



Identify-Based Networking Systems Configuration Guide

Version 1.0 December 2005

Corporate 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: 408 526-4100



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)



CONTENTS

CHAPTER 1

Introduction to Identity-Based Networking Systems 1-1

Overview	1-1
What is IEEE 802.1X?	1-2
Key Components of IEEE 802.1X	1-3
Supplicant	1-3
Authenticator	1-3
Authentication Server	1-3
EAP Methods	1-3
EAP-MD5	1-4
EAP-TLS	1-4
PEAP with EAP-MSCHAPv2	1-6
EAP-FAST	1-7
Cisco Systems Product and Software Support	1-8
Cisco Catalyst Series Switches	1-8
Cisco Systems Routers	1-9
Cisco Systems Wireless LAN Access Points and Controllers	1-10
Cisco Secure Access Control Server	1-10

CHAPTER 2

Authenticators 2-1

Cisco IOS	2-1
RADIUS Configuration for Cisco IOS	2-1
Global IEEE 802.1X Configuration for Cisco IOS	2-2
Interface IEEE 802.1X Configuration for Cisco IOS	2-2
Verify IEEE 802.1X Operation for Cisco IOS	2-2
Basic Configuration Example for Cisco IOS	2-3
show dot1x interface Example for Cisco IOS	2-3
Cisco Catalyst OS	2-4
RADIUS Configuration for Cisco Catalyst OS	2-4
Global IEEE 802.1X Configuration for Cisco Catalyst OS	2-4
Port IEEE 802.1X Configuration for Cisco Catalyst OS	2-4
Verify IEEE 802.1X Operation for Cisco Catalyst OS	2-5
Basic Configuration Example for Cisco Catalyst OS	2-5
show port dot1x [mod/port] Example for Cisco Catalyst OS	2-5
Cisco Aironet Wireless LAN Access Points Running Cisco IOS	2-6

RADIUS Configuration for Cisco Aironet Wireless LAN APs Running Cisco IOS	2-6
Global Configuration for Cisco Aironet Wireless LAN APs Running Cisco IOS	2-6
Interface Configuration for Cisco Aironet Wireless LAN APs Running Cisco IOS	2-7
Verify IEEE 802.1X Operation for Cisco Aironet Wireless LAN APs Running Cisco IOS	2-7
Basic Configuration Example for Cisco Aironet Wireless LAN APs Running Cisco IOS	2-7
show dot11 associations Example for Cisco Aironet Wireless LAN APs Running Cisco IOS	2-8

CHAPTER 3**Deploying EAP—MD5 3-1**

Authentication Server Configuration	3-1
Create a User in the ACS Database	3-1
Configure the User in the ACS Database	3-2
Configure a AAA Server	3-3
Configure a AAA Client	3-4
Summary of Network Configuration	3-5
Global Authentication Setup for EAP-MD5	3-6
Client Configuration	3-7
Open the Meetinghouse AEGIS client	3-7
Create the Machine Authentication Profile	3-8
Configure the Machine Authentication Profile	3-9
Create the User Authentication Profile	3-9
Configure the User Authentication Profile	3-10
Create a Network Profile	3-11
Configure the Port Settings	3-12
Configure the Network Profile	3-13
Apply the Network Profile	3-14
Verify Client Authentication	3-15

CHAPTER 4**Deploying EAP—TLS 4-1**

Authentication Server Configuration	4-1
Create an Unknown User Policy	4-1
Configure an Unknown User Policy	4-2
Select an External User Database	4-3
Choose to Configure the Windows Database	4-4
Configure the Windows Database	4-5
Configure a AAA Server	4-7
Configure a AAA Client	4-8
Verify the Network Configuration	4-8
Global Authentication Setup for EAP-TLS	4-8
Client Configuration	4-9

Open the Funk Odyssey Client	4-9
Configure Machine Account Parameters for Connection Settings	4-10
Create a Machine Profile	4-11
Configure Authentication Information for the Machine Profile	4-12
Configure the Authentication Method for the Machine Profile	4-14
Create a User Profile	4-15
Configure the Authentication Information for the User Profile	4-16
Configure the Authentication Method for the User Profile	4-18
Add a Trusted Server	4-19
Configure a Trusted Server Entry	4-20
Select the Trusted Root Certification Authority	4-21
Save the Trusted Server Entry	4-21
Verify the Trusted Servers	4-22
Apply an Adapter to the User Profile	4-23
Add the Adapter to the User Profile	4-23
Verify the Network Connection for the User Profile	4-24

CHAPTER 5

Deploying PEAP with EAP-MSCHAPv2 5-1

Authentication Server Configuration	5-1
Create an External User Database	5-1
Configure an External User Database	5-1
Select an External User Database	5-1
Choose to Configure the Windows Database	5-2
Configure the Windows Database	5-2
Configure a AAA Server	5-3
Configure a AAA Client	5-3
Verify the Network Configuration	5-3
Global Authentication Setup	5-3
Client Configuration	5-4
Enable IEEE 802.1X for the Local Area Connection	5-4
Configure the PEAP Properties	5-6
Configure the EAP-MSCHAPv2 Properties	5-7

CHAPTER 6

Deploying EAP-FAST 6-1

Authentication Server Configuration	6-1
Create an External User Database	6-1
Configure an External User Database	6-1
Select an External User Database	6-1
Choose to Configure the Windows Database	6-2

Configure the Windows Database	6-2
Configure a AAA Server	6-2
Configure a AAA Client	6-2
Verify the Network Configuration	6-2
Global Authentication Setup	6-2
Client Configuration	6-4
Create a Profile for EAP-FAST	6-5
Edit the Profile Configuration	6-5
Configure the System Parameters of the Profile	6-6
Configure the Network Security for the Profile	6-7
Configure the EAP-FAST Settings for the Profile	6-8

APPENDIX A

Optional Cisco IOS & Cisco Catalyst OS Configuration Commands A-1

Cisco IOS	A-1
RADIUS Configuration for Cisco IOS	A-1
Global IEEE 802.1X Configuration for Cisco IOS	A-2
Interface IEEE 802.1X Configuration for Cisco IOS	A-2
Cisco Catalyst OS	A-3
Global IEEE 802.1X Configuration for Cisco Catalyst OS	A-3
Port IEEE 802.1X Configuration for Cisco Catalyst OS	A-4
Cisco Aironet Wireless LAN Access Points Running Cisco IOS	A-4
RADIUS Configuration for Cisco Aironet Wireless LAN Access Points Running Cisco IOS	A-5
Interface Configuration for Cisco Aironet Wireless LAN Access Points Running Cisco IOS	A-5

APPENDIX B

Installing an X.509v3 PKI Certificate on the Client B-1

Access the Certificate Authority	B-1
Request a Certificate	B-2
Complete the Certificate Request	B-3
Install the Certificate	B-4
Certificate Installation Complete	B-5
Verify Certificate Installation	B-6

APPENDIX C

Installing an X.509v3 PKI Certificate on the CS ACS C-1

Select ACS Certificate Setup	C-1
Select Generate Certificate Signing Request	C-2
Submit a Certificate Signing Request	C-3
Copy the Certificate Signing Request	C-4
Access the Certificate Authority	C-5

Request an Advanced Certificate	C-6
Submit a Certificate Request	C-7
Complete the Certificate Request	C-7
Download the Certificate onto ACS	C-8
Install the Certificate onto ACS	C-9
Verify ACS Certificate Installation	C-10

APPENDIX D**References D-1**

Cisco Product Documentation	D-1
Partner Product Documentation	D-1
Industry Standards	D-2



Introduction to Identity-Based Networking Systems

Overview

The need for complete network security has never been greater nor as well understood. Malicious users threaten to steal, manipulate, and impede information. Numerous solutions address perimeter defense, but the greatest threat of information theft and unauthorized access remains within the internal network boundaries.

One point of concern is the relative ease of physical and logical access to a corporate network. Both physical and logical access has been extended to enable a greater level of mobility, providing several benefits to business operations and overall productivity. However this greater level of mobility, combined with very limited security solutions, has also increased the overall risk of network exposure.

This document outlines a framework and system based on technology standards that allow the network administrator to implement true identity-based network access control, down to the user and individual access-port at the network edge. The system provides user and/or device identification using strong authentication technologies known to be secure and reliable. The identity of the users and/or devices can be further leveraged by mapping them to policies that grant or deny network access, set network parameters, and work with other security features to enforce items such as posture assessments.

This configuration guide focuses on the basic deployment of an identity-based networking system using IEEE 802.1X. The Identity-Based Networking System from Cisco Systems provides the network with these services and capabilities:

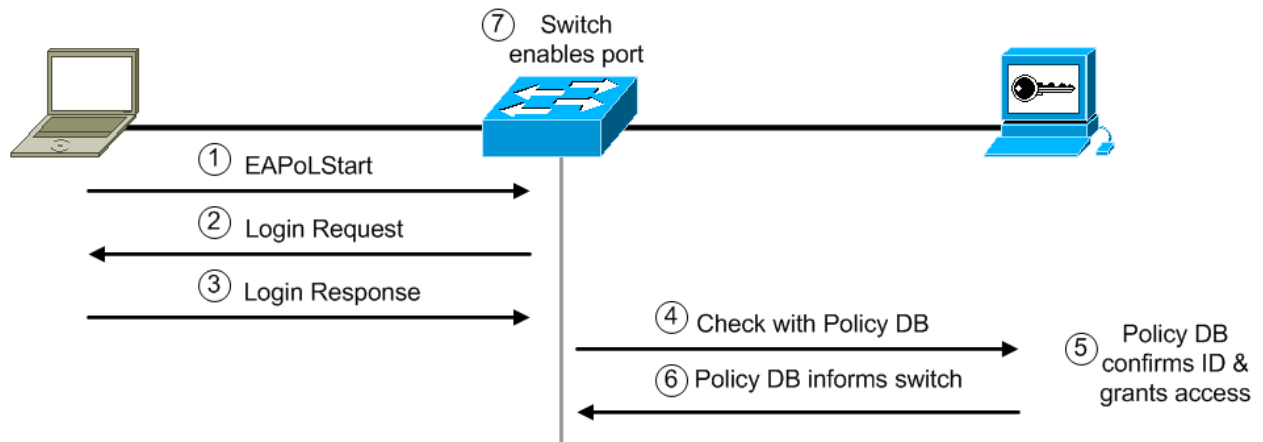
- User and/or device authentication
- Map the identity of a network entity to a defined set of policies configured by management
- Grant or deny network access, at the port level, based on configured authorization policies
- Enforce additional policies, such as resource access, when access is granted

These capabilities are introduced when a Cisco end-to-end system is implemented with the Cisco Catalyst family of switches, wireless LAN access points and controllers, and the CiscoSecure Access Control Server (ACS). Additional components of the system include an IEEE 802.1X compliant client operating system, such as Windows XP, and an optional X.509 Public Key Infrastructure (PKI) certificate architecture. Cisco IP phones also interoperate with an identity-based networking system based on IEEE 802.1X when deployed on a Cisco end-to-end infrastructure.

In compliance with the IEEE 802.1X standard, Cisco Catalyst switches can perform basic port-based network access control. Once IEEE 802.1X compliant client software is configured on the end device, the Cisco Catalyst switches running IEEE 802.1X features authenticate the requesting user or system in conjunction with a back-end CiscoSecure ACS server.

The high level message exchange in [Figure 1-1](#) illustrates how port-based access control works within an identity-based system. First a client, such as a laptop, connects to an IEEE 802.1X-enabled network and sends a start message to the LAN switch. Once the start message is received, the LAN switch sends a login request to the client and the client replies with a login response. The switch forwards the response to the policy database, which authenticates the user. After the user identity is confirmed, the policy database authorizes network access for the user and informs the LAN switch. The LAN switch then enables the port connected to the client.

Figure 1-1 Port-Based Access Control



User or device credentials and reference information are processed by the CiscoSecure ACS. The CiscoSecure ACS is able to reference user or device policy profile information either:

- Internally using the integrated user database
- Externally using database sources such as Microsoft Active Directory, LDAP, Novell NDS, or Oracle databases

This enables the integration of the system into existing user management structures and schemes, thereby simplifying overall deployment.

What is IEEE 802.1X?

The development of protocols, such as IEEE 802.1X, combined with the ability of network devices and components to communicate using existing protocols, provides network managers with the flexibility to manage network access control and policies. The association of the identity of a network-connected entity to a corresponding set of control policies has never before been as secure and as flexible. Proper design and deployment offer the network manager increased security and control of access to network segments and resources.

IEEE 802.1X is a protocol standard that provides an encapsulation definition for the transport of the Extensible Authentication Protocol (EAP) at the media-access control layer over any Point-to-Point Protocol (PPP) or IEEE 802 media. IEEE 802.1X enables the implementation of port-based network access control to a network device. IEEE 802.1X transports EAP messages between a supplicant and an authenticator. The authenticator then typically relays the EAP information to an authentication server via the RADIUS protocol. IEEE 802.1X not only provides the capability to permit or deny network connectivity based on user or machine identity, but also works in conjunction with higher layer protocols to enforce network policy.

The next section provides a detailed explanation of the IEEE 802.1X components.

Key Components of IEEE 802.1X

Supplicant

The supplicant is a device (workstation, laptop, etc.) that requests access to the LAN and switch services and responds to requests from the authenticator (switch). The device must be running IEEE 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. The client is the *supplicant* in the IEEE 802.1X specification.

Authenticator

The authenticator is a device (such as a Cisco Catalyst switch) that controls physical access to the network based on the authentication status of the client. The authenticator usually acts as an intermediary (proxy) between the client and the authentication server. The authenticator requests identity information from the client via EAP, verifies that information with the authentication server via RADIUS, and then relays a response to the client based on the response from the authentication server.

When the switch receives EAP over LAN (EAPOL) frames and relays them to the authentication server, the Ethernet header and EAP frame are re-encapsulated into the RADIUS format. The EAP frames are not modified or examined during encapsulation and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the RADIUS header is removed, leaving the EAP frame, which is then encapsulated in the IEEE 802.1X format and sent to the client.

Authentication Server

The authentication server performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication server is transparent to the client. The RADIUS security system with EAP extensions is the only supported authentication server. RADIUS uses a client-server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

EAP Methods

IEEE 802.1X supports several different EAP methods for providing identity-based network access control. Four of the EAP methods are defined in this section and the following chapters explain how to configure them. The four methods include:

- EAP-Message Digest 5 (MD5)
- EAP-Transport Level Security (EAP-TLS)
- Protected EAP (PEAP)
- EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)

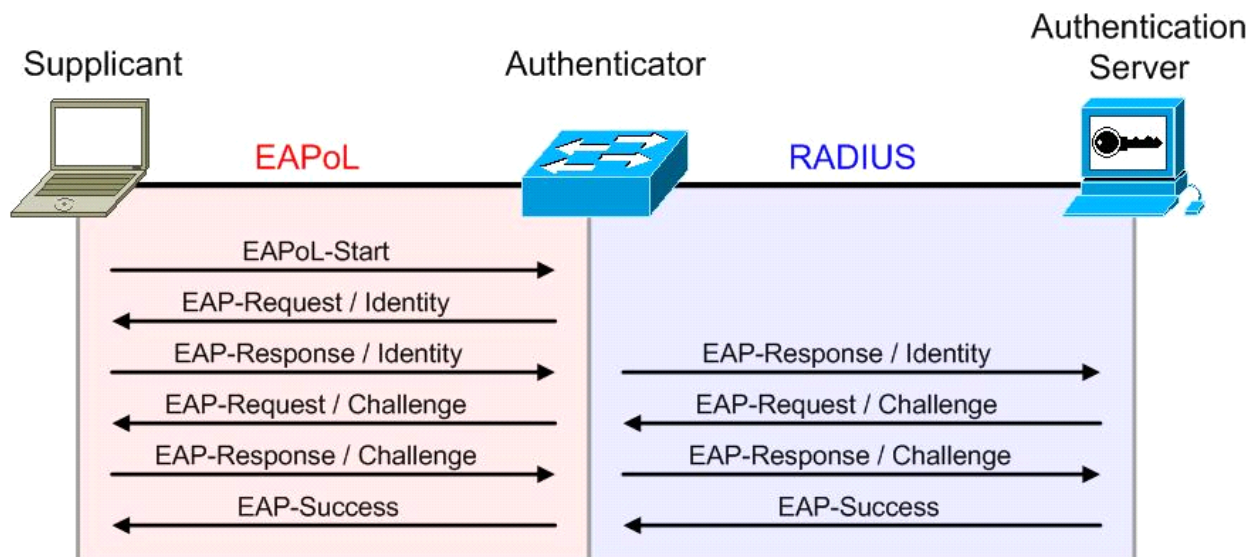
EAP-MD5

EAP-MD5 is a standard, non-proprietary EAP type. It is based on RFC 1994 (CHAP) and RFC 2284 (EAP). An MD5-Challenge within an EAP message is analogous to the PPP CHAP protocol, with MD5 specified as the hash algorithm. Because MD5 support is included in RFC 3748, all EAP deployments should support the MD5-Challenge mechanism.

EAP-MD5 is one of the easiest EAP types to deploy, however it is not very secure and is more susceptible to attacks, such as offline dictionary attacks, than other EAP methods.

Figure 1-2 illustrates the EAP-MD5 message exchange between the supplicant, authenticator, and authentication server. First, a client running the IEEE 802.1X supplicant connects to the network and sends an EAPoL-Start message to the authenticator. The authenticator sends an EAP Identity request to the supplicant and the supplicant replies with an EAP Identity response. The authenticator forwards the response to the authentication server via RADIUS. The authentication server sends an EAP-MD5 Challenge to the supplicant and the supplicant replies with a response. The authentication server confirms the user identity and instructs the authenticator to authorize network access for the user. The authenticator then enables the port connected to the supplicant.

Figure 1-2 EAP-MD5 Message Exchange



EAP-TLS

EAP-TLS was developed by Microsoft Corporation to enable the use of EAP as an extension of PPP to provide authentication within PPP and TLS to provide integrity-protected ciphersuite negotiation and key exchange. EAP-TLS, which is defined in RFC 2716, uses X.509 public key infrastructure (PKI) certificate-authenticated IEEE 802.1X port-based access control and is specifically targeted to address a number of weaknesses in other EAP protocols such as EAP-MD5. In addressing these weaknesses, however, the complexity of deployment increases because not only servers, but also clients require certificates for mutual authentication.

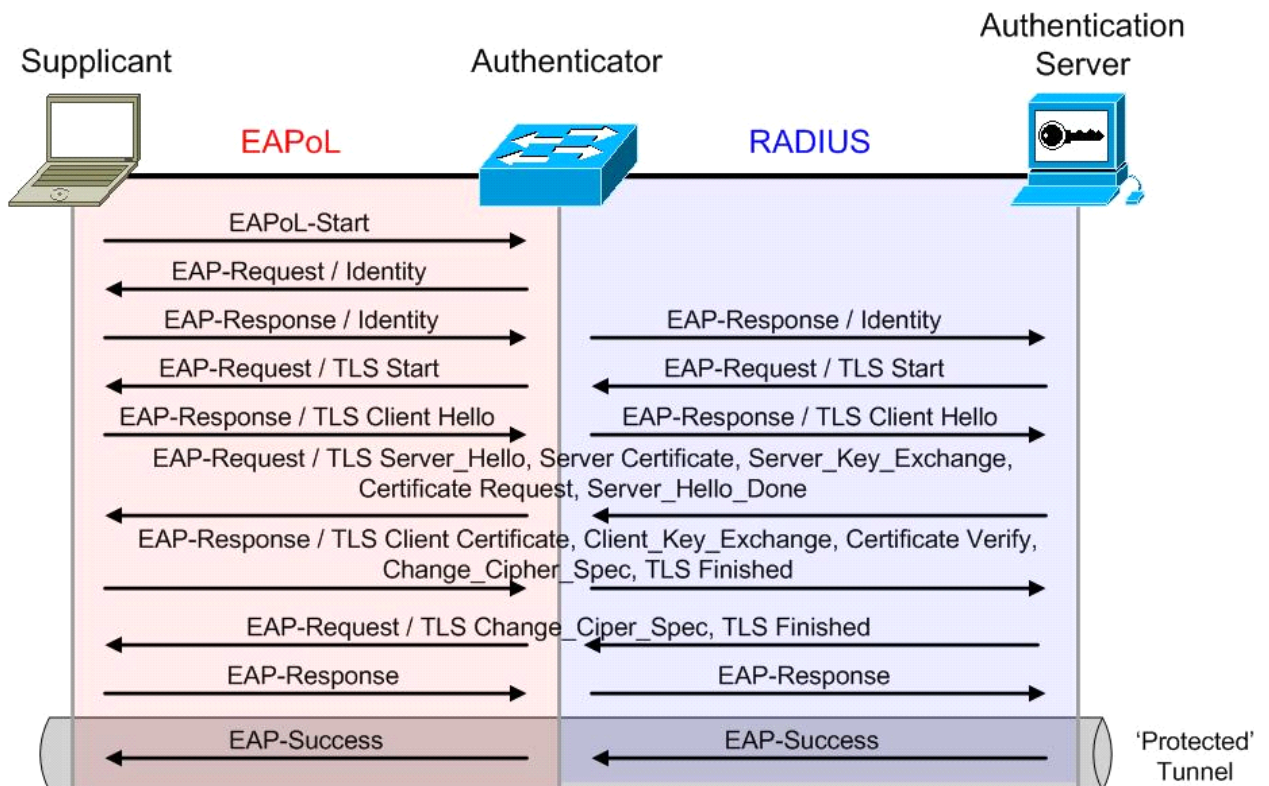
Some of the benefits of EAP-TLS include:

- The ability to provide per packet confidentiality and integrity protection, which protects user identity
- A standardized mechanism for key exchange
- Built-in support for fragmentation and reassembly
- Support for acknowledged success/failure indications

Within IEEE 802.1X, the EAP-TLS exchange of messages provides mutual authentication, negotiation of the encryption method, and encrypted key determination between a supplicant and an authentication server.

Figure 1-3 illustrates the EAP-TLS message exchange between the supplicant, authenticator, and authentication server. First, a client running the IEEE 802.1X supplicant connects to the network and sends an EAPoL-Start message to the authenticator. The authenticator sends an EAP Identity request to the supplicant and the supplicant replies with an EAP Identity response. The authenticator forwards the response to the authentication server via RADIUS. The authentication server sends an EAP-TLS Start message to the supplicant and the supplicant replies with an EAP-TLS Client Hello. The authentication server sends its X.509 PKI certificate to the supplicant and requests that the supplicant send its certificate. The supplicant verifies the certificate with the authentication server's public key and sends its certificate to the authentication server along with an updated ciphersuite. The authentication server verifies the supplicant's certificate, thus authenticating the identity of the user, and confirms the ciphersuite. With the TLS tunnel now established, the authentication server instructs the authenticator to authorize network access for the user. The authenticator then enables the port connected to the supplicant.

Figure 1-3 EAP-TLS Message Exchange



PEAP with EAP-MSCHAPv2

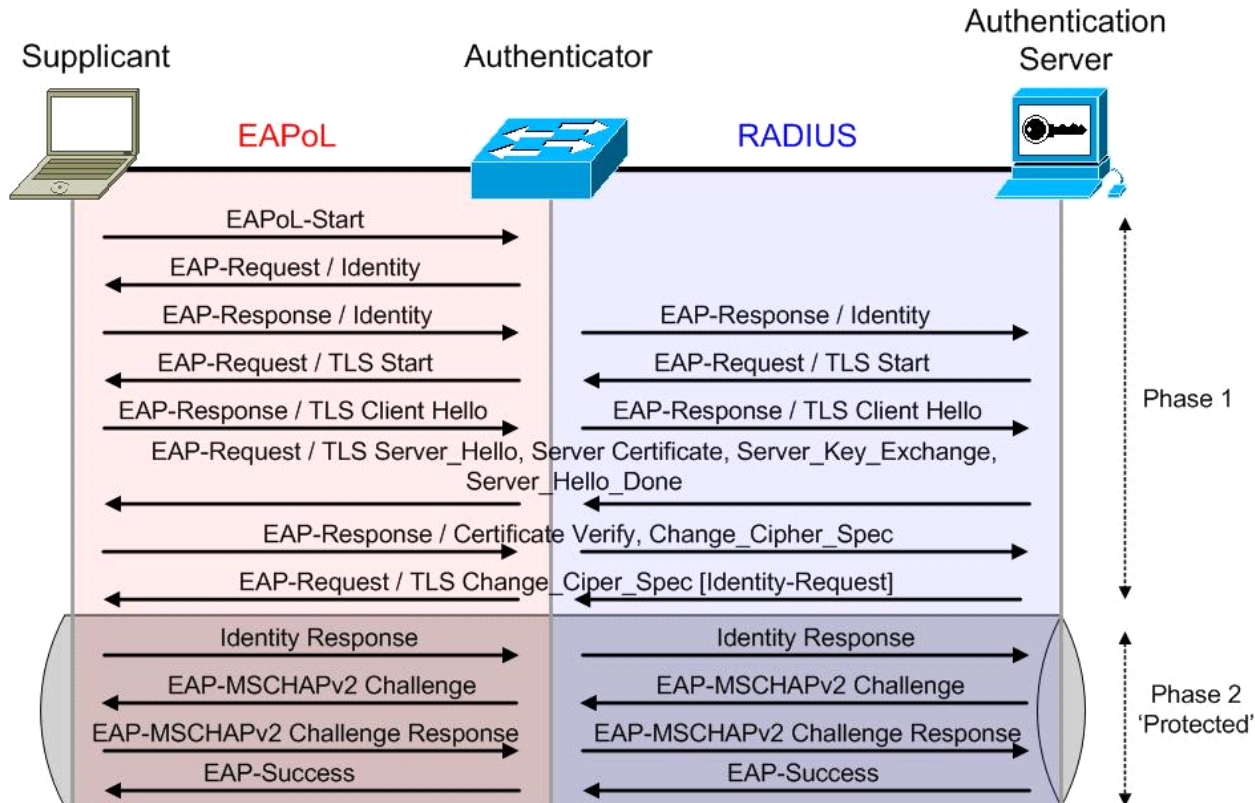
PEAP was developed by Cisco Systems, Microsoft Corporation, and RSA Security Inc. PEAP is an EAP type that addresses security issues by first creating a secure channel that is both encrypted and integrity-protected with TLS. Then, a new EAP negotiation with virtually any EAP type (EAP-MSCHAPv2 for example) occurs, authenticating the network access attempt of the client. Because the TLS channel protects EAP negotiation and authentication for the network access attempt, password-based authentication protocols that are normally susceptible to an offline dictionary attack can be used for authentication. By wrapping the EAP messages within TLS, any EAP method running within PEAP is provided with built-in support for key exchange, session resumption, fragmentation, and reassembly. Furthermore, PEAP makes it possible to authenticate LAN clients without requiring them to have certificates, simplifying the architecture of secure wired/wireless LANs.

**Note**

PEAP is supported in Windows XP Service Pack 1 (SP1), Windows XP Service Pack 2 (SP2), Windows Server 2003, and Windows 2000 Service Pack 4 (SP4).

MS-CHAPv2 is a password-based, challenge-response, mutual authentication protocol that uses MD4 and DES to encrypt responses. The authenticator challenges a supplicant and the supplicant can challenge the authentication server. If either challenge is not correctly answered, the connection can be rejected. MS-CHAPv2 was originally designed by Microsoft as a PPP authentication protocol to provide better protection for dial-up and VPN connections, although it is now an EAP type as well. Although MS-CHAPv2 provides better protection than previous challenge-response authentication protocols, it is still susceptible to an offline dictionary attack. A malicious user can capture a successful MS-CHAPv2 exchange and guess passwords until the correct one is determined. Used in the combination with PEAP, however, the MS-CHAPv2 exchange is protected with the strong security of the TLS channel.

Figure 1-4 illustrates the PEAP with MS-CHAPv2 message exchange between the supplicant, authenticator, and authentication server. First, a client running the IEEE 802.1X supplicant connects to the network and sends an EAPoL-Start message to the authenticator. The authenticator sends an EAP Identity request to the supplicant and the supplicant replies with an EAP Identity response. The authenticator forwards the response to the authentication server via RADIUS. The authentication server sends an EAP-TLS Start message to the supplicant and the supplicant replies with an EAP-TLS Client Hello. The authentication server sends its X.509 PKI certificate to the supplicant. The supplicant verifies the certificate with the authentication server's public key and sends an updated ciphersuite. The authentication server agrees to the ciphersuite. With the TLS tunnel now established, the authentication server sends an EAP-MSCHAPv2 challenge to the supplicant and the supplicant replies with a response. The authentication server confirms the user identity and instructs the authenticator to authorize network access for the user. The authenticator then enables the port connected to the supplicant.

Figure 1-4 PEAP with EAP-MSCHAPv2 Message Exchange

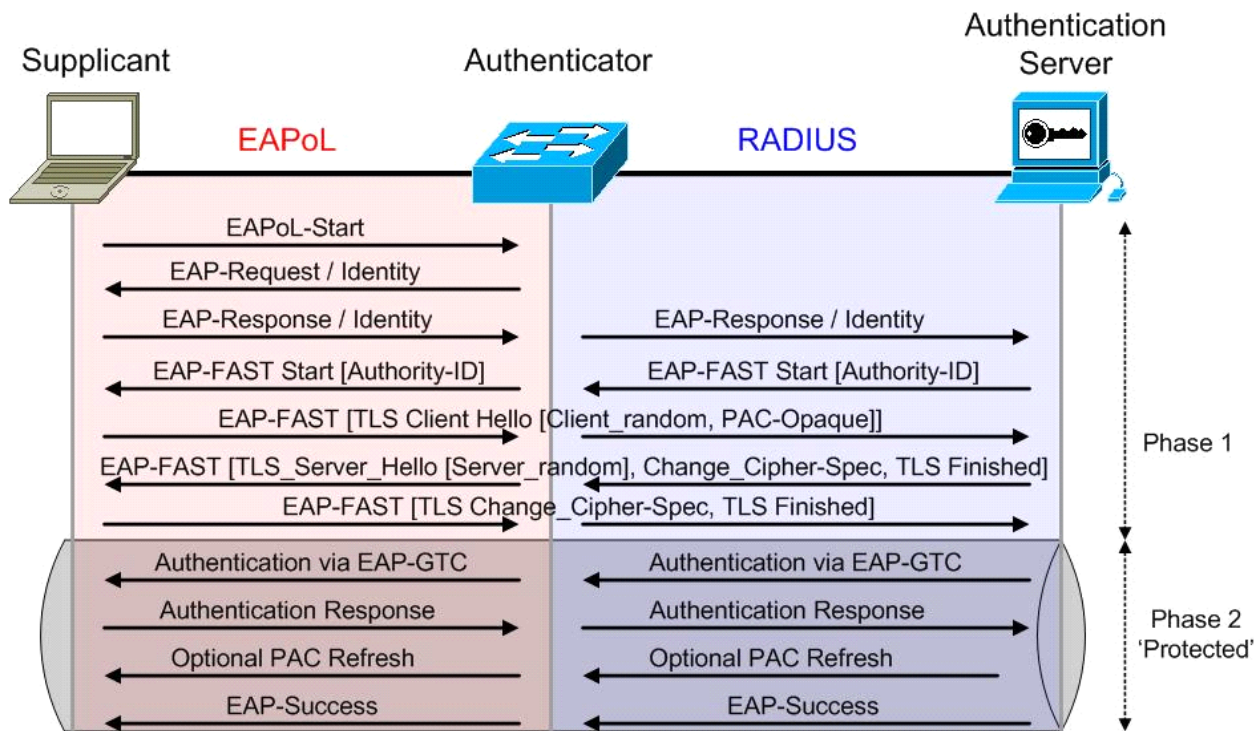
EAP-FAST

EAP-FAST was developed by Cisco Systems and submitted to the IETF as an Internet draft in February 2004. The Internet draft was revised and submitted in April 2005. The EAP-FAST protocol is a client-server security architecture that encrypts EAP transactions within a TLS tunnel. While similar to PEAP in this respect, it differs significantly in that the EAP-FAST tunnel establishment is based upon strong shared secret keys that are unique to users. These secrets are called Protected Access Credentials (PACs) and may be distributed automatically (automatic or in-band provisioning) or manually (manual or out-of-band provisioning) to client devices. Because handshakes based upon shared secrets are intrinsically faster than handshakes based upon a PKI infrastructure, EAP-FAST is the significantly faster of the two solutions that provide encrypted EAP transactions.

Figure 1-5 illustrates the EAP-FAST message exchange between the supplicant, authenticator, and authentication server using EAP-GTC as the inner method. First, a client running the IEEE 802.1X supplicant connects to the network and sends an EAPoL-Start message to the authenticator. The authenticator sends an EAP Identity request to the supplicant and the supplicant replies with an EAP Identity response. The authenticator forwards the response to the authentication server via RADIUS. The authentication server sends an EAP-FAST Start message, which includes the Authority ID, to the supplicant. Based on the Authority ID sent by the authentication server, the supplicant selects a stored Protected Access Credential (PAC), which is a unique shared key used to mutually authenticate the supplicant and server. The supplicant then replies to the authentication server with a PAC opaque (based on the PAC key). The authentication server decrypts the PAC opaque using a master key to derive the PAC key. At this point, both the supplicant and server possess the same PAC key and create a TLS tunnel.

The authentication server sends an EAP-GTC (Generic Token Card) request to the supplicant and the supplicant replies with a response. The authentication server confirms the user identity and instructs the authenticator to authorize network access for the user. The authenticator then enables the port connected to the supplicant.

Figure 1-5 EAP-FAST Message Exchange

**Note**

There is an optional Phase 0 in which the PAC is initially distributed to the client.

Cisco Systems Product and Software Support

This section provides information regarding the hardware platforms and **minimum** software releases required to support the basic identity-based networking system.

Cisco Catalyst Series Switches

Table 1-1 Cisco Catalyst Series Switches

Cisco Catalyst 6500 Catalyst OS	6.2(2)
Cisco Catalyst 6500 IOS	12.1(12b)E
Cisco Catalyst 4500 Catalyst OS	6.2(1)
Cisco Catalyst 4500 IOS	12.1(12c)EW

Table 1-1 Cisco Catalyst Series Switches

Cisco Catalyst 4948 EMI/SMI	12.2(20)EWA
Cisco Catalyst 3750 EMI	12.1(11)AX
Cisco Catalyst 3750 SMI	12.1(11)AX
Cisco Catalyst 3560EMI	12.1(19)EA1
Cisco Catalyst 3560 SMI	12.1(19)EA1
Cisco Catalyst 3550 EMI	12.1(8)EA1
Cisco Catalyst 3550 SMI	12.1(8)EA1
Cisco Catalyst 2970	12.1(11)AX
Cisco Catalyst 2950 EI	12.1(6)EA2
Cisco Catalyst 2950 SI	12.1(9)EA1
Cisco Catalyst 2940	12.1(13)AY

**Note**

[Table 1-1](#) provides a reference for the minimum supported software required to enable identity-based networking; it is recommended that the user refer to the Software Center on Cisco Connection Online for current information regarding newer and deferred software releases.

Cisco Systems Routers

Table 1-2 Cisco Systems Routers

831, 836, 837	12.3(2)XA
871, 876, 877, 878	12.3(8)YI
1701, 1711, 1712, 1721, 1751, 1760	12.3(2)XA
1801, 1802, 1803, 1811, 1812	12.3(8)YI
1841, 2800, 3800 HWIC-4ESW & HWIC-9ESW	12.3(8)T4
2800, 3800 NM-16ESW & NMD-36ESW	12.3(4)T
2800, 3800 NME-16ES-1G, NME-X-23ES-1G, NME-XD-24ES-1S & NME-XD-48ES-2S	12.2(25)SEC

**Note**

[Table 1-2](#) provides a reference for the minimum supported software required to enable identity-based networking; it is recommended that the user refer to the Software Center on Cisco Connection Online for current information regarding newer and deferred software releases.

Cisco Systems Wireless LAN Access Points and Controllers

Table 1-3 *Cisco Systems Wireless LAN Access Points and Controllers*

1100, 1200 Aironet Wireless LAN Access Point	12.2(4)JA
1100, 1200 Aironet Wireless LAN Access Point (EAP-FAST support)	12.2(15)JA
851, 857, 871, 876, 877, 878 Routers	12.3(8)YI
1801, 1802, 1803, 1811, 1812 Routers	12.3(8)YI
HWIC-AP Wireless LAN card for 1841, 2800, 3800 Routers	12.4(2)T
Cisco Catalyst 6500 Series Wireless LAN Services Module	1.1
2000, 4100, 4400 Wireless LAN Controller	2.2.127.9



Note

[Table 1-3](#) provides a reference for the minimum supported software required to enable identity-based networking; it is recommended that the user refer to the Software Center on Cisco Connection Online for current information regarding newer and deferred software releases.

Cisco Secure Access Control Server

Table 1-4 *Cisco Secure Access Control Server*

Release 3.0	IEEE 802.1X support with EAP-MD5 & EAP-TLS
Release 3.1	IEEE 802.1X support with PEAP (EAP-GTC) for wireless clients
Release 3.2	IEEE 802.1X support with PEAP (EAP-MSCHAPv2) for Microsoft Windows clients; IEEE 802.1X machine authentication support for EAP-TLS and PEAP with MS-CHAPv2
Release 3.2.3	IEEE 802.1X support with EAP-FAST (this includes machine authentication support)



Note

[Table 1-4](#) provides a reference for the minimum supported software required to enable identity-based networking; it is recommended that the user refer to the Software Center on Cisco Connection Online for current information regarding newer and deferred software releases.



Authenticators

As previously defined in [Key Components of IEEE 802.1X, page 1-3](#), the authenticator controls the physical access to the network based on the authentication status of the client. The authenticator acts as an intermediary between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The authenticator communicates with the client via EAPOL and with the authentication server via RADIUS.

This chapter is dedicated to the authenticator because the basic configuration of the Cisco Catalyst switch or Cisco Aironet wireless LAN access point remains constant within any IEEE 802.1X deployment regardless of the EAP method chosen for authentication. The EAP method is agreed upon by the client and authentication server and the authenticator simply proxies the information between the two of them.



Note

Wireless LAN controllers are not covered in this document.

Cisco IOS

Cisco Catalyst switches running Cisco IOS require certain commands to enable IEEE 802.1X. Additional commands can be configured to enable optional functionality or change default parameters. The necessary global and interface commands are explained in the following sections. A basic example is also provided to highlight the minimum configuration requirements.

RADIUS Configuration for Cisco IOS

The RADIUS commands required to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco IOS are provided in this section.

Table 2-1 RADIUS Configuration Commands for Cisco IOS

aaa new-model	Enable AAA.
aaa authentication dot1x [<list name> default] group radius	Create an IEEE 802.1X authentication method list. A named method list can be defined or the key word “default” can be used and applied to all ports. Though other methods appear as configuration options, only “group radius” is supported.
radius-server host [host name IP address] auth-port [port] acct-port [port]	Specify the IP address of the RADIUS server. Additionally, the authentication and accounting port numbers can be changed from the default values of 1645 and 1646.
radius-server key [string]	Specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.

Global IEEE 802.1X Configuration for Cisco IOS

The global configuration commands required to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco IOS are provided in this section.

Table 2-2 Global IEEE 802.1X Configuration Commands for Cisco IOS

dot1x system-auth-control	Enable IEEE 802.1X authentication globally on the switch.
----------------------------------	---

Interface IEEE 802.1X Configuration for Cisco IOS

The interface configuration commands required to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco IOS are provided in this section.

Table 2-3 Interface IEEE 802.1X Configuration Commands for Cisco IOS

switchport mode access / no switchport	IEEE 802.1X can only be configured on static Layer 2 access ports, voice VLAN ports, and Layer 3 routed ports; IEEE 802.1X is not supported on dynamic access ports, trunk ports, or EtherChannel.
dot1x port-control [force-authorized force-unauthorized auto]	Enable IEEE 802.1X authentication on the port. The default is force-authorized.

Verify IEEE 802.1X Operation for Cisco IOS

The **show** commands used to verify the operation of IEEE 802.1X on a Cisco Catalyst switch running Cisco IOS are provided in this section.

Table 2-4 IEEE 802.1X Show Commands for Cisco IOS

show dot1x	Display the operational status of IEEE 802.1X.
show dot1x [all interface]	Display the IEEE 802.1X status for all ports or a specific port.
show dot1x statistics interface [interface]	Display IEEE 802.1X statistics for a specific port.
show aaa servers	Display the status and operational information for all configured AAA servers.

Basic Configuration Example for Cisco IOS

A basic configuration example is provided to highlight the minimum command set required to enable IEEE 802.1X on a Cisco Catalyst switch running Cisco IOS.

```
aaa new-model
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
interface Gigabit 3/0/1
    switchport mode access
    dot1x port-control auto
!
radius-server host 10.1.1.5 auth-port 1812 acct-port 1813 key cisco
```



Note

It is important that the user understand the ramifications of adding the AAA commands to the Cisco IOS configuration because they affect device access as well. For example, by adding the AAA commands listed in the sample configuration above, Telnet access is restricted as well unless the appropriate accounts are added to the backend servers or local accounts are added to the device.

show dot1x interface Example for Cisco IOS

The output of this command shows that the supplicant with the MAC address 0006.5b88.06b1 has successfully passed IEEE 802.1X authentication. The output also shows the IEEE 802.1X parameters configured for the interface.

```
Switch#show dot1x interface Gigabit 3/0/3
Supplicant MAC 0006.5b88.06b1
AuthSM State= AUTHENTICATED
BendSM State= IDLE
Posture = N/A
PortStatus= AUTHORIZED
MaxReq = 2
MaxAuthReq= 2
HostMode           = Single
PortContro= Auto
ControlDirection= Both
QuietPeriod= 60 Seconds
Re-authentication = Disabled
ReAuthPeriod= 3600 Seconds
ServerTimeout= 30 Seconds
SuppTimeout= 30 Seconds
TxPeriod= 30 Seconds
```

Guest-Vlan= 0

Cisco Catalyst OS

Cisco Catalyst switches running Cisco Catalyst OS require certain commands to enable IEEE 802.1X. Additional commands can be configured to enable optional functionality or change default parameters. The RADIUS, global, and port commands are explained in the following sections. A basic example is also provided to highlight the minimum configuration requirement.

RADIUS Configuration for Cisco Catalyst OS

The RADIUS commands required to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco Catalyst OS are provided in this section.

Table 2-5 *RADIUS Configuration Commands for Cisco Catalyst OS*

set radius server [IP address] auth-port [port] acct-port [port] [primary]	Specify the IP address of the radius server. Additionally, the authentication and accounting ports can be changed from the default values of 1812 and 1813. The primary parameter can be configured to ensure that this specific RADIUS server is contacted first.
set radius key [key]	Specify the key used to authenticate all transactions between the RADIUS client and server.

Global IEEE 802.1X Configuration for Cisco Catalyst OS

The global configuration commands required to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco Catalyst OS are provided in this section.

Table 2-6 *Global IEEE 802.1X Configuration Commands for Cisco Catalyst OS*

set dot1x system-auth-control [enable disable]	Disable/Enable dot1x on the system.
---	-------------------------------------

Port IEEE 802.1X Configuration for Cisco Catalyst OS

The port configuration commands required to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco Catalyst OS.

Table 2-7 *Port IEEE 802.1X Configuration Commands for Cisco Catalyst OS*

set port dot1x [module/port] port-control [force-authorized force-unauthorized auto]	Specifies the port control type. The default is force-authorized.
--	---

Verify IEEE 802.1X Operation for Cisco Catalyst OS

The **show** commands used to verify the operation of IEEE 802.1X on a Cisco Catalyst switch running Cisco Catalyst OS are provided in this section.

Table 2-8 IEEE 802.1X Show Commands for Cisco Catalyst OS

show radius	Displays configured RADIUS parameters.
show dot1x	Displays system IEEE 802.1X capabilities.
show dot1x group [all authenticated group name]	Displays IEEE 802.1X user group information.
show dot1x user [all user name]	Displays IEEE 802.1X user information.
show dot1x vlan [all VLAN ID]	Displays information about IEEE 802.1X authenticated users in a VLAN.
show dot1x vlan-group [all VLAN-group-name]	Displays IEEE 802.1X VLAN group information.
show port dot1x [module/port]	Displays all the configurable and current state values associated with the authenticator port access entity (PAE) and backend authenticator and statistics for the different types of Extensible Authentication Protocol (EAP) packets transmitted and received by the authenticator on a specific port.
show port dot1x statistics [module/port]	Displays statistics for different EAP packets transmitted and received by the authenticator on a specific port.
show port dot1x [module/port] guest-vlan [VLAN ID none]	Displays the active VLAN that functions as an IEEE 802.1X guest VLAN.
show port dot1x auth-fail-vlan [VLAN ID none]	Displays information about ports that have VLANs for users that have failed IEEE 802.1X authentication.

Basic Configuration Example for Cisco Catalyst OS

A basic configuration example is provided to highlight the minimum command set required to enable IEEE 802.1X on a Cisco Catalyst switch running Cisco Catalyst OS.

```
set radius server 10.1.1.5 auth-port 1812 primary
set radius key cisco
!
set dot1x system-auth-control enable
!
set port dot1x 6/15 port-control auto
```

show port dot1x [mod/port] Example for Cisco Catalyst OS

The output of this command shows that the supplicant connected to port 6/15 has successfully passed IEEE 802.1X authentication. The output also shows the IEEE 802.1X parameters configured for the port.

```
Switch> (enable) show port dot1x 6/15
```

Port	Auth-State	BEnd-State	Port-Control	Port-Status	
6/15	authenticated	idle	auto	authorized	
Port	Port-Mode	Re-authentication	Shutdown-timeout	Control-Mode	
				admin	oper
6/15	SingleAuth	disabled	disabled	Both	Both
Port	Posture-Token	Critical	Termination	action	Session-timeout
6/15	-	NO	NoReAuth	-	

Cisco Aironet Wireless LAN Access Points Running Cisco IOS

Cisco Aironet wireless LAN access points (AP) running Cisco IOS require certain commands to enable IEEE 802.1X. Additional commands can be configured to enable optional functionality or change default parameters. The RADIUS, global, and interface commands are explained in the following sections. A basic example is also provided to highlight the minimum configuration requirement.

RADIUS Configuration for Cisco Aironet Wireless LAN APs Running Cisco IOS

The RADIUS commands required to configure IEEE 802.1X on an Cisco Aironet wireless LAN access point running Cisco IOS are provided in this section.

Table 2-9 *RADIUS Configuration Commands for Cisco Aironet Wireless LAN APs Running Cisco IOS*

aaa new-model	Enable AAA.
aaa authentication login [<list name> default] group radius	Create an authentication method list. A named method list can be defined or the key word “default” can be used and applied to all ports.
radius-server host [host name IP address] auth-port [port] acct-port [port]	Specify the IP address of the RADIUS server. Additionally, the authentication and accounting port numbers can be changed from the default values of 1645 and 1646.
radius-server key [string]	Specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.

Global Configuration for Cisco Aironet Wireless LAN APs Running Cisco IOS

The global configuration commands required to configure IEEE 802.1X on an Cisco Aironet wireless LAN access point running Cisco IOS are provided in this section.

Table 2-10 Global IEEE 802.1X Configuration Commands for Cisco Aironet Wireless LAN APs Running Cisco IOS

dot11 ssid [ssid-string]	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.
authentication open eap [list name]	Set the authentication type to open for this SSID. Open authentication allows any device to authenticate and then attempt to communicate with the access point.
authentication network-eap [list name]	Configure the radio interface (for the specified SSID) to support network-EAP authentication. Network-EAP authentication requires that the IEEE 802.1X client authenticate before it can access the network. Adding EAP to open authentication enables IEEE 802.1X authentication in addition to 802.11 open authentication.

Interface Configuration for Cisco Aironet Wireless LAN APs Running Cisco IOS

The port configuration commands required to configure IEEE 802.1X on an Cisco Aironet wireless LAN access point running Cisco IOS.

Table 2-11 Interface Configuration Commands for Cisco Aironet Wireless LAN APs Running Cisco IOS

ssid [ssid string]	Assign a globally configured SSID to a radio interface.
---------------------------	---

Verify IEEE 802.1X Operation for Cisco Aironet Wireless LAN APs Running Cisco IOS

The **show** commands used to verify the operation of IEEE 802.1X on an Cisco Aironet wireless LAN access point running Cisco IOS are provided in this section.

Table 2-12 IEEE 802.1X Show Commands for Cisco Aironet Wireless LAN APs Running Cisco IOS

show dot11 associations	Display the radio association table, radio association statistics, or to selectively display association information about all repeaters, all clients, a specific client, or basic service clients.
show aaa servers	Display the status and operational information for all configured AAA servers.

Basic Configuration Example for Cisco Aironet Wireless LAN APs Running Cisco IOS

A basic configuration example is provided to highlight the minimum command set required to enable IEEE 802.1X on an Cisco Aironet wireless LAN access point running Cisco IOS.

```
aaa new-model
```

```

!
aaa authentication login eap_methods group radius
!
dot11 ssid cisco
    authentication open eap eap_methods
    authentication network-eap eap_methods
!
interface Dot11Radio0
ssid cisco
!
ip radius source-interface BV11
!
radius-server host 10.1.1.5 auth-port 1812 acct-port 1813
radius-server key cisco

```

**Note**

A named authentication list is created with the command **aaa authentication login** in the Cisco Aironet wireless LAN access point configuration—instead of using the default: named list option which was used for the Cisco IOS and Cisco Catalyst OS examples in previous sections—because the **authentication** [open | network-eap] commands used in the SSID configuration mode require a list name.

show dot11 associations Example for Cisco Aironet Wireless LAN APs Running Cisco IOS

The output of this command shows that the supplicant with MAC address 0002.8ade.5af5 has successfully passed IEEE 802.1X authentication via EAP.

ap#**show dot11 associations**

```

802.11 Client Stations on Dot11Radio0:
SSID [cisco] :

```

MAC Address	IP address	Device Name	Parent State
0002.8ade.5af5	12.1.1.52	350-client	sdelairselfEAP-Assoc



Deploying EAP—MD5

This chapter describes how to deploy IEEE 802.1X port-based access control using EAP-MD5 between the supplicant and authentication server. The Meetinghouse AEGIS client, version 2.3.3.0, is used as the supplicant for this scenario. Cisco Secure ACS 4.0 is used as the authentication server. A Cisco Catalyst switch functions as the authenticator and provides wired LAN connectivity between the supplicant and authentication server.

Authentication Server Configuration

The steps provided in this section explain how to configure Cisco Secure ACS 4.0 for EAP-MD5 authentication.



Note

This section explains only those details necessary to configure EAP-MD5 authentication; refer to the Cisco Secure ACS Configuration Guides for information regarding other features and functionality.

Create a User in the ACS Database

Click **User Setup** in main menu. Enter the user name in the User box and click the **Add/Edit** button.



Note

EAP-MD5 is on the only EAP authentication method that cannot leverage an external user database such as Windows Active Directory; the internal ACS database is required for EAP-MD5.

Figure 3-1 Create a User in the ACS Database

CISCO SYSTEMS

User Setup

Select

User:

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Configure the User in the ACS Database

In the User Setup section, ensure that the CiscoSecure Database is chosen for Password Authentication. Enter the user password. Repeat a second time to confirm the password. Click **Submit**.



Note

You enter a password for use with MD5 as an EAP-type.

Figure 3-2 Configure the User in the ACS Database

CISCO SYSTEMS

User Setup

User: user1a

☐ Account Disabled

Supplementary User Info

Real Name: user1a

Description:

User Setup

Password Authentication:

CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

Submit Delete Cancel

Configure a AAA Server

Click **Network Configuration** on the main menu. Under the AAA Server table, click **Add Entry**. On the Add AAA Server screen, enter the AAA Server Name, AAA Server IP Address, and Key. For AAA Server Type, select CiscoSecure ACS. For Traffic Type, leave the default setting of inbound/outbound. Click **Submit + Apply**.



Note

By default, a AAA Server entry containing the host name and IP address of the local machine running ACS already exists in the AAA Server table.

Figure 3-3 Configure a AAA Server

CISCO SYSTEMS

Network Configuration

Edit

Add AAA Server

AAA Server Name: TSE-MSEExchange

AAA Server IP Address: 10.1.1.5

Key: cisco

☐ Log Update/Watchdog Packets from this remote AAA Server

AAA Server Type: CiscoSecure ACS

Traffic Type: inbound/outbound

Submit Submit + Apply Cancel

Back to Help

Configure a AAA Client

From the Network Configuration screen, click **Add Entry** under the AAA Clients table to add an authenticator. On the Add AAA Client screen, enter the AAA Client Host Name, AAA Client IP Address, and Key. For the Authenticate Using option, select RADIUS (Cisco IOS/PIX 6.0).



Note

The RADIUS (Cisco IOS/PIX 6.0) option enables the use of Cisco IOS RADIUS Vendor-Specific Attributes (VSAs). Other security control protocol options are available for RADIUS and TACACS+.

Click **Submit + Apply**.



Note

The Key must match the key configured on the IOS or Catalyst OS authenticator.

Figure 3-4 Configure a AAA Client

CISCO SYSTEMS

Network Configuration

Add AAA Client

AAA Client Hostname: TSE-C3750

AAA Client IP Address: 12.1.1.99

Key: cisco

Authenticate Using: RADIUS (Cisco IOS/PIX 6.0)

- ☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- ☐ Log Update/Watchdog Packets from this AAA Client
- ☐ Log RADIUS Tunneling Packets from this AAA Client
- ☐ Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Apply Cancel

Summary of Network Configuration

After the AAA Server and AAA Client have been configured, the Network Configuration menu is displayed with the updated list of entries.

Figure 3-5 Summary of Network Configuration

CISCO SYSTEMS

Network Configuration

Select

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
TSE-C3750	12.1.1.99	RADIUS (Cisco IOS/PIX 6.0)

Add Entry Search

AAA Servers		
AAA Server Name	AAA Server IP Address	AAA Server Type
TSE-MSEExchange	10.1.1.5	CiscoSecure ACS

Add Entry Search

Global Authentication Setup for EAP-MD5

Click **System Configuration** on the main menu. From the System Configuration menu, select Global Authentication Setup to configure the EAP method. Check the Allow EAP-MD5 box in the EAP-MD5 section. Click **Submit + Restart**.



Note

EAP-MD5 is enabled by default when CiscoSecure ACS is installed.

Figure 3-6 Global Authentication Setup for EAP-MD5

The screenshot shows the Cisco Systems System Configuration web interface. On the left is a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'System Configuration' and contains the following sections:

- Select one or more of the following options:**
 - ☐ Certificate SAN comparison
 - ☐ Certificate CN comparison
 - ☐ Certificate Binary comparison
- EAP-TLS session timeout (minutes):** 120
- LEAP**
 - ☐ Allow LEAP (For Aironet only)
- EAP-MD5**
 - ☒ Allow EAP-MD5
- AP EAP request timeout (seconds):** 20
- MS-CHAP Configuration**
 - ☐ Allow MS-CHAP Version 1 Authentication
 - ☐ Allow MS-CHAP Version 2 Authentication

At the bottom of the main content area is a yellow button labeled 'Back to Help'. At the very bottom are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'.

Client Configuration

The steps provided in this section explain how to configure the Meetinghouse AEGIS client, version 2.3.3.0, for EAP-MD5 authentication.

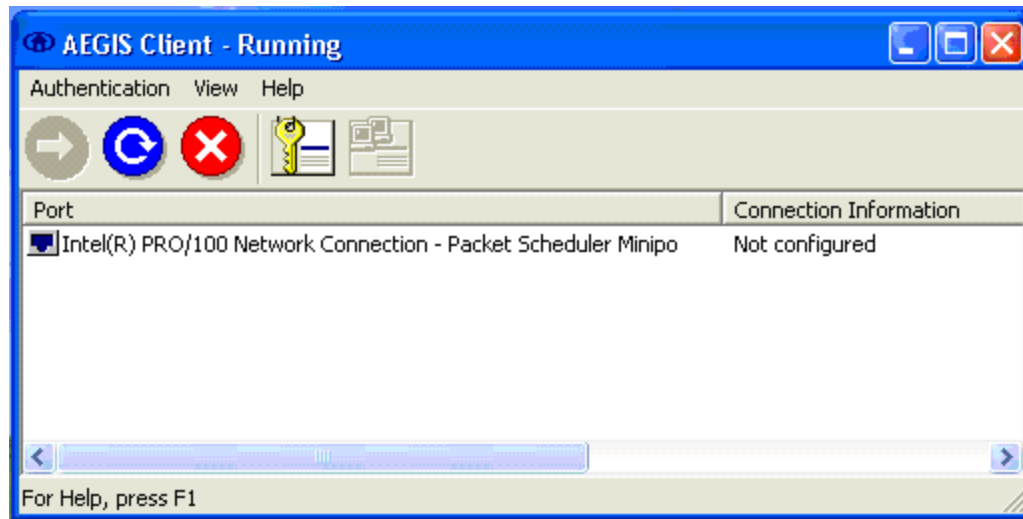


Note

The Meetinghouse AEGIS client is running on the Windows XP operating system with Service Pack 2.

Open the Meetinghouse AEGIS client

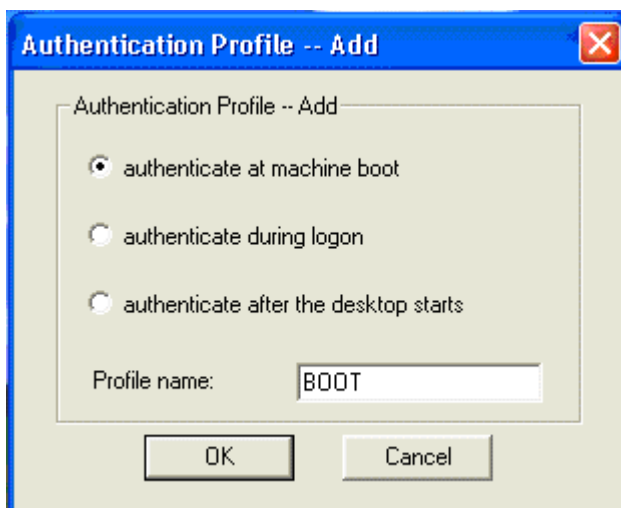
Open the Meetinghouse AEGIS client, click the **Authentication** menu, and select Authentication Profile.

Figure 3-7 Meetinghouse AEGIS Client

Create the Machine Authentication Profile

On the Authentication Profile menu, select the authenticate at machine boot option and enter a Profile name. For this scenario, the profile name is BOOT. This profile uses the machine credentials for authentication instead of user credentials. The use of machine authentication can reduce the total time required to logon to the backend directory system because it enables the machine processes to initialize prior to the user logon.

Click **OK**.

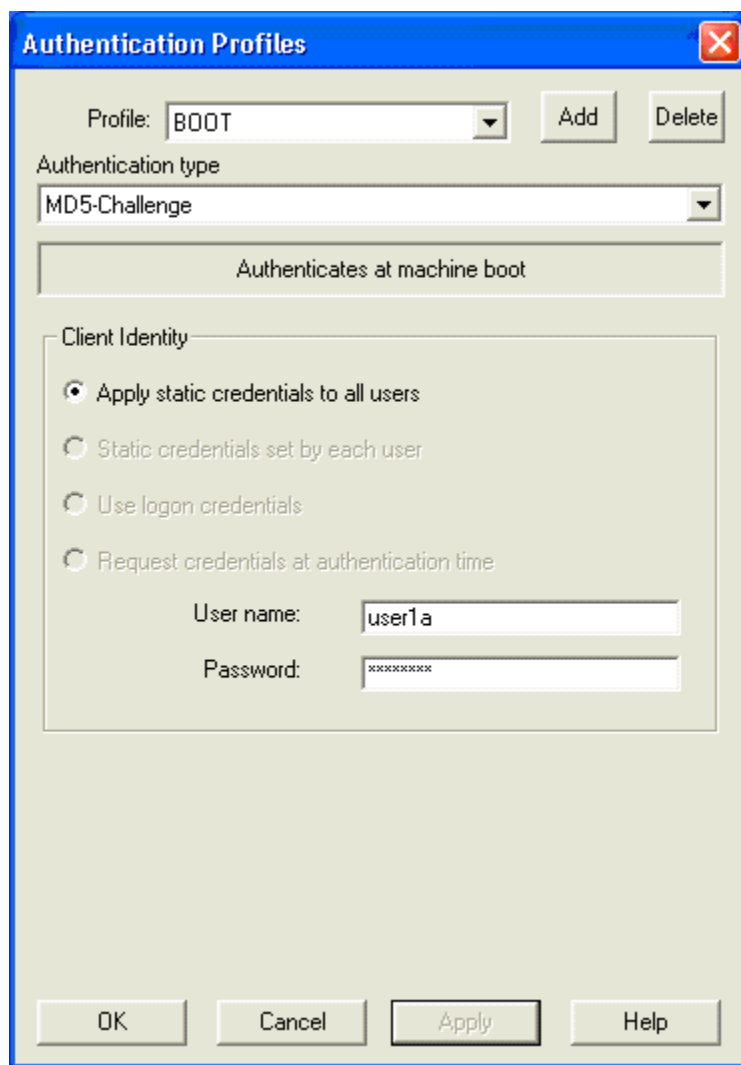
Figure 3-8 Create a Machine Authentication Profile

Configure the Machine Authentication Profile

Select the MD5-Challenge option for Authentication type and set the Client Identity method. For this scenario, the Apply static credentials to all users option is used. This enables an administrator to set static credentials for the machine regardless of the user. Since machine authentication occurs at boot time, there is no way to glean the Windows credentials for authentication. There are other options, such as Static credentials set by each user and Request credentials at authentication time, however these all require individual user intervention.

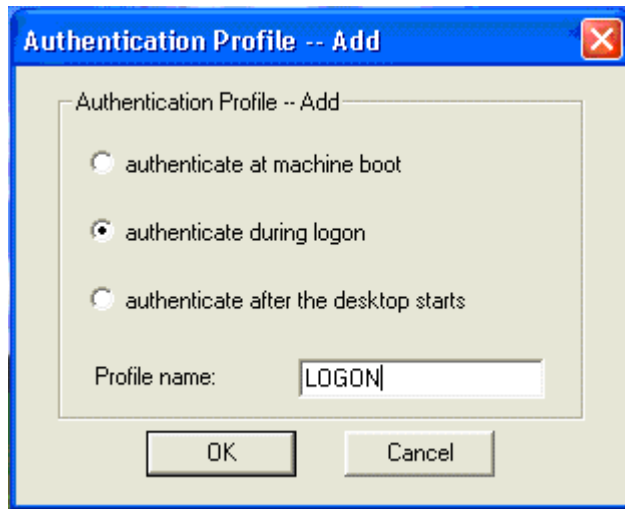
Click **OK**.

Figure 3-9 *Configure the Machine Authentication Profile*



Create the User Authentication Profile

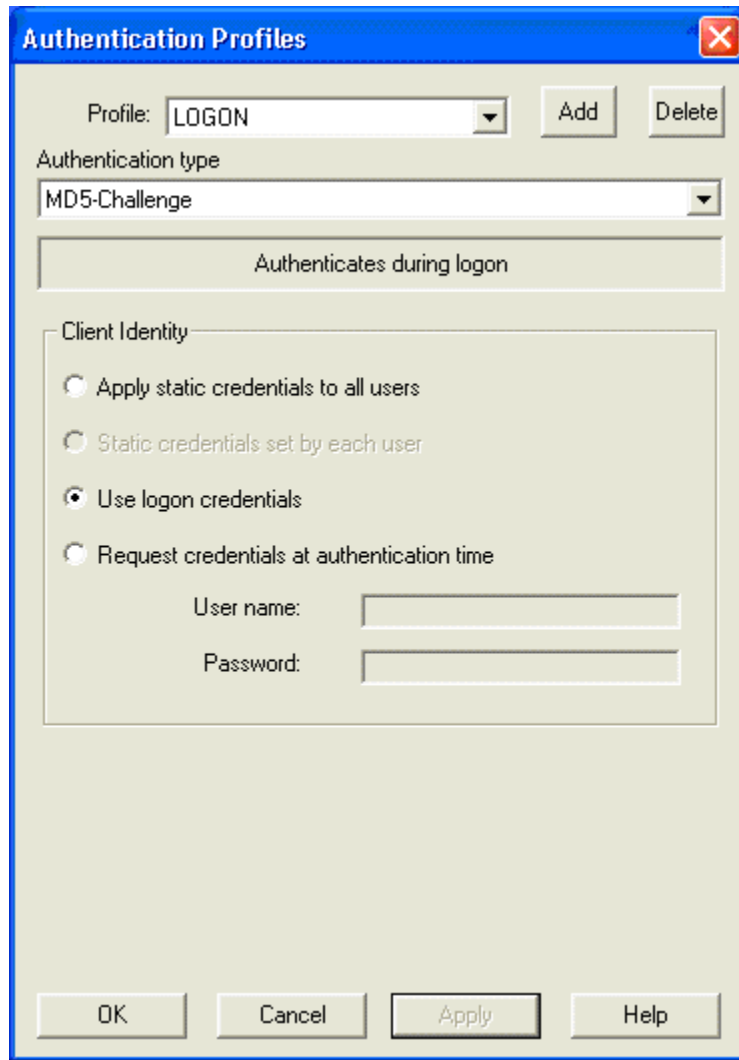
On the Authentication Profile menu, select the authenticate during logon option. For this scenario, the profile name is LOGON. Click **OK**.

Figure 3-10 Create the User Authentication Profile

Configure the User Authentication Profile

Select the MD5-Challenge option for Authentication type and set the Client Identity method. For this scenario, the Use logon credentials option is chosen which means the Windows username and password is used for EAP-MD5 authentication. There are other options, but the Use logon credentials option provides a Single Sign-On (SSO) method. The Apply static credentials to all users may not provide a way to identify specific users when they access the network. The Request credentials at authentication time is similar to the Use logon credentials option, but creates a second step for the user.

Click **OK**.

Figure 3-11 *Configure the User Authentication Profile*

Authentication Profiles

Profile: LOGON Add Delete

Authentication type
MD5-Challenge

Authenticates during logon ☒

Client Identity

☐ Apply static credentials to all users

☐ Static credentials set by each user

☒ Use logon credentials

☐ Request credentials at authentication time

User name:

Password:

OK Cancel Apply Help

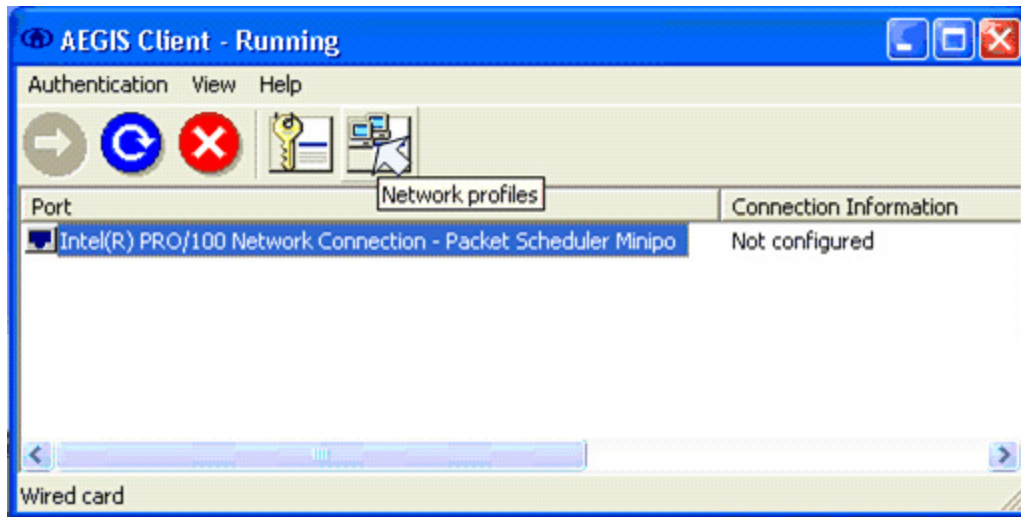
Create a Network Profile

The final step is to create a Network Profile that references the configured authentication profiles. To do this, select the correct network adapter from the list provided and then click the **Network Profiles** icon.

**Note**

The Meetinghouse AEGIS client binds to any network adapter that it finds, therefore it is important to apply the Network Profile to the correct adapter.

Figure 3-12 Create a Network Profile



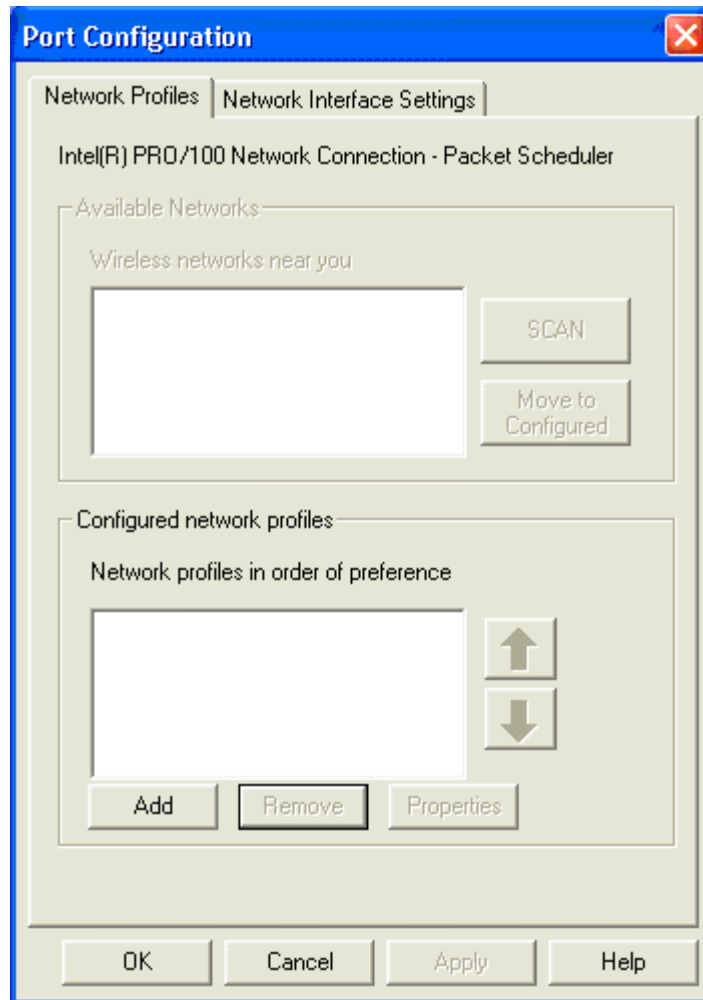
Configure the Port Settings

Click **Add** to create the network profile for the selected network adapter.



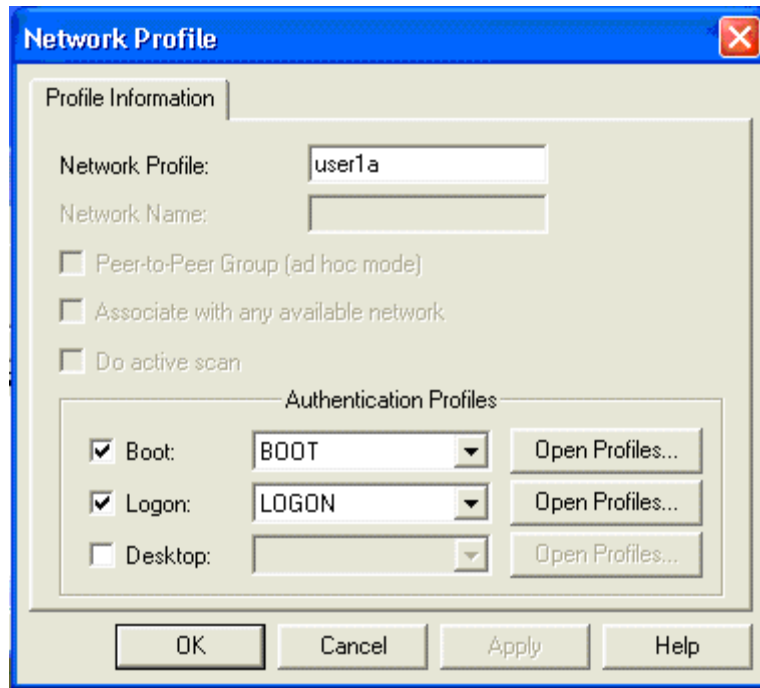
Note

The Network Interface Settings tab is used to configure protocol settings, such as the authentication timeout, as well as interface and DHCP options. For this scenario, the default parameters were used.

Figure 3-13 *Configure the Port Settings*

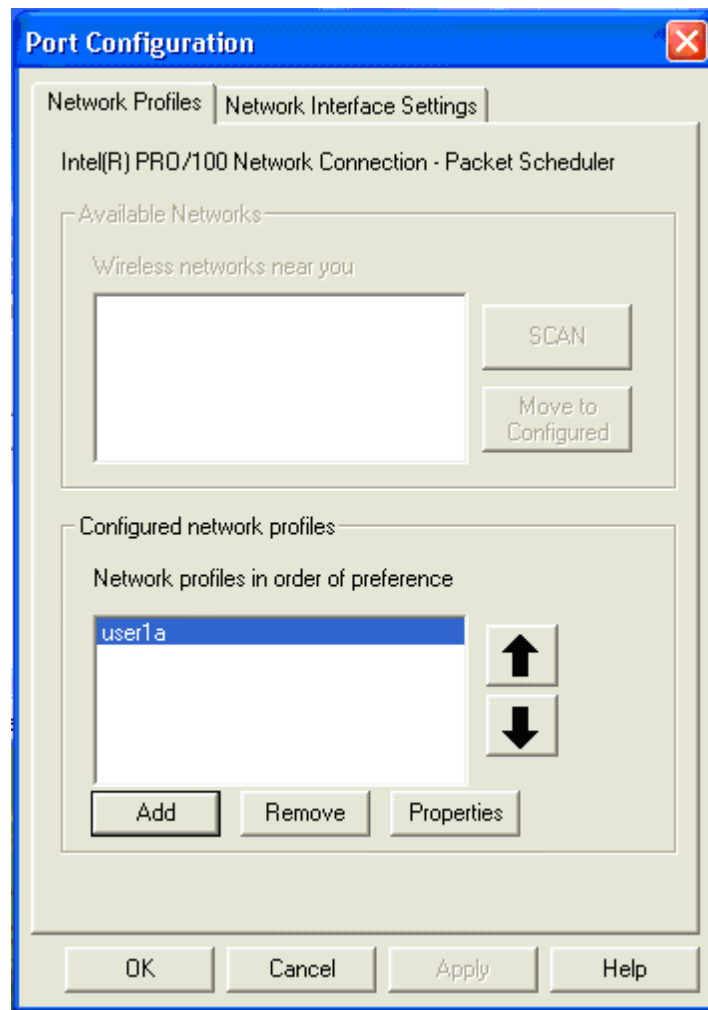
Configure the Network Profile

Enter a name for the network profile. Click the check box for the Boot Authentication Profile, and then select the BOOT profile from the drop-down menu. Repeat this step for the Logon Authentication Profile, this time choosing the LOGON profile from the drop-down menu. Click **OK**.

Figure 3-14 *Configure the Network Profile*

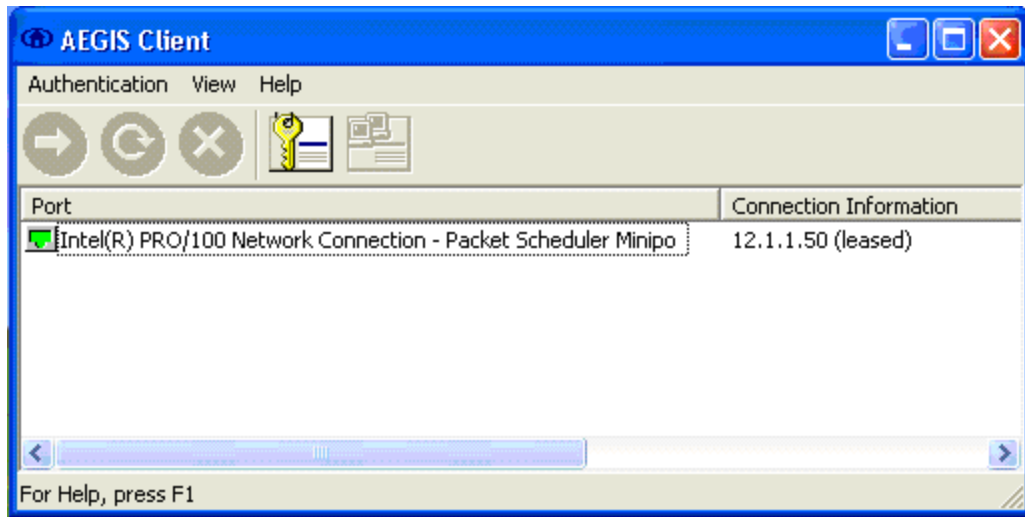
Apply the Network Profile

The Network Profile that was configured in the previous step is now present in the Configured Network Profiles box. Click **OK** to apply the profile to the network adapter.

Figure 3-15 *Apply the Network Profile*

Verify Client Authentication

After the Network Profile is applied to the network adapter, IEEE 802.1X is successfully configured for machine and user authentication. Once authenticated, the client receives an IP address via DHCP and gains network access.

Figure 3-16 *Verify Client Authentication*



Deploying EAP—TLS

This chapter describes how to deploy IEEE 802.1X port-based access control using EAP-TLS between the supplicant and authentication server. The Funk Oddyssey client, version 4.02.0.2000, is used as the supplicant for this scenario. Cisco Secure ACS 4.0 is used as the authentication server. A Cisco Catalyst switch functions as the authenticator and provides wired LAN connectivity between the supplicant and authentication server.

Authentication Server Configuration

The steps provided in this section explain how to configure Cisco Secure ACS 4.0 for EAP-TLS authentication.



Note

This section explains only those details necessary to configure EAP-TLS authentication; refer to the Cisco Secure ACS Configuration Guides for information regarding other features and functionality.

Create an Unknown User Policy

Click **External User Databases** on the main menu. In the External User Databases menu, select Unknown User Policy.



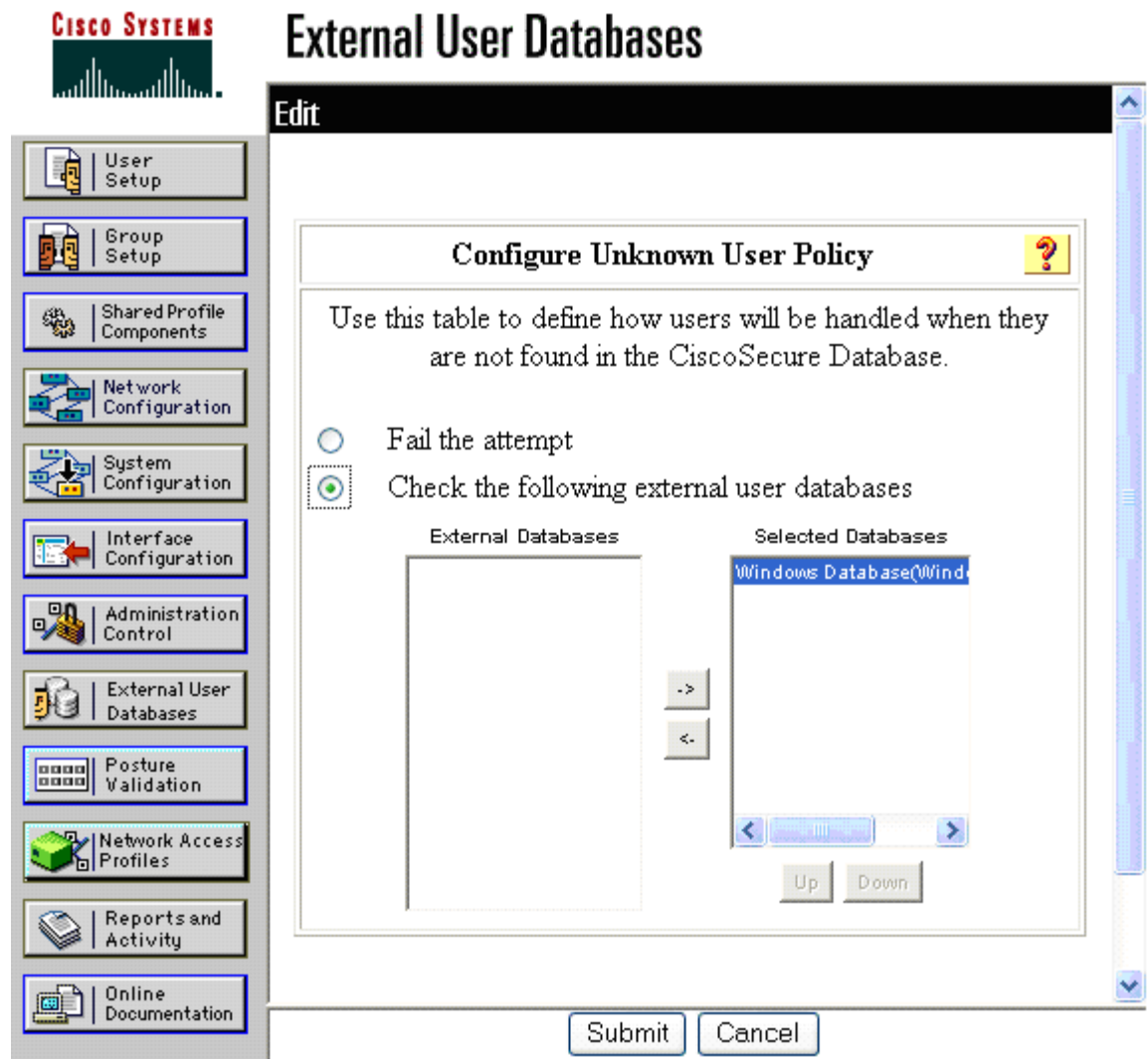
Note

EAP-TLS does not require the use of an external user database such as Windows Active Directory; the internal ACS database could be used with this EAP method.

Figure 4-1 Create an Unknown User Policy

Configure an Unknown User Policy

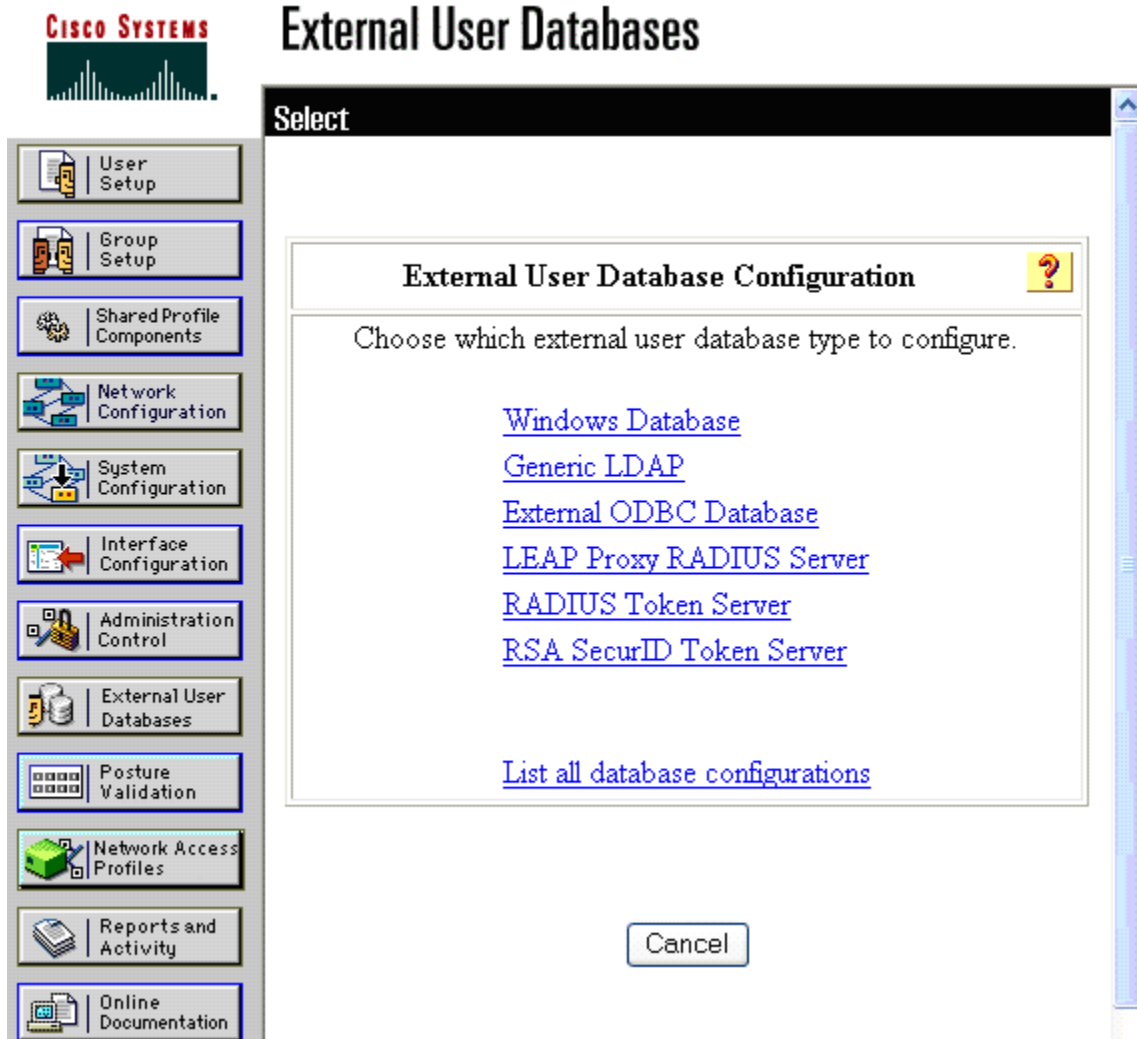
In the Configure Unknown User Policy section, select the Check the following external user databases radio button. Move the Windows Database option from the External Databases column to the Selected Databases column. Click **Submit**.

Figure 4-2 *Configure an Unknown User Policy*

Select an External User Database

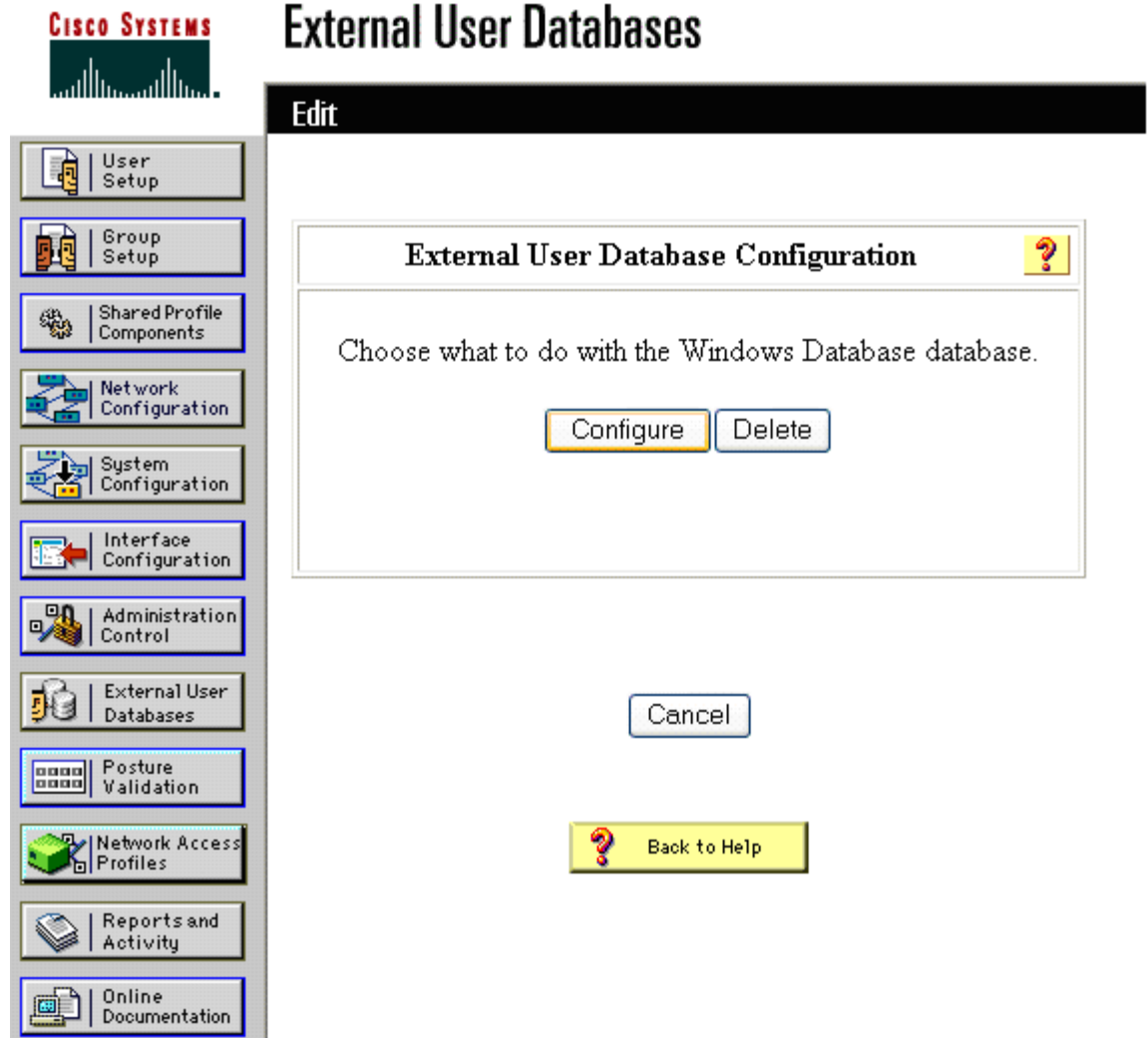
Select the Database Configuration option from the External User Databases menu. In the External User Database Configuration section, select the Windows Database option.

Figure 4-3 Select an External User Database



Choose to Configure the Windows Database

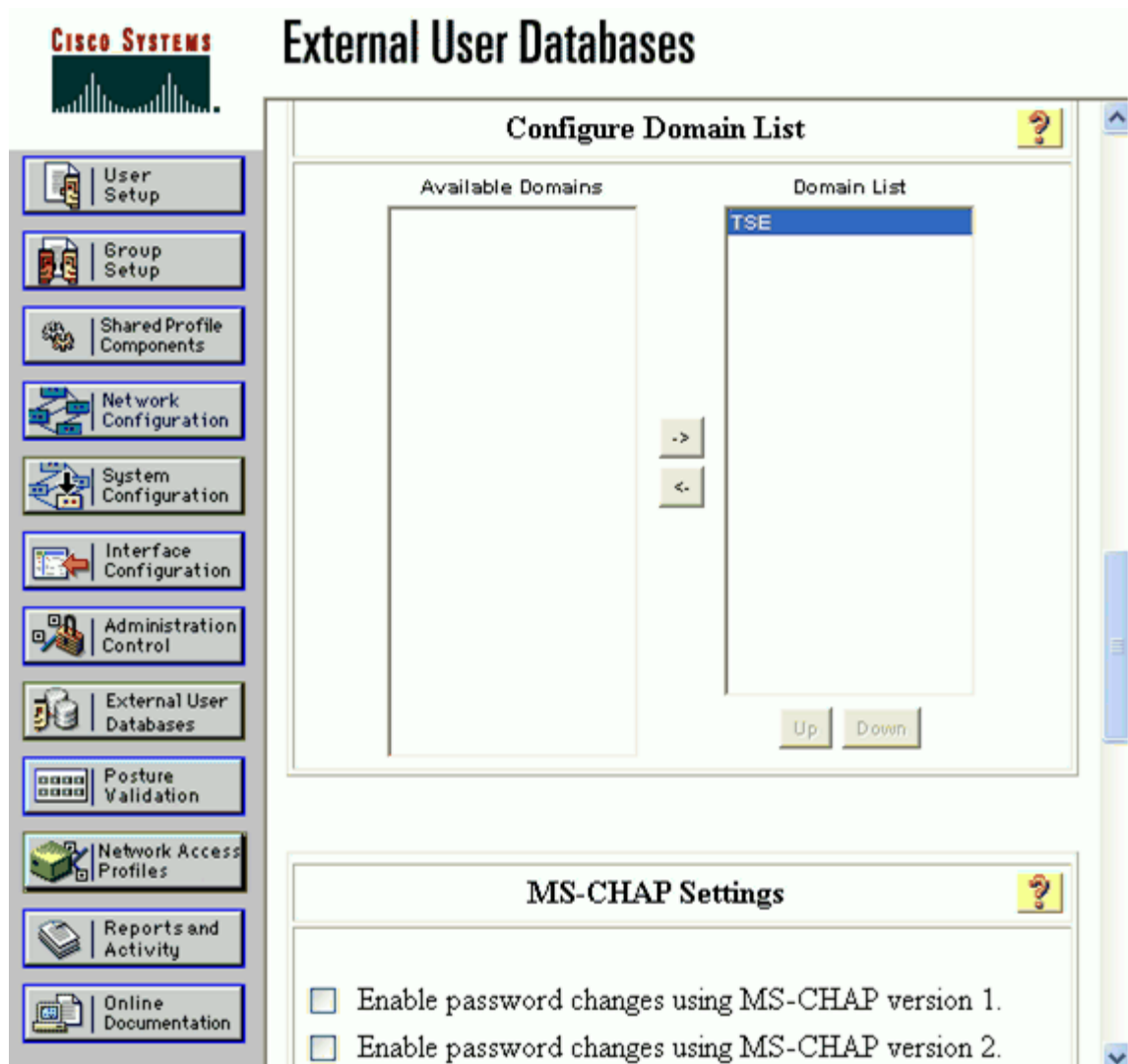
Click the **Configure** button in the External User Database Configuration section.

Figure 4-4 Choose to Configure the Windows Database

Configure the Windows Database

Scroll down to the Configure Domain List section of the Windows User Database Configuration menu. Select and move the correct domain name from the Available Domains column to the Domain List column.

Figure 4-5 Configure the Windows Database



Next, scroll down to the Machine Authentication section and check the Enable EAP-TLS Machine Authentication box. Click **Submit**.



Note

The Enable EAP-TLS machine authentication box is checked to enable machine authentication using machine certificates with EAP-TLS; the option is configured for this scenario because the supplicant is configured, in the next section, to use a machine account profile.

There are several other machine authentication options that can be configured:

- **EAP-TLS Strip Domain Name**—If you want Cisco Secure ACS to remove the domain name from a username derived from the Subject Alternative Name (SAN) field in an end-user certificate, select this checkbox.
- **EAP-TLS and PEAP machine authentication name prefix**—If an administrator wants Cisco Secure ACS to substitute a different string of characters for the string host/ at the beginning of any machine name being authenticated by PEAP (EAP-MSCHAPv2) or EAP-TLS, type the string in this box.

- Enable machine access restrictions—To use machine authentication as a condition for user authorization, select this box. Microsoft PEAP and EAP-TLS users accessing the network with a computer that failed machine authentication are authenticated normally but receive only the authorizations defined by the group mapping list.
- Group map for successful user authentication without machine authentication—When the machine access restrictions feature is enabled, this list specifies the user group whose authorizations are applied to an EAP-TLS or Microsoft PEAP user who passes authentication but uses a computer that failed machine authentication.

Figure 4-6 Enable EAP-TLS Machine Authentication

CISCO SYSTEMS

External User Databases

Windows EAP Settings

☐ Enable password change inside PEAP or EAP-FAST.

☐ EAP-TLS Strip Domain Name.

Machine Authentication.

☐ Enable PEAP machine authentication.

☒ Enable EAP-TLS machine authentication.

EAP-TLS and PEAP machine authentication name prefix:

☐ Enable machine access restrictions.

Aging time (hours):

Group map for successful user authentication without machine authentication:

User Groups that are exempt from passing machine authentication:

Available User Groups	Selected User Groups
Default Group	
Group 1	
Group 2	
Group 3	
Group 4	

Configure a AAA Server

Refer to [Configure a AAA Server, page 3-3](#). The procedure is the same for all EAP methods.

Configure a AAA Client

Refer to [Configure a AAA Client, page 3-4](#). The procedure is the same for all EAP methods.

Verify the Network Configuration

Refer to [Summary of Network Configuration, page 3-5](#). The procedure is the same for all EAP methods.

Global Authentication Setup for EAP-TLS

Click **System Configuration** in the main menu. On the System Configuration menu, select Global Authentication Setup to configure the EAP method. Check the Allow EAP-TLS box and all three of the certificate comparison options in the EAP-TLS section. Click **Submit + Restart**.

**Note**

Refer to [Appendix C, “Installing an X.509v3 PKI Certificate on the CS ACS,”](#) for instructions on how to install a certificate onto the CiscoSecure ACS.

**Note**

The Certificate Comparison options specify how ACS verifies the user identity as presented in the EAP Identity response from the end-user client. The user identity is verified against information in the certificate presented by the end-user client. This comparison occurs after an EAP-TLS tunnel is established between ACS and the end-user client. The Certificate Comparison options include the Subject Alternative Name field of the end-user certificate, the Common Name field of the end-user certificate, and a binary comparison of the end-user certificate to the end-user certificate stored in Active Directory. If more than one option is selected, ACS performs the comparisons in the order listed and stops after the first successful comparison.

Figure 4-7 Global Authentication Setup for EAP-TLS

The screenshot shows the 'System Configuration' window for EAP-TLS. On the left is a navigation pane with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'System Configuration' and contains three sections: EAP-TLS, LEAP, and EAP-MD5. The EAP-TLS section has a checked 'Allow EAP-TLS' checkbox, followed by 'Select one or more of the following options:' with three checked options: 'Certificate SAN comparison', 'Certificate CN comparison', and 'Certificate Binary comparison'. Below these is a text input field for 'EAP-TLS session timeout (minutes):' with the value '120'. The LEAP section has an unchecked 'Allow LEAP (For Aironet only)' checkbox. The EAP-MD5 section has an unchecked 'Allow EAP-MD5' checkbox and a text input field for 'AP EAP request timeout (seconds):' with the value '20'. At the bottom is an 'MS-CHAP Configuration' section with two unchecked options: 'Allow MS-CHAP Version 1 Authentication' and 'Allow MS-CHAP Version 2 Authentication'. At the very bottom are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'.

CISCO SYSTEMS

System Configuration

EAP-TLS

☒ Allow EAP-TLS

Select one or more of the following options:

- ☒ Certificate SAN comparison
- ☒ Certificate CN comparison
- ☒ Certificate Binary comparison

EAP-TLS session timeout (minutes):

LEAP

☐ Allow LEAP (For Aironet only)

EAP-MD5

☐ Allow EAP-MD5

AP EAP request timeout (seconds):

MS-CHAP Configuration

☐ Allow MS-CHAP Version 1 Authentication

☐ Allow MS-CHAP Version 2 Authentication

Client Configuration

The steps provided in this section explain how to configure the Funk Odyssey client, version 4.02.0.2000, for EAP-TLS authentication.

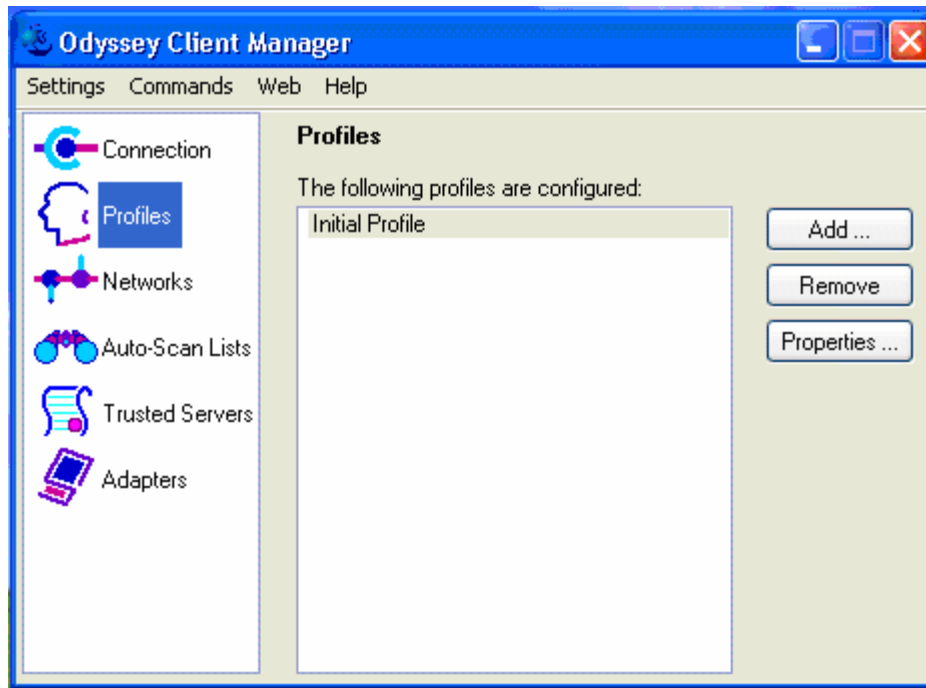


Note

The Funk Odyssey client is running on the Windows XP operating system with Service Pack 2.

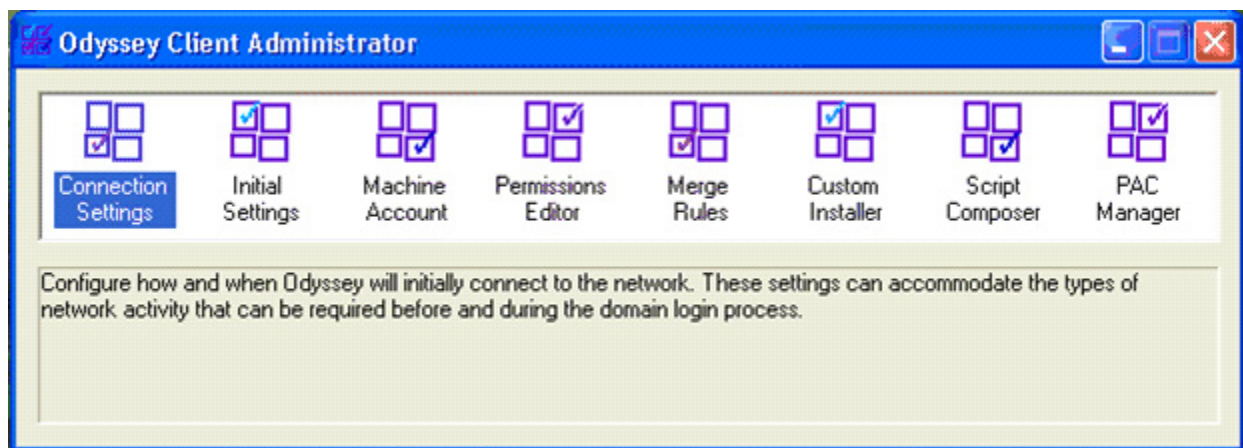
Open the Funk Odyssey Client

Open the Funk Odyssey client, click the **Authentication** menu, and select Authentication Profile.

Figure 4-8 *Funk Odyssey Client*

Configure Machine Account Parameters for Connection Settings

To configure machine authentication, the Machine Account parameters must first be configured for the Connection Settings. On the Odyssey Client Manager menu, select Settings and then Odyssey Client Administrator. On the Odyssey Client Administrator menu, select Connection Settings.

Figure 4-9 *Select Connection Settings from the Odyssey Client Administrator Menu*

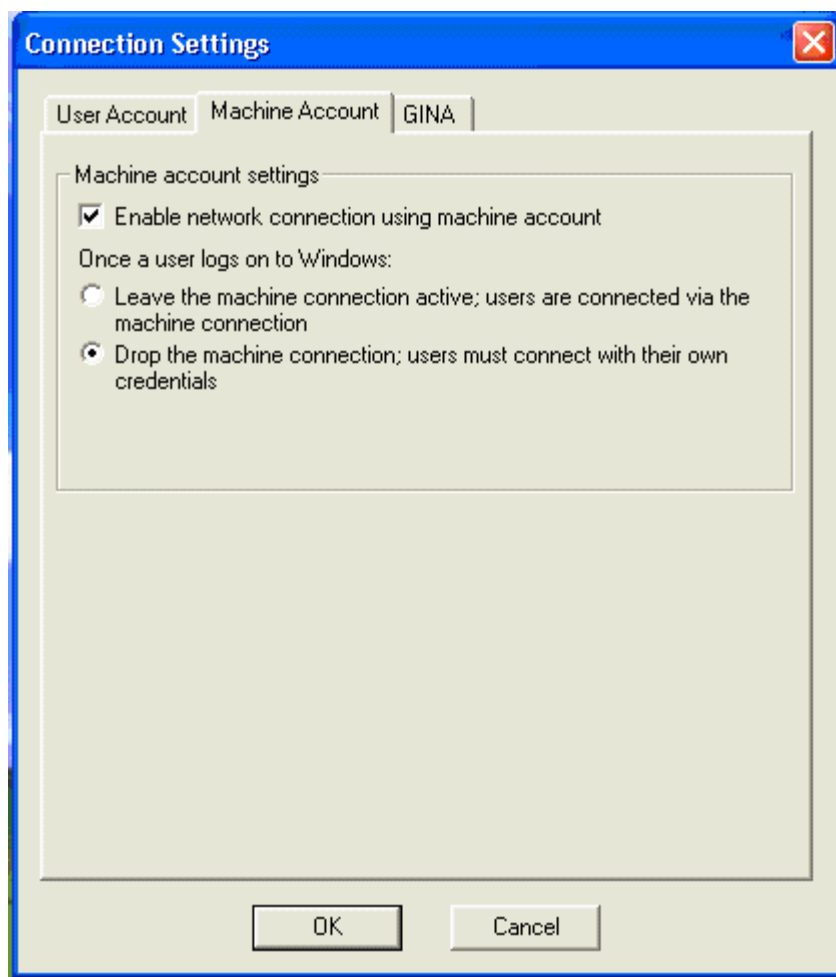
In the Connection Settings window, select the Machine Account tab. In the Machine account settings section, check the Enable network connection using machine account box. Next select the Drop the machine connection; users must connect with their own credentials radio button. Click **OK**.

**Note**

The Drop the machine connection; users must connect with their own credentials option instructs the client to reference the user profile instead of the machine profile when a user logs onto the system, therefore enabling administrators to not only account for individual machines but also individual users.

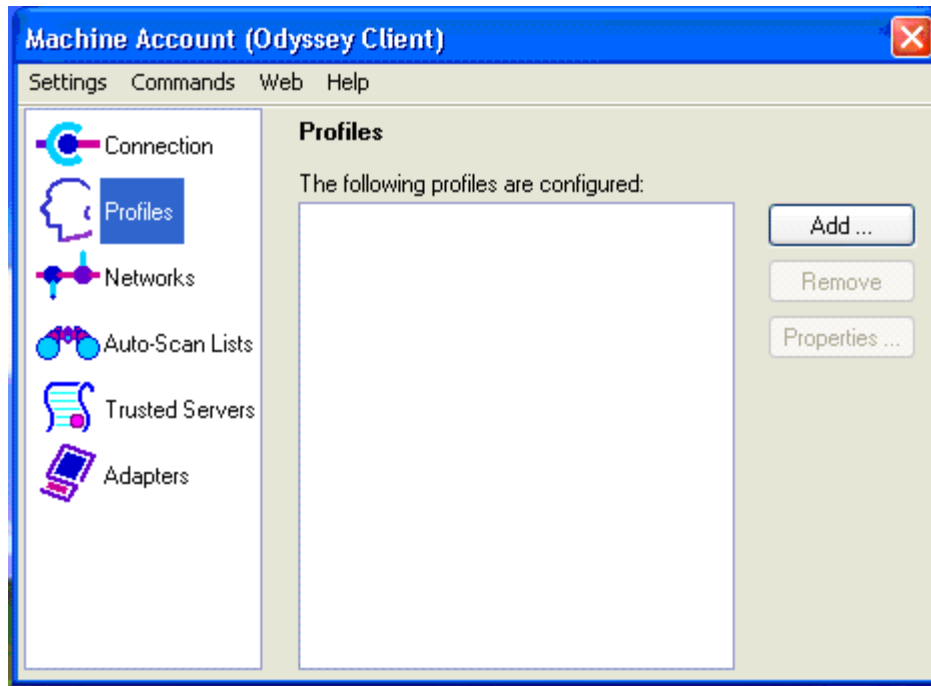
There are two optional tabs, User Account and GINA, which can also be configured for Connection Settings. The User Account tab is used to configure the timing of network authentication that relies on user credentials. The GINA tab is used to configure the Odyssey GINA module which allows users of Windows XP or 2000 to connect to the network using their Windows logon credentials prior to Windows logon (this can be helpful when users have startup processes that require network connections).

Figure 4-10 *Configure the Machine Account Parameters for the Connection Settings*



Create a Machine Profile

On the Odyssey Client Administrator menu, select the Machine Account option. The Machine Account (Odyssey Client) window opens, which looks identical to the Odyssey Client Manager window used to create a user profile. Highlight the Profiles option in the menu and click **Add**.

Figure 4-11 Create a Machine Profile

Configure Authentication Information for the Machine Profile

In the Add Profile screen, enter a name for the profile. For this scenario, the profile is named BOOT. On the User Info tab, check the Use machine credentials box. On the Password tab at the bottom of the User Info tab, leave the default values checked.

Figure 4-12 Configure the Password Information for the Machine Profile

Add Profile

Profile name:

User Info Authentication TTLS Settings PEAP Settings

Login name:

☐ Use machine credentials

Realm (optional): @

Password Certificate SIM Card

☒ Permit login using password

☐ Use Windows password

☐ Prompt for password

☒ Use the following password:

☐ Unmask

OK Cancel

Next click the **Certificate** tab at the bottom of the User Info tab. Check the Permit login using my certificate box. Then click the **Browse** tab to select the correct certificate for the machine.

**Note**

Refer to [Appendix B, “Installing an X.509v3 PKI Certificate on the Client,”](#) for instructions on how to install a certificate onto a client machine.

Figure 4-13 Configure the Certificate Information for the Machine Profile

The screenshot shows the 'Add Profile' dialog box with the 'Certificate' tab selected. The 'Profile name' field contains 'BOOT'. The 'User Info' tab is also visible. The 'Login name' field is empty. The 'Use machine credentials' checkbox is unchecked. The 'Realm (optional)' field contains '@'. The 'Certificate' tab is selected, showing the 'Permit login using my certificate' checkbox checked. The text 'winxp1.tse.com' is entered in the field below. There are 'View ...' and 'Browse ...' buttons. At the bottom are 'OK' and 'Cancel' buttons.

Configure the Authentication Method for the Machine Profile

On the Authentication tab, click **Add** next to the Authentication Protocols box. Select EAP-TLS and click **OK**. Next, highlight EAP-TTLS (which is listed as an authentication protocol by default) and click **Remove**. Check the Validate server certificate box.



Note

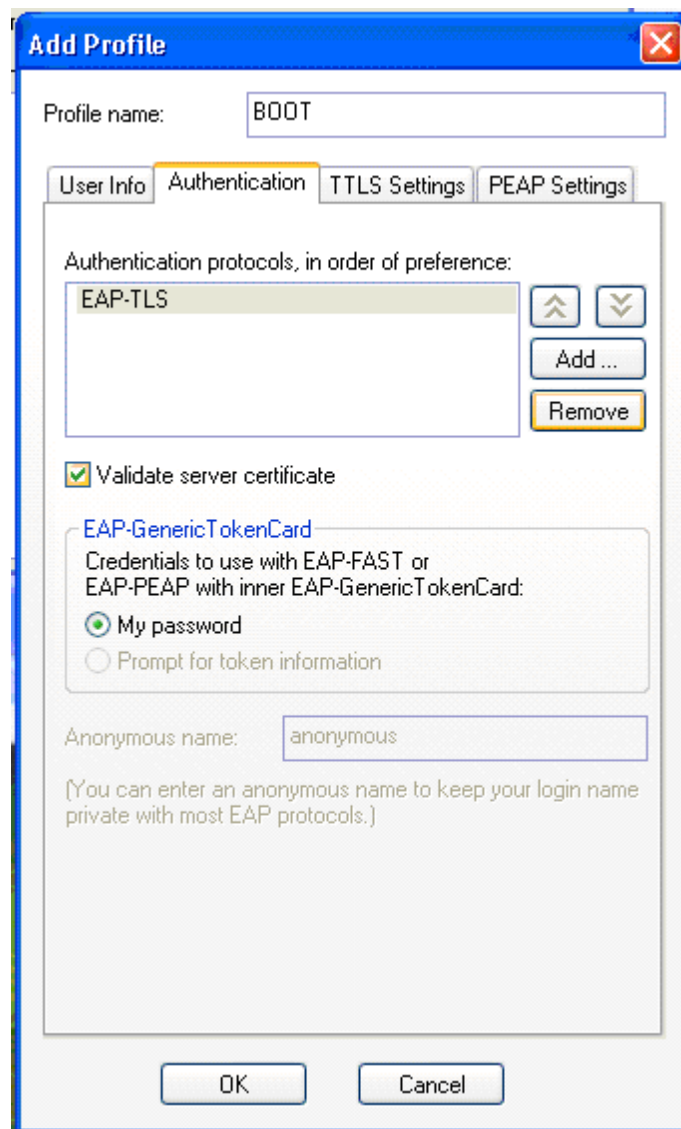
The Validate server certificate box is checked (by default) to enable mutual authentication. Certain protocols, such as EAP-TTLS, PEAP, and EAP-TLS, provide this capability which enables the user to verify the identity of the authentication server based on its certificate as the server verifies the user identity based on the user certificate. The same option is checked in the User Profile section.

Click **OK** to save the Profile.

**Note**

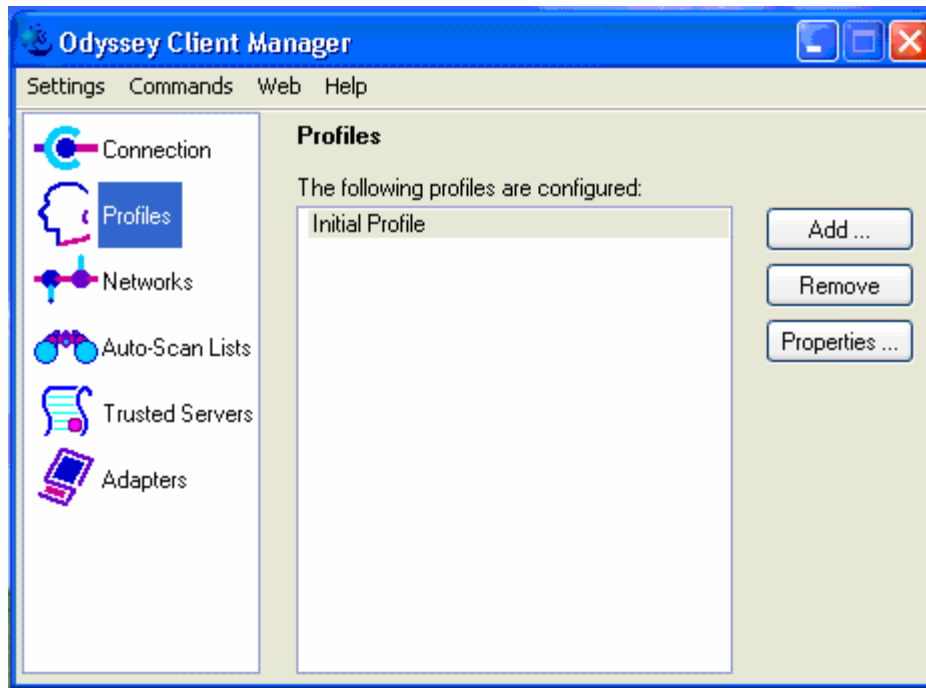
Disregard the default parameter checked for the EAP-GenericTokenCard section. This information only applies to PEAP and EAP-FAST.

Figure 4-14 *Configure the Authentication Method for the Machine Profile*



Create a User Profile

In the Funk Odyssey Client Manager, highlight the Profiles option in the left menu and select **Add** to create a new user profile.

Figure 4-15 Create a User Profile

Configure the Authentication Information for the User Profile

In the Add Profile screen, enter a name for the profile. For this scenario, the profile is named LOGON. On the User Info tab, the Login name is automatically populated with the name of the user who is currently logged into the machine along with their domain. On the Password tab at the bottom of the User Info tab, leave the default values of Permit login using password and Use Windows password checked.

Figure 4-16 Configure the Password Information for the User Profile

The screenshot shows the 'Add Profile' dialog box with the following details:

- Title Bar:** Add Profile
- Profile name:** LOGON
- Tabs:** User Info, Authentication, TTLS Settings, PEAP Settings
- Login name:** TSE\user1a
- Sub-tabs (under User Info):** Password, Certificate, SIM Card
- Password Sub-tab Options:**
 - ☒ Permit login using password
 - ☒ Use Windows password
 - ☐ Prompt for password
 - ☐ Use the following password:
- Password Field:** (Empty text box)
- Unmask:** ☐ Unmask
- Buttons:** OK, Cancel

Next click the **Certificate** tab at the bottom of the User Info tab. Check the Permit login using my certificate box. Then click the **Browse** tab to select the correct certificate for the current user.

**Note**

Refer to [Appendix B, “Installing an X.509v3 PKI Certificate on the Client,”](#) for instructions on how to install a certificate onto a client machine.

Figure 4-17 Configure the Certificate Information for the User Profile

The screenshot shows the 'Add Profile' dialog box with the 'Certificate' tab selected. The 'Profile name' field contains 'LOGON'. The 'Login name' field contains 'TSE\user1a'. Under the 'Certificate' tab, the checkbox 'Permit login using my certificate:' is checked, and the text 'user1a' is entered in the field below it. There are 'View ...' and 'Browse ...' buttons to the right of the text field. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

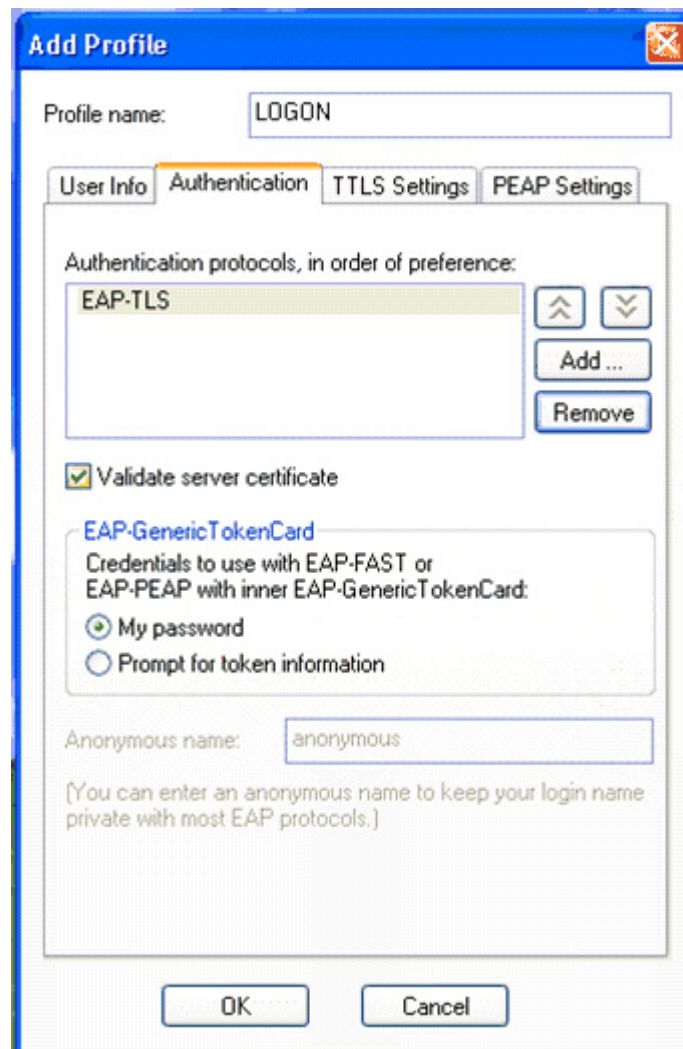
Configure the Authentication Method for the User Profile

On the Authentication tab, click **Add** next to the Authentication Protocols box. Select EAP-TLS and click **OK**. Next, highlight EAP-TTLS (which is listed as an authentication protocol by default) and click **Remove**. Check the Validate server certificate box. Click **OK** to save the Profile.

**Note**

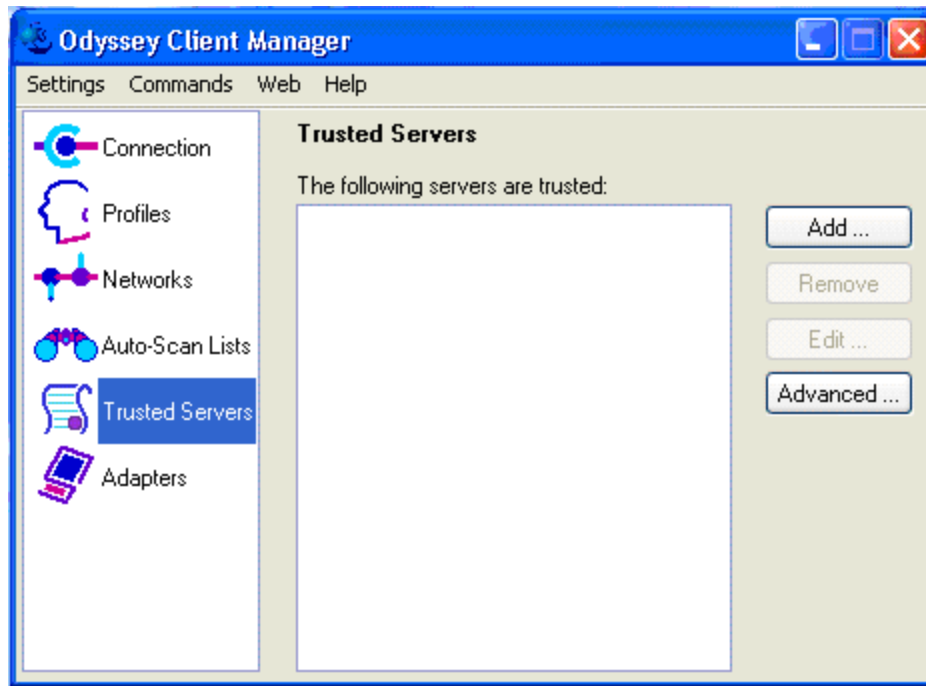
Disregard the default parameter checked for the EAP-GenericTokenCard section. This information only applies to PEAP and EAP-FAST.

Figure 4-18 Configure the Authentication Method for the User Profile



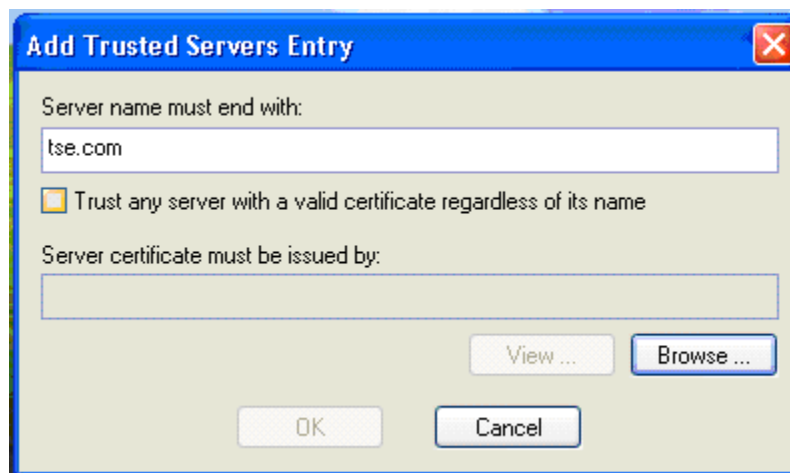
Add a Trusted Server

In the Funk Odyssey Client manager, highlight the Trusted Servers option in the left menu and click **Add** to create a new trusted server entry.

Figure 4-19 Add a Trusted Server

Configure a Trusted Server Entry

Add the domain name to the Server name must end with text box. For this scenario, the tse.com domain is used.

Figure 4-20 Configure a Trusted Server Entry

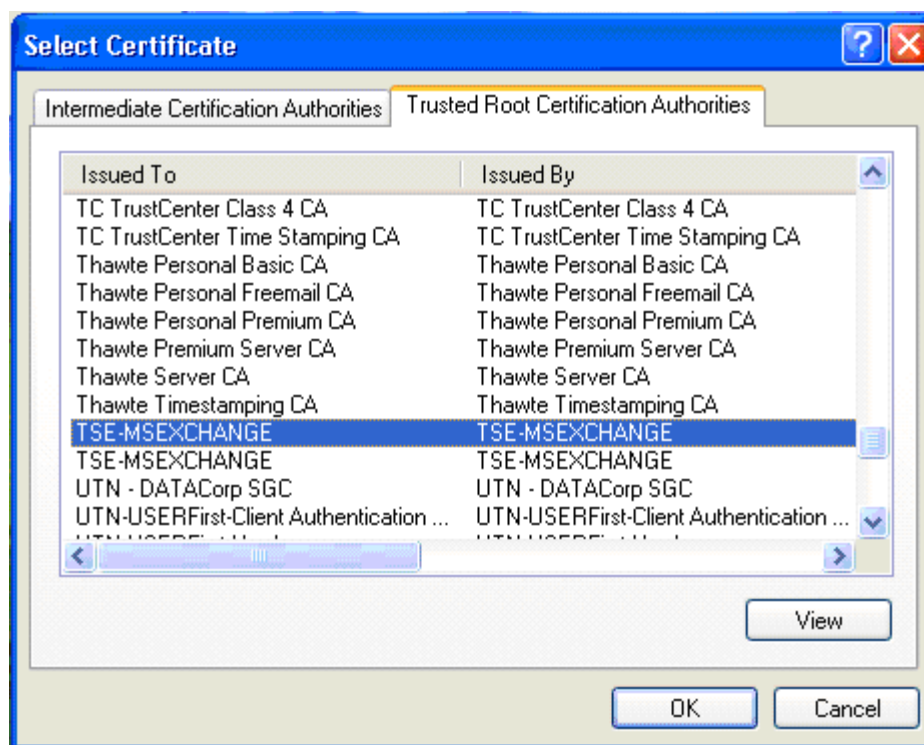
**Note**

An alternative option to entering the domain name for the trusted server is to check the **Trust any server with a valid certificate** regardless of its name box which allows all servers with a specified signed certificate to be trusted.

Select the Trusted Root Certification Authority

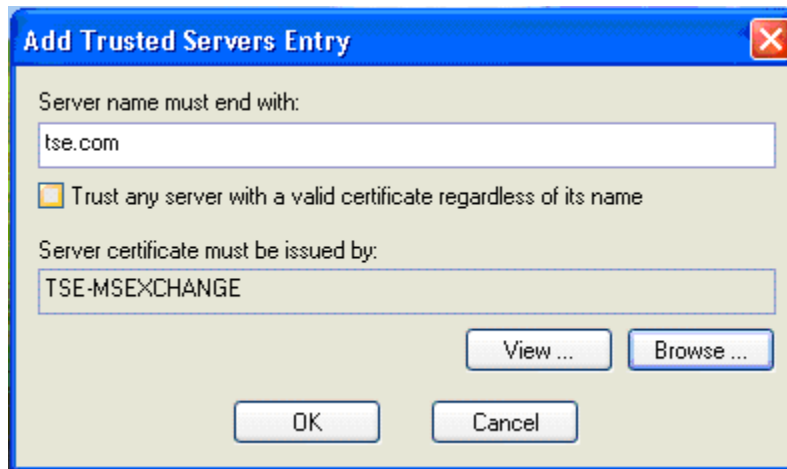
Click **Browse** in the Add Trusted Servers Entry window to select a value for the Server certificate must be issued by option. Click the **Trusted Root Certification Authorities** tab in the Select Certificate window. Highlight the certificate authority that issued the certificate. Click **OK**.

Figure 4-21 Select the Trusted Root Certification Authority



Save the Trusted Server Entry

Click **OK** in the Add Trusted Servers Entry window to save the configuration for the Trusted Server Entry.

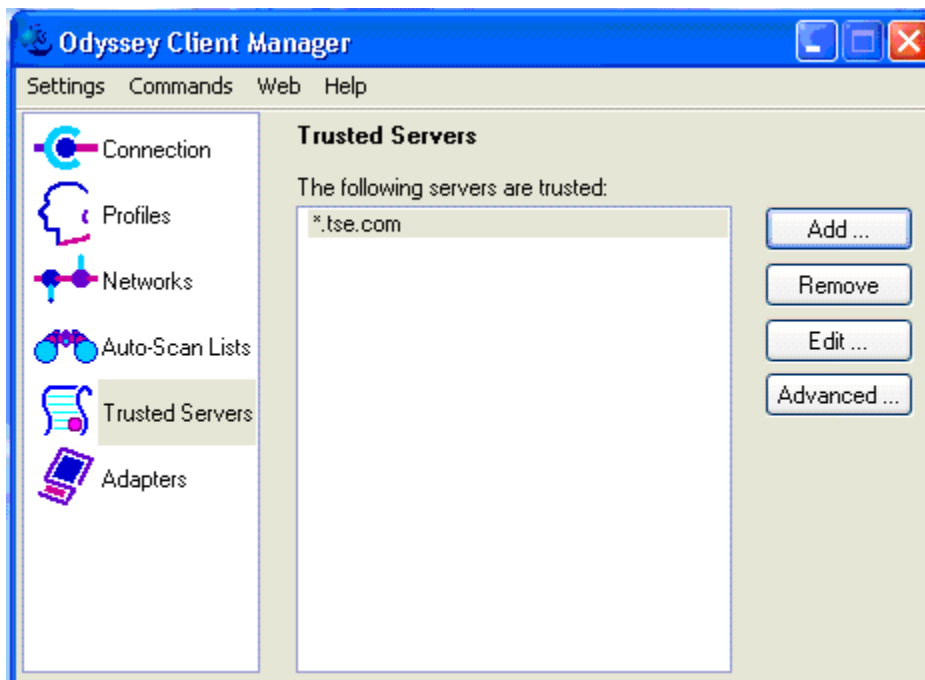
Figure 4-22 Save the Trusted Server Entry

Verify the Trusted Servers

After a trusted server has been configured the entry appears in the Trusted Servers list.

**Note**

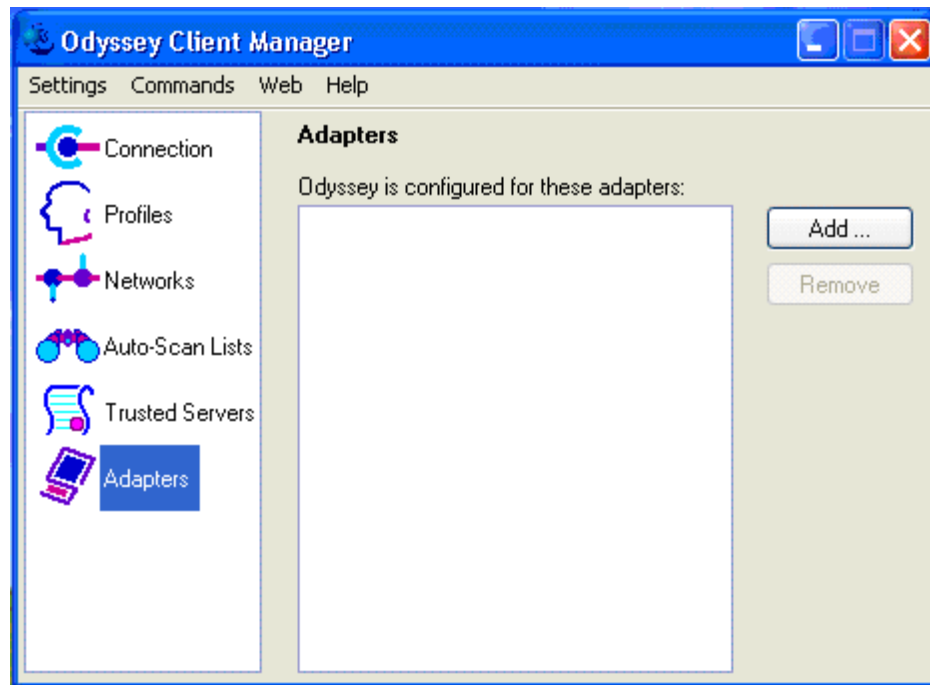
By adding the Trusted Servers initially, users within the administrative domain do not need to enable trust when accessing the network.

Figure 4-23 Verify the Trusted Servers

Apply an Adapter to the User Profile

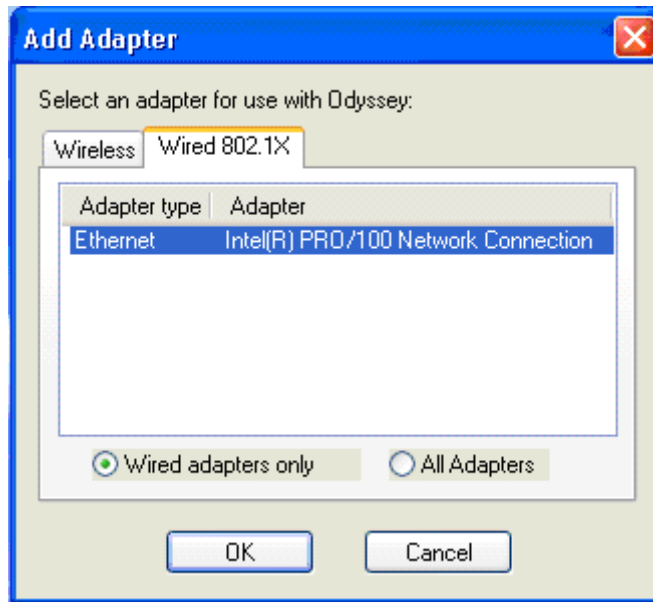
Highlight the Adapters option on the Funk Odyssey Client Manager main menu. Click **Add**.

Figure 4-24 Apply an Adapter to the User Profile



Add the Adapter to the User Profile

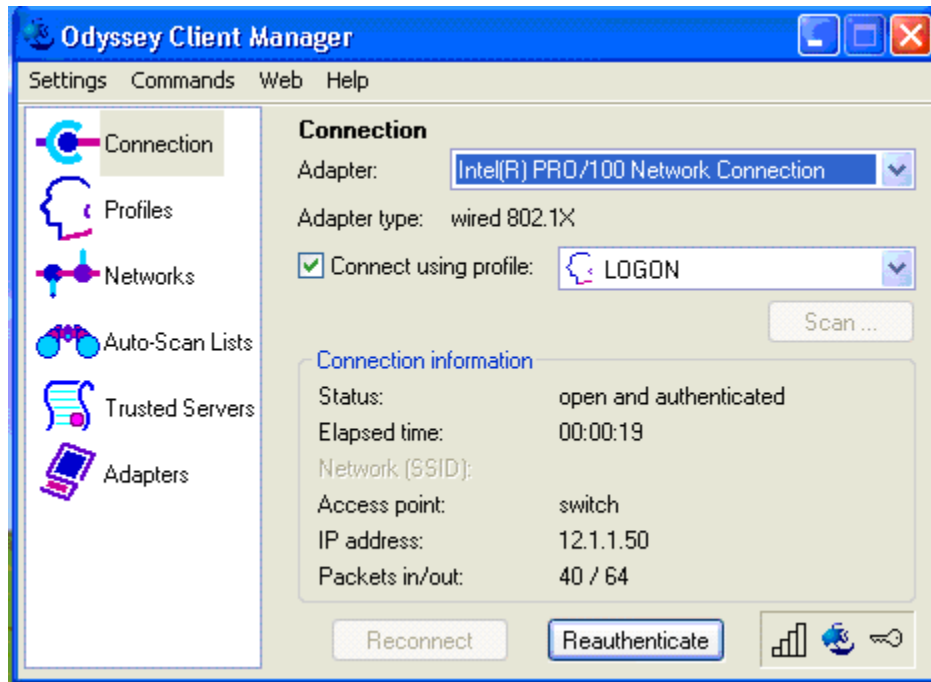
A wired connection is used for this scenario. To select the correct adapter, click the **Wired 802.1X** tab and select the correct the Ethernet adapter. Click **OK**.

Figure 4-25 Add the Adapter to the User Profile

Verify the Network Connection for the User Profile

Highlight the Connection option on the Funk Odyssey Client Manager main menu. Ensure that the correct adapter is selected from the Adapter drop-down menu. Check the Connect using profile box and select the LOGON profile that was created in the previous steps from the drop-down menu.

After the client has successfully passed IEEE 802.1X authentication via EAP-TLS, the status, displayed in the Connection information section, transitions to open and authenticated.

Figure 4-26 Verify the Network Connection for the User Profile



Deploying PEAP with EAP-MSCHAPv2

This chapter describes how to deploy IEEE 802.1X port-based access control using PEAP with EAP-MSCHAPv2 between the supplicant and authentication server. The native Microsoft Windows XP client is used as the supplicant for this scenario. Cisco Secure ACS 4.0 is used as the authentication server. A Cisco Catalyst switch functions as the authenticator and provides wired LAN connectivity between the supplicant and authentication server.

Authentication Server Configuration

The steps provided in this section explain how to configure Cisco Secure ACS 4.0 for PEAP with EAP-MSCHAPv2 authentication.



Note

This section explains only those details necessary to configure PEAP with EAP-MSCHAPv2 authentication; refer to the Cisco Secure ACS Configuration Guides for information regarding other features and functionality.

Create an External User Database

Refer to [Create an Unknown User Policy, page 4-1](#). The procedure is the same for PEAP with EAP-MSCHAPv2.



Note

PEAP does not require the use of an external user database such as Windows Active Directory; the internal ACS database could be used with this EAP method.

Configure an External User Database

Refer to [Configure an Unknown User Policy, page 4-2](#). The procedure is the same for PEAP with EAP-MSCHAPv2.

Select an External User Database

Refer to [Select an External User Database, page 4-3](#). The procedure is the same for PEAP with EAP-MSCHAPv2.

Choose to Configure the Windows Database

Refer to [Choose to Configure the Windows Database, page 4-4](#). The procedure is the same for PEAP with EAP-MSCHAPv2.

Configure the Windows Database

Refer to [Configure the Windows Database, page 4-5](#). The first step is the same for PEAP with EAP-MSCHAPv2. For the last step, scroll down to the Machine Authentication section and check the Enable PEAP Machine Authentication box. Click **Submit**.

Figure 5-1 Enable PEAP Machine Authentication

The screenshot shows the Cisco Systems External User Databases configuration interface. On the left is a navigation pane with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases (selected), Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'External User Databases' and contains a 'Windows EAP Settings' section. This section has two checkboxes: 'Enable password change inside PEAP or EAP-FAST.' (unchecked) and 'EAP-TLS Strip Domain Name.' (unchecked). Below these is the 'Machine Authentication.' section, which includes: 'Enable PEAP machine authentication.' (checked), 'Enable EAP-TLS machine authentication.' (unchecked), 'EAP-TLS and PEAP machine authentication name prefix.' (text box containing 'host/'), 'Enable machine access restrictions.' (unchecked), 'Aging time (hours):' (text box containing '12'), 'Group map for successful user authentication without machine authentication:' (dropdown menu showing '<No Access>'), and 'User Groups that are exempt from passing machine authentication:' (empty text box). At the bottom, there are two lists: 'Available User Groups' containing 'Default Group', 'Group 1', 'Group 2', 'Group 3', and 'Group 4'; and 'Selected User Groups' which is empty. A right-pointing arrow button is located between the two lists.

Configure a AAA Server

Refer to [Configure a AAA Server, page 3-3](#). The procedure is the same for all EAP methods.

Configure a AAA Client

Refer to [Configure a AAA Client, page 3-4](#). The procedure is the same for all EAP methods.

Verify the Network Configuration

Refer to [Summary of Network Configuration, page 3-5](#). The procedure is the same for all EAP methods.

Global Authentication Setup

Click **System Configuration** in the main menu. From the System Configuration menu, select Global Authentication Setup to configure the EAP method. Check the Allow EAP-MSCHAPv2 box in the PEAP section. Click **Submit + Restart**.

**Note**

The Allow EAP-MSCHAPv2 is the only box checked for the PEAP inner methods because that is the only method used in this scenario with the native Microsoft Windows XP SP2 IEEE 802.1X supplicant.

Figure 5-2 Global Authentication Setup for PEAP

CISCO SYSTEMS

System Configuration

Edit

Global Authentication Setup

EAP Configuration

PEAP

☒ Allow EAP-MSCHAPv2

☐ Allow EAP-GTC

☐ Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect: ☐

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

☐ Allow EAP-TLS

Select one or more of the following options:

Client Configuration

The steps provided in this section explain how to configure the native Microsoft Windows XP client for PEAP with EAP-MSCHAPv2 authentication.



Note

The native client is running on the Windows XP operating system with Service Pack 2.

Enable IEEE 802.1X for the Local Area Connection

To configure the IEEE 802.1X parameters, click **Start, Control Panel**, and then select Network and Internet Connections. Next, select Network Connections, then open the correct Local Area Connection Properties menu.

From the Local Area Connection Properties window, select the Authentication tab. Check the Enable IEEE 802.1X authentication for this network box. Select Protected EAP (PEAP) from the drop-down menu for the EAP type. Check the Authenticate as computer when computer information is available to enable machine authentication and subsequently reduce the overall Active Directory login period.

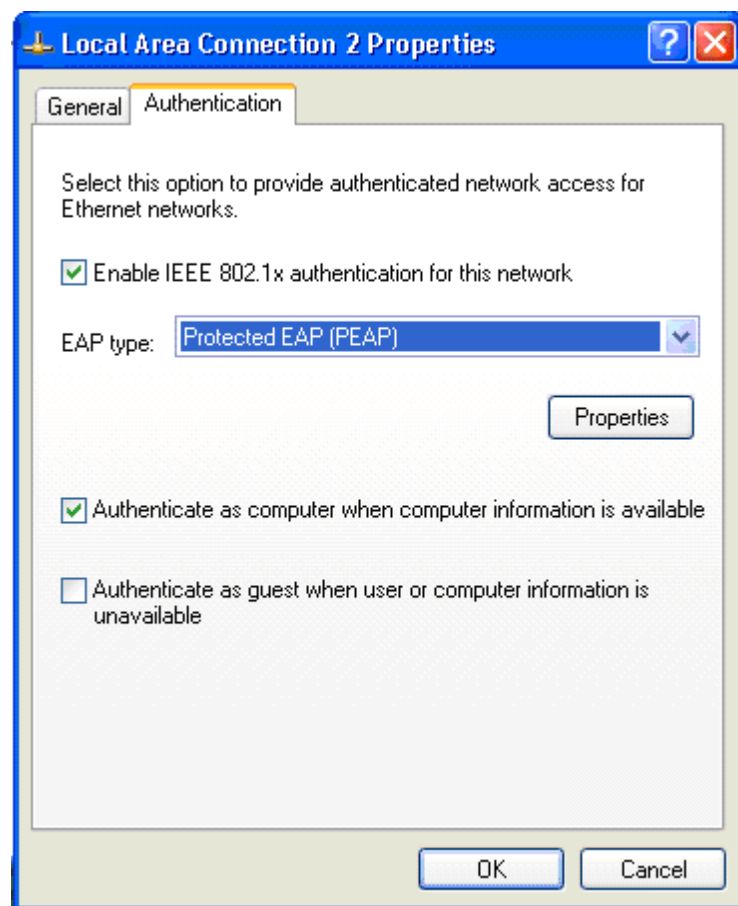
**Note**

The use of the Authenticate as computer when computer information is available is recommended because it provides quicker login times to enterprise Active Directory domains and it does not present any security risks in doing so. If this feature is enabled on both the supplicant and the ACS, it can reduce the time required to log into an enterprise Active Directory domain because the machine authentication has already taken place prior to the login screen appearing. If this feature is enabled on the supplicant but **not** in ACS, the authentication fails and the ports are placed in a “held” state upon reboot of the supplicant. This can increase login times because the supplicant has to wait until the timers expire and attempt to re-authenticate with user credentials.

**Note**

The use of the Authenticate as guest when user or computer information is unavailable checkbox is not currently recommended.

Figure 5-3 *Enable IEEE 802.1X Authentication for the Local Area Connection*



Configure the PEAP Properties

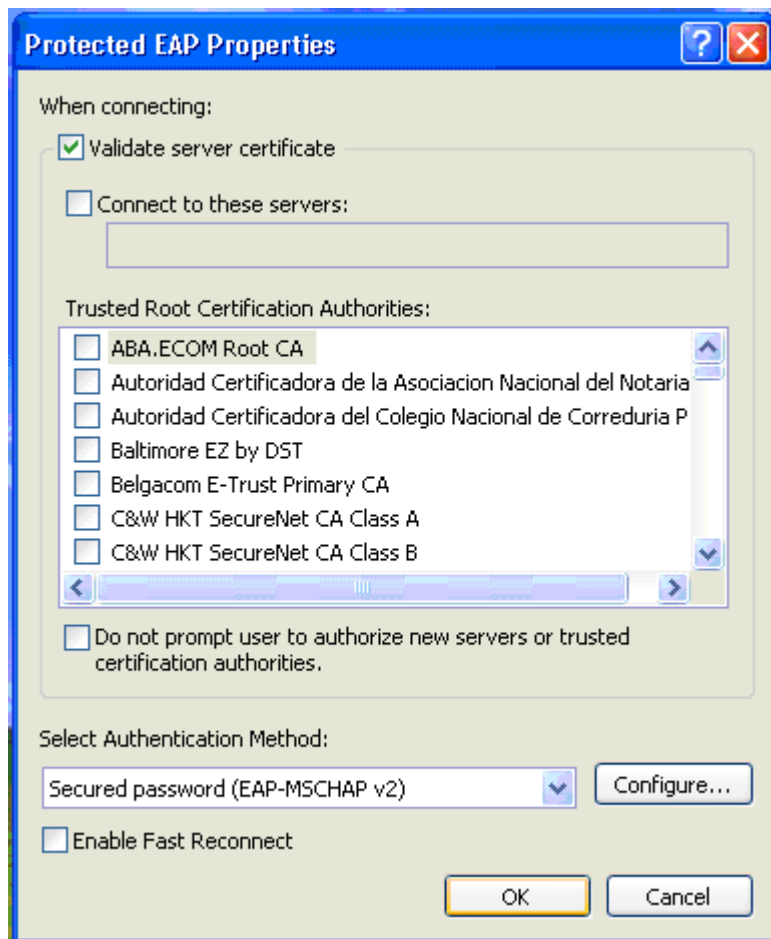
On the Protected EAP Properties menu, check the Validate server certificate box in the When connecting section. For this scenario, it is not necessary to check the Connect to these servers box or check any boxes in the Trusted Root Certification Authorities section. A certificate has already been installed on the desktop/laptop PC so the Certificate Authority has already been added to the Trusted Root Certification Authorities list.

**Note**

It is important to remember though that user and/or computer certificates are not required for PEAP; only the authentication servers require a certificate from a valid commercial certificate authority which the client must also trust.

The Do not prompt user to authorize new servers or trusted certification authorities parameter can be checked to disable a message screen from appearing when a user accesses a network outside of their domain and must verify new servers or certification authorities.

The Enable Fast Reconnect parameter can be enabled to allow PEAP to quickly resume a TLS session for a reauthentication attempt. If PEAP Part 2 was successful, a RADIUS server can cache the TLS session created during PEAP Part 1, therefore the session can be resumed without having to perform PEAP Part 1 or PEAP Part 2 again. This option is disabled by default; if enabled on the client, this option must be configured on the authentication server as well. Fast Reconnect is only recommended for wireless LAN deployments.

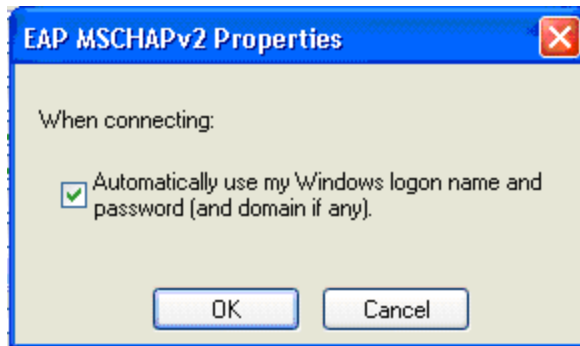
Figure 5-4 *Configure the PEAP Properties*

Configure the EAP-MSCHAPv2 Properties

On the Protected EAP Properties menu, select the Secured password (EAP-MSCHAPv2) option from the drop-down menu in the Select Authentication Method section. Click the **Configure...** button. Ensure that the Automatically use my Windows logon name and password (and domain if any) box is checked (the box should be checked by default). Click **OK**.

Click **OK** on the Protected EAP Properties window and click **OK** on the Local Area Connection window to save the configuration.

Figure 5-5 *Configure the EAP-MSCHAPv2 Properties*





Deploying EAP-FAST

This chapter describes how to deploy IEEE 802.1X port-based access control using EAP-FAST between the supplicant and authentication server. The Cisco Aironet wireless LAN client is used as the supplicant for this scenario. Cisco Secure ACS 4.0 is used as the authentication server. A Cisco Aironet wireless LAN access point functions as the authenticator and provides wireless LAN connectivity between the supplicant and authentication server.

Authentication Server Configuration

The steps provided in this section explain how to configure Cisco Secure ACS 4.0 for EAP-FAST authentication.



Note

This section explains only those details necessary to configure EAP-FAST authentication; refer to the Cisco Secure ACS Configuration Guides for information regarding other features and functionality.

Create an External User Database

Refer to [Create an Unknown User Policy, page 4-1](#). The procedure is the same for EAP-FAST.



Note

EAP-FAST does not require the use of an external user database such as Windows Active Directory; the internal ACS database could be used with this EAP method.

Configure an External User Database

Refer to [Configure an Unknown User Policy, page 4-2](#). The procedure is the same for EAP-FAST.

Select an External User Database

Refer to [Select an External User Database, page 4-3](#). The procedure is the same for EAP-FAST.

Choose to Configure the Windows Database

Refer to [Choose to Configure the Windows Database, page 4-4](#). The procedure is the same for EAP-FAST.

Configure the Windows Database

Refer to [Configure the Windows Database, page 4-5](#). The first step of this procedure is the same for EAP-FAST. Click Submit.

Configure a AAA Server

Refer to [Configure a AAA Server, page 3-3](#). The procedure is the same for all EAP methods.

Configure a AAA Client

Refer to [Configure a AAA Client, page 3-4](#). The procedure is the same for all EAP methods.

Verify the Network Configuration

Refer to [Summary of Network Configuration, page 3-5](#). The procedure is the same for all EAP methods.

Global Authentication Setup

Click **System Configuration** in the main menu. From the System Configuration menu, select Global Authentication Setup to configure the EAP method. Scroll down to the EAP-FAST section and click **EAP-FAST Configuration**.

Check the Allow EAP-FAST box. Leave the default values for Active Master Key TTL, Retired Master Key TTL, and Tunnel PAC TTL. Type the DNS host name of the ACS server in the Authority ID info text box.

**Note**

The Authority ID info is the textual identity of this ACS server which can be used by the end-user to determine which ACS server to be authenticated against.

Check the Allow anonymous in-band PAC provisioning box.

**Note**

Allowing anonymous in-band PAC provisioning enables the ACS to establish a secured connection with the end-user client for the purpose of providing the client with a new PAC. This option allows an anonymous TLS handshake between the end-user client and ACS.

Figure 6-1 Global Authentication Setup for EAP-FAST

The screenshot shows the Cisco Systems System Configuration interface. On the left is a navigation pane with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main area is titled 'System Configuration' with an 'Edit' button. Below this is the 'EAP-FAST Configuration' section. A sub-window titled 'EAP-FAST Settings' contains the following configuration options:

- ☒ Allow EAP-FAST
- Active master key TTL: 1 months
- Retired master key TTL: 3 months
- Tunnel PAC TTL: 1 weeks
- Client initial message: (empty text box)
- Authority ID Info: TSE-MSEXCHANGE
- ☒ Allow anonymous in-band PAC provisioning
- ☐ Allow authenticated in-band PAC provisioning
 - ☐ Accept client on authenticated provisioning
 - ☐ Require client certificate for provisioning
- ☒ Allow Machine Authentication
- Machine PAC TTL: 1 weeks

At the bottom of the settings window are three buttons: 'Submit', 'Submit + Restart', and 'Cancel'.

Check the Allow Machine Authentication box and leave the Machine PAC TTL set to the default value. Check the Allow Stateless Session Resume box and leave the Authorization PAC TTL set to the default value.

**Note**

The Allow Stateless Session Resume box should normally be checked as this enables the ACS to provision authorization PACs for EAP-FAST clients and always perform phase 2 of EAP-FAST.

For Allowed Inner Methods, check one or more of the options to determine which EAP method is used inside the EAP-FAST tunnel.

**Note**

Since Allow anonymous in-band PAC provisioning is used for this scenario, EAP-MSCHAP must be selected because it is the only inner method used for phase zero of EAP-FAST. EAP-GTC must also be checked because it is used for EAP-FAST phase two.

Select one or more of the options for the Select one or more of the following EAP-TLS comparison methods. Check the EAP-FAST master server box.

**Note**

Selecting the EAP-FAST master server check box determines whether ACS creates its own master keys and uses its own EAP-FAST settings and Authority ID or if it uses the EAP-FAST settings, master keys, and Authority ID received from another (slave or replicated) ACS that has been replicated.

Click **Submit + Restart**.

Figure 6-2 Enable EAP-FAST Machine Authentication and Choose the Allowed Inner Methods

Client Configuration

The steps provided in this section explain how to configure the Cisco Aironet wireless LAN client for EAP-FAST authentication.

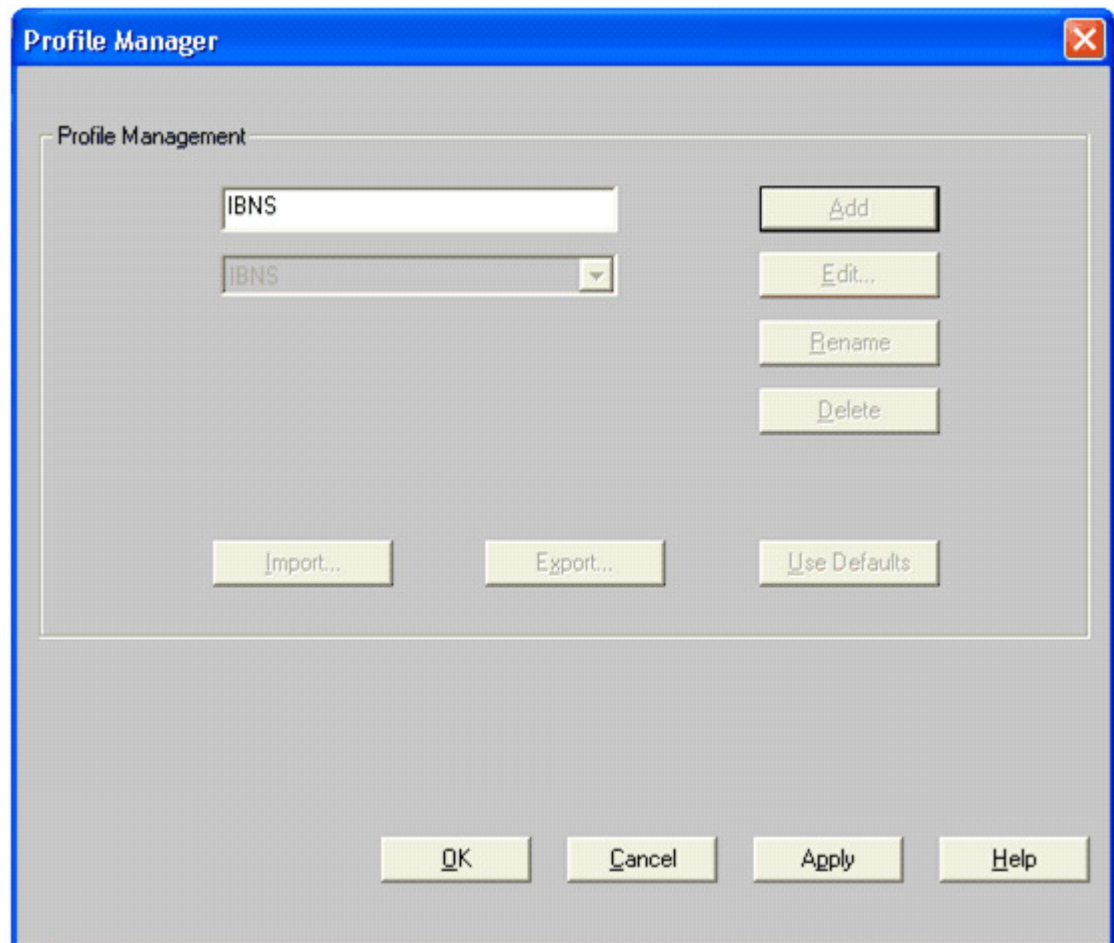
**Note**

The Cisco Aironet wireless LAN client is running on the Windows XP operating system with Service Pack 2.

Create a Profile for EAP-FAST

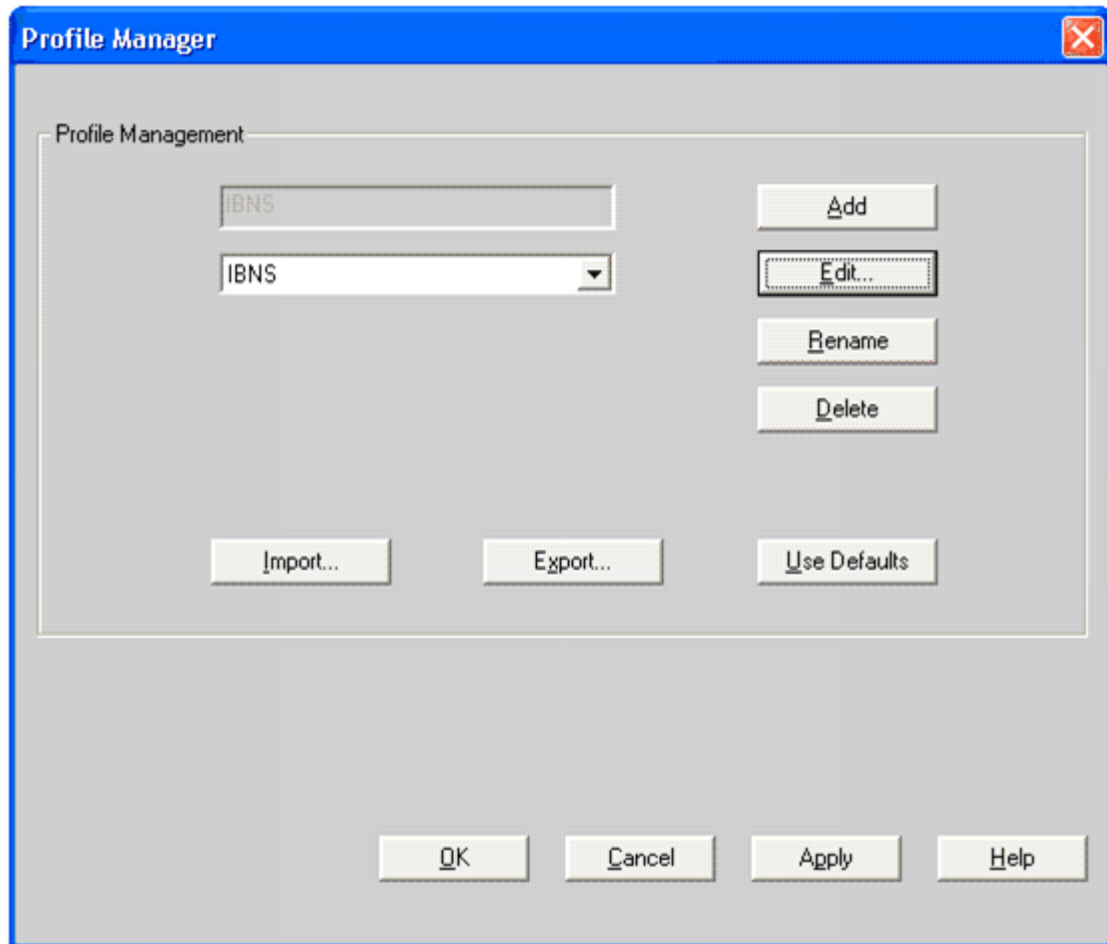
Open the Cisco Aironet wireless LAN Client Utility and select Profile Manager from the main menu. Click the **Add** button and enter the name of the new profile. The profile used for this scenario is named IBNS. Click **Apply** to save the profile.

Figure 6-3 Create a Profile for EAP-FAST



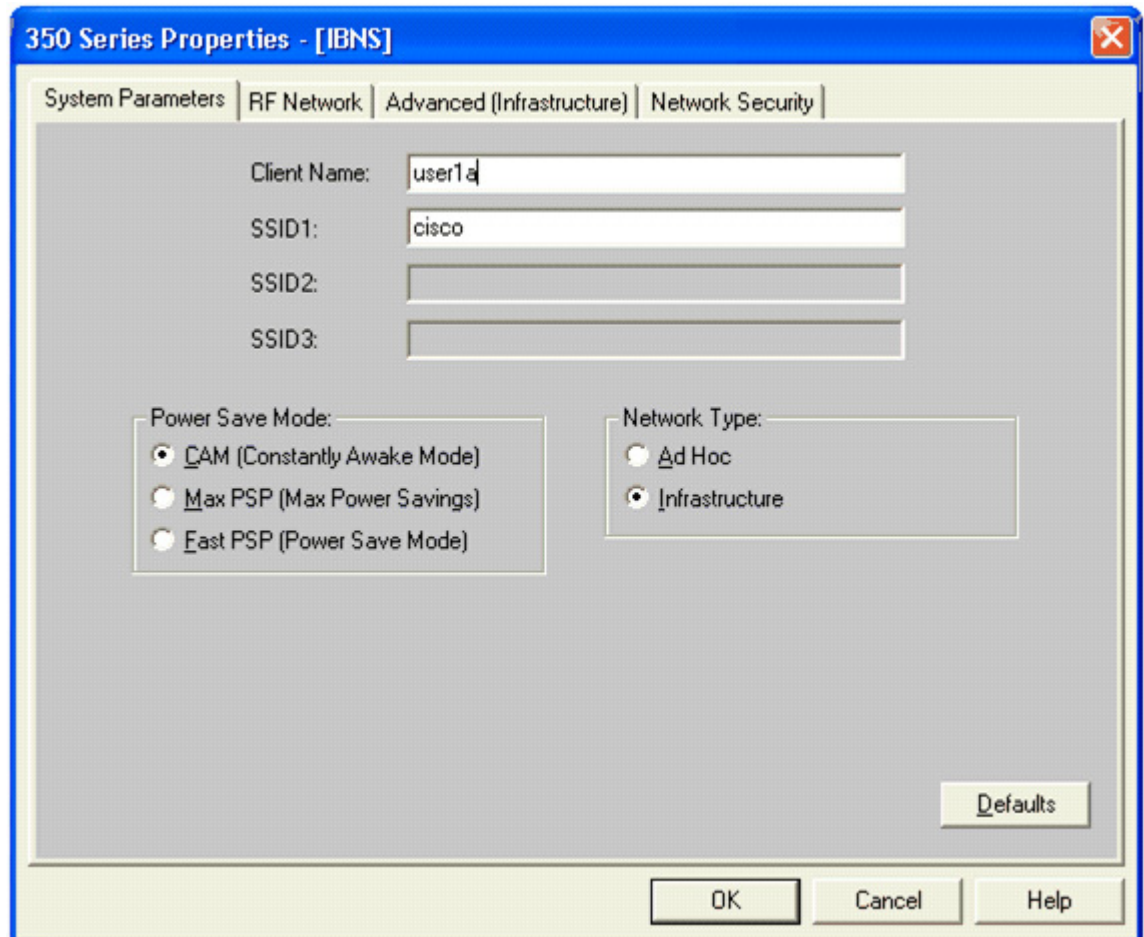
Edit the Profile Configuration

From the Profile Manager window, select the profile from the drop-down box that you want to configure. For this scenario, the IBNS profile is selected. Click **Edit** to configure the profile parameters.

Figure 6-4 *Edit the Profile Configuration*

Configure the System Parameters of the Profile

On the System Parameters window, enter the Client Name and SSID for the profile. For this scenario, user1a is used for the Client Name and cisco is used for the SSID. The default options are used for the Power Save Mode and Network Type parameters.

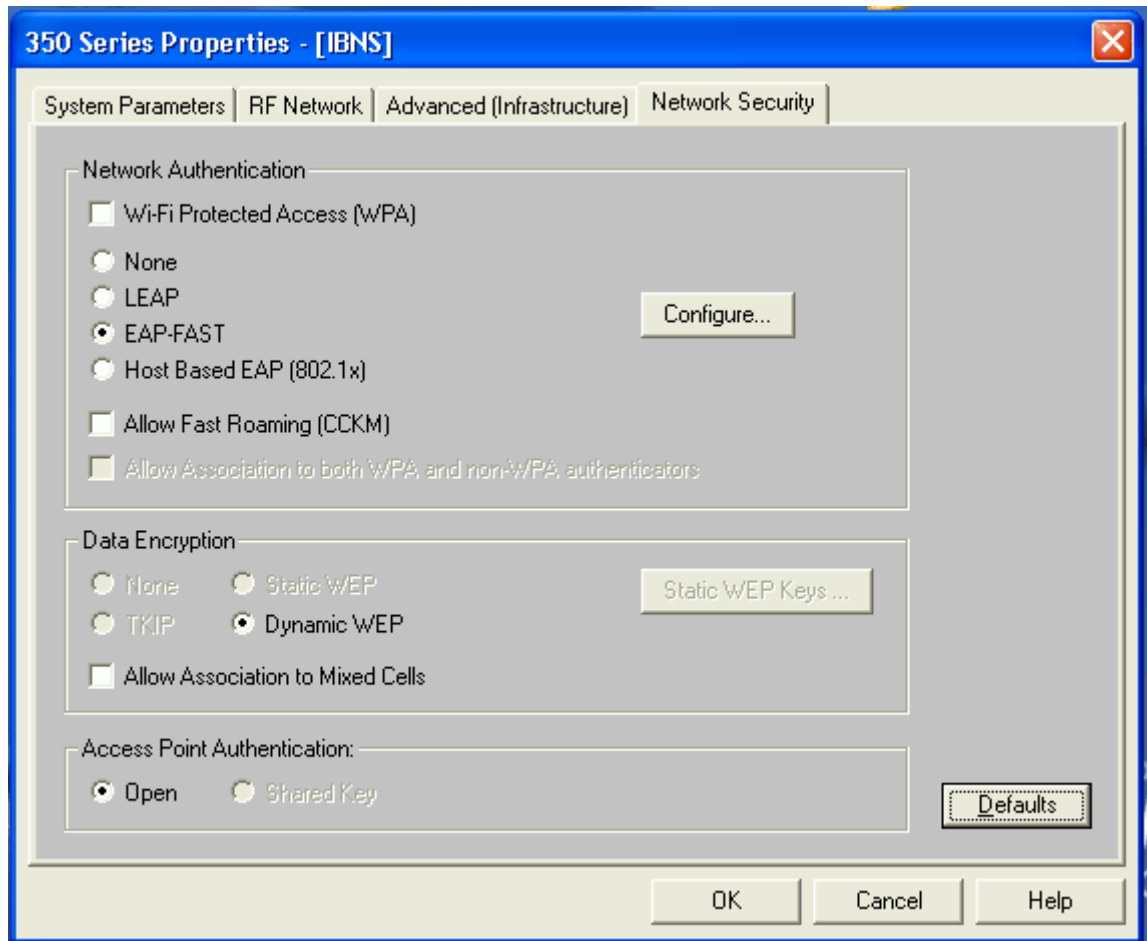
Figure 6-5 *Configure the System Parameters of the Profile*

Configure the Network Security for the Profile

On the Network Security window in the Network Authentication section, select the EAP-FAST radio button.

In the Data Encryption section, leave the default setting of Dynamic WEP, which means that the WEP keys are dynamically generated during the EAP authentication process.

In the Access Point Authentication section, leave the default setting Open.

Figure 6-6 *Configure the Network Security for the Profile*

Configure the EAP-FAST Settings for the Profile

Click the **Configure** button in the Network Authentication section of the Network Security window to configure the EAP-FAST settings for the profile. Use the default settings of Use Temporary User Name and Password and User Windows Logon User Name and Password listed in the User Name and Password Settings section. This is the default option and causes the Windows username and password to be used as the EAP-FAST username and password. Use the following default settings for the Logon Options:

- Include Windows Logon Domain with User Name—This option is needed in environments with more than one domain.
- No Network Connection Unless User is Logged In—This option forces the client adapter to disassociate after a user logs off so that another user cannot gain access to the wireless network using their credentials.
- Authentication Timeout Value (seconds)—This option specifies the amount of time (in seconds) before an EAP-FAST authentication attempt is considered to be failed and an error message appears.

In the Protected Access Credentials section, use the default value of Allow Automatic PAC Provisioning for This Profile box. This ensures that a PAC is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.).

**Note**

The value for the Select a PAC Authority to use with the profile remains blank until the user attempts to login into the network. After the first successful logon, the PAC Authority value is populated via the automatic PAC provisioning process.

Click **OK** on the EAP-Settings window to save the configuration.

Click **OK** on the Profile Properties window to save the System Parameters and Network Security options configured in the previous steps.

Figure 6-7 Configure the EAP-FAST Settings for the Profile

EAP-FAST Settings

User Name and Password Settings

- ☒ Use Temporary User Name and Password
 - ☒ Use Windows Logon User Name and Password
 - ☐ Automatically Prompt for User Name and Password
 - ☐ Manually Prompt for User Name and Password
- ☐ Use Saved User Name and Password
 - User Name:
 - Password:
 - Confirm Password:
 - Domain:

Logon Options

- ☒ Include Windows Logon Domain with User Name
- ☒ No Network Connection Unless User Is Logged In
- Authentication Timeout Value (seconds):
- ☐ Restrict Time Finding Domain Controller to (seconds):

Protected Access Credentials (PAC)

- ☒ Allow Automatic PAC Provisioning for This Profile
- Select a PAC Authority to use with this profile:
-

OK Cancel Help Defaults



Optional Cisco IOS & Cisco Catalyst OS Configuration Commands

This appendix provides a reference for the optional Cisco IOS and Cisco Catalyst OS commands that can be used to configure IEEE 802.1X.

Cisco IOS

Cisco Catalyst switches running Cisco IOS require certain commands to enable IEEE 802.1X, however additional commands can be configured to enable optional functionality or change default parameters. These additional RADIUS, global, and interface commands are explained in the following sections.

RADIUS Configuration for Cisco IOS

The optional RADIUS configuration commands used to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco IOS are provided in this section.

Table A-1 *Optional RADIUS Configuration Commands for Cisco IOS*

aaa authorization network [<list name> default] group radius	(Optional) Configure the switch for user RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.
ip radius source-interface [interface]	(Optional) Specify the interface of the source address in RADIUS packets.
radius-server vsa send [authentication accounting]	(Optional) Enable the switch to recognize and use VSAs as defined by RADIUS IETF attribute 26. The authentication or accounting options can be specified to limit the set of vendor-specific recognized attributes to only authentication or accounting.

Global IEEE 802.1X Configuration for Cisco IOS

The optional global configuration commands used to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco IOS are provided in this section.

Table A-2 *Optional Global Configuration Commands for Cisco IOS*

dot1x guest-vlan supplicant	(Optional) Allow IEEE 802.1X capable supplicants to enter the Guest VLAN.
------------------------------------	---

Interface IEEE 802.1X Configuration for Cisco IOS

The optional interface configuration commands used to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco IOS are provided in this section.

Table A-3 *Optional Interface Configuration Commands for Cisco IOS*

dot1x control-direction [in both]	(Optional) Change the port control to unidirectional or bidirectional control. The default is bidirectional mode.
dot1x default	(Optional) Reset the configurable IEEE 802.1X parameters to their default values.
dot1x guest-vlan [VLAN ID]	(Optional) Specify an active VLAN as an IEEE 802.1X guest VLAN.
dot1x host-mode	(Optional) Allow single or multiple hosts (clients) on an IEEE 802.1X-authorized port. The default is single host mode.
dot1x max-reauth-req [count]	(Optional) Set the number of times that the switch retransmits identity requests before restarting. The default is 2 (once every 30 seconds).
dot1x max-req [count]	(Optional) Set the number of times that the switch retransmits EAPoL data frames before restarting. The default is 2 times (once every 30 seconds).
dot1x reauthentication	(Optional) Enable periodic re-authentication of the client. Disabled by default.
dot1x timeout [reauth-period quiet-period tx-period] [seconds]	(Optional) Configure timers for items such as reauth-period, quiet-period, server-timeout, supp-timeout and tx-period. The default for the reauth-period is 3600 seconds. The default for the quiet-period is 60 seconds. The default for the server-timeout is 30 seconds. The default for the supp-timeout is 30 seconds. The default for the tx-period is 5 seconds.

Cisco Catalyst OS

Cisco Catalyst switches running Cisco Catalyst OS require certain commands to enable IEEE 802.1X, however additional commands can be configured to enable optional functionality or change default parameters. These additional RADIUS, global, and interface commands are explained in the following sections.

Global IEEE 802.1X Configuration for Cisco Catalyst OS

The optional global configuration commands used to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco Catalyst OS are provided in this section.

Table A-4 Optional Global Configuration Commands for Cisco Catalyst OS

set dot1x max-req [count]	(Optional) Specifies the maximum number of times that the state machine retransmits an EAP-Request frame to the supplicant before it times out the authentication session. The default is 2.
set dot1x max-reauth-req	(Optional) Set Max No. of Retries to supplicant
set dot1x quiet-period [seconds]	(Optional) Specifies the idle time between authentication attempts. The default is 60 seconds.
set dot1x radius-accounting [enable disable]	(Optional) Specifies IEEE 802.1X RADIUS accounting and tracking. The default is disabled.
set dot1x radius-keepalive [enable disable]	(Optional) Specifies IEEE 802.1X RADIUS keepalive state. The default is enabled.
set dot1x radius-vlan-assignment [enable disable]	(Optional) Specifies IEEE 802.1X RADIUS VLAN assignment. The default is disabled.
set dot1x re-authperiod [seconds]	(Optional) Specifies the time constant for the retransmission reauthentication time. The default is 3600 seconds.
set dot1x server-timeout [seconds]	(Optional) Specifies the time constant for the retransmission of packets by the backend authenticator to the authentication server. The default is 30 seconds.
set dot1x shutdown-timeout [seconds]	(Optional) Specifies the amount time that a port is shut down after a security violation. The default is 300 seconds.
set dot1x supp-timeout [seconds]	(Optional) Specifies the time constant for the retransmission of EAP-Request packets. The default is 30 seconds.
set dot1x tx-period [seconds]	(Optional) Specifies the time for the retransmission of EAP-Request/Identity frame. The default is 30 seconds.
set dot1x vlan-group [VLAN group] [VLAN ID]	(Optional) Specifies the VLAN group name.

Port IEEE 802.1X Configuration for Cisco Catalyst OS

The optional port configuration commands used to configure IEEE 802.1X on a Cisco Catalyst switch running Cisco Catalyst OS are provided in this section.

Table A-5 *Optional Port Configuration Commands for Cisco Catalyst OS*

set port dot1x [module/port] auth-fail-vlan [VLAN none]	(Optional) Sets the VLAN that provides limited access to end hosts that have failed IEEE 802.1X authentication. The default is none.
set port dot1x [module/port] critical	(Optional) Set the port as critical.
set port dot1x [module/port] guest-vlan [VLAN none]	(Optional) Specifies an active VLAN as an IEEE 802.1X guest VLAN. The default is none.
set port dot1x [module/port] initialize	(Optional) Initialize IEEE 802.1X on a port. This command clears the current state machine for new authentications.
set port dot1x [module/port] multiple-authentication [enable disable]	(Optional) Specifies multiple authentications so that more than one host can gain access to the port. The default is disabled.
set port dot1x [module/port] multiple-host [enable disable]	(Optional) Specifies multiple-user access. The default is disabled.
set port dot1x [module/port] port-control-direction [both in]	(Optional) Specifies the traffic control direction on a port. The default is both.
set port dot1x [module/port] re-authenticate [enable disable]	(Optional) Manually initiates a reauthentication of the entity connected to the port. The default is disabled.
set port dot1x [module/port] re-authentication [enable disable]	(Optional) Automatically initiates reauthentication of the entity connected to the port within the reauthentication time period. The default is disabled.
set port dot1x [module/port] shutdown-timeout [enable disable]	(Optional) Specifies the shutdown-timeout period for a port after a security violation. The default is disabled.
set port dot1x [module/port] test-eapol-capable	(Optional) Test eapol capability.

Cisco Aironet Wireless LAN Access Points Running Cisco IOS

Cisco Aironet wireless LAN access points running Cisco IOS require certain commands to enable IEEE 802.1X, however additional commands can be configured to enable optional functionality or change default parameters. These additional RADIUS, global, and interface commands are explained in the following sections.

RADIUS Configuration for Cisco Aironet Wireless LAN Access Points Running Cisco IOS

The optional RADIUS configuration commands used to configure IEEE 802.1X on an Cisco Aironet wireless LAN access point running Cisco IOS are provided in this section.

Table A-6 *Optional RADIUS Configuration Commands for Cisco Aironet Wireless LAN APs Running Cisco IOS*

aaa authorization network [<list name> default] group radius	(Optional) Configure the switch for user RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.
ip radius source-interface [interface]	(Optional) Specify the interface of the source address in RADIUS packets.
radius-server vsa send [authentication accounting]	(Optional) Enable the switch to recognize and use VSAs as defined by RADIUS IETF attribute 26. The authentication or accounting options can be specified to limit the set of vendor-specific recognized attributes to only authentication or accounting.

Interface Configuration for Cisco Aironet Wireless LAN Access Points Running Cisco IOS

The optional interface configuration commands used to configure IEEE 802.1X on an Cisco Aironet wireless LAN access point running Cisco IOS are provided in this section.

Table A-7 *Optional Interface Configuration Commands for Cisco Aironet Wireless LAN APs Running Cisco IOS*

dot1x client-timeout [seconds]	(Optional) Enter the number of seconds the access point should wait for a reply from a client attempting to authenticate before the authentication fails.
dot1x reauth-period [seconds server]	(Optional) Enter the interval in seconds that the access point waits before forcing an authenticated client to reauthenticate. Enter the server keyword to configure the access point to use the reauthentication period specified by the authentication server. If you use this option, configure your authentication server with RADIUS attribute 27, Session-Timeout. This attribute sets the maximum number of seconds of service to be provided to the client before termination of the session or prompt. The server sends this attribute to the access point when a client device performs EAP authentication.



Installing an X.509v3 PKI Certificate on the Client

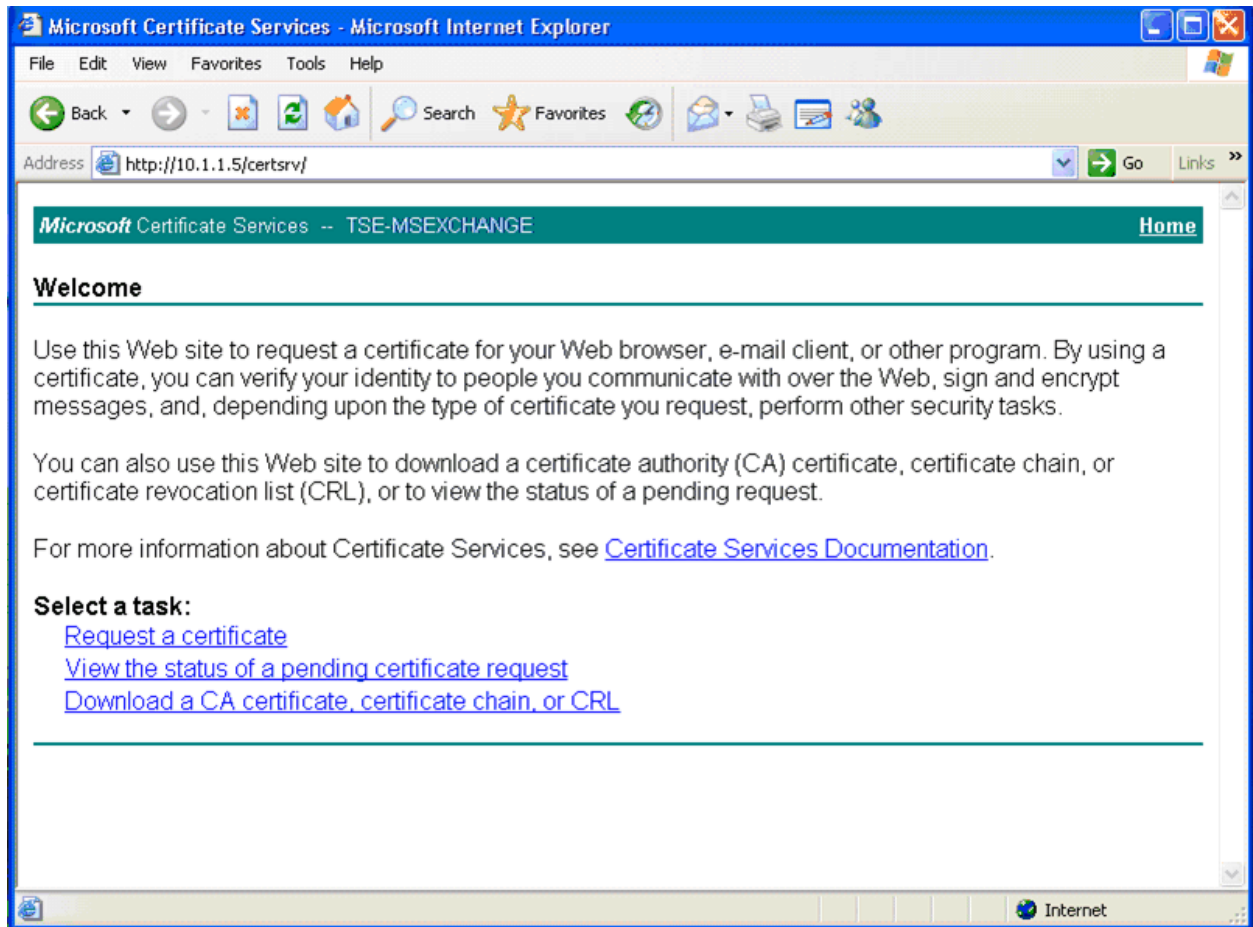
This appendix explains the process of installing an X.509 PKI certificate on a desktop/laptop PC. The certificate is needed if EAP-TLS is used as the authentication method with IEEE 802.1X and can also be used with PEAP or EAP-FAST.

As with the previous sections on deploying EAP methods, the desktop/laptop PC used in this appendix is running Microsoft Windows XP with Service Pack 2.

Access the Certificate Authority

Open a web browser and enter the address of the Certificate Authority (CA):

<http://<CA address or hostname>/certsrv/>. Login when prompted to do so. On the Welcome screen, select the Request a Certificate link in the task list.

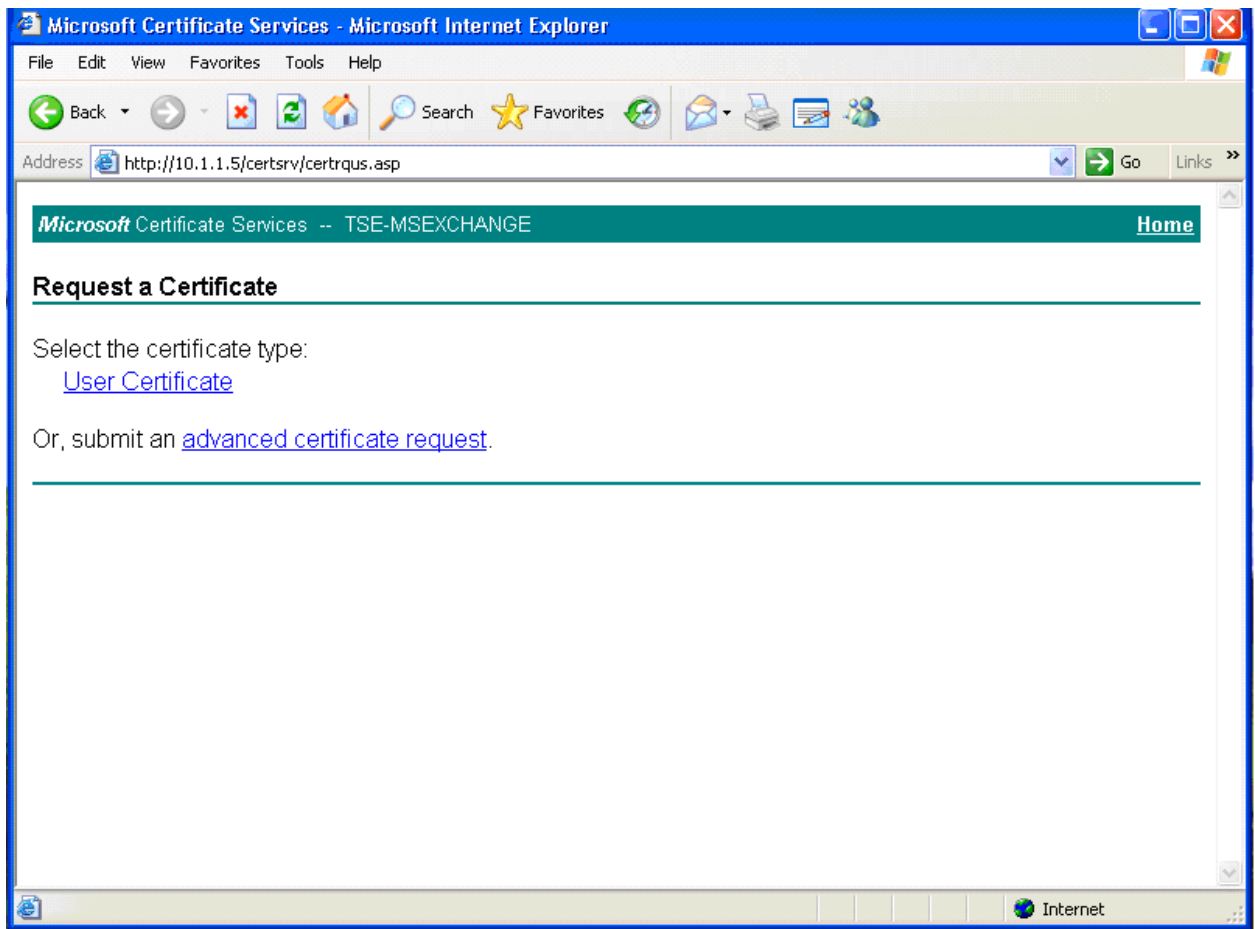
Figure B-1 Access the Certificate Authority

Request a Certificate

On the Request a Certificate screen, select the User Certificate option for the certificate type.

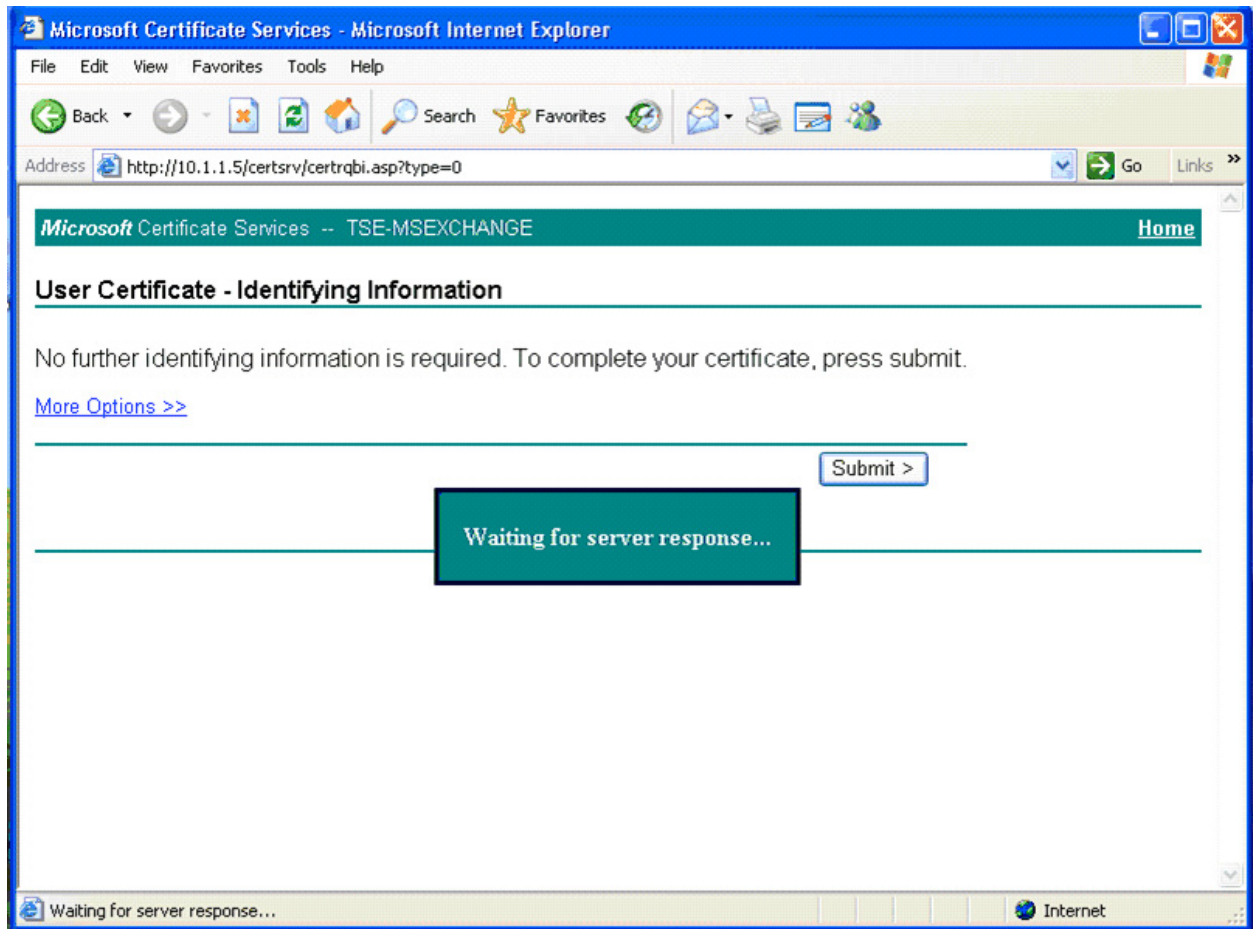
**Note**

If prompted, click **Yes** to trust the server from which the certificate is requested.

Figure B-2 Request a Certificate

Complete the Certificate Request

On the User Certificate – Identifying Information screen, select Submit to complete the request. A status message will appear stating Waiting for server response... while the request is being completed.

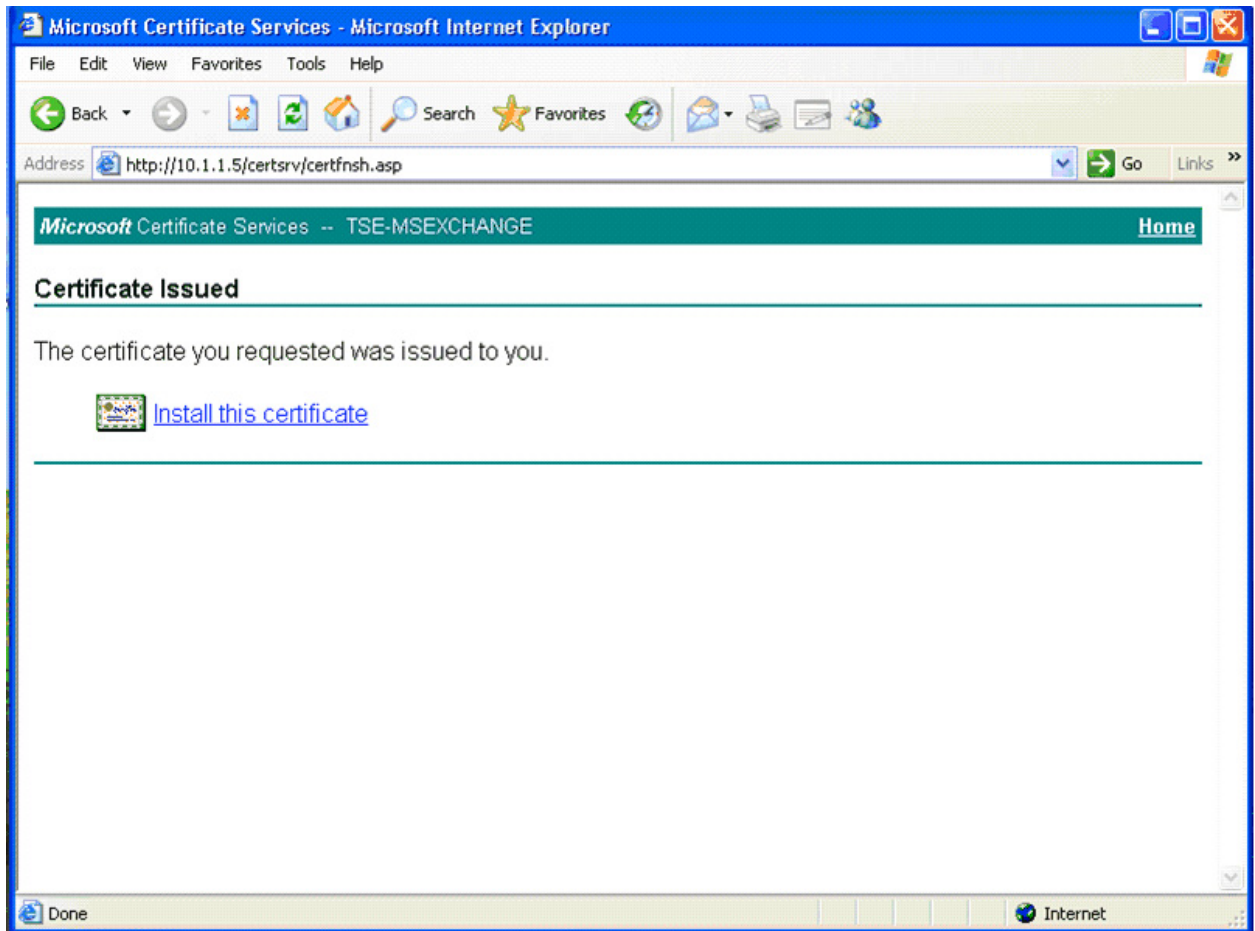
Figure B-3 Complete the Certificate Request

Install the Certificate

After the certificate has been issued, select the Install the certificate option to install the certificate on the desktop/laptop PC.

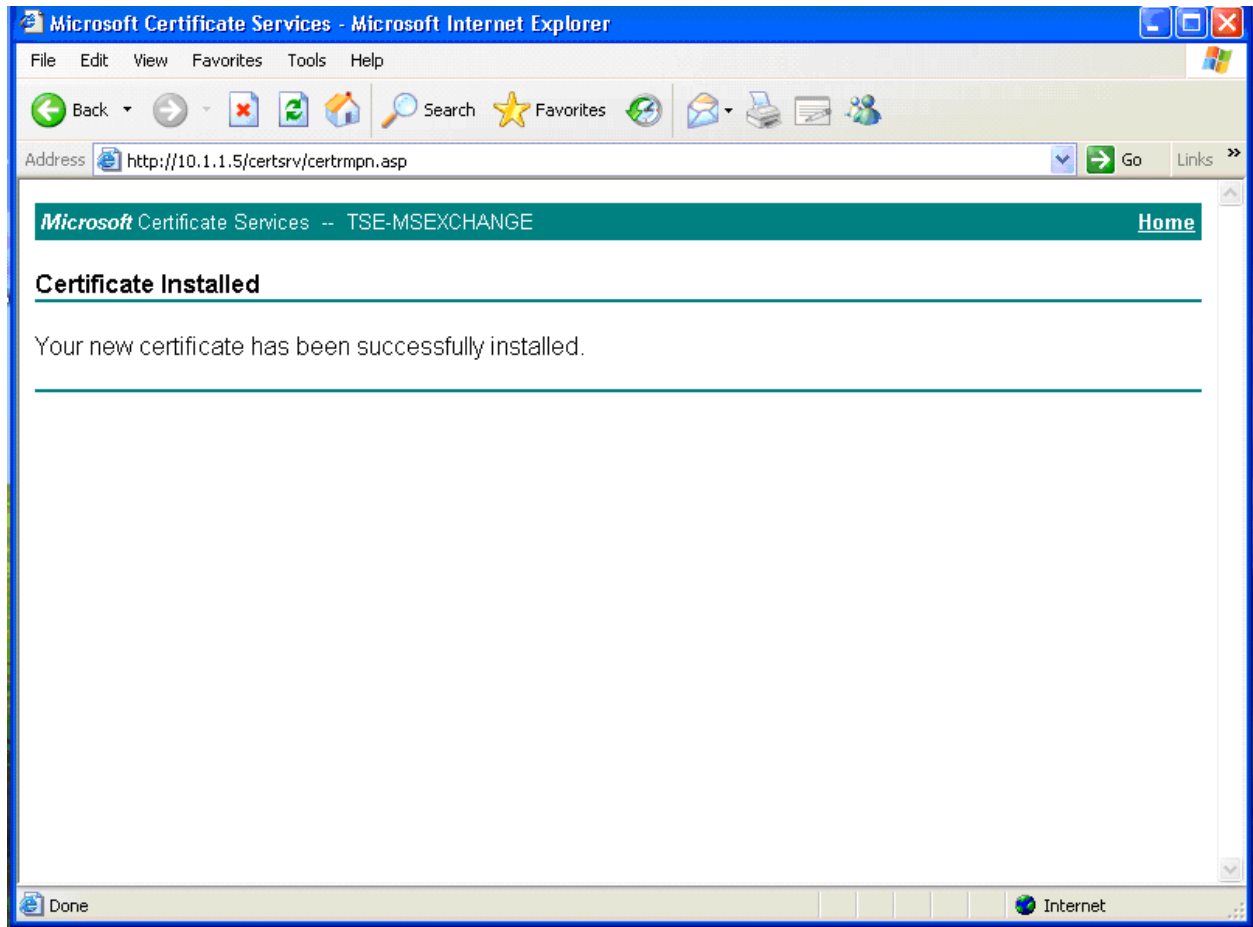
**Note**

If prompted, click **Yes** to trust the server from which the certificate is requested.

Figure B-4 *Install the Certificate*

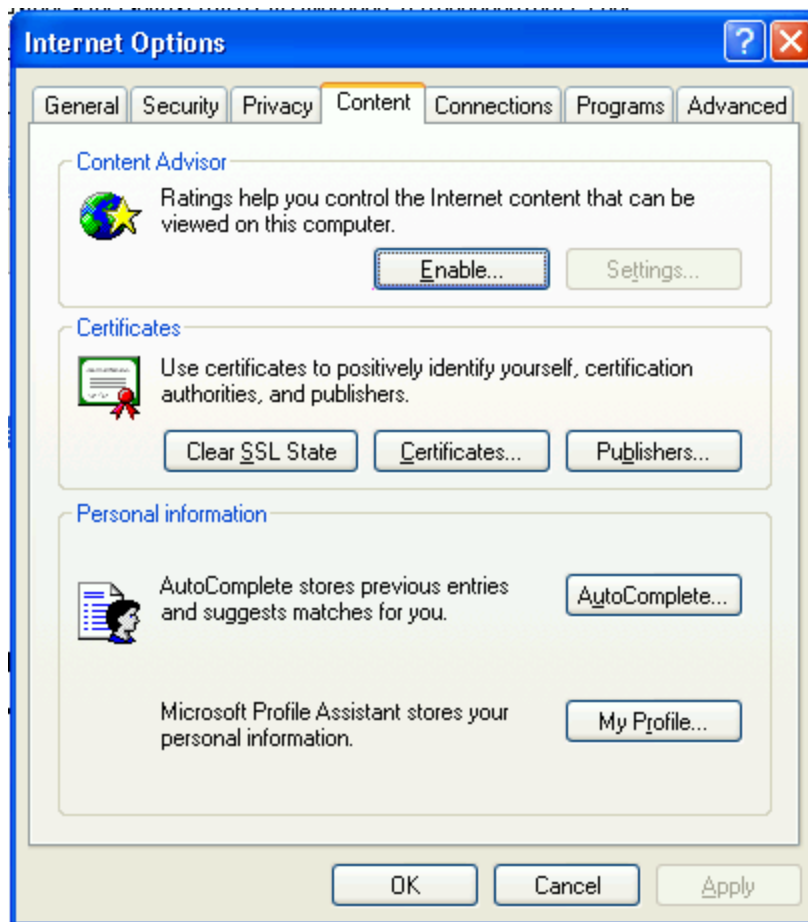
Certificate Installation Complete

After the certificate is successfully installed, the Certificate Installed screen appears.

Figure B-5 Certificate Installation Complete

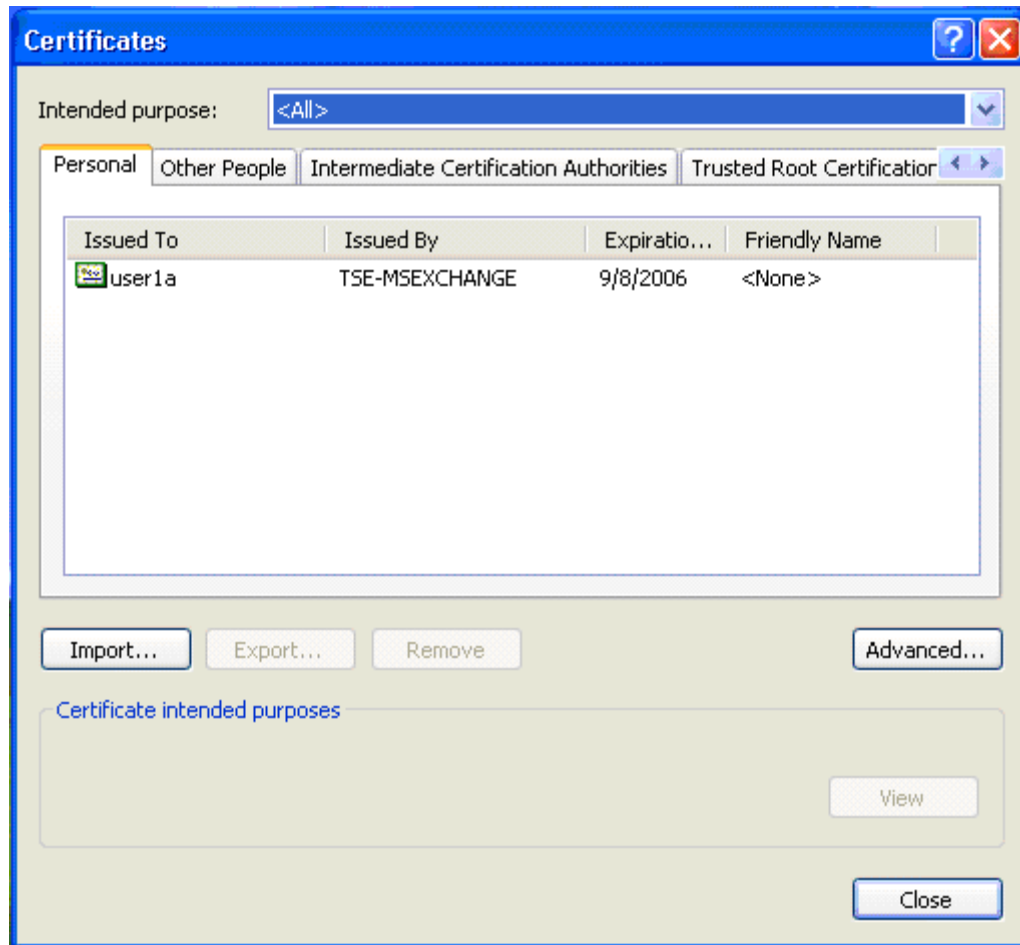
Verify Certificate Installation

To verify the certificate installation, select Tools from the menu in the web browser, Internet Options, and then the Content tab.

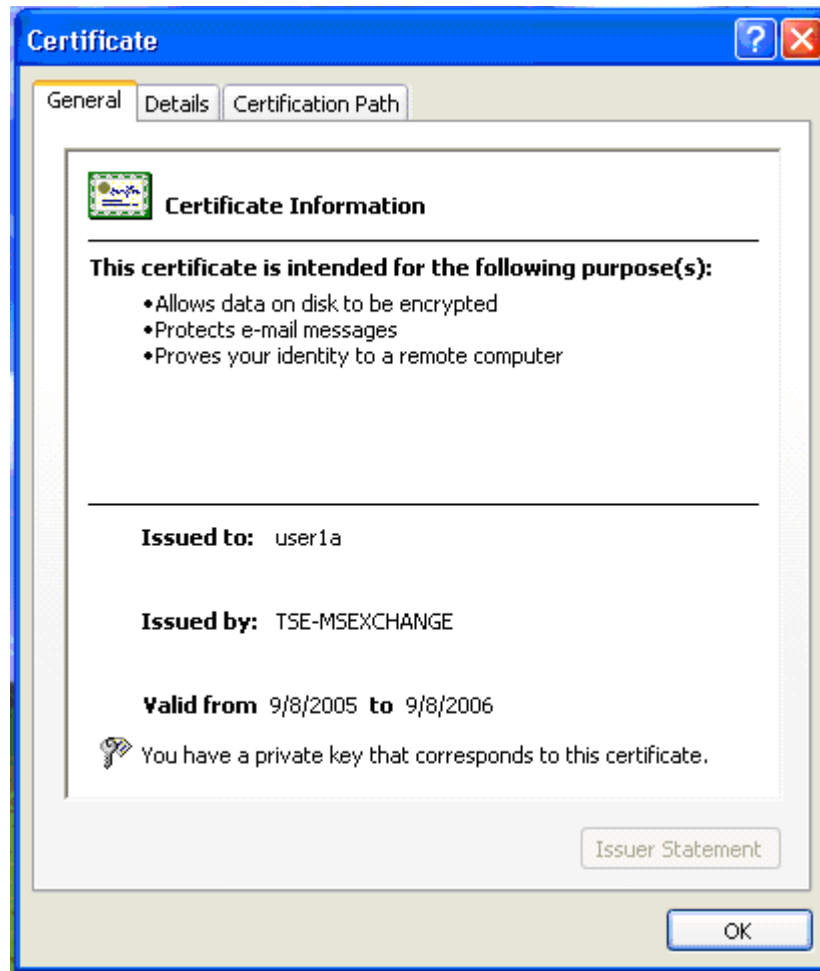
Figure B-6 Verify Certificate Installation

In the Certificates section, select the Certificates button. A screen appears listing the certificates issued and installed on the desktop/laptop PC.

Figure B-7 View a List of Installed Certificates



To view the details, highlight the certificate and click the **View** button.

Figure B-8 View the Details of a Certificate



Installing an X.509v3 PKI Certificate on the CS ACS

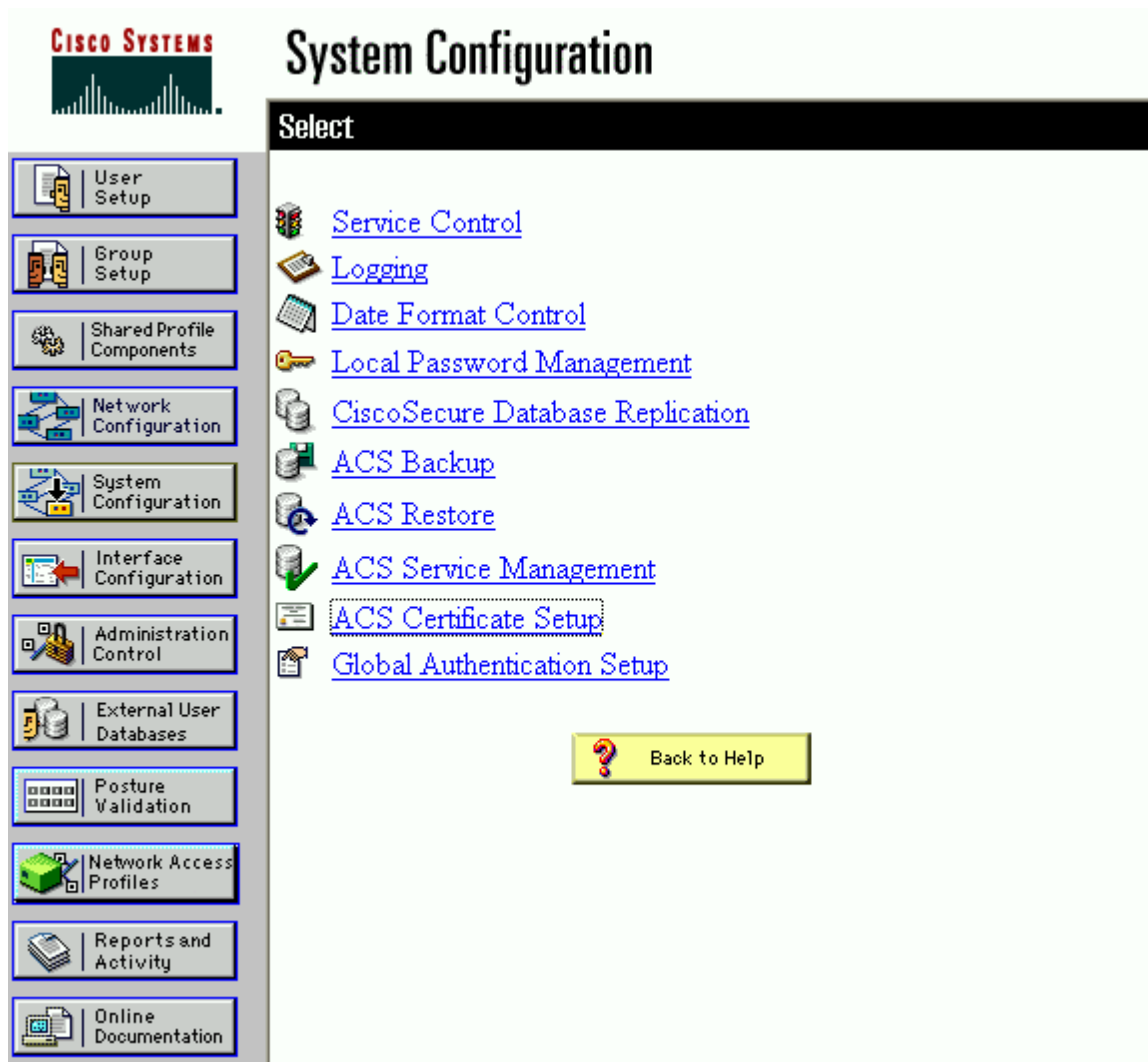
This appendix explains the process of installing an X.509 PKI certificate on a CiscoSecure ACS. The certificate is needed if EAP-TLS or PEAP is used as the authentication method with IEEE 802.1X.

The CiscoSecure ACS is running on Windows Server 2003 Enterprise Edition.

Select ACS Certificate Setup

Select System Configuration from the main menu. From the System Configuration menu, select ACS Certificate Setup.

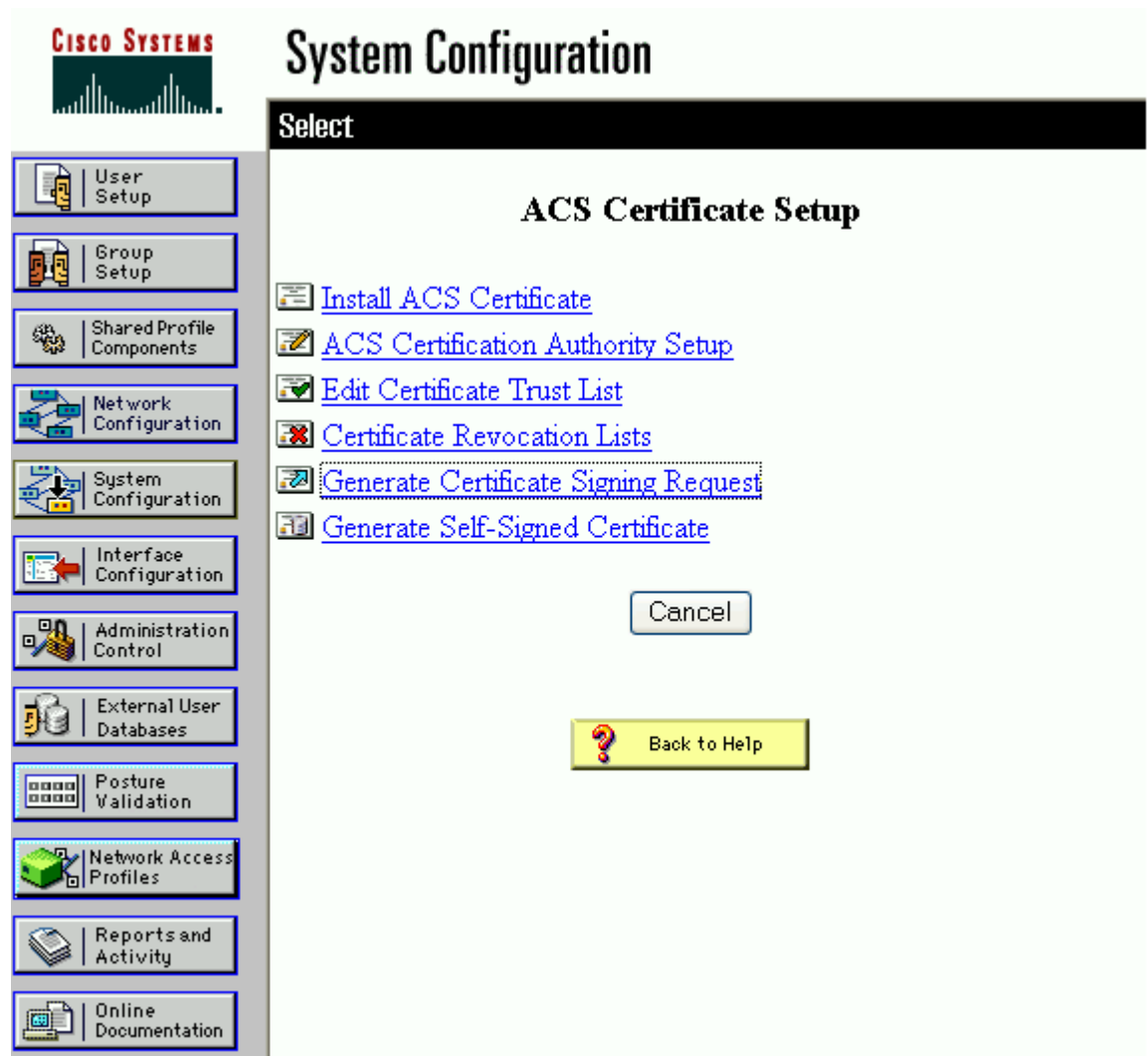
Figure C-1 Select ACS Certificate Setup



Select Generate Certificate Signing Request

From the ACS Certificate Setup menu, select Generate Certificate Signing Request.

Figure C-2 Select Generate Certificate Signing Request



Submit a Certificate Signing Request

Enter the common name value in the Certificate Subject box. The common name is a value that is part of a certificate and is required by ACS for the Certificate Subject value. Enter the complete directory path and file name in the Private key file box. For this scenario, C:\acs_server_cert\acs_server_cert.pvk was entered as the Private key file value.



Note

The administrator must choose or create a directory to store the private key file.

Enter a password in the Private key password box. Re-enter the same password in the Retype private key password box. Select the appropriate Key length and Digest to sign with value. This scenario used a Microsoft CA so a value of 1024 was used for the key length and SHA1 was used for the digest. Click **Submit**.

Figure C-3 Submit a Certificate Signing Request

The screenshot shows the Cisco System Configuration web interface. On the left is a navigation menu with icons and labels for various configuration areas: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'System Configuration' with an 'Edit' button. Below this is the 'Generate Certificate Signing Request' section. It contains a form titled 'Generate new request' with a help icon. The form fields are: 'Certificate subject' with value 'cn=TSE-ACS1', 'Private key file' with value 'c:\acs_server_cert\acs_', 'Private key password' with masked characters '.....', 'Retype private key password' with masked characters '.....', 'Key length' with a dropdown menu showing '1024 bits', and 'Digest to sign with' with a dropdown menu showing 'SHA1'. Below the form is a 'Back to Help' button. At the bottom of the form are 'Submit' and 'Cancel' buttons.

Copy the Certificate Signing Request

Copy the certificate signing request in the right frame. The information is used to request the ACS certificate.

Figure C-4 Copy the Certificate Signing Request

System Configuration

Edit

Generate Certificate Signing Request

Generate new request

Certificate subject: cn=TSE-ACS1

Private key file: c:\acs_server_cert\acs_

Private key password:

Retype private key password:

Key length: 1024 bits

Digest to sign with: SHA1

Back to Help

Submit Cancel

Now your certificate signing request is ready. You can copy/past certification authority enrollment tool.

```

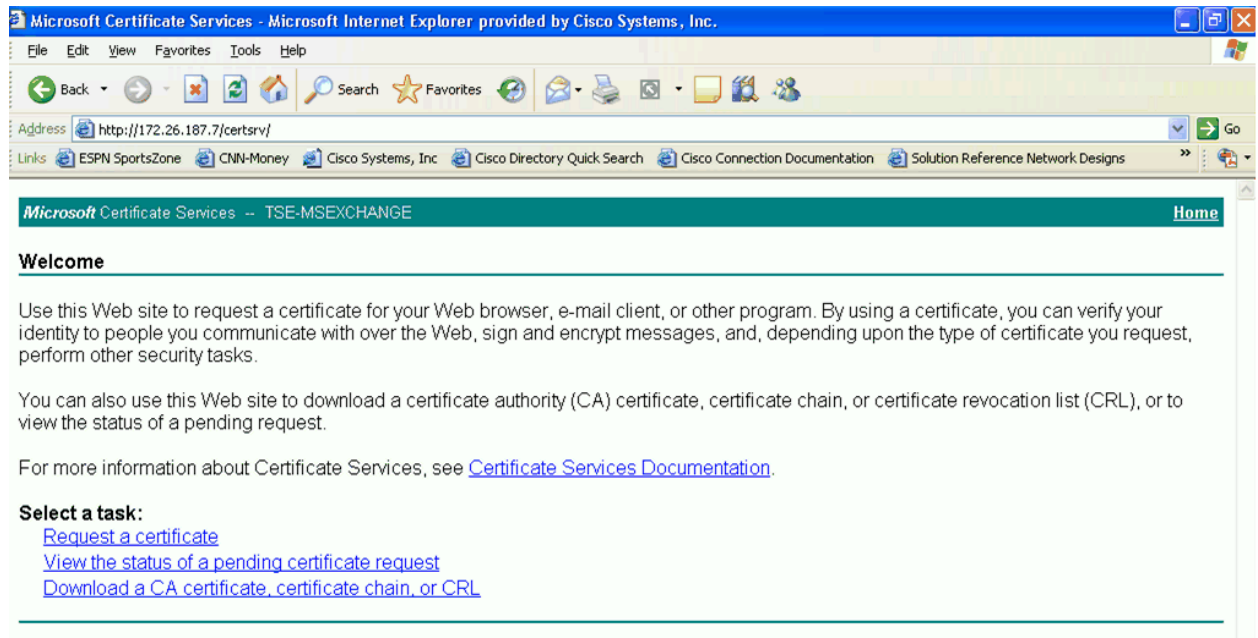
-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCAQAwEzERMA8GA1UEAxMIbVFNFLUFDUzEwZDQYJKo:
BQADgYOAAMIGJAoGBAMY/BELLEUXpgGNrNzaG5y3o7vxIRA4E4iAT1E:
bNyI9o0eTXCFZTESgskOzHfLTCJj1gBvOPXr8FD6gtMIjWxMsdUrcd:
2q+TYzq15B4WMUH5h8VVsD6OX9tR2adYIA8cWgbD5ENvQFR9FkYTxO:
AAGgZTBjBgkqhkiG9w0BCQ4xVjBUMAsGA1UdDwQEAwICrDAdBgNVHQ:
71SrSwOyVb/v1WAYkK/YBwkEwYDVRO1BAwwCgYIKwYBBQUHAAwEwEQ:
QgEBBAQDAgZAMAOGCSqGSIl3DQEBBQUAA4GBABaGy8991kTKt+eUOz:
Eg/Stjfa/obHgxcQaE5VswUZjDP8MzV1kDjOTh9EP3eqcGRpc3Q8Lw:
GxZGJxK6RZjmFctw85FyysYd3sInPG6nRg1031qWK8T84atDousTLf:
oEgAHuJZLQ2wRcsI
-----END CERTIFICATE REQUEST-----

```

Access the Certificate Authority

Open a web browser and enter the address of the Certificate Authority (CA):

<http://<CA address or hostname>/certsrv/>. Login when prompted to do so. On the Welcome screen, select the Request a Certificate link in the task list.

Figure C-5 Access the Certificate Authority

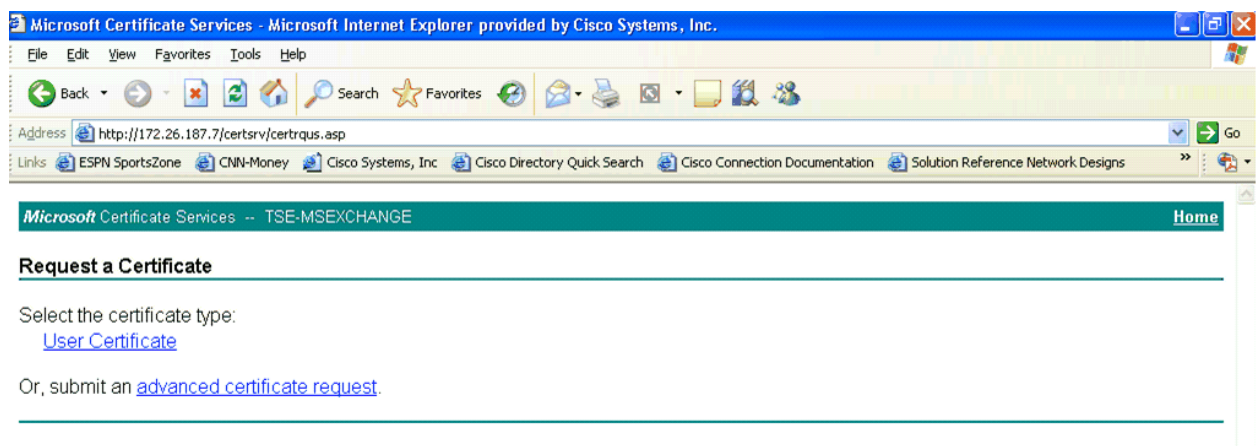
Request an Advanced Certificate

On the Request a Certificate screen, select the advanced certificate request option.



Note

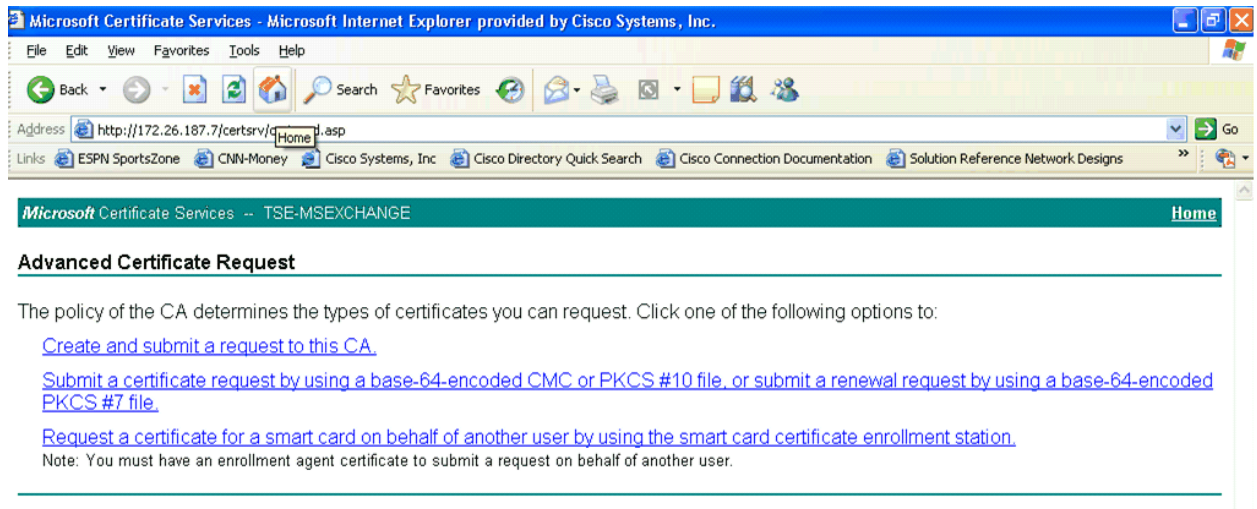
If prompted, click **Yes** to trust the server from which the certificate is requested.

Figure C-6 Request an Advanced Certificate

Submit a Certificate Request

Click **Submit a certificate request** by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Figure C-7 Submit a Certificate Request



Complete the Certificate Request

On the Submit a Certificate Request or Renewal Request, paste the certificate signing request into the Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7) box. Choose the Web Server Certificate Template. Click **Submit**.

Figure C-8 Complete the Certificate Request

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address <http://172.26.187.7/certsrv/certrqxt.asp> Go Links

Microsoft Certificate Services -- TSE-MSEXCHANGE [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
diE94KMqsEsP09qcxJuvHvIAPj7IT6/XfSXdvE4a
ugIj6NxEL4sSY6IAOrWnz8Tr6HbwnRXAistaKrY4
+1+FED9qtjeG+OMJksV3PGXLHuYv6kCVrInuGKIW
ltndkcRVkMv8bz4p&pLe/Pef6Wdf3bgzrx6wB/fE
wvcjo3fdgKBXqVM5w04AgtWHG58VY2b4PqLDyaNx
```

[Browse for a file to insert.](#)

Certificate Template:

Web Server

Additional Attributes:

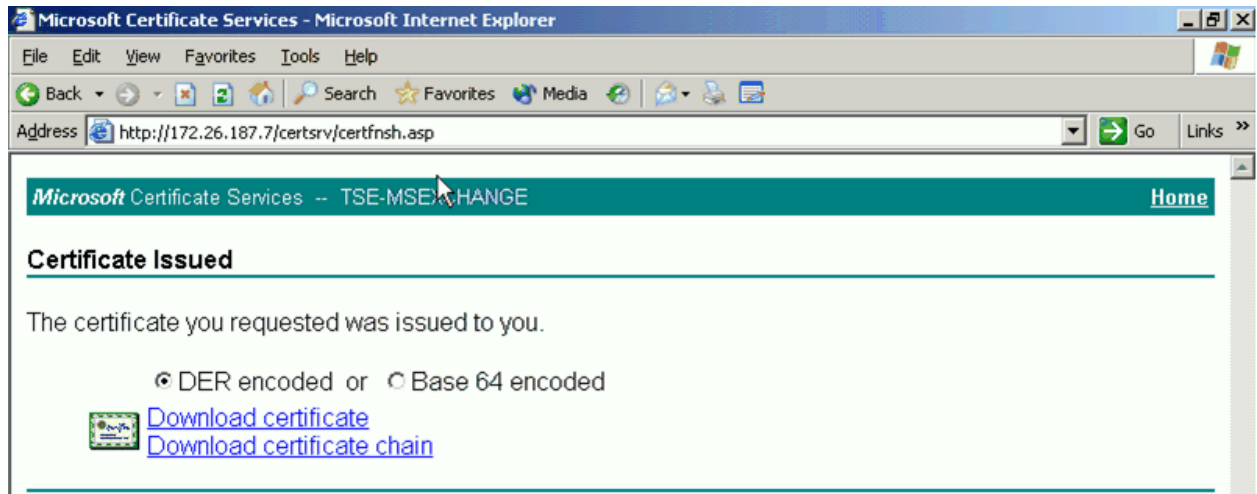
Download the Certificate onto ACS

Click **Download certificate** to save the certificate onto the ACS. The certificate chain may also be saved onto ACS by clicking the **Download certificate chain**.



Note

Save the certificate in the same directory as the private key file which was created in [Submit a Certificate Signing Request, page C-3](#).

Figure C-9 Download Certificate Issued

Install the Certificate onto ACS

Click **System Configuration** from the ACS main menu. Select ACS Certificate Setup from the System Configuration menu. Select Install ACS Certificate from the ACS Certificate Setup menu.

Select the Read certificate from file radio button and enter the complete path and file name for the certificate in the Certificate file box. This option is chosen for this scenario because the certificate file was already saved to the ACS in a previous step. Click **Submit**.

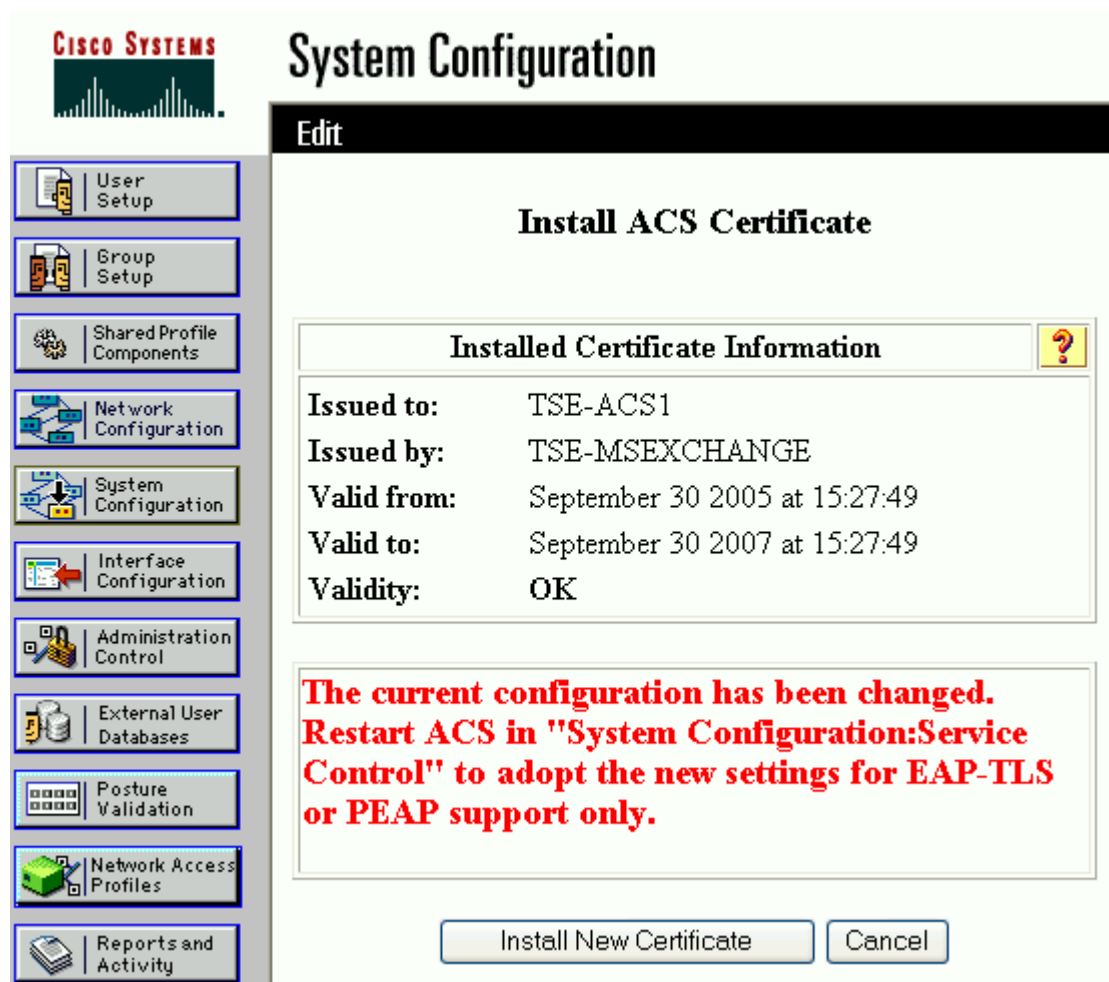
Figure C-10 Install the Certificate onto ACS

The screenshot shows the Cisco Systems System Configuration web interface. On the left is a vertical navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'System Configuration' with an 'Edit' button. Below this is the 'Install ACS Certificate' section. It contains a dialog box titled 'Install new certificate' with a help icon. The dialog has two radio buttons: 'Read certificate from file' (selected) and 'Use certificate from storage'. Under 'Read certificate from file', there is a 'Certificate file' text box containing '.server_cert\certnew.cer'. Under 'Use certificate from storage', there is a 'Certificate CN' text box. Below these are 'Private key file' (containing '.cert\acs_server_cert.pvk') and 'Private key password' (containing seven dots). A 'Back to Help' button with a question mark icon is located below the dialog. At the bottom of the main content area are 'Submit' and 'Cancel' buttons.

Verify ACS Certificate Installation

Once the certificate installation is complete, the Installed Certificate Information is displayed. To apply the configuration changes, select System Configuration from the ACS main menu. Next select Service Control from the System Configuration menu. Click **Restart** to apply the configuration changes.

Figure C-11 Verify ACS Certificate Installation





References

This appendix provides a list of references that were used to create this document.

Cisco Product Documentation

- Cisco Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEC
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sec/3750scg/index.htm>
- Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)SG
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_2_25s/conf/index.htm
- Catalyst 4000 Series Software Configuration Guide, 8.3 GLX and 8.4 GLX
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/8_3/configur/index.htm
- Catalyst 6500 Series Software Configuration Guide, 8.4
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_4/config_gd/index.htm
- Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.3(7)JA
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/acsspts/b1237ja/i1237sc/index.htm>
- Cisco Aironet 1200 Series EAP-FAST Deployment Guide
http://www.cisco.com/en/US/partner/products/hw/wireless/ps430/prod_configuration_guide09186a008046dc81.html
- User Guide for CiscoSecure ACS for Windows Server 4.0
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/

Partner Product Documentation

- Meetinghouse AEGIS Enterprise Client
http://store.mtghouse.com/newWeb/cgi-bin/products_aegis_enterprise.asp
- Funk Odyssey Client User and Administration Guide, 4.0
<http://www.funk.com/Docs/odyc40man.pdf>
- Microsoft – Define 802.1X Authentication for Wireless Networks on Client Computers
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/fe1d12a1-650a-4006-b389-e1f4ea68b991.msp>

Industry Standards

- RFC 1994 - PPP Challenge Handshake Authentication Protocol (CHAP)
<http://www.faqs.org/rfcs/rfc1994.html>
- RFC 2716 - PPP EAP TLS Authentication Protocol
<http://www.faqs.org/rfcs/rfc2716.html>
- RFC 2759 - Microsoft PPP CHAP Extensions, Version 2
<http://www.faqs.org/rfcs/rfc2759.html>
- DRAFT Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control (Revision)
<http://standards.ieee.org/reading/ieee/std/lanman/restricted/802.1X-2004.pdf>
- RFC 2865 - Remote Authentication Dial In User Service (RADIUS)
<http://www.faqs.org/rfcs/rfc2865.html>
- RFC 3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
<http://www.faqs.org/rfcs/rfc3580.html>
- RFC 3748 - Extensible Authentication Protocol (EAP)
<http://www.faqs.org/rfcs/rfc3748.html>
- Protected EAP Protocol (PEAP) Version 2
<http://www.faqs.org/ftp/pub/internet-drafts/draft-josefsson-pppext-eap-tls-eap-10.txt>
- EAP Flexible Authentication via Secure Tunneling (EAP-FAST)
<http://www.ietf.org/internet-drafts/draft-cam-winget-eap-fast-02.txt>