Cisco Secure Services Client with EAP−FAST Authentication

Document ID: 72788

Introduction

This document describes how to configure the Cisco Secure Services Client (CSSC) with the Wireless LAN controllers, Microsoft Windows 2000® software, and Cisco Secure Access Control Server (ACS) 4.0 through EAP−FAST. This document introduces the EAP−FAST architecture and provides deployment and configuration examples. CSSC is the client software component that provides the communication of user credentials to the infrastructure in order to authenticate a user to the network and assign appropriate access.

These are some of the advantages of the CSSC solution as outlined in this document:

- Authentication of each user (or device) prior to access permission to the WLAN/LAN with Extensible Authentication Protocol (EAP)
- End−to−end WLAN security solution with server, authenticator, and client components
- Common solution for wired and wireless authentication
- Dynamic, per user encryption keys derived in the authentication process
- No requirement for Public Key Infrastructure (PKI) or certificates (certificate verification optional)
- Access policy assignment and/or NAC−enabled EAP framework

Note: Refer to the Cisco SAFE Wireless Blueprint for information about the deployment of secure wireless.

The 802.1x authentication framework has been incorporated as part of the 802.11i (Wireless LAN Security)

standard to enable layer−2 based authentication, authorization, and accounting functions in an 802.11 wireless LAN network. Today, there are several EAP protocols available for deployment in both wired and wireless networks. Commonly deployed EAP protocols include LEAP, PEAP, and EAP−TLS. In addition to these protocols, Cisco has defined and implemented EAP Flexible Authentication through Secured Tunnel (EAP−FAST) protocol as a standards−based EAP protocol available for deployment in both wired and wireless LAN networks. The EAP−FAST protocol specification is publicly available on the IETF web site .

As with some other EAP protocols, EAP−FAST is a client−server security architecture that encrypts EAP transactions within a TLS tunnel. While similar to PEAP or EAP−TTLS in this respect, it differs in that EAP−FAST tunnel establishment is based upon strong shared secret keys that are unique to each user versus PEAP/EAP−TTLS (which use a server X.509 certificate to protect the authentication session). These shared secret keys are called Protected Access Credentials (PACs) and can 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 more efficient than handshakes based upon a PKI infrastructure, EAP−FAST is the fastest and less processor−intensive EAP type of those that provide protected authentication exchanges. EAP−FAST is also designed for simplicity of deployment since it does not require a certificate on the wireless LAN client or on the RADIUS infrastructure yet incorporates a built−in provisioning mechanism.

These are some of the major capabilities of the EAP−FAST protocol:

- Single sign−on (SSO) with Windows username/password
- Support for login script execution
- Wi−Fi Protected Access (WPA) support without third party supplicant (Windows 2000 and XP only)
- Simple deployment with no requirement for PKI infrastructure
- Windows Password Aging (that is, support for server−based password expiration)
- Integration with Cisco Trust Agent for Network Admission Control with appropriate client software

Prerequisites

Requirement

There is an assumption that the installer has knowledge of basic Windows 2003 installation and Cisco WLC installation since this document only covers the specific configurations to facilitate the tests.

For initial installation and configuration information for the Cisco 4400 Series Controllers, refer to the Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers. For initial installation and configuration information for the Cisco 2000 Series Controllers, refer to the Quick Start Guide: Cisco 2000 Series Wireless LAN Controllers.

Before you begin, install the Microsoft Windows Server 2000 with the latest service pack software. Install the controllers and lightweight access points (LAPs) and ensure that the latest software updates are configured.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2006 or 4400 Series Controller that runs 4.0.155.5
- Cisco 1242 LWAPP AP
- Windows 2000 with Active Directory
- Cisco Catalyst 3750G Switch
- Windows XP with CB21AG Adapter Card and Cisco Secure Services Client Version 4.05

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Design Parameters

Database

When you deploy a WLAN network and seek an authentication protocol, it is commonly desired to use a current database for user/machine authentication. Typical databases that can be used are Windows Active Directory, LDAP, or a One Time Password (OTP) database (that is, RSA or SecureID). All of these databases are compatible with the EAP−FAST protocol, but when you plan for deployment, there are some compatibility requirements that must be considered. The initial deployment of a PAC file to clients is accomplished through anonymous auto−provisioning, authenticated provisioning (through the current client X.509 certificate), or manual provisioning. For the purpose of this document, anonymous auto−provisioning and manual provisioning are considered.

Automatic PAC provisioning uses Authenticated Diffie−Hellman Key Agreement Protocol (ADHP) to establish a secure tunnel. The secure tunnel can be established either anonymously or through a server authentication mechanism. Within the established tunnel connection, MS−CHAPv2 is used to authenticate the client and, upon successful authentication, to distribute the PAC file to the client. After the PAC has been successfully provisioned, the PAC file can be used to initiate a new EAP−FAST authentication session in order to gain secure network access.

Automatic PAC provisioning is relevant to the database in use because, since the auto−provisioning mechanism relies upon MSCHAPv2, the database used to authenticate users must be compatible with this password format. If you use EAP−FAST with a database that does not support MSCHAPv2 format (such as OTP, Novell, or LDAP), it is required to employ some other mechanism (that is, manual provisioning or authenticated provisioning) to deploy user PAC files. This document gives an example of auto provisioning with a Windows user database.

Encryption

EAP−FAST authentication does not require the use a specific WLAN encryption type . The WLAN encryption type to be used is determined by the client NIC card capabilities. It is recommended to employ WPA2 (AES−CCM) or WPA(TKIP) encryption, dependent upon the NIC card capabilities in the specific deployment. Note that the Cisco WLAN solution allows the coexistence of both WPA2 and WPA client devices on a common SSID.

If the client devices do not support WPA2 or WPA, it is possible to deploy 802.1X authentication with dynamic WEP keys, but, due to the well−known exploits against WEP keys, this WLAN encryption mechanism is not recommended. If it is required to support WEP−only clients, it is recommended to employ a session−timeout interval, which requires that the clients derive a new WEP key on a frequent interval. Thirty minutes is the recommended session interval for typical WLAN data rates.

Single Sign−on and Machine Credentials

Single Sign−On refers to the ability of a single user sign−on or entry of authentication credentials to be used to access multiple applications or multiple devices. For the purposes of this document, Single Sign−On refers to the use of the credentials that are used to log on to a PC for authentication to the WLAN.

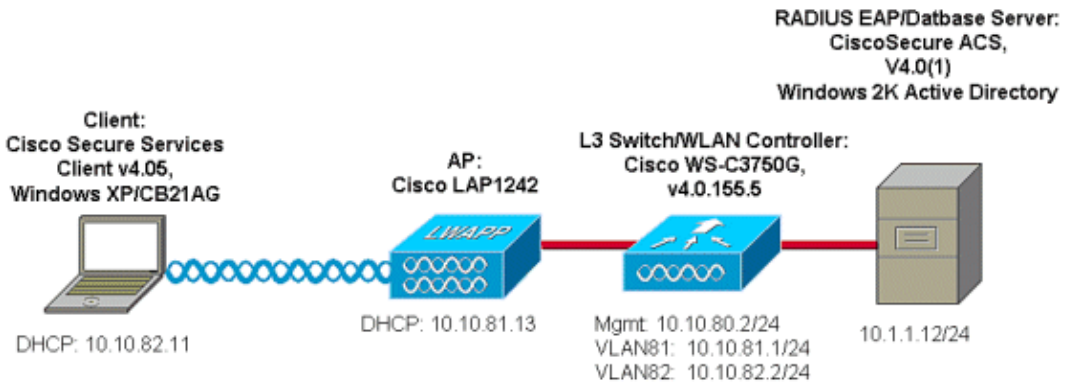
With the Cisco Secure Services Client, it is possible to use the logon credentials of a user to also authenticate

to the WLAN network. If it is desired to authenticate a PC to the network prior to the user logon to the PC, it is required to use either stored user credentials or credentials tied to a machine profile. Either of these methods is useful in cases where it is desired to run logon scripts or map drives when the PC boots up, as opposed to when a user logs on.

Network Diagram

This is the Network diagram used in this document. In this network, there are four subnets used. Note that it is not necessary to segment these devices into different networks, but this affords the most flexibility for integration with actual networks. The Catalyst 3750G Integrated Wireless LAN Controller provides Power Over Ethernet (POE) switchports, L3 switching, and WLAN Controller capability on a common chassis.

1. Network 10.1.1.0 is the server network where the ACS resides.
2. Network 10.10.80.0 is the management network used by the WLAN Controller.
3. Network 10.10.81.0 is the network where the APs reside.
4. Network 10.10.82.0 is used for the WLAN clients.



Configure the Access Control Server (ACS)

In this section, you are presented with the information to configure the features described in this document.

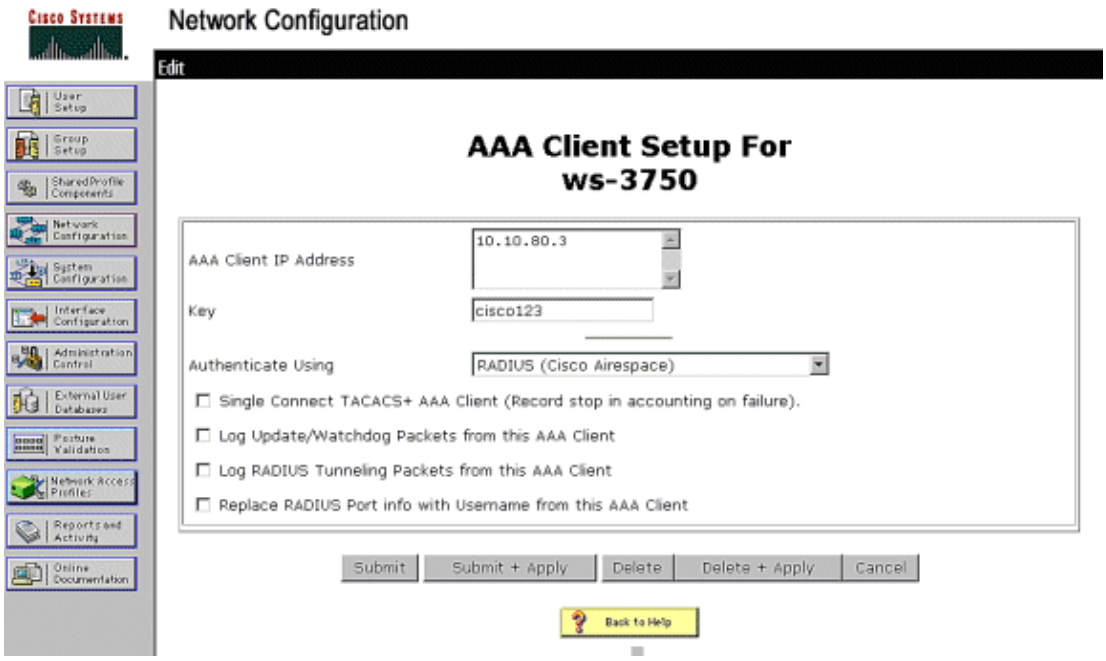
Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Add Access Point as AAA−Client (NAS) in ACS

This section describes how to configure ACS for EAP−FAST with in−band PAC provisioning with Windows Active Directory as the external database.

1. Log on to **ACS > Network Configuration** and click **Add Entry**.
2. Fill in the WLAN Controller name, IP address, shared secret key, and under Authenticate Using, choose RADIUS (Cisco Airespace), which also includes RADIUS IETF attributes.

   Note: If the Network Device Groups (NDG) are enabled, first choose the appropriate NDG and add the WLAN Controller to it. Refer to the ACS Configuration Guide for details about the NDG.
3. Click **Submit+ Restart**.

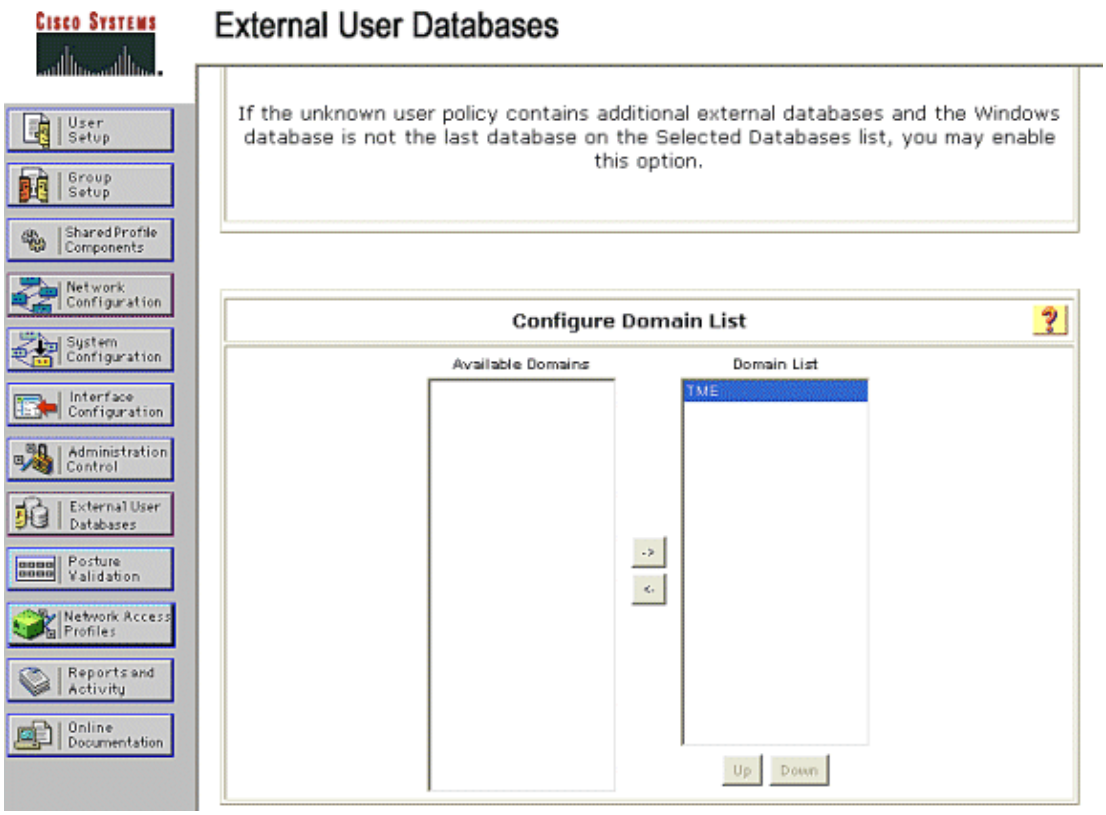


Configure ACS in Order to Query the External Database

This section describes how to configure the ACS in order to query the external database.

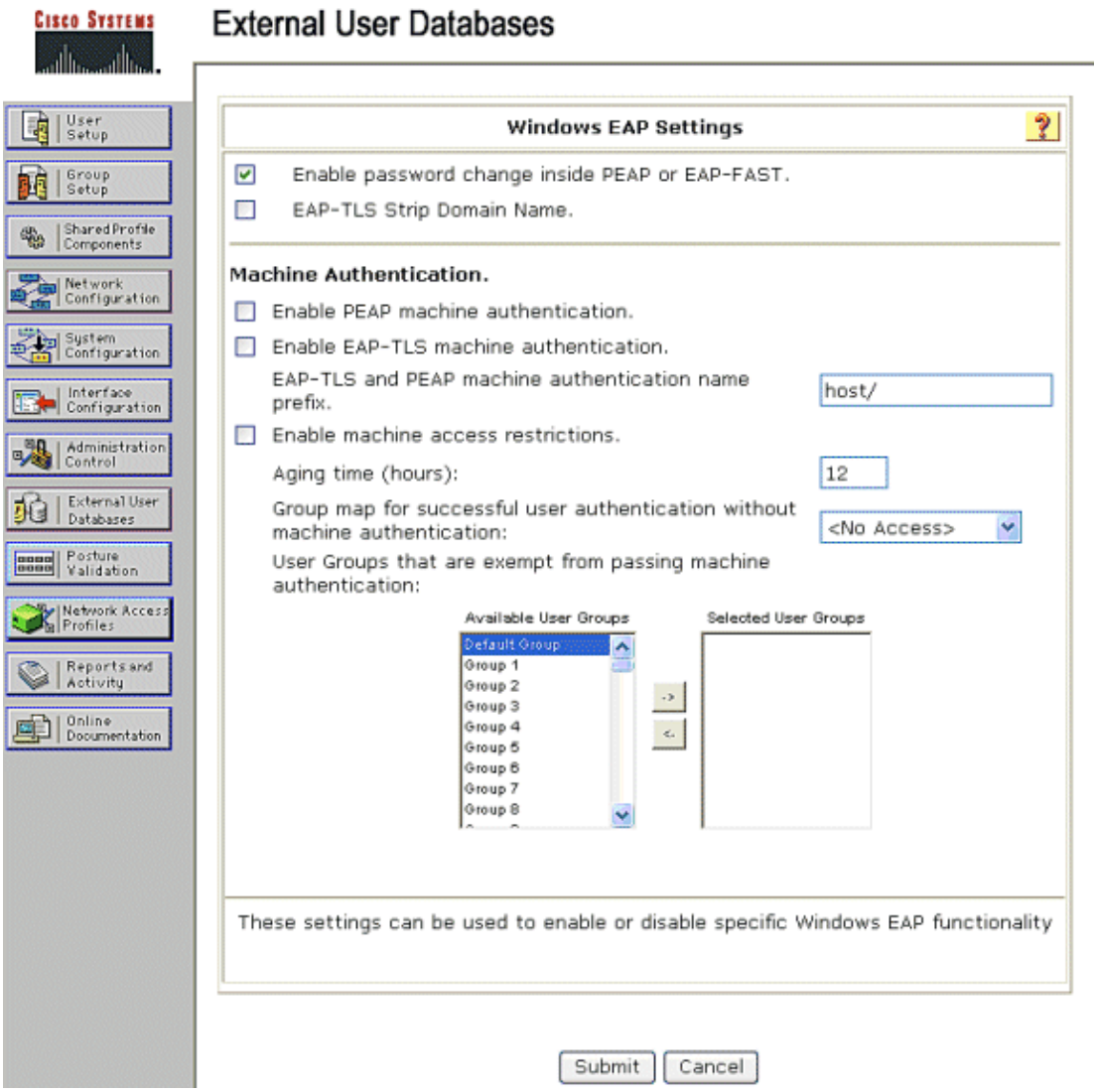
1. Click **External User Database > Database Configuration > Windows Database > Configure**.
2. Under Configure Domain List, move **Domains** from Available Domains to Domain List.

   Note: The server that runs the ACS must have knowledge of these domains in order for the ACS application to detect and use those domains for authentication purposes.



3. Under the Windows EAP Settings, configure the option to permit the password change inside PEAP or EAP−FAST session. Refer to the Configuration Guide for Cisco Secure ACS 4.1 in order to get more details about EAP−FAST and Windows Password aging.
4. Click **Submit**.

Note: You can also enable the Dialin Permission feature for EAP−FAST under the Windows User Database Configuration in order to permit the Windows external database to control access permission. The MS−CHAP Settings for password change on the Windows database configuration page are only applicable to non−EAP MS−CHAP authentication. In order to enable password change in conjunction with EAP−FAST, it is necessary to enable password change under the Windows EAP Settings.

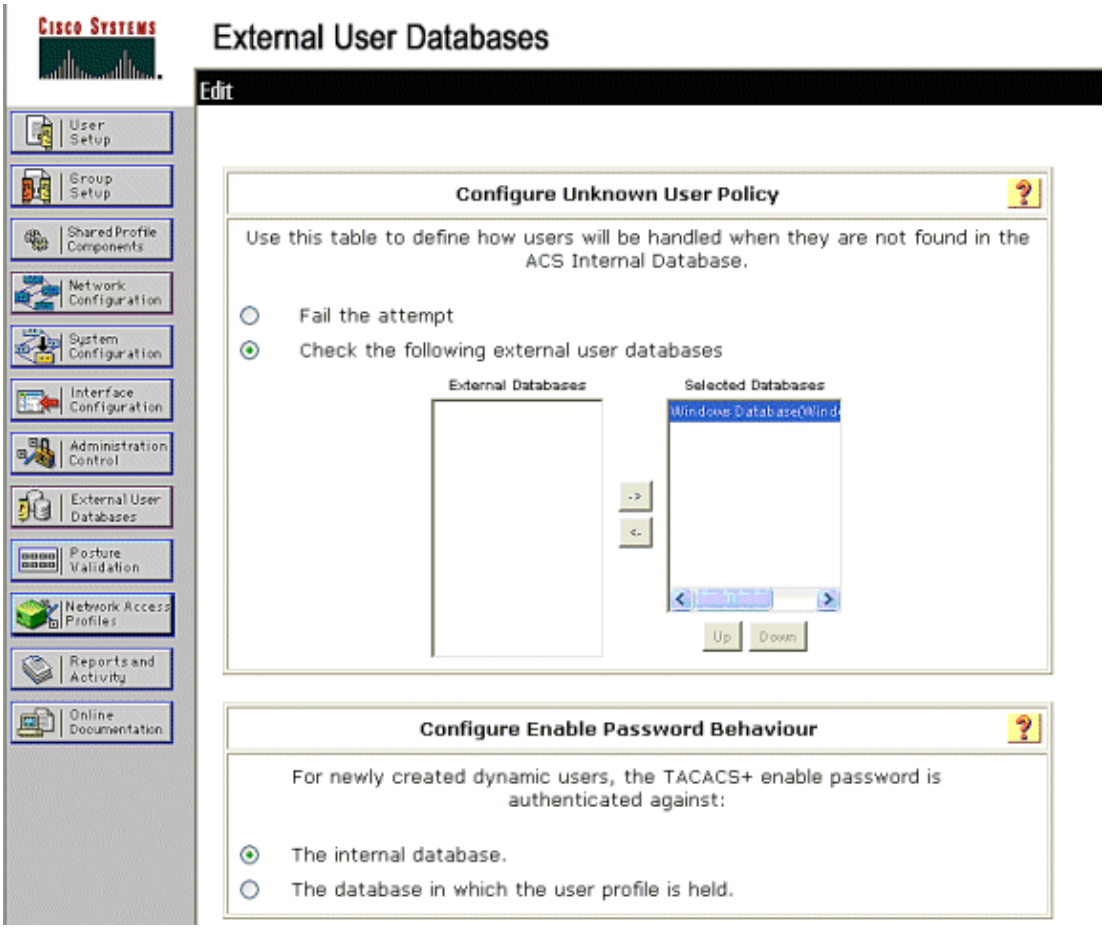


5. Click **External User Database > Unknown User Policy** and choose the **Check the following external user databases** radio button.
6. Move the Windows Database from **External Databases** to **Selected Databases**.
7. Click **Submit**.

Note: From this point on, the ACS checks the Windows DB. If the user is not found in the ACS local database, it places the user in the ACS default group. Refer to the ACS documentation for more details about Database Group Mappings.

Note: As the ACS queries the Microsoft Active Directory database to verify user credentials, additional access−rights settings need to be configured on Windows. Refer to the Installation Guide

for Cisco Secure ACS for Windows Server for details.



Enable EAP−FAST Support on the ACS

This section describes how to enable EAP−FAST support on the ACS.

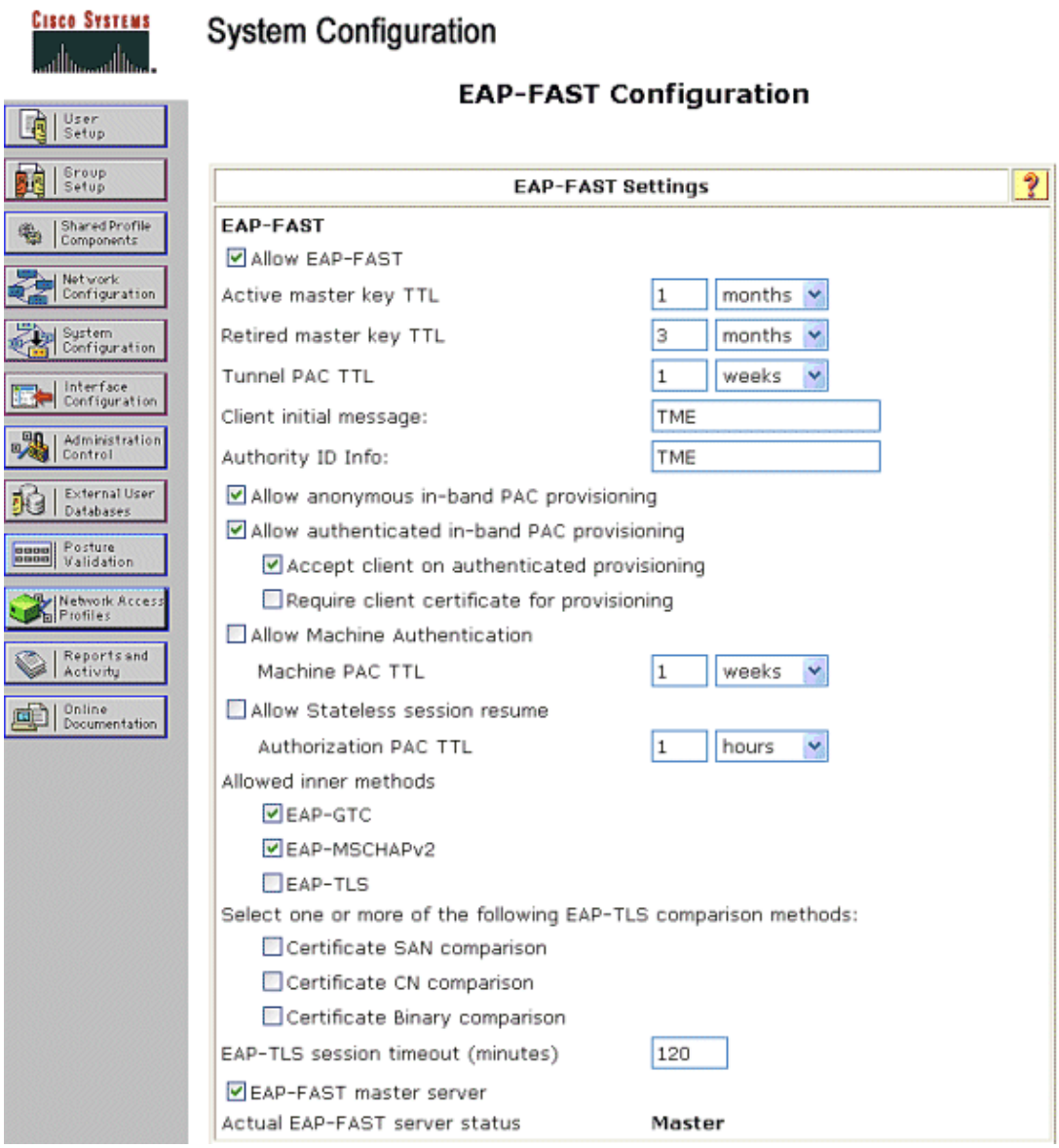
1. Go to **System Configuration > Global Authentication Setup > EAP−FAST Configuration**.
2. Choose **Allow EAP−FAST**.
3. Configure these recommendations: Master key TTL/ Retired master key TTL/ PAC TTL. These settings are configured by default in Cisco Secure ACS:

   - Master Key TTL:1 month
   - Retired Key TTL: 3 months
   - PAC TTL: 1 week
4. Fill out the **Authority ID Info** field. This text is shown on some EAP−FAST client software where selection of the PAC Authority is the controller.

   Note: The Cisco Secure Services Client does not employ this descriptive text for the PAC authority.
5. Choose the **Allow in−band PAC provisioning** field. This field enables Automatic PAC Provisioning for properly−enabled EAP−FAST clients. For this example, auto−provisioning is employed.
6. Choose **Allowed inner methods**: EAP−GTC and EAP−MSCHAP2. This permits the operation of both EAP−FAST v1 and EAP−FAST v1a clients. (Cisco Secure Services Client supports EAP−FAST v1a.) If it is not necessary to support EAP−FAST v1 clients, it is only necessary to enable EAP−MSCHAPv2 as an inner method.
7. Choose the **EAP−FAST Master Server** checkbox to enable this EAP−FAST server as the master. This permits other ACS servers to utilize this server as the master PAC authority to avoid the provision of unique keys for each ACS in a network. Refer to the ACS Configuration Guide for

details.

8. Click **Submit+Restart**.



Cisco WLAN Controller

For the purposes of this Deployment Guide, a Cisco WS3750G Integrated Wireless LAN Controller (WLC) is used with Cisco AP1240 Lightweight APs (LAP) to provide the WLAN infrastructure for CSSC tests. The configuration is applicable for any Cisco WLAN controller. The software version employed is 4.0.155.5.

Configure the Wireless LAN Controller

Basic Operation and Registration of LAP to the Controller

Use the startup configuration wizard on the command−line interface (CLI) in order to configure the WLC for basic operation. Alternatively, you can use the GUI in order to configure the WLC. This document explains the configuration on the WLC with the startup configuration wizard on the CLI.

After the WLC boots for the first time, it enters into the startup configuration wizard. Use the configuration wizard to configure basic settings. You can access the wizard through the CLI or the GUI. This output shows

an example of the startup configuration wizard on the CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration.
```

These parameters set up the WLC for basic operation. In this example configuration, the WLC uses **10.10.80.3** as the management interface IP address and **10.10.80.4** as the AP−manager interface IP address.

Before any other features can be configured on the WLCs, the LAPs have to register with the WLC. This document assumes that the LAP is registered to the WLC. Refer to the Register the Lightweight AP to the WLCs section of WLAN Controller Failover for Lightweight Access Points Configuration Example for information on how the Lightweight APs register with the WLC. For reference with this configuration example, the AP1240s are deployed on a separate subnet (10.10.81.0/24) from the WLAN controller (10.10.80.0/24), and DHCP option 43 is used to provide for controller discovery.

RADIUS Authentication Through Cisco Secure ACS

The WLC needs to be configured to forward the user credentials to the Cisco Secure ACS server. The ACS server then validates the user credentials (through the configured Windows database) and provides access to the wireless clients.

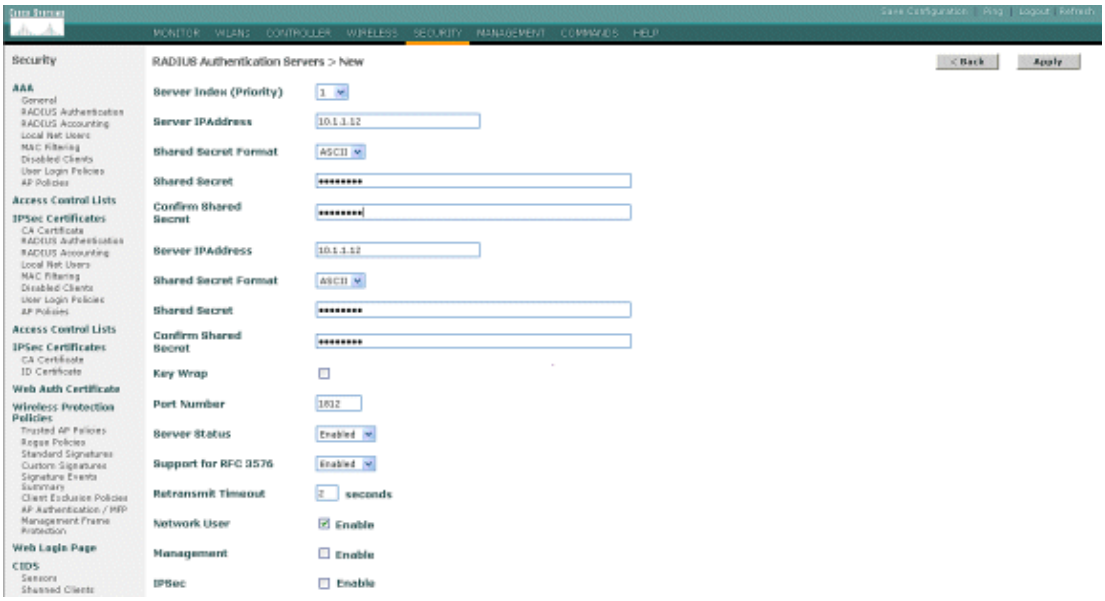
Complete these steps to configure the WLC for communication to the ACS server:

1. Click **Security** and **RADIUS Authentication** from the controller GUI to display the RADIUS Authentication Servers page. Then click **New** to define the ACS server.

2. Define the ACS server parameters in the RADIUS Authentication Servers > New page. These parameters include the ACS IP Address, Shared Secret, Port Number, and Server Status.

   Note: The port numbers 1645 or 1812 are compatible with ACS for RADIUS authentication.

   The Network User and Management check boxes determine if the RADIUS−based authentication applies for network users (for example, WLAN clients) and management (that is, administrative users). The example configuration uses the Cisco Secure ACS as the RADIUS server with IP address 10.1.1.12:



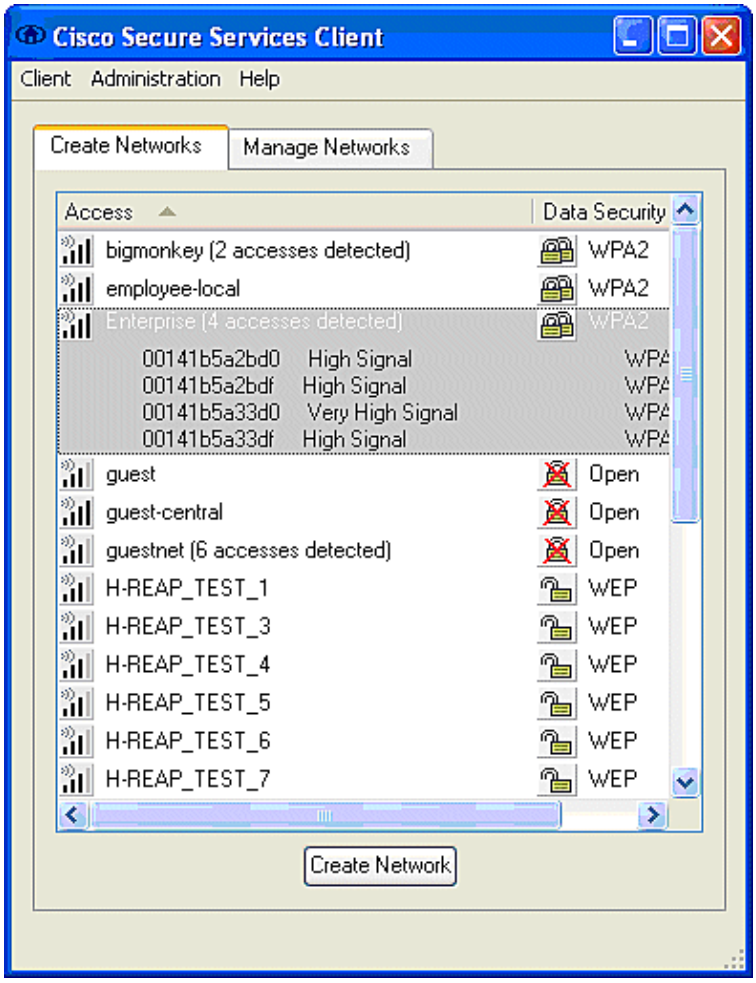
Configuration of the WLAN Parameters

This section describes the configuration of the Cisco Secure Services Client. In this example, CSSC v4.0.5.4783 is used with a Cisco CB21AG client adapter. Prior to the installation of the CSSC software, verify that only the drivers for the CB21AG are installed, not the Aironet Desktop Utility (ADU).

Once the software is installed and it runs as a service, it scans for available networks and displays those available.

Note: CSSC disables Windows Zero Config.

Note: Only those SSID that are enabled for broadcast are visible.



Note: The WLAN Controller, by default, broadcasts the SSID, so it is shown in the Create Networks list of scanned SSIDs. In order to create a Network Profile, you can simply click the **SSID** in the list (Enterprise) and the **Create Network** radio button.

If the WLAN infrastructure is configured with broadcast SSID disabled, you must manually add the SSID; click the **Add** radio button under Access Devices and manually enter the appropriate **SSID** (for example, Enterprise). Configure Active probe behavior for the client, that is, where the client actively probes for its configured SSID; specify **Actively search for this access device** after you enter the SSID on the Add Access Device window.

Note: The port settings do not permit enterprise modes (802.1X) if the EAP authentication settings are not first configured for the profile.

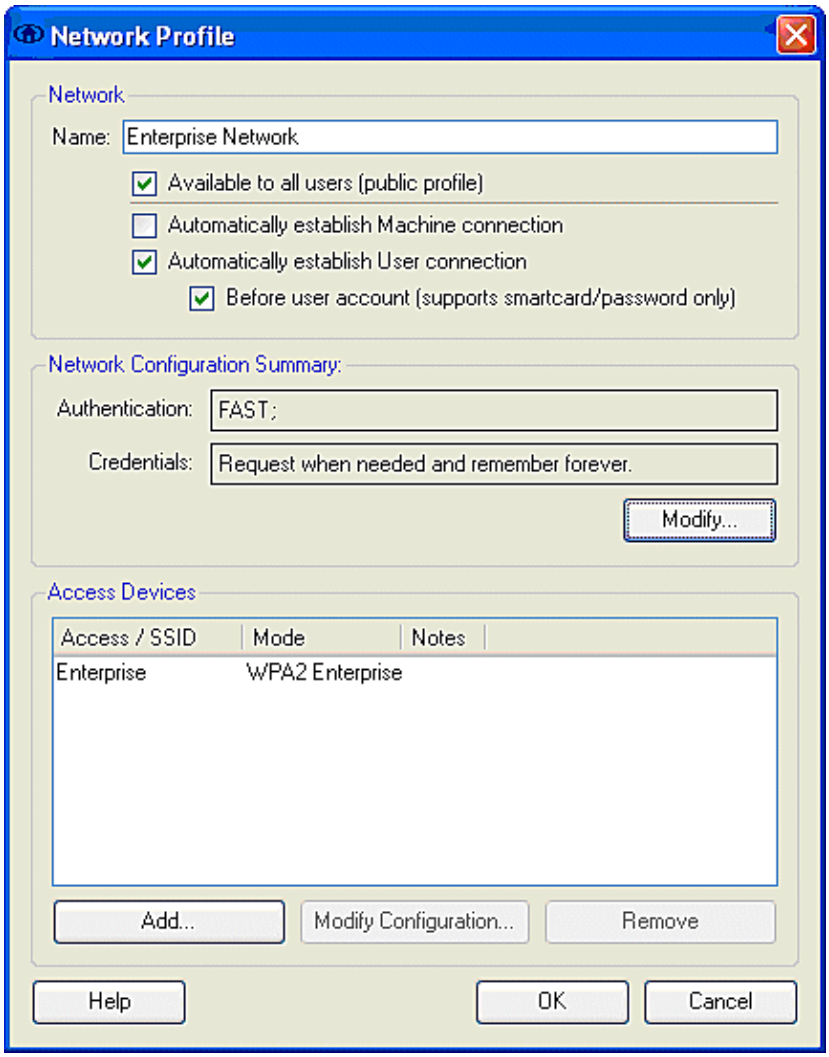
The **Create Network** radio button launches the Network Profile window, which permits you to associate the chosen (or configured) SSID with an authentication mechanism. Assign a descriptive name for the profile.

Note: Multiple WLAN security types and/or SSIDs can be associated under this authentication profile.

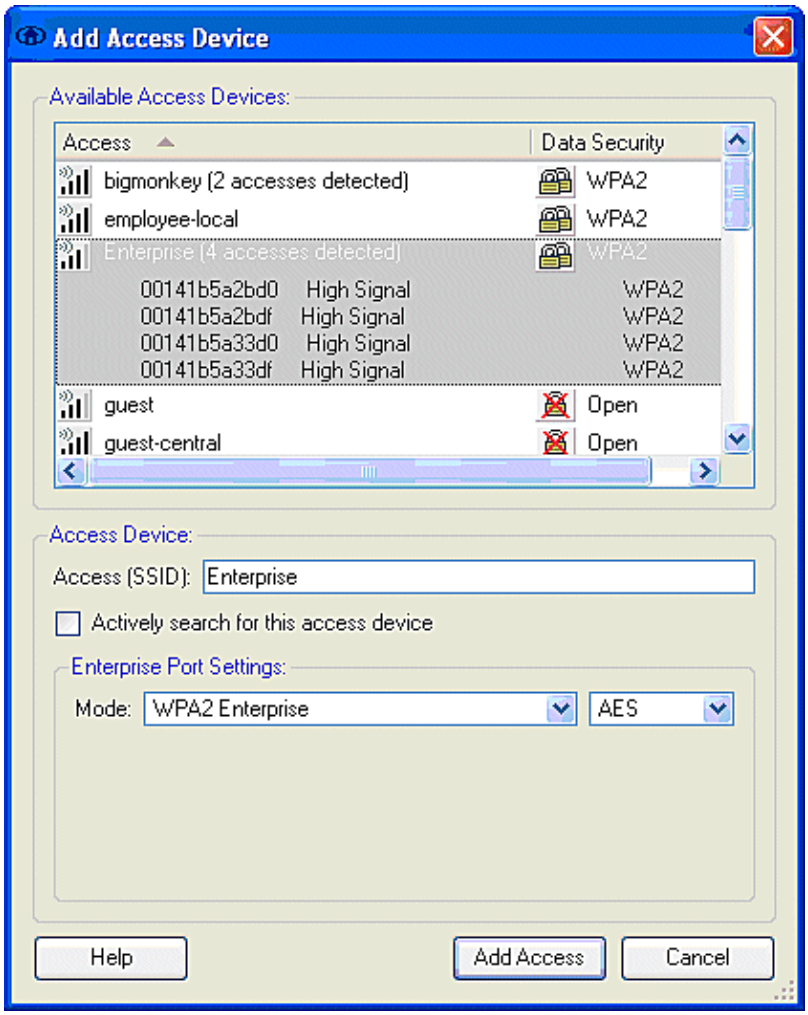
In order to have the client to automatically connect to the network when in RF coverage range, choose **Automatically establish User connection**. Uncheck **Available to all users** if it is not desirable to use this profile with other user accounts on the machine. If **Automatically establish** is not chosen, it is necessary for the user to open the CSSC window and manually initiate the WLAN connection with the **Connect** radio button.

If it is desired to initiate the WLAN connection prior to the user log on, choose **Before user account**. This

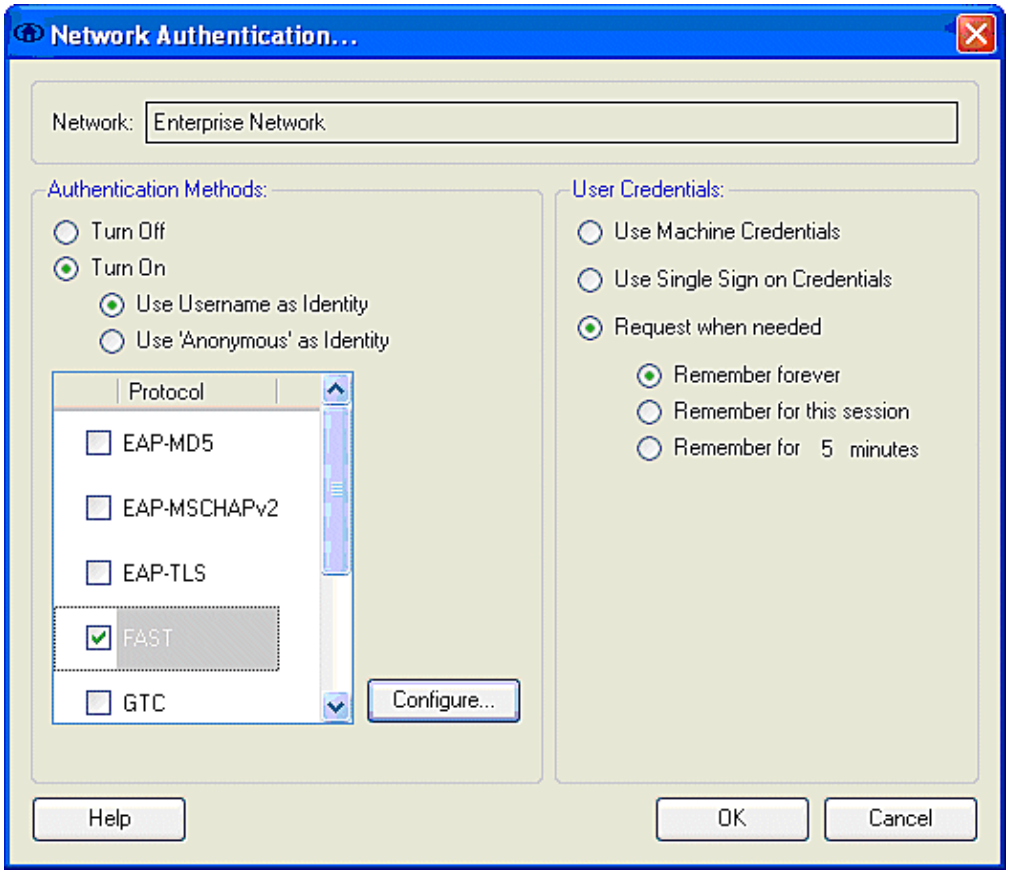
permits Single−Sign−On operation with saved user credentials (password or certificate/Smartcard when you use TLS within EAP−FAST).



Note: For WPA/TKIP operation with the Cisco Aironet 350 Series Client Adapter, it is necessary to disable the WPA handshake validation since there is currently an incompatibility between the CSSC client and 350 drivers with respect to the WPA handshake hash validation. This is disabled under **Client > Advanced Settings > WPA/WPA2 Handshake Validation**. The disabled handshake validation still permits the security features inherent in WPA (TKIP per−packet keying and Message Integrity Check), but disables the initial WPA key authentication.



Under Network Configuration Summary, click **Modify** to configure the EAP / credentials settings. Specify **Turn On** Authentication, Choose **FAST** under Protocol, and choose **'Anonymous' as Identity** (in order to use no username inthe initial EAP request). It is possible to use the **Use Username as Identity**as the outer EAP identity, but many customers do not wish to expose the user IDs in the initial unencrypted EAP request. Specify **Use Single Sign on Credentials** to use log on credentials for network authentication. Click **Configure** to set up EAP−FAST parameters.



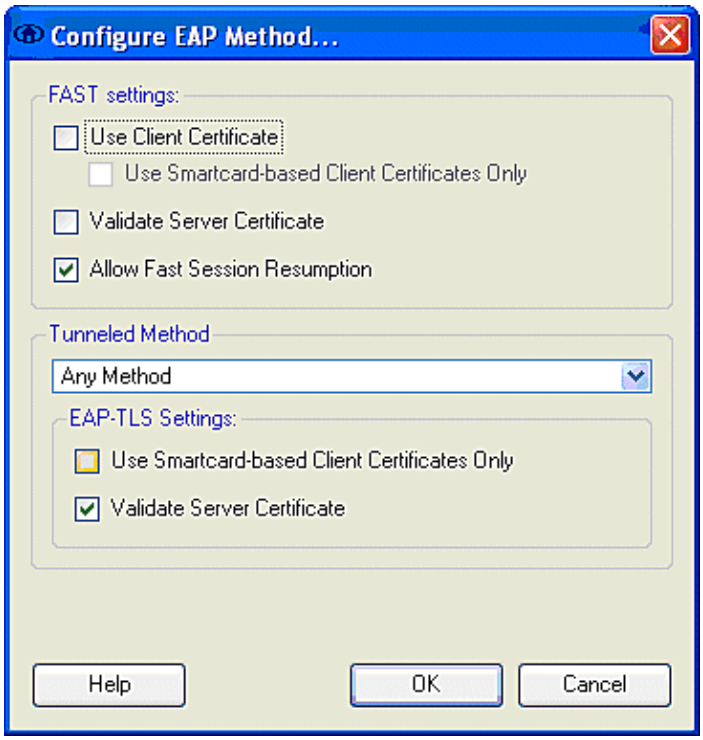
Under FAST settings, it is possible to specify **Validate Server Certificate**, which permits the client to validate the EAP−FAST server (ACS) certificate prior to the establishment of an EAP−FAST session. This provides protection for the client devices from connection to an unknown or rogue EAP−FAST server and inadvertent submittal of their authentication credentials to an untrusted source. This does require that the ACS server have a certificate installed and the client also has the correspondent Root Certificate Authority certificate installed. In this example, server certificate validation is not enabled.

Under FAST settings, it is possible to specify **Allow Fast Session Resumption**, which permits the resumption of an EAP−FAST session based upon the tunnel (TLS session) information rather than the requirement of a full EAP−FAST reauthentication. If the EAP−FAST server and client have common knowledge of the TLS session information negotiated within the initial EAP−FAST authentication exchange, session resumption can occur.

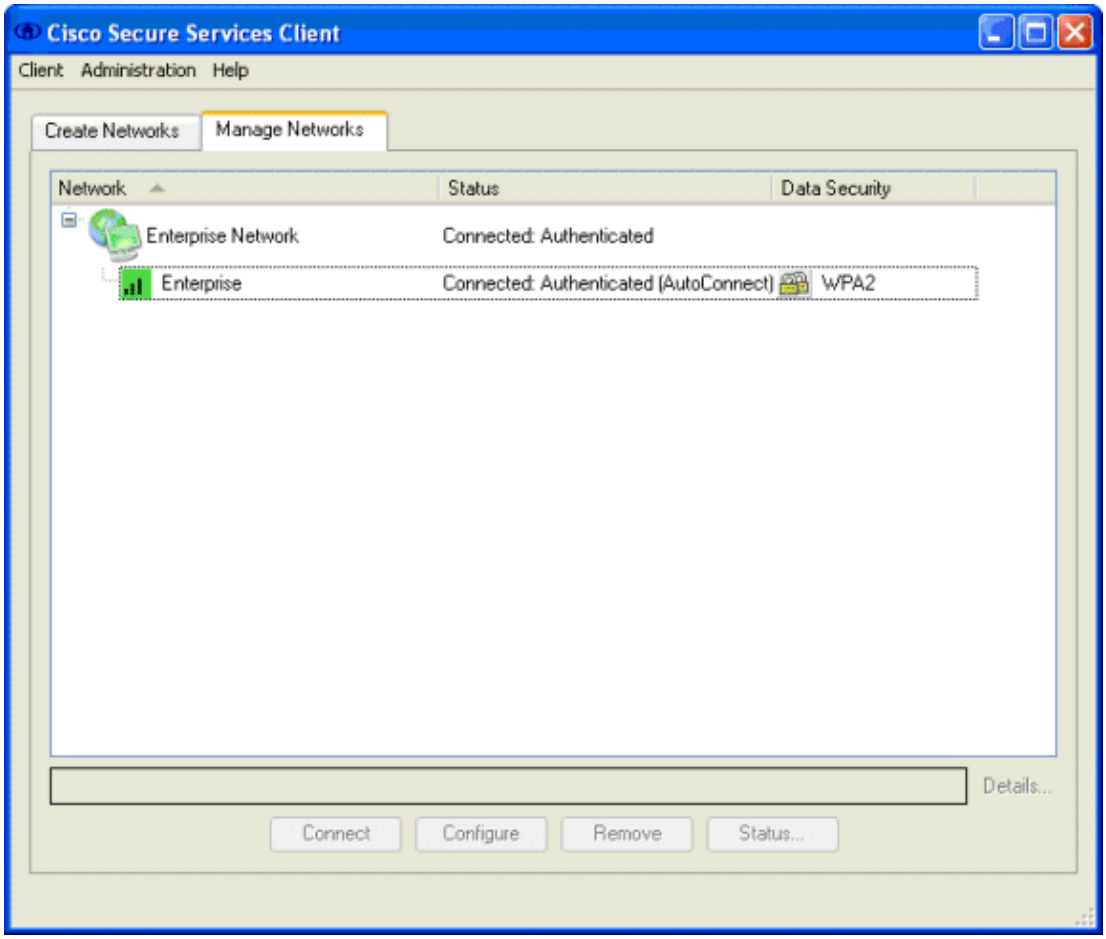
Note: Both EAP−FAST server and client must be configured for EAP−FAST session resume.

Under Tunneled Method > EAP−TLS Settings, specify **Any Method** to permit the EAP−MSCHAPv2 for PAC auto−provision and EAP−GTC for authentication. If you use a Microsoft−format database, such as Active Directory, and if if does not support any EAP−FAST v1 clients on the network, you can also specify the use of only **MSCHAPv2** as the Tunneled Method.

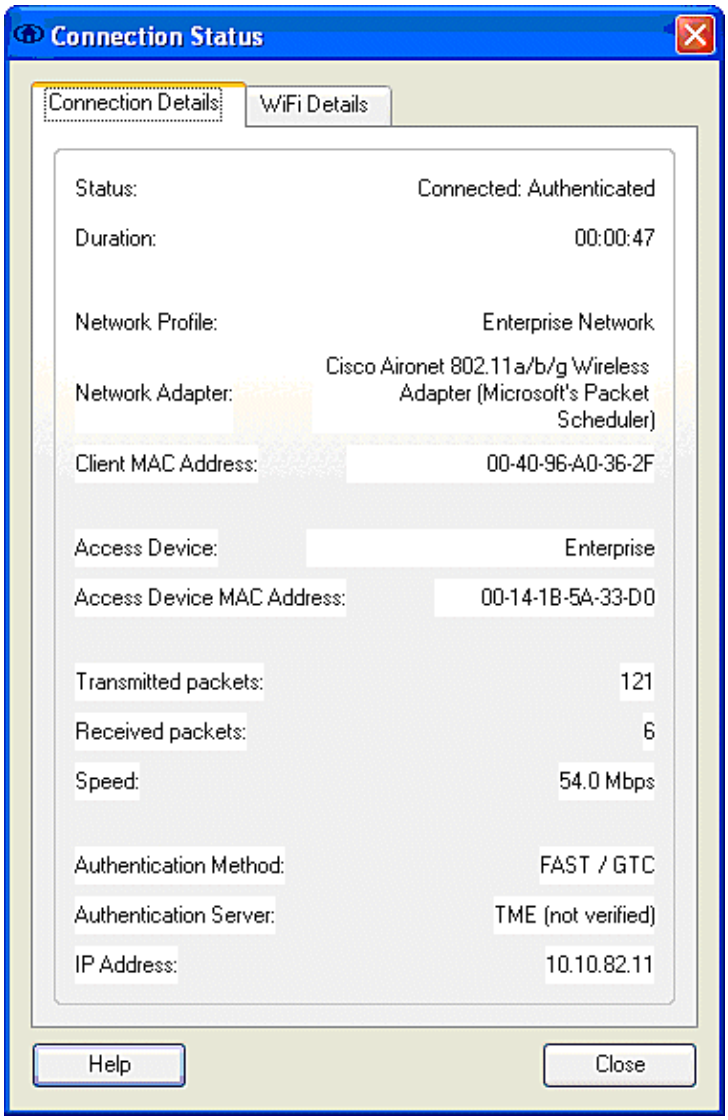
Note: Validate Server Certificate is enabled by default under the EAP−TLS settings on this window. Since the example does not use EAP−TLS as the inner authentication method, this field is not applicable. If this field is enabled, it enables the client to validate the server certificate in addition to the server validation of the client certificate within EAP−TLS.

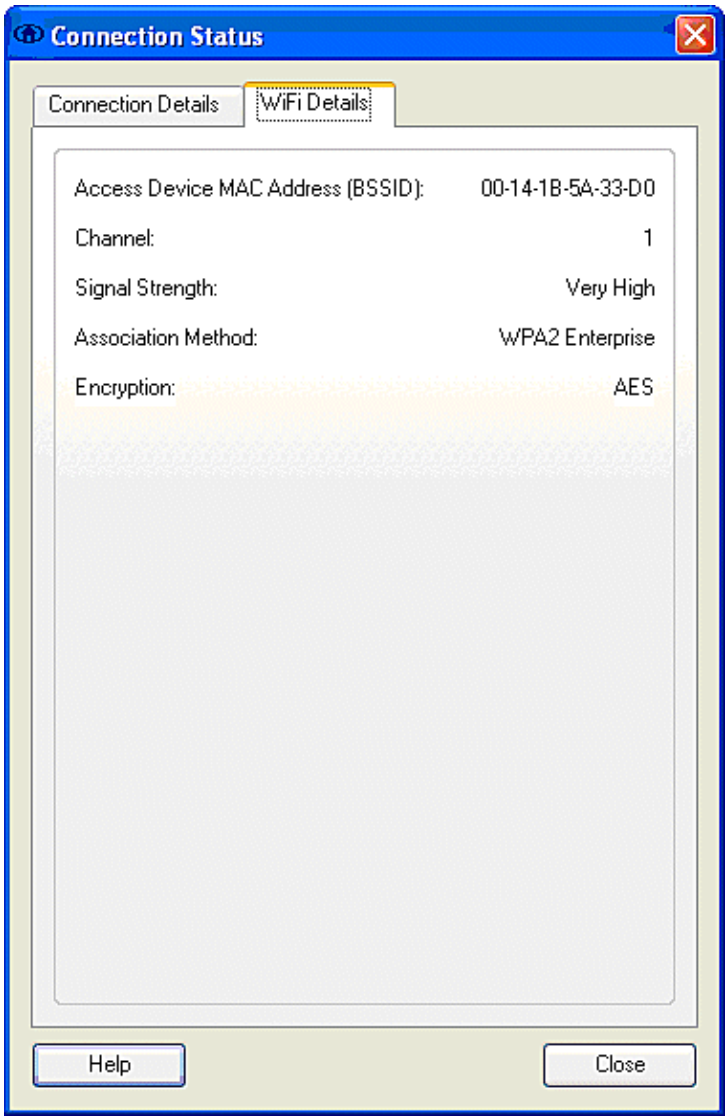


Click **OK** to save the EAP−FAST settings. Since the client is configured for "automatically establish" under profile, it automatically initiates association/authentication with the network. From the Manage Networks tab, the Network, Status, and Data Security fields indicate the connection status of the client. From the example, it is seen that the Profile Enterprise Network is in use, and the Network Access Device is the SSID Enterprise, which indicates Connected:Authenticated and uses Autoconnect. The Data Security field indicates the 802.11 encryption type that is employed, which, for this example, is WPA2.



After the client authenticates, choose **SSID** under the Profile in the Manage Networks tab and click **Status** to query connection details. The Connection Details window provides information on the client device, connection status and statistics, and authentication method. The WiFi Details tab provides details on the 802.11 connection status, which includes the RSSI, 802.11 channel, and authentication/encryption.


Connection Status
Connection Details
WiFi Details
Status:
Connected: Authenticated
Duration:
00:00:47
Network Profile:
Enterprise Network
Network Adapter:
Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:
00-40-96-A0-36-2F
Access Device:
Enterprise
Access Device MAC Address:
00-14-1B-5A-33-D0
Transmitted packets:
121
Received packets:
6
Speed:
54.0 Mbps
Authentication Method:
FAST / GTC
Authentication Server:
TME (not verified)
IP Address:
10.10.82.11
Help
Close



As a system administrator, you are entitled to the diagnostic utility, Cisco Secure Services Client System Report, which is available with the standard CSSC distribution. This utility is available from the start menu or from the CSSC directory. In order to obtain data, click **Collect Data > Copy to Clipboard > Locate Report File**. This directs a Microsoft File Explorer window to the directory with the zipped report file. Within the zipped file, the most useful data is located under log (log_current).

The utility gives the current status of CSSC, interface, and driver details, along with the WLAN information (SSID detected, association status, etc.). This can be useful, especially to diagnose connectivity issues between CSSC and the WLAN adapter.

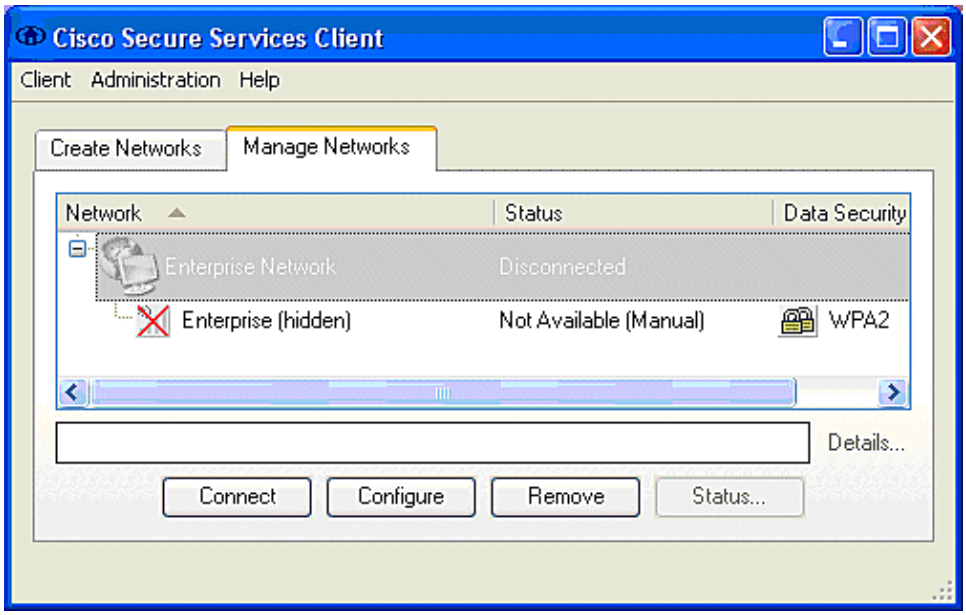
Verify Operation

After the configuration of the Cisco Secure ACS server, WLAN controller, CSSC client, and presumably correct configuration and database population, the WLAN network is configured for EAP−FAST authentication and secure client communication. There are numerous points that can be monitored to check the progress / errors for a secure session.

In order to test the configuration, attempt to associate a wireless client with the WLAN Controller with EAP−FAST authentication.

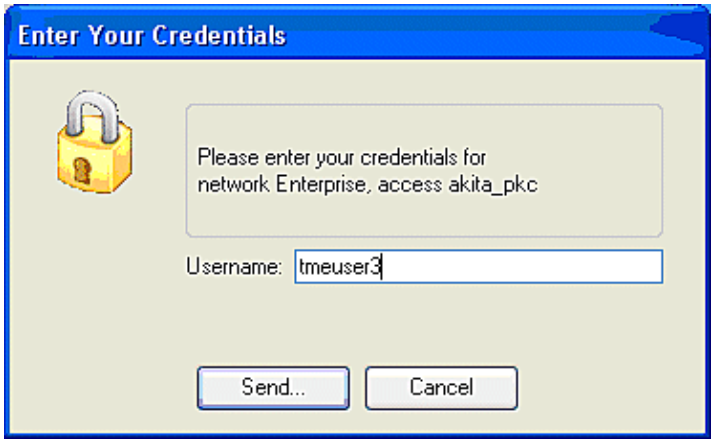
1. If CSSC is configured for Auto−Connection, the client attempts this connection automatically. If it is not configured for Auto−Connection and Single Sign−on operation, the user must initiate the WLAN connection through the **Connect** radio button. This initiates the 802.11 association process over which the EAP authentication occurs.

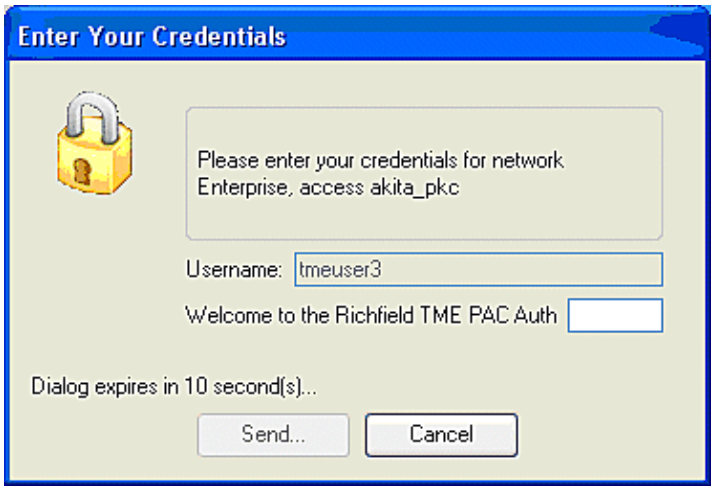
   This is an example:



2. The user is subsequently prompted to provide the username and then the password for the EAP−FAST authentication (from the EAP−FAST PAC Authority or ACS).

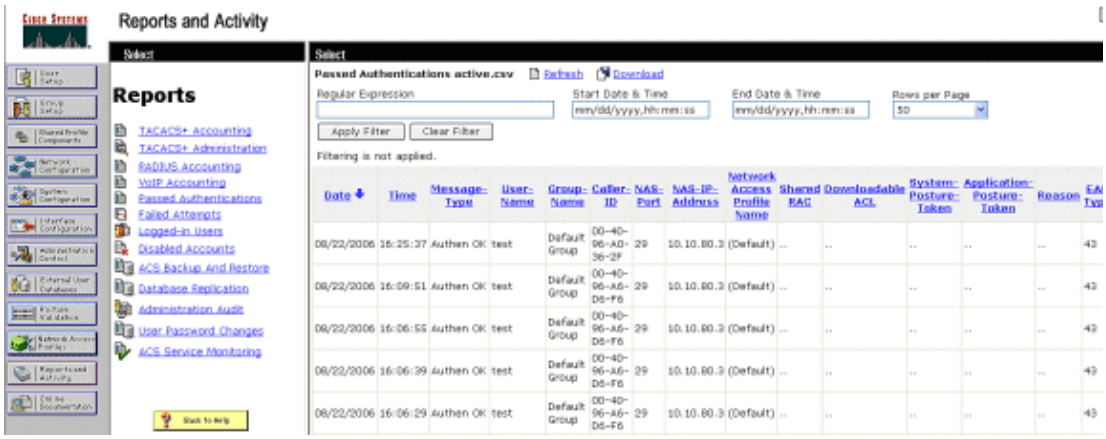
   This is an example:



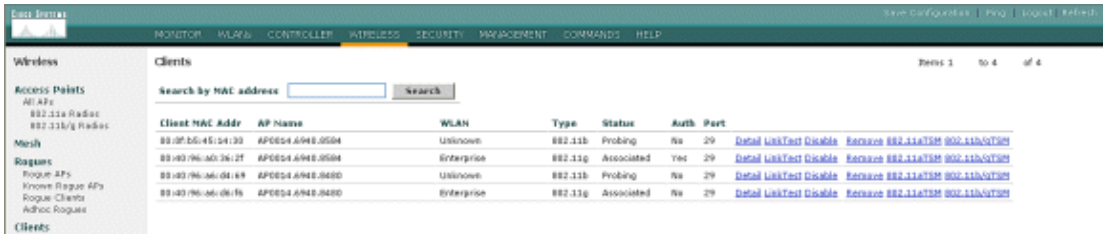


3. The CSSC client, by way of the WLC, then passes the user credentials to the RADIUS server (Cisco Secure ACS) in order to validate the credentials. ACS verifies the user credentials with a comparison of the data and the configured database (in the example configuration, the external database is Windows Active Directory) and provides access to the wireless client whenever the user credentials are valid. The Passed Authentications report on the ACS server shows that the client has passed the RADIUS/EAP authentication.

   This is an example:



4. Upon successful RADIUS/EAP authentication, the wireless client (00:40:96:ab:36:2f in this example) is authenticated with the AP/ WLAN controller.

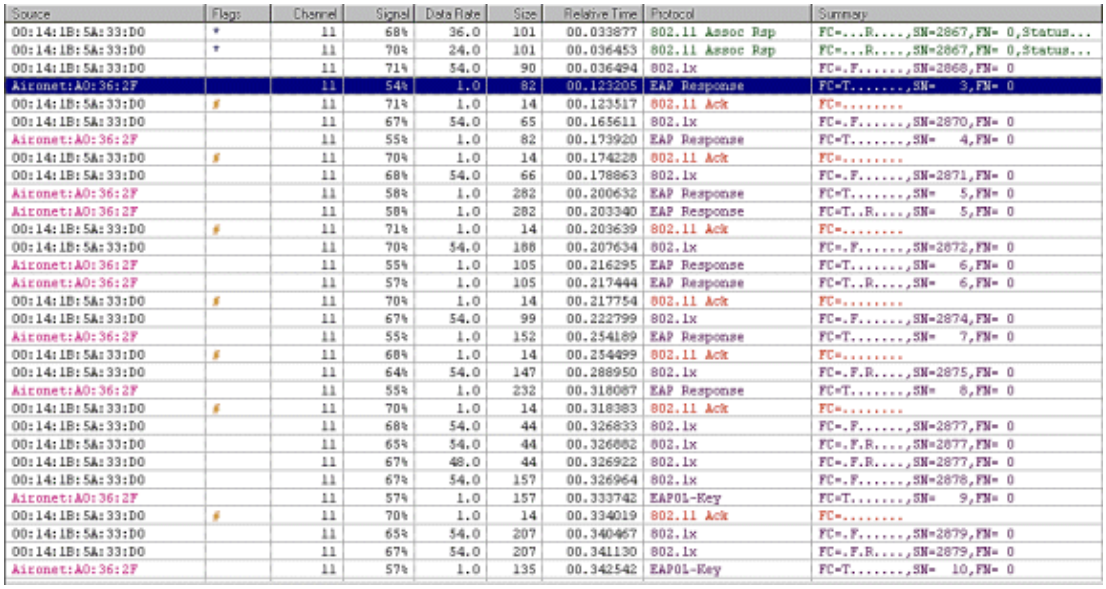


Appendix

In addition to the diagnostic and status information, which is available at the Cisco Secure ACS and Cisco WLAN Controller, there are additional points that can be used to diagnose EAP−FAST authentication. Although the majority of authentication issues can be diagnosed without the use of a WLAN sniffer or debugging EAP exchanges at the WLAN controller, this reference material is included to help troubleshoot.

Sniffer Capture for EAP−FAST Exchange

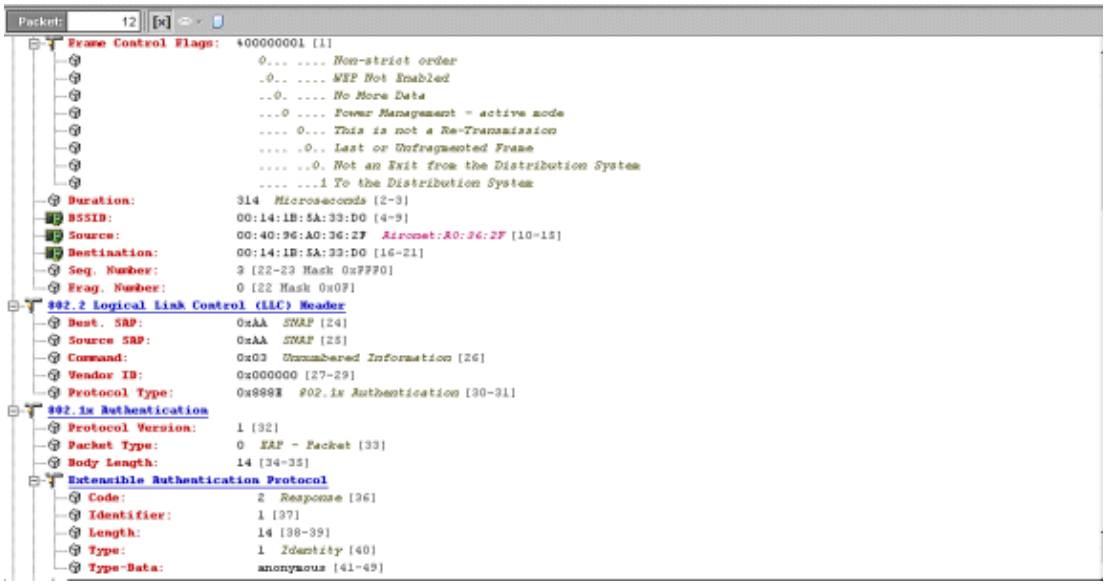
This 802.11 sniffer capture shows the authentication exchange.



Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F......,SN=2868,FN= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.......,SN= 3,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.123517	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	67%	54.0	65	00.165611	802.1x	FC=.F......,SN=2870,FN= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.......,SN= 4,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.174228	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F......,SN=2871,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.......,SN= 5,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T..R....,SN= 5,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.203639	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	70%	54.0	188	00.207634	802.1x	FC=.F......,SN=2872,FN= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.......,SN= 6,FN= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T..R....,SN= 6,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.217754	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F......,SN=2874,FN= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.......,SN= 7,FN= 0
00:14:1B:5A:33:D0	#	11	68%	1.0	14	00.254499	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R....,SN=2875,FN= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.......,SN= 8,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.318383	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F......,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F......,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T.......,SN= 9,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.334019	802.11 Ack	FC=........
00:14:1B:5A:33:D0		11	65%	54.0	207	00.340467	802.1x	FC=.F......,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R....,SN=2879,FN= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T.......,SN= 10,FN= 0

This packet shows the initial EAP−FAST EAP response.

Note: As configured at the CSSC client, anonymous is used as the outer EAP identity in the initial EAP response.



Debug at the WLAN Controller

These debug commands can be employed at the WLAN controller to monitor progress of the authentication exchange:

- **debug aaa events enable**
- **debug aaa detail enable**
- **debug dot1x events enable**
- **debug dot1x states enable**

This is an example of the start of an authentication transaction between the CSSC client and ACS as monitored at the WLAN controller with the debugs:

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
   length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
   0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x −
   moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP−
   Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
   (count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
   Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x − moving mobile
   00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
   Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006:       Callback.......0x10372764
Thu Aug 24 18:20:54 2006:       protocolType...0x00040001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F−11:00
Thu Aug 24 18:20:54 2006:       Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
   Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access−Challenge received from
   RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006:       structureSize..147
Thu Aug 24 18:20:54 2006:       resultCode.....255
Thu Aug 24 18:20:54 2006:       protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F−11:00
Thu Aug 24 18:20:54 2006:       Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access−Challenge
   for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
   (id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
   updated EAP−Identifer 1 ===> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
   AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
   mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

This is the successful completion of the EAP exchange from the controller debug (with WPA2 authentication):

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access−
   Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
   override for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
   00:40:96:a0:36:2f source: 4, valid bits: 0x0
qosLevel: −1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout:
   −1 dataAvgC: −1, rTAvgC: −1, dataBurstC: −1, r1'
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
   policy for station 00:40:96:a0:36:2f − VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
   for station 00:40:96:a0:36:2f (RSN 2)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
   00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: New PMKID: (16)
```

```
Thu Aug 24 18:20:54 2006:      [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
   72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
   to mobile 00:40:96:a0:36:2f (EAP Id 0)
Thu Aug 24 18:20:54 2006: Including PMKID in M1  (16)
Thu Aug 24 18:20:54 2006:
   [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
   mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
   Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
   while in Authenticating state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Authenticated state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-
   Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
   (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
   in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission
   timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
   to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messa1
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
   EAPOL-Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1)
   in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
   PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
   Accounting Interim: 0x138dd764
Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs:
Thu Aug 24 18:20:54 2006:
   AVP[01] User-Name.................enterprise (10 bytes)
Thu Aug 24 18:20:54 2006: AVP[02]
   Nas-Port..........................0x0000001d (29) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[03]
   Nas-Ip-Address....................0x0a0a5003 (168448003) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[04]
   Class.............................CACS:0/28b5/a0a5003/29 (22 bytes)
Thu Aug 24 18:20:54 2006: AVP[05]
   NAS-Identifier....................ws-3750 (7 bytes)
Thu Aug 24 18:20:54 2006: AVP[06]
   Airespace / WLAN-Identifier........0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[07]
   Acct-Session-Id...................44ede3b0/00:40:
   96:a0:36:2f/14 (29 bytes)
Thu Aug 24 18:20:54 2006: AVP[08]
   Acct-Authentic....................0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[09]
   Tunnel-Type.......................0x0000000d (13) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[10]
   Tunnel-Medium-Type................0x00000006 (6) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[11]
   Tunnel-Group-Id...................0x3832 (14386) (2 bytes)
Thu Aug 24 18:20:54 2006: AVP[12]
   Acct-Status-Type..................0x00000003 (3) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[13]
   Acct-Input-Octets.................0x000b99a6 (760230) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[14]
   Acct-Output-Octets................0x00043a27 (277031) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[15]
   Acct-Input-Packets................0x0000444b (17483) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[16]
```

```
   Acct-Output-Packets..............0x0000099b (2459) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[17]
   Acct-Session-Time................0x00000a57 (2647) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[18]
   Acct-Delay-Time..................0x00000000 (0) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[19]
   Calling-Station-Id...............10.10.82.11 (11 bytes)
Thu Aug 24 18:20:54 2006: AVP[20]
   Called-Station-Id................10.10.80.3 (10 bytes)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
   Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated
```

Related Information

- **Installation Guide for Cisco Secure ACS for Windows Server**
- **Configuration Guide for Cisco Secure ACS 4.1**
- **Restrict WLAN Access based on SSID with WLC and Cisco Secure ACS Configuration Example**
- **EAP−TLS under Unified Wireless Network with ACS 4.0 and Windows 2003**
- **Dynamic VLAN Assignment with RADIUS Server and Wireless LAN Controller Configuration Example**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2009 − 2010 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Dec 06, 2006 Document ID: 72788