next**. Figure 7-11 appears.

Figure 7-11 Installation CD or Floppy Disk Option Window



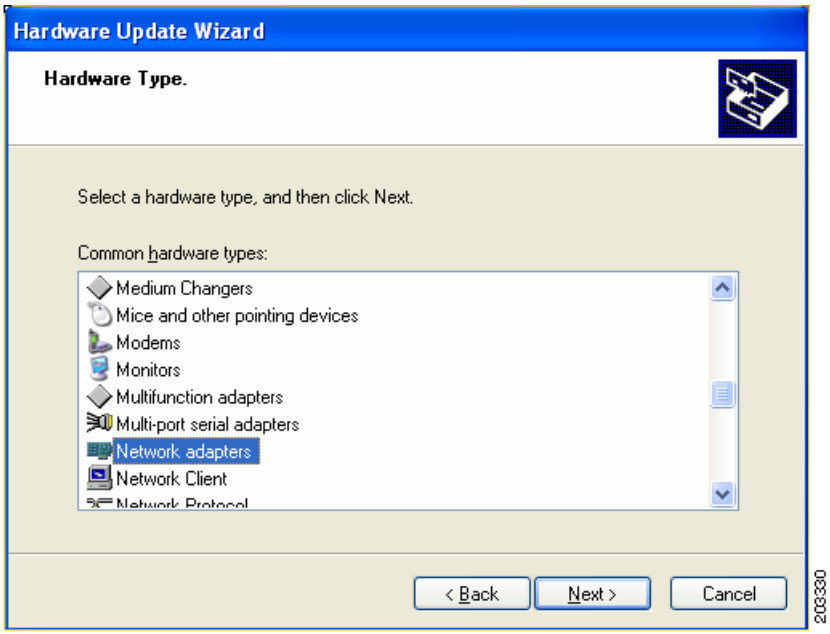
Step 6 Check **Install from a list or specific location (Advanced)** and click **Next**. Figure 7-12 appears.

Figure 7-12 Search and Installation Options Window



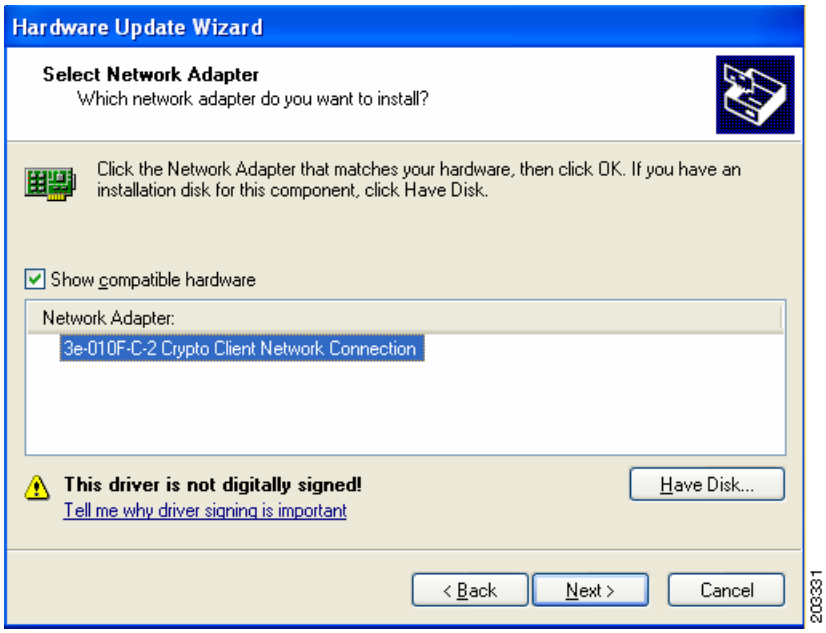
Step 7 Check **Don't search. I will choose the driver to install** and click **Next**. Figure 7-13 appears.

Figure 7-13 Windows Hardware Type Window



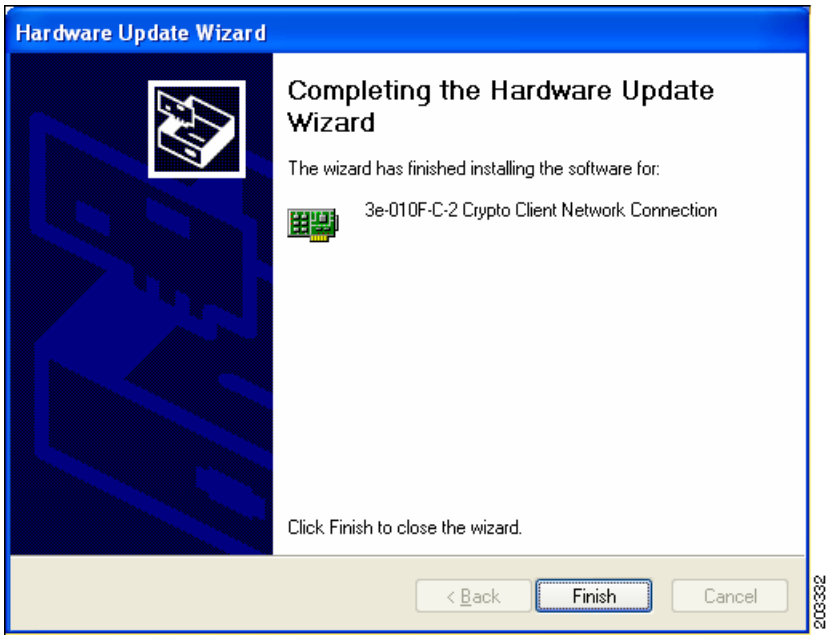
Step 8 Choose **Network adapter** and click **Next**. Figure 7-14 appears.

Figure 7-14 Select Network Adapter Window



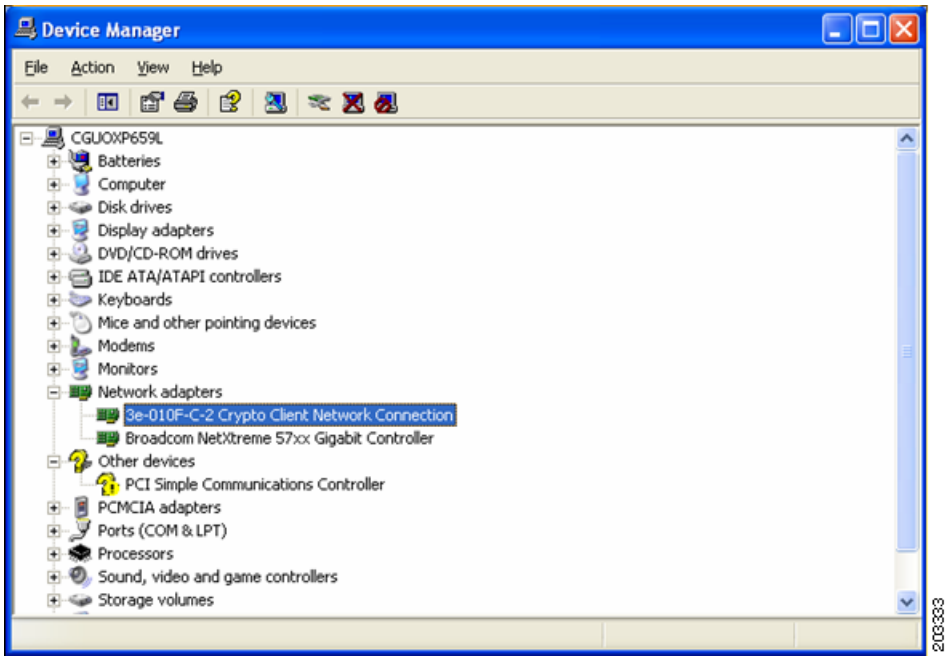
Step 9 Choose the 3eTI network connection and click **Next**. Figure 7-15 appears.

Figure 7-15 Installation Complete Window



Step 10 The hardware driver installation is complete. Click **Finish**. The Device Manager window reappears (see Figure 7-16).

Figure 7-16 Updated Windows Device Manager Window



Step 11 To verify that the driver is installed properly, right click on the 3eTI network connection and choose **Properties**. Ensure that the adapter properties window indicates **This device is working properly** under the Device status.

FIPS 140-2 Level I Compliant Deployment Example

This section describes a deployment example that explains how to configure typical network authentication profiles for SSC to ensure compliance with FIPS 140-2 Level 1 requirements. SSC 5.1.0 is the first release that supports the Cisco SSC FIPS module, which is currently in process for validation with the National Institute of Standards and Technology (NIST). When the service starts up, it executes in the FIPS operating mode.

The network administrator is responsible to configure and deploy FIPS-compliant profiles for the intended user base. The SSC Management utility is used to create FIPS-compliant profiles for wired or wireless media.

A fully FIPS-compliant solution requires three components to be installed and configured on the client:

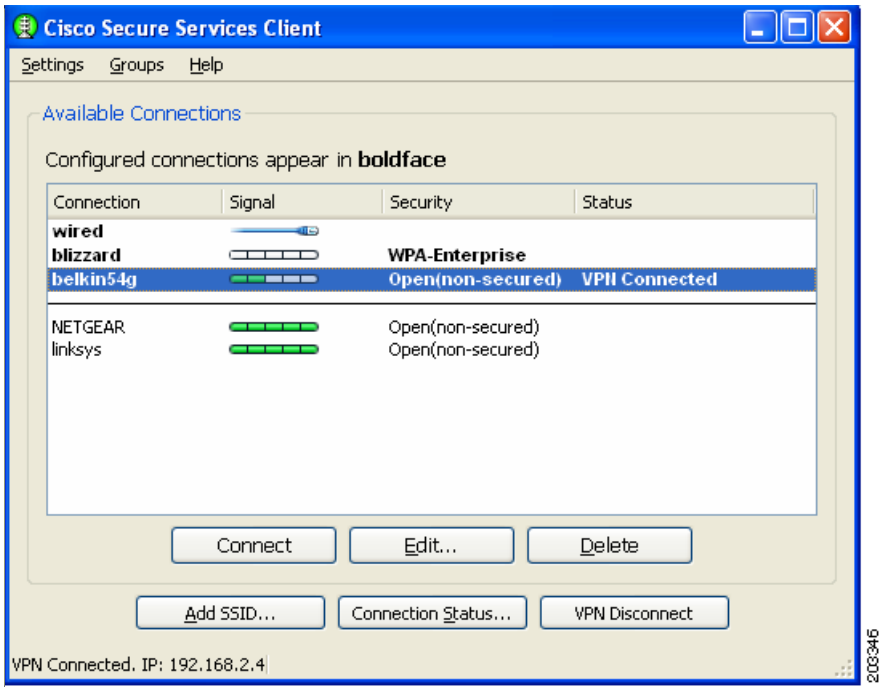
1. SSC running the SSC FIPS module (SSC 5.1.1).
2. A FIPS-compliant network profile configured by the network administrator.
3. An installed 3eTI FIPS CKL module with supported NIC adapter drivers.

When SSC and the management toolkit software are installed and running on the network administrator's PC, SSC scans for available wireless networks and displays the available networks.

Note Only the wireless network devices with their SSID's enabled for broadcast are visible.

The configured connections displayed in bold (see Figure 7-17) can be configured by the network administrator or the user. The profiles configured by the network administrator are permanent and cannot be deleted or revised by the user.

Figure 7-17 Typical Cisco SSC Window



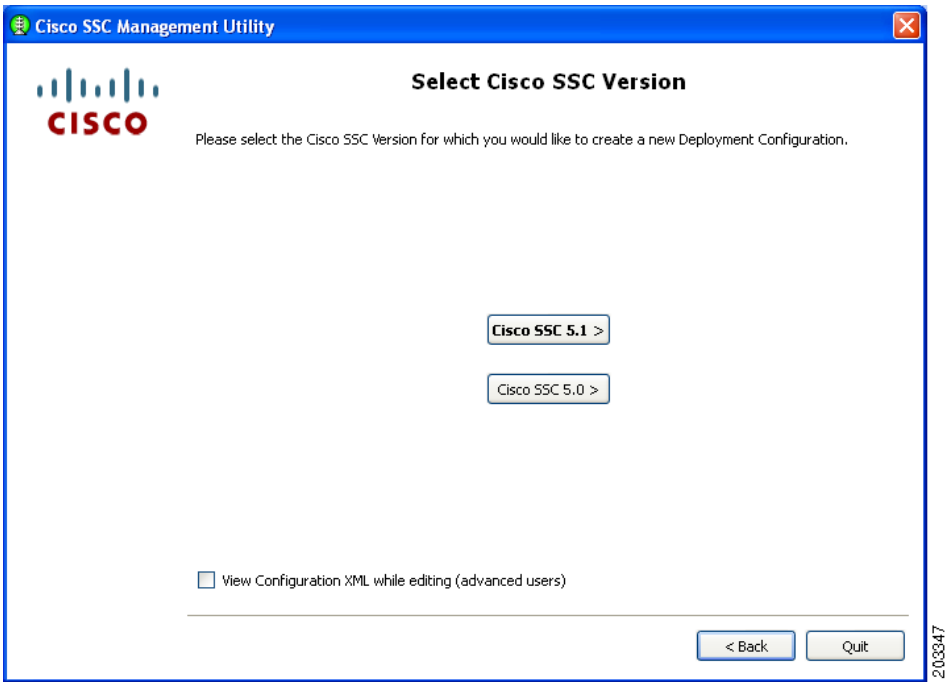
To configure typical SSC profiles for FIPS compliance, follow these instructions:

Step 1 Navigate to the directory in which the management toolkit is installed and double-click **sscManagementUtility.exe**. Figure 7-18 appears.

Figure 7-18 Cisco SSC Management Utility Main Window

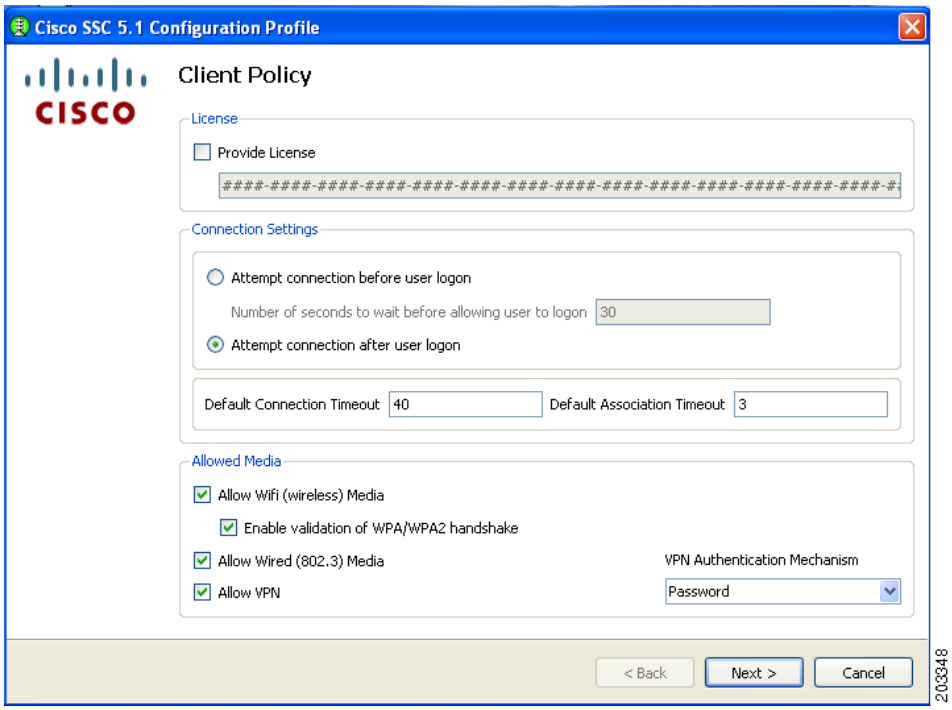
Step 2 To create a new configuration profile, click **Create New Configuration Profile**. Figure 7-19 appears.

Figure 7-19 Select Cisco SSC Version Window



Step 3 Click **Cisco SSC 5.1.1** and Figure 7-20 appears.

Figure 7-20 Client Policy Window



You must ensure that all needed options are checked in the Allowed Media area to allow that media to be configured, such as *Allow Wired (802.3) Media*.

Step 4 follow these steps:

a. Check **Allow Wi-Fi (wireless) Media**.

b. Check **Allow Wired (802.3) Media**.

c. Check **Provide License** and enter the license if it is available.

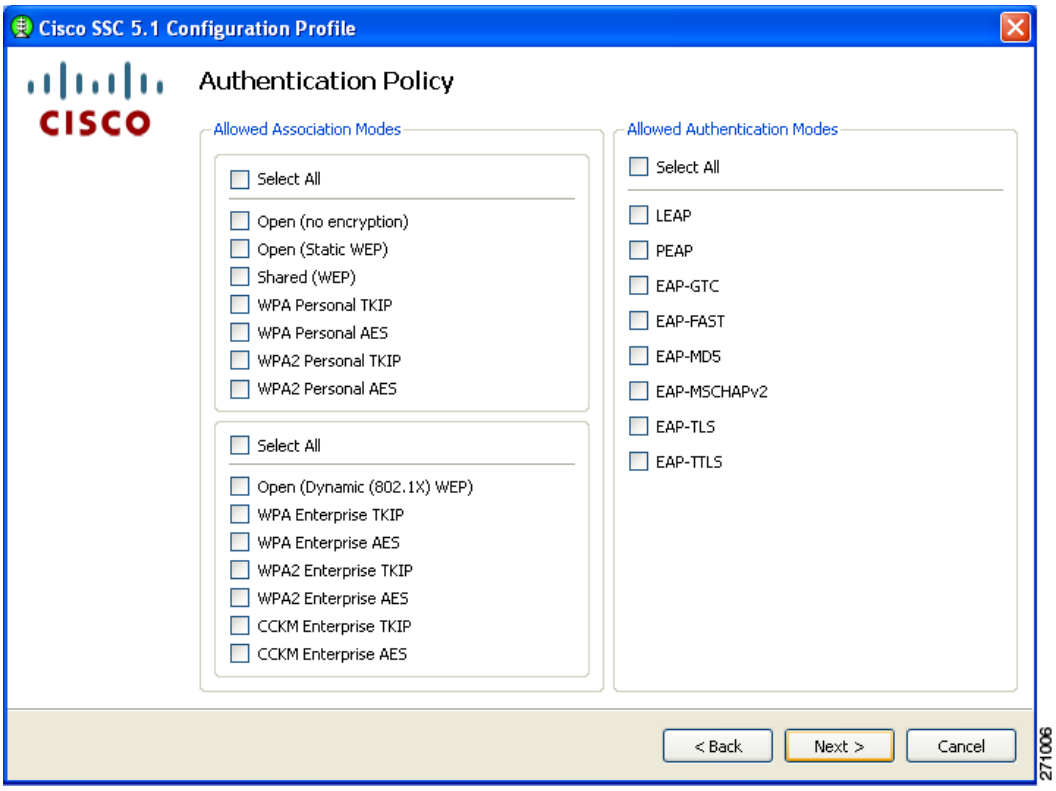
d. If VPN is installed on the PC and supported on the enterprise network infrastructure, check **Allow VPN**. Choose the appropriate VPN Authentication Mechanism for your network.

e. Check **Enable validation of WPA/WPA2 handshake**. As a part of FIPS compliance, this option is enabled.

Note Some network adapter drivers might not work correctly when this option is checked.

f. Click **Next** and Figure 7-21 appears.

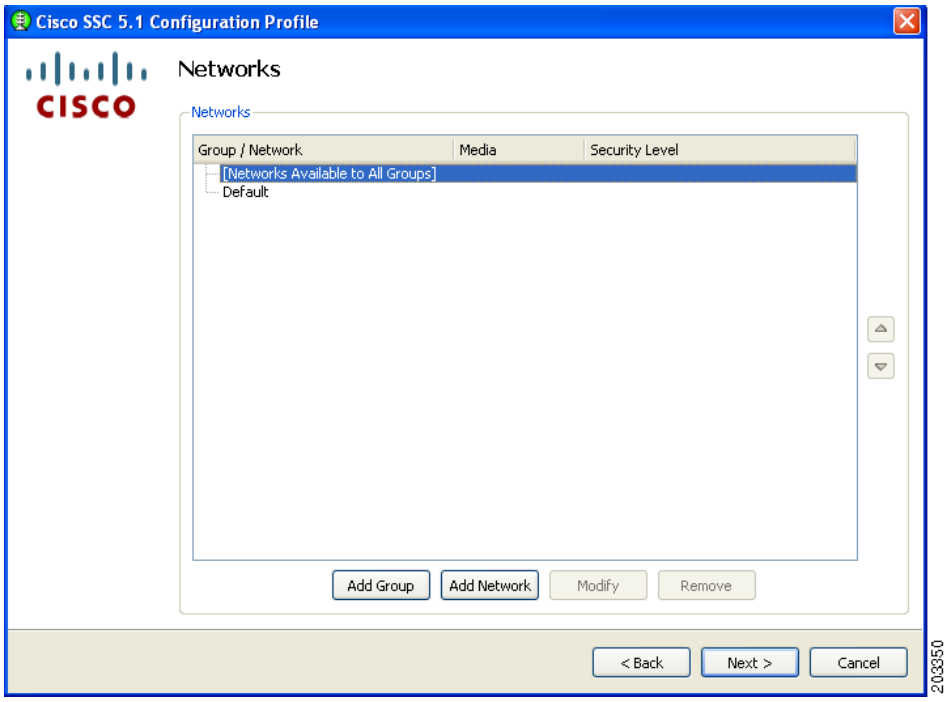
Figure 7-21 Authentication Policy Window



Step 5 Check the appropriate association and authentication modes that are allowed on your network and click **Next**. Figure 7-22 appears.

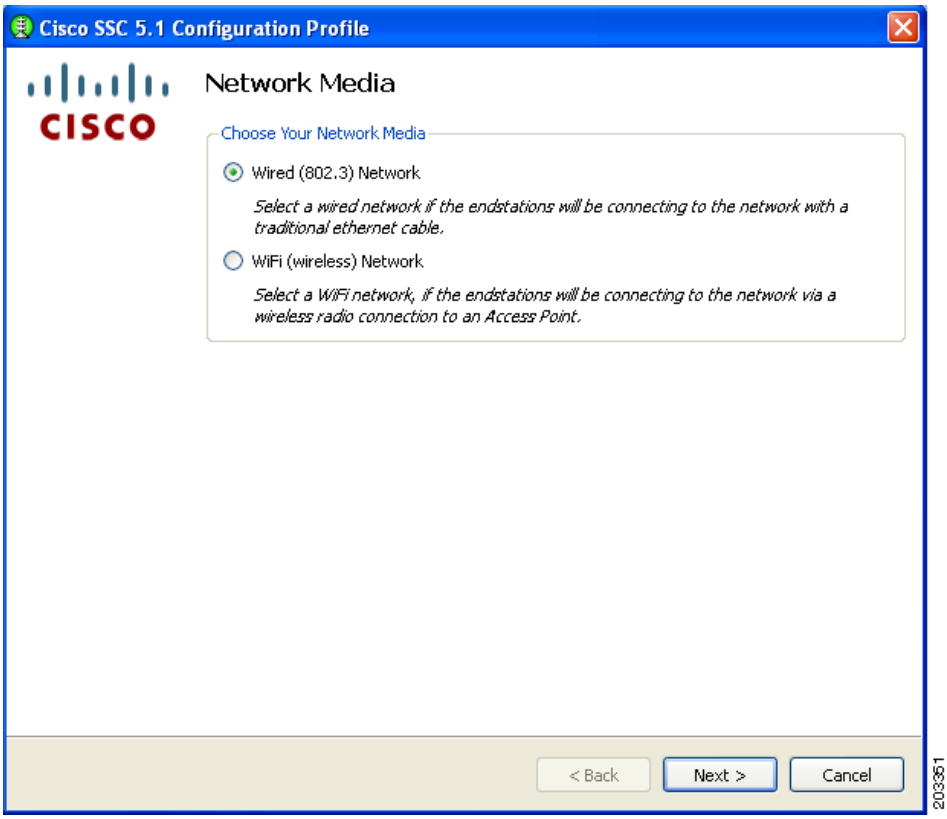
SSC can be configured to support both FIPS-compliant and non-compliant profiles. FIPS-compliant profiles include WPA2 Personal AES and WPA2 Enterprise AES. Supported EAP types with WPA2 Enterprise AES include: EAP TLS, PEAP, and EAP Fast.

Figure 7-22 Networks Window



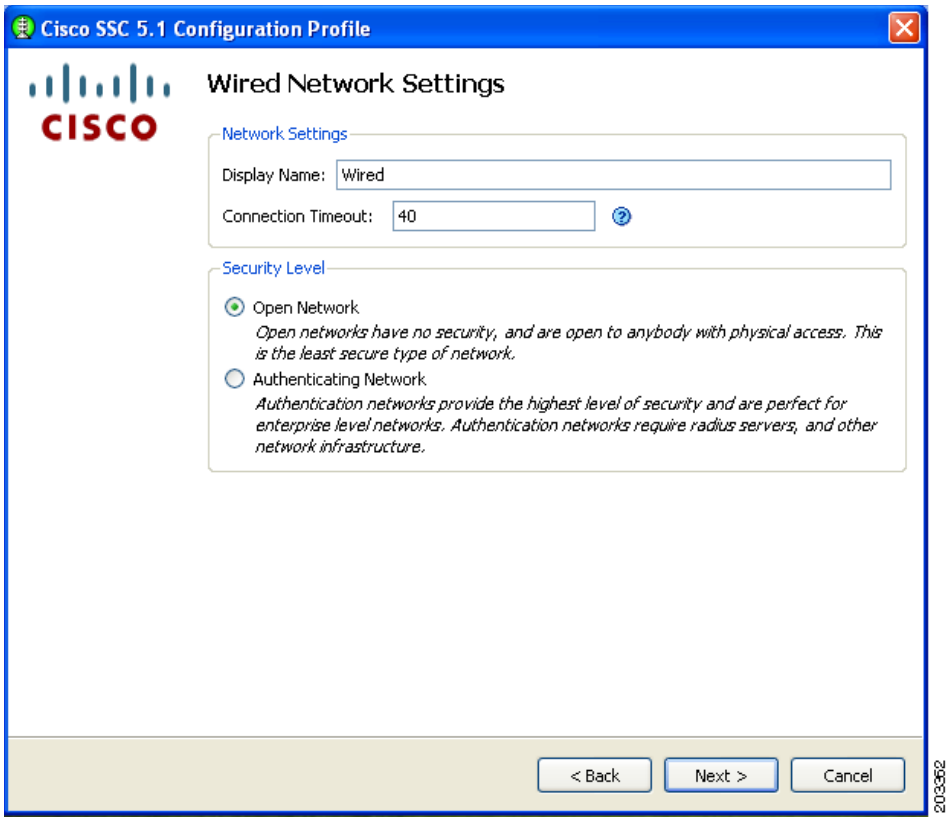
Step 6 Click **Add Network**. The first network to create is a wired network. This causes SSC to limit the connections to only one at a time. Figure 7-23 appears.

Figure 7-23 Network Media Window



Step 7 Check **Wired (802/3) Network** and click **Next**. Figure 7-24 appears.

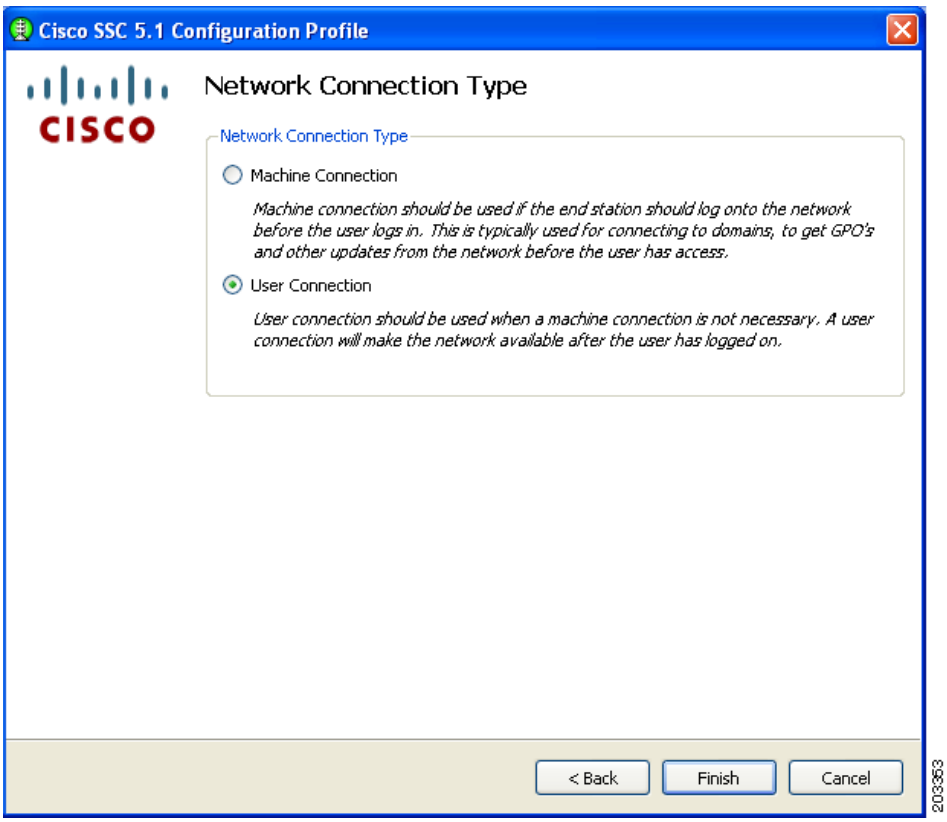
Figure 7-24 Wired Network Settings Window



Step 8 Enter **Wired** in the Display Name field and check **Open Network**.

Step 9 Click **Next** and Figure 7-25 appears.

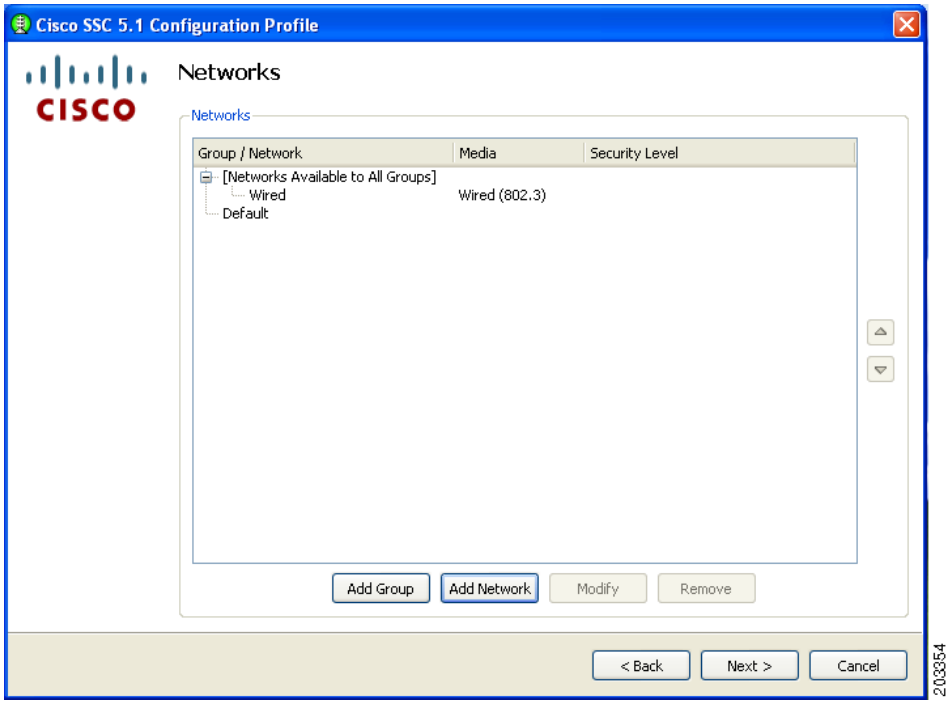
Figure 7-25 Network Connection Type Window



Step 10 Check **User Connection** and click **Finish**. You have configured your wired non-authentication port. The next operation is necessary to configure a FIPS-compliant wireless authentication profile.

Figure 7-26 appears.

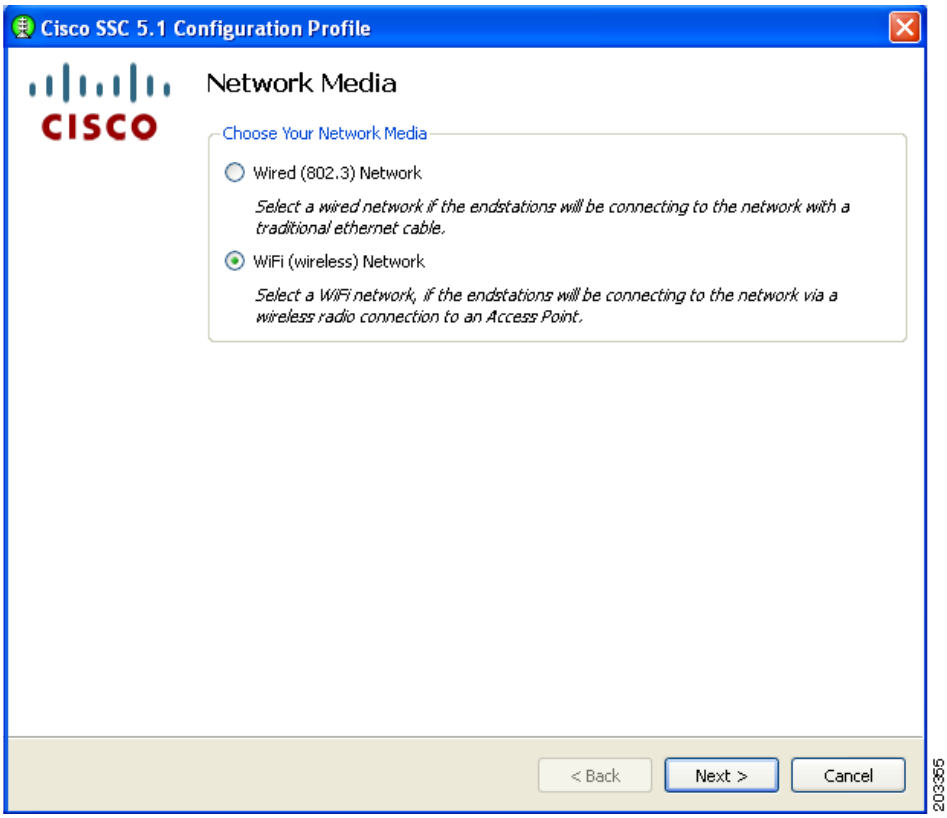
Figure 7-26 Networks Window



In Figure 7-26, the wired network is shown configured.

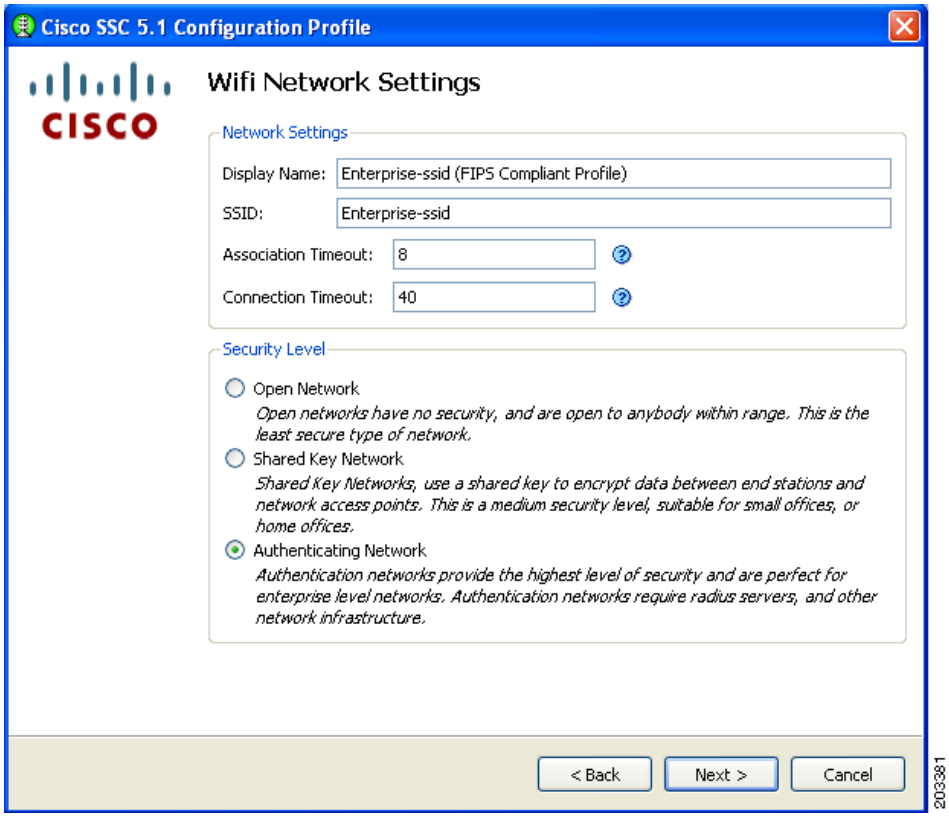
Step 11 Click **Add Network** and Figure 7-27 appears.

Figure 7-27 Network Media Window



Step 12 Check **Wi-Fi (wireless) Network** and click **Next**. Figure 7-28 appears.

Figure 7-28 Wi-Fi Network Settings Window



Note Some smartcard authentication systems require almost 60 seconds to complete an authentication. When using a smartcard, it might be necessary to increase the Connection Timeout value.

Step 13 follow these steps:

a. Enter the Display Name for the profile. It is recommended that the display name set by the network administrator to indicate that it is a FIPS-compliant profile, such as adding *FIPS* in addition to the display name (see Figure 7-28). This profile identification indicates that when connected using this administrator-deployed profile, the network authentication profile conforms to FIPS requirements.

b. Enter the SSID value in the SSID field.The SSID should be set to a valid enterprise SSID. The SSID value is case sensitive.

c. Change the Association Timeout from the default of 3 to value of 8 to 10 seconds.

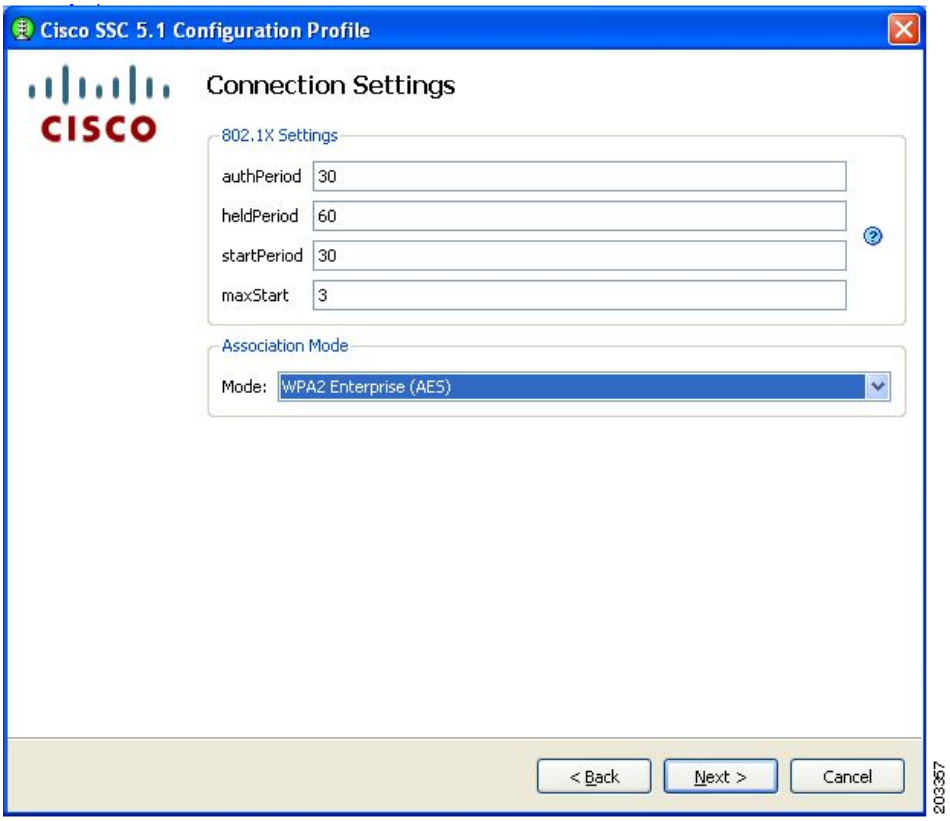
Note The Cisco AIR-CB21client adapter is not sensitive to this value; however, other wireless client adapters, such as the Intel 3945 client adapter require the increased association timeout value.

d. Click **Next**.

Step 14 When the CCX Settings window appears, ignore the settings and click **Next**. Figure 7-29 appears.

Note The CCX Setting window options are not applicable to Windows XP or Windows 2000 environments.

Figure 7-29 Connection Settings Window



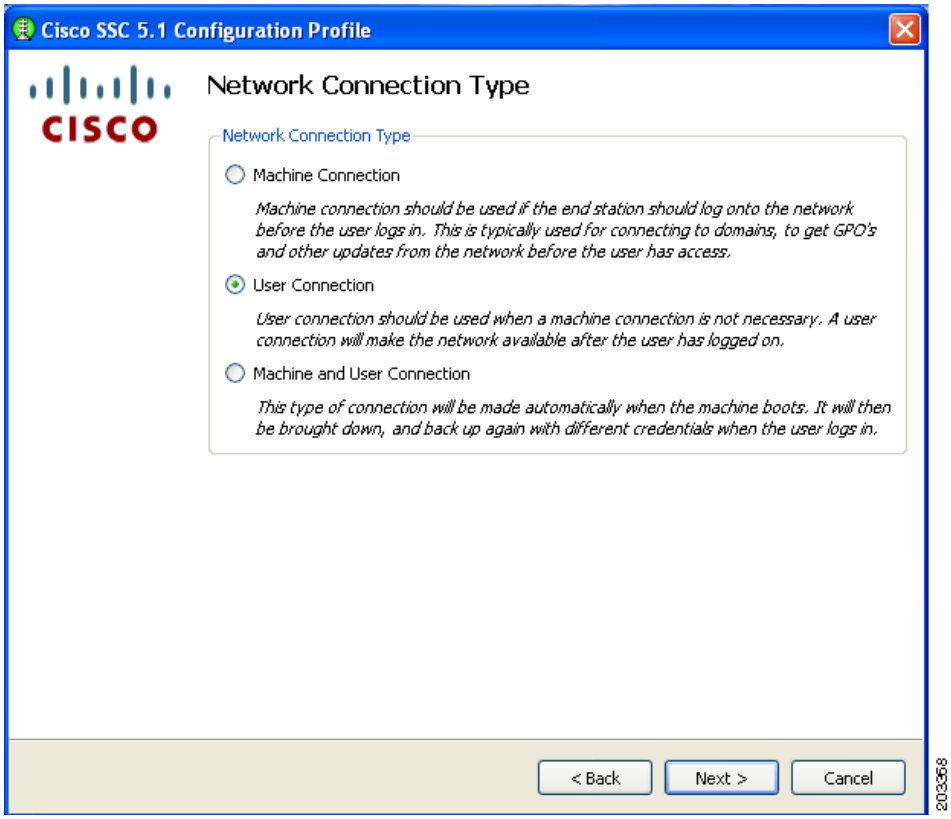
Step 15 Click the Association Mode drop-down arrow and choose **WPA2 Enterprise (AES)**.

Step 16 When configuring the 802.1X settings, Cisco recommends that you use the 802.1X default settings.

These settings are optimized for several different wireless environments and for a wired authenticating profile. Other setting values can be used, but they might not produce optimized operation.

Step 17 Click **Next** and Figure 7-30 appears.

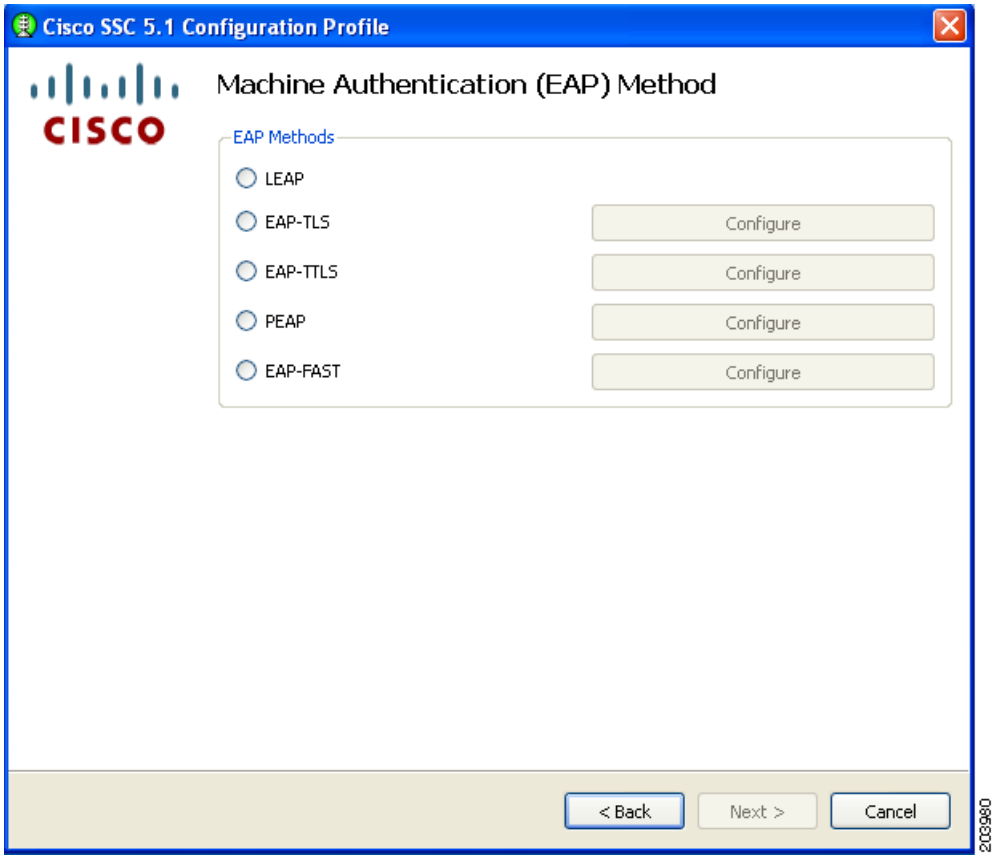
Figure 7-30 Network Connection Type Window



Any of the three options can be selected and will be FIPS-compliant.

Step 18 For this example, check **User Connection** and click **Next**. Figure 7-31 appears.

Figure 7-31 User Authentication (EAP) Method Window



Step 19 Follow one of these steps with the following EAP methods:

- Check **EAP-TLS** and click **Next**. Go to Step 20.
- Check **PEAP** and click **Next**. Go to Step 21.
- Check **EAP-Fast** and click **Next**. Go to Step 22.

Step 20 If you checked EAP-TLS, Figure 7-32 appears.

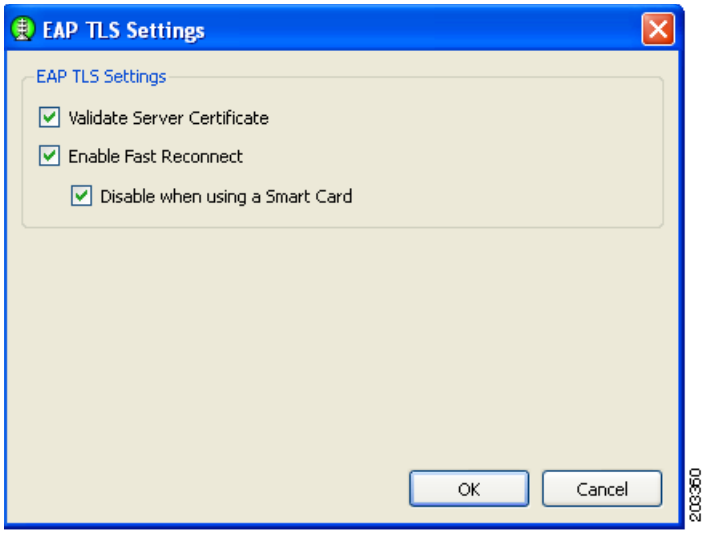
When using smartcards, there are two typical usage scenarios:

- The smartcard must be inserted for every smartcard re-authentication.
- The smartcard must be inserted for the first authentication, then the smartcard can be removed and only needs to be reinserted when the user logs out.

Both usage scenarios are acceptable for a FIPS-compliant profile.

Follow these steps:

Figure 7-32 EAP-TLS Settings Window



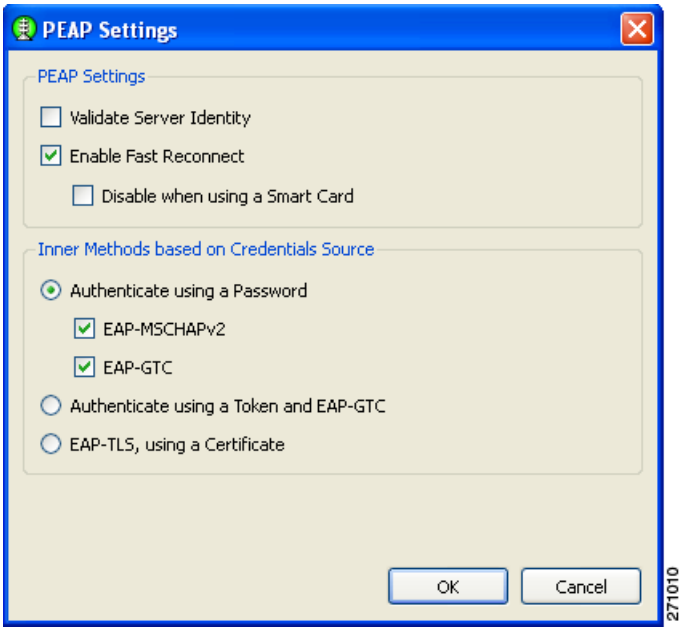
a. In a FIPS-compliant profile, check **Validate Server Certificate**.

b. Click **OK**. The User Authentication (EAP) Method window reappears.

c. Click **Next** on the User Authentication (EAP) Method window and go to Step 23.

Step 21 If you checked PEAP, Figure 7-33 appears.

Figure 7-33 PEAP Settings Window



For a FIPS-compliant profile, follow these steps:

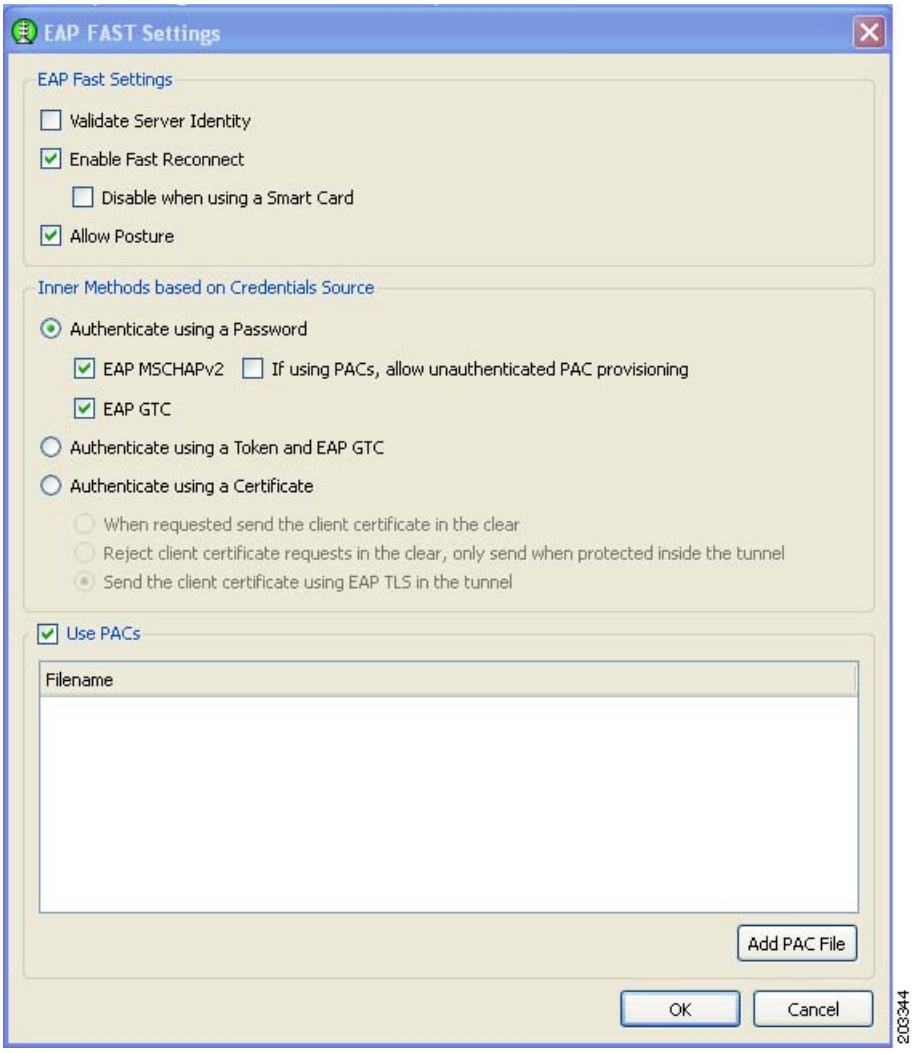
a. Check **Validate Server Identity**.

b. Click **OK** and the User Authentication (EAP) Method window reappears.

c. Click **Next** on the User Authentication (EAP) Method window and go to Step 23.

Step 22 If you checked EAP-Fast, Figure 7-34 appears.

Figure 7-34 EAP-Fast Settings Window



For a FIPS-compliant profile, follow these steps:

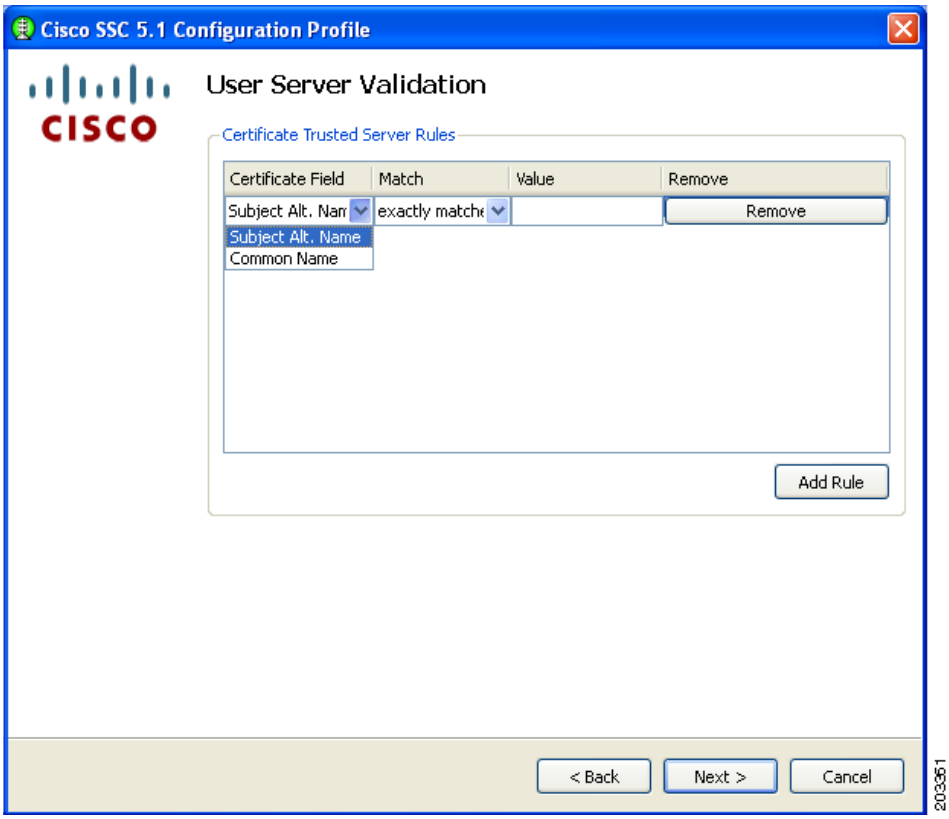
a. Check **Validate Server Identity**.

b. Click **OK** the User Authentication (EAP) Method window reappears.

c. Click **Next** on the User Authentication (EAP) Method window and go to Step 23.

Step 23 If you previously checked Validate Server Identity, Figure 7-35 appears.

Figure 7-35 Certificate Trusted Server Validation Rules Window



Step 24 Optional, define server validation rules by following these steps:

a. Click **Add Rule**.

b. Click the drop-down arrows and highlight the desired options.

c. Enter a value in the Value field.

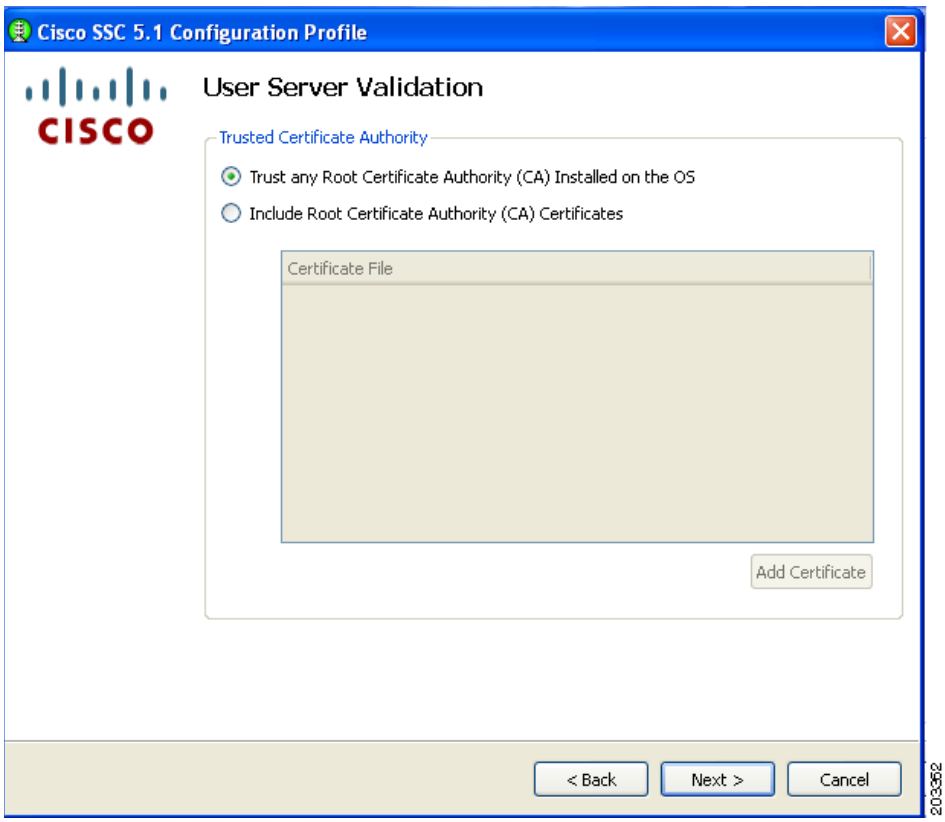
Note Click **Remove** to remove the rule.

d. When complete, click **Next** and Figure 7-36 appears.

Even when certificate rules are not created, these validations occur implicitly to satisfy FIPS:

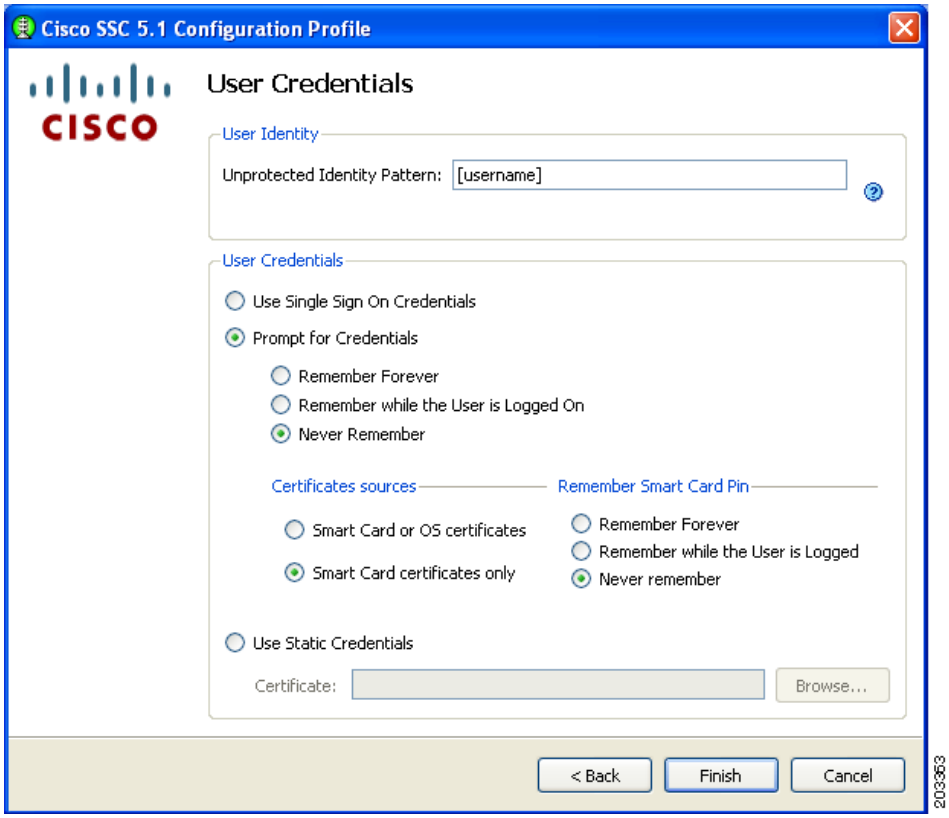
- The received server certificate has not expired.
- The server certificate chain is valid.
- The root node of the server certificate chain is trusted.

Figure 7-36 Trusted Server Authority Validation Window



Step 25 Accept the default setting or check the desired option. Click **Next** and Figure 7-37 appears.

Figure 7-37 Credentials Window



Step 26 Follow these steps:

a. Enter a username the Unprotected Identity Pattern field.

b. Check one of these options:

- **Single Sign On Credentials**
- **Prompt for Credentials**
- **Use Static Credentials**

c. If using Prompt for Credentials, check one of these options:

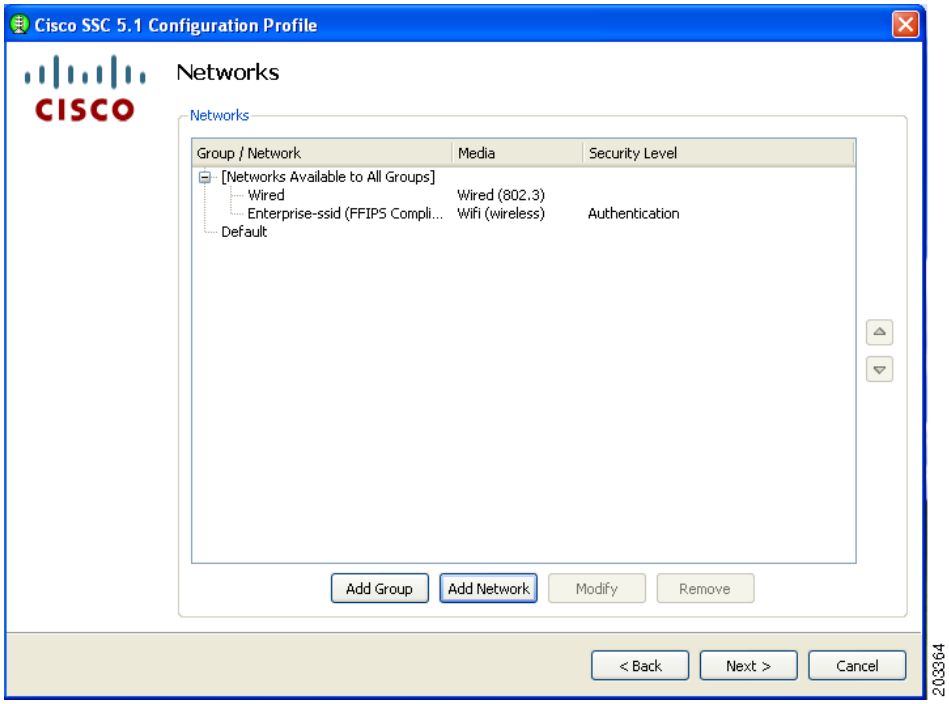
- **Never Remember**
- **Remember while the User is Logged On**

For FIPS-compliance, Never Remember and Remember while the User is Logged On are the only acceptable selections. All relevant security critical parameters are handled securely and cleared when no longer needed.

Note The Single Sign On and Use Static Credentials can be used in FIPS enabled mode.

d. Click **Finish** and Figure 7-38 appears.

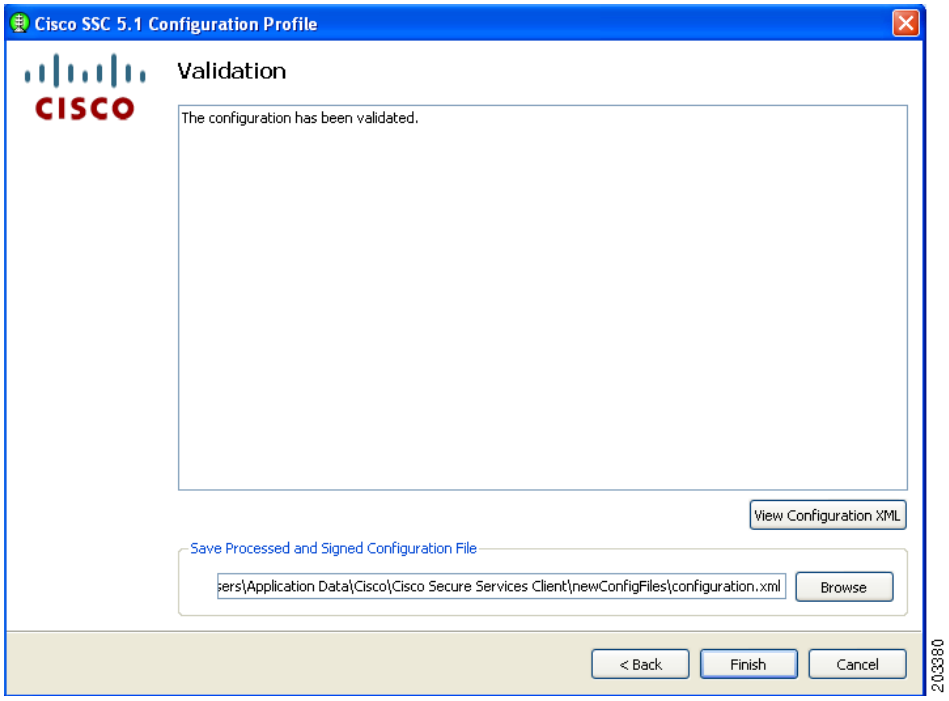
Figure 7-38 Configured Networks Window



This window lists the networks that have been created for this profile.

Step 27 Click **Next** and Figure 7-39 appears.

Figure 7-39 Validation Window



This window allows the administrator to view the configuration XML and save the configuration in an encrypted file for deployment. The administrator can also save an un-encrypted file for review, but this file must never be deployed.

Step 28 Follow these steps:

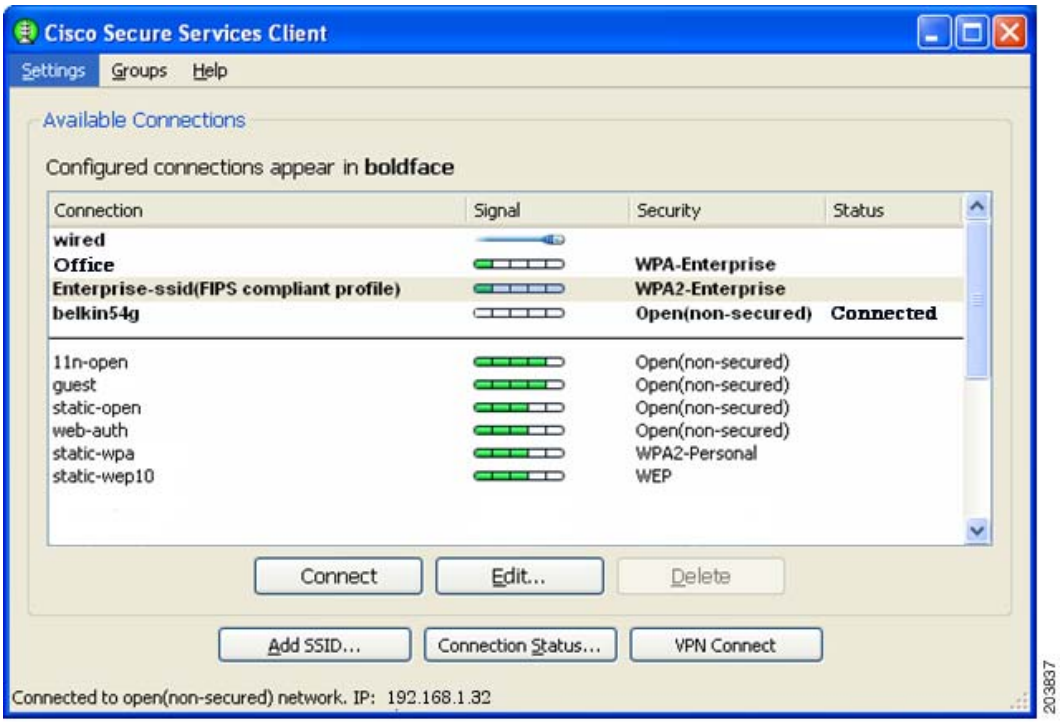
a. Accept the default location for storage of the encrypted configuration file or click **Browse** to browse to a different folder.

b. Optional, uncheck Save Original Configuration File.

c. Click **Finish**.

The configuration is now complete. If you open the SSC main window (see Figure 7-40), the new Enterprise-ssid (FIPS-compliant profile) have been added to the list of connections.

Figure 7-40 Available Connections Window



In Figure 7-40 the Enterprise-ssid profile is easily identified as a FIPS-compliant profile. For this profile, the delete button is disabled so that the user cannot delete the profile. Also, all the administrator configured credential settings are unavailable, when the Edit button is clicked. The only option that can be user-configured is to automatically initiate VPN connections on the FIPS-compliant network connection between the access point and the client PC.

Obtaining SSC and 3eTI Driver Installer Software

SSC 5.1.0 software is available from the Cisco Software Center:

- SSCMgmtToolKit—Contains the sscManagementUtility and support files.
- Cisco_SSC-XP2K_5.1.0.zip—Contains the SSC files. For SSC license information, refer to the "SSC License Information" section on page 2-5.
- CiscoClientUtilities_5.1.0.zip—Contains the Log Packager.

The SSC software can be obtained from the Cisco Software Center at this URL:

http://www.cisco.com/public/sw-center/index.shtml

Click **Wireless Software > Client Adapters and Client Software > Cisco Secure Services Client** and follow the prompts to 5.1.0 under Latest Releases.

Note You must register with Cisco.com or be a registered user to download software.

The FIPS 3eTI CKL supported driver installer cannot be downloaded from the Cisco Software Center and must be ordered from Cisco. A non-expiring license for the SSC software can be ordered from Cisco using these product numbers:

- AIR-SC5.0-XP2K—Cisco SSC Release 5.1 software license.
- AIR-SSCFIPS-DRV—3eTI CKL supported driver installer

The ordered 3eTI CKL supported driver installer software is shipped to the customer on a product CD.

Note The SSCMgmtToolKit (SSC Management Utility) and the Cisco Client Utilities are only available for download from the Cisco Software Center.

APPENDIX **A**

Cisco SSC 5.1.1 Log Messages

This appendix lists the log messages produced by SSC 5.1.1:

- **Starting Cisco_SSCservice.exe:** *version number*—indicates the SSC service is starting.
- **Cisco Trust Agent successfully loaded**.
- **Failed to load Cisco Trust Agent**.
- **Password sent**.
- **Certificate sent**.
- **Manual user** *logon type* **logon processing initiated by user** *user id*.
- **Normal Shutdown** *version number*—indicates a normal shutdown.
- **Fatal Shutdown** *version number*—indicates a fatal shutdown.
- **Machine startup**—indicates the client is beginning its boot time processing.
- **Account logon**—indicates the client detected a user logon.
- **SSO credentials (Microsoft)**—indicates when the client collects credentials from the Microsoft GINA (whether they are used or not during a network authentication).
- **Account logoff**—indicates the client detects a user logoff.
- **Adapter detected** *Adapter Id*—indicates a new adapter is detected in the system. The *Adapter Id* refers to the adapter's globally unique identifier (GUID).
- **Adapter removed** *Adapter Id*—indicates a previously reported adapter is lost (or removed).
- **Adapter controlled** *Adapter Id*—indicates control is taken of a particular adapter (the SSC intermediate driver begins to respond to network frames and attempt to set features of the adapter).
- *Adapter Id* **Adapter control failed** *error code*—indicates when the SSC client attempts to take control of an adapter but fails. The *error code* is an internal error code.
- **{WPA | WPA2} unsupported.** *Adapter Id*—indicates when control is taken of an adapter and if the adapter does or does not support WPA or WPA2.
- **Wireless Zero Config deactivated** *Adapter Id*— indicates when control was taken of an adapter that Wireless Zero Config was detected and automatically deactivated for that adapter.
- **Adapter control released** *Adapter Id*—indicates control was released for a particular adapter.

- **Connection Association Started** (*Wi-Fi Association /Encryption Mode*)—when a connection is requested on a Wi-Fi adapter an association must occur. This log message indicates the SSC client is attempting to associate to an SSID. *Wi-Fi Association/Encryption mode* could be one of these values:
  - Open
  - Shared 40 bit key
  - Shared 128 bit key
  - Static WEP 40 bit key
  - Static WEP 128 bit key
  - Dynamic WEP 40 bit key
  - Dynamic WEP 128 bit key
  - WPA-Personal TKIP encryption
  - WPA-Personal AES encryption
  - WPA-Enterprise TKIP encryption
  - WPA-Enterprise AES encryption
  - WPA2-Personal TKIP encryption
  - WPA2-Personal AES encryption
  - WPA2-Enterprise TKIP encryption
  - WPA2-Enterprise AES encryption
- **Starting wired connection, skipping association**.
- *Adapter Id* **Connection Association Success (link up)**—indicates an association has completed successfully.
- **Connection Association Failed. (Failure:** *error number*)—indicates an association has not completed successfully. *error number* is an internal error code.
- *Adapter Id* **Connection Authentication Started**—indicates an authentication attempt was started.
- *Adapter Id* **Identity requested**—when an identity request comes in from the access point.
- *Adapter Id* **Identity sent**—whenever an identity is sent.
- *Adapter Id* **EAP suggested by server:** *Authentication Method name*—indicates an EAP authentication method was suggested by the server. *Authentication Method name* is one of these values:
  - EAP-PEAP
  - EAP-TTLS
  - EAP-TLS
  - EAP-LEAP
  - EAP-MD5
  - EAP-GTC
  - EAP-FAST
  - EAP-MSCHAPv2
  - MSCHAPv2
  - MSCHAP

  - CHAP
  - PAP
- *Adapter Id* **EAP requested by client: (***Authentication Method name*, …, *Authentication Method name*)—indicates an EAP authentication method was requested by the client. *Authentication Method name* is one of these values:
  - EAP-PEAP
  - EAP-TTLS
  - EAP-TLS
  - EAP-LEAP
  - EAP-MD5
  - EAP-GTC
  - EAP-FAST
  - EAP-MSCHAPv2
  - MSCHAPv2
  - MSCHAP
  - CHAP
  - PAP
- *Adapter Id* **Port State** *Port State* and **Status** *Port status*—indicates the state and status of the adapter's port.

  Port State is one of values:
  - AC_PORT_STATE_STOPPED—indicates port is stopped
  - AC_PORT_STATE_CONNECTING—when it is waiting to start authentication
  - AC_PORT_STATE_AUTHENTICATING—is actively performing the initial 802.1X authentication
  - AC_PORT_STATE_AUTHENTICATED—successfully completed authentication
  - AC_PORT_STATE_REAUTHENTICATING—is actively performing 802.1X reauthentication
  - AC_PORT_STATE_UNAUTHENTICATED—when port wants to authenticate, but can't because of other conditions such as link is down or incorrect credentials
  - AC_PORT_STATE_AUTH_NOT_REQUIRED—when 802.1X authentication is not required. This state only exists for wired adapters or wireless adapters in WEP mode.

  Port status depends on the Port State value. This indicates a sub-state of the port state.
- *Adapter Id* **FAST: unauthenticated provisioning supported**—indicates FAST unauthenticated provisioning is supported by the adapter.
- *Adapter Id* **FAST: phase 1 tunnel for unauthenticated provisioning**.
- *Adapter Id* **Allowing session resumption**—indicates when the SSC client begins a TLS-based authentication (PEAP, TTLS, FAST or TLS) and attempts session resumption with a previous session id.
- *Adapter Id* **Authentication Success**—indicates an authentication completed successfully.
- *Adapter Id* **Authentication Failed**—indicates an authentication completed unsuccessfully.

- *Adapter Id* **IP Address Received:** *IP Address*—indicates a connection received an IP Address.
- *Adapter Id* **DHCP: Sending DHCP request.**
- *Adapter Id* **DHCP: Request failed**.
- *Adapter Id* **Wireless Zero Config reactivated for adapter**.
- *Access Id* **Wi-Fi access device has invalid channel number:** *SSID*, *channel*
- *Adapter Id* **Couldn't find pre-shared key in profile**.
- *Adapter Id***: EAP-TTLS method requested by client:** *method name*.
- **Starting Wi-Fi connection, trying ssid** *ssid name*.
- **Licensing: No license found**.
- **Licensing: License read:** *License string.*
- *License string***: (do not translate) is the license string read from the license file**.
- **Licensing: License invalid (trial period expired** *License string*, *trial period*).
- **Licensing: License invalid (termination date reached:** *License string*, *termination date*). *termination date* is the date in format yyyy-mm-dd that the license expired.
- **Licensing: License invalid because product id does not match:** *License string*, *licensed product id*.
- **Licensing: License invalid (OEM id does not match:** *License string*, *licensed OEM id*).
- **Licensing: License invalid (maintenance date reached:** *License string*, *maintenance date*). The *maintenance date* value is *the d*ate in format yyyy-mm-dd that the license's maintenance expired.
- **Licensing: License invalid (unknown problem:** *License string*).
- **Licensing: License is valid and accepted:** *License string*.
- **Licensing: Ignoring trial license. Tampering detected:** *License string*—whenever the license history file fails decryption this message is output with each new trial license that is encountered.
- **Licensing: License invalid, can not decode license:** *License string*.
- **The configuration is invalid and will be ignored. Error:** *error string*.
- **Trusted Server list empty, server can not be validated**.
- **Validating the server:** *Authentication Server Id*.
- **Server certificate validated:** *Authentication Server Id*
- *Authentication Session Id* **Server certificate invalid (unknown CA)**.
- **Server certificate invalid (name mismatch:** *CN/DC/Alt name from server cert*).
- **Invalid key type in distribution package**.
- *Outer method***: invalid/unsupported inner authentication method:** *inner method*.
- **Invalid outer EAP method:** *method name*.
- *Outer method***: No inner authentication methods configured**.
- **Disallowed element in configuration: wireless adapters unlicensed**.
- **Disallowed element in configuration: wired adapters unlicensed**.
- **Disallowed element in configuration: EAP method:** *method name*.
- **Disallowed element in configuration: Association mode:** *association mode*.

- **Symbolic name:** *GUID of adapter*, **MacAddr:** (M*AC address of adapter*), **Mtu:** (*MTU size*), **Media:** (*percentage*), **Encryption:** (*encryption modes*), **Auth:** (*auth modes*).
- **Server certificate chain invalid**.
- **Server certificate chain is not trusted**.
- **Invalid wep key length:** *key length*, **should be %d or %d**.
- **The wildcard** (*pattern string*) **in the pattern is unknown and will be removed**.
- **Internal error** *error number*, **contact software manufacturer**—indicates you should contact Cisco support.
- **Attempting VPN connection:** *VPN profile name*—indicates the name of the VPN profile on which the VPN connection is being initiated.
- **Received credential request from VPN client**—indicates that a credential request was sent to the GUI.
- **VPN credentials received from user**—indicates that the VPN credentials were received from the GUI.
- **VpnStateMachine new state = connected**—indicates that a successful VPN connection has been established.

APPENDIX B

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN

NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

APPENDIX **C**

Configuring a Single-User Account for FIPS

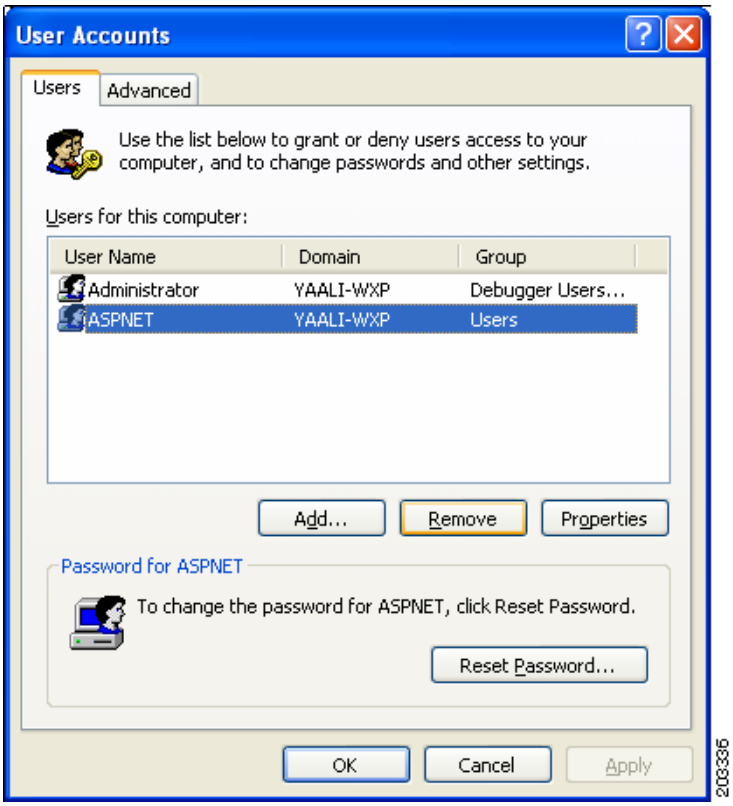
Note FIPS functionality is not supported by the Windows Vista version of SSC.

To configure a single-user account for FIPS on a PC, follow these instructions:

Step 1 Open the Windows Control Panel by clicking **Start > Settings > Control Panel**.

Step 2 Double-click **User Accounts** and Figure C-1 appears.

Figure C-1 Windows User Accounts Window



Step 3 Ensure that the User Tab lists only one administrator account. Remove all other user accounts, by highlighting the user account and clicking **Remove**.

For additional details, refer to Microsoft's Knowledge Base articles on creating and configuring user accounts in Windows.