Protected EAP (PEAP) Application Note

Revision 4.0
June 2004

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

Text Part Number: OL-6005-01
CONTENTS

Prerequisites 2
PEAP Installation Special Notes 3
Installation and Configuration of the Cisco Secure Access Control Server 3
ACS Installation Procedures 4
Cisco Aironet Access Point Software Installation and Configuration 15
  Configuration of Access Points Running Cisco IOS Software 15
  Configuration of Access Point Running VxWorks Software 19
Cisco Aironet Client Utility Installation and Configuration 22
  ACU Installation Precautions 23
  PEAP Client First-Phase Configuration 23
    ACS Configuration 23
    ACU Configuration for PEAP Operation 23
    Windows Configuration for EAP Authentication 25
    Configuration for PEAP (EAP-GTC) Authentication 27
    Configuration for PEAP (EAP-MSCHAP v2) Authentication 29
PEAP Client Second-Phase Configuration and Operation 31
  OTP Configuration and Verification 32
  PIN Change Prompt for OTP Client Devices 33
  Static User Credentials Configuration and Verification for PEAP (EAP-GTC) 34
  Static User Credentials Configuration and Verification (PEAP EAP-MSCHAP v2) 35
  Password Change Prompt and GUI 36
  Cisco PEAP (EAP-GTC) Password Change 37
  Microsoft PEAP (EAP-MSCHAP v2) Password Change 37
Cisco Aironet Desktop Utility for CB21AG Client Adapter 38
  Cisco PEAP (EAP-GTC) Configuration 40
  Cisco Aironet PEAP (EAP-MSCHAP v2) Configuration 42
ACU Installation and Configuration for Windows CE 43
  Windows CE Software Support for PEAP Operation 43
  ACU Configuration on Windows CE Devices 45
Certificate Manager Configuration 46
Authentication Manager Configuration 47
Troubleshooting PEAP Installations 49
Appendix A: Configuration of the Digital Certificate on the ACS  51
  Obtaining the CA Certificate from the Windows CA Server    55
Appendix B: Example of a PEAP Configuration for an Access Point Running Cisco IOS Software   60
Protected EAP (PEAP) Application Note

This document describes the installation and configuration requirements for the Protected Extensible Authentication Protocol (PEAP) software supported by Cisco Aironet client software version 5.05 or later and Cisco Access Control Server (ACS) version 3.1 or later. PEAP is an 802.1X authentication type for wireless LANs (WLANs). PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging. PEAP is a component of the Cisco Wireless Security Suite.

PEAP provides the following security benefits:

- PEAP relies on Transport Layer Security (TLS) to allow non-encrypted authentication types such as EAP-Generic Token Card (GTC) and One Time Password (OTP) support.
- PEAP uses server-side Public-Key Infrastructure (PKI)-based digital certification authentication.
- PEAP allows authentication to an extended suite of directories, including Lightweight Directory Access Protocol (LDAP), Novell NDS, and OTP databases.
- PEAP uses TLS to encrypt all user-sensitive authentication information.
- PEAP supports password change at expiration.
- PEAP does not expose the logon user name in the EAP identity response.
- PEAP is not vulnerable to dictionary attacks.

PEAP is based on server-side EAP-TLS. With PEAP, organizations can avoid the issues associated with installing digital certificates on every client device as required by EAP-TLS; instead, they can select the methods of client authentication, such as logon passwords or OTPs that best suit their corporate needs.

Full support for PEAP authentication and accounting functionality is available with Cisco Aironet access points and bridges running Cisco IOS software version 12.2(11)JA or later or running software version 11.23T or later. PEAP can also be used with Cisco Aironet access point software version 11.06 and later through support for EAP-TLS. Since PEAP is an enhancement of EAP-TLS authentication, PEAP encapsulates a second-phase authentication transaction within the TLS framework.
Prerequisites

- Windows XP client devices
  - The Windows XP operating system provides native support for 802.1X.
  - The operating system 802.1X support is used to configure wireless client authentication parameters.
  - Microsoft Service Pack 1 for Windows XP also provides the Microsoft PEAP (EAP-MSCHAPv2) supplicant.

  **Note**  
  There may be issues with Microsoft’s pre-SP1 802.1X implementation (for additional information refer to Microsoft knowledge base articles KB313896, KB 311787, and KB826942).

- Windows 2000 clients
  - Microsoft patch version Q313664 (using 802.1x Authentication on Computers Running Windows 2000) or Microsoft Service Pack 4 for Windows 2000

- Windows CE clients
  - Pocket PC (PPC) 2002
  - PPC 2003 or Windows CE .Net

- Cisco Aironet PCM, PCI, LMC 350 and 340 series client adapters
- Cisco Aironet MPI350 series mini-PCI client adapters
- Cisco Aironet CB20A client adapters
- Cisco Aironet client software and firmware
  - Aironet Client Utility (ACU) version 5.05 or later is required for use with PEAP (EAP-GTC).
  - Client adapter driver version 8.2.3 is required for PCM, PCI, LMC client adapters, and driver version 3.4.9 is required for mini-PCI client adapters.
  - Client radio firmware version 4.25.30 is required for PCM, PCI, LMC client adapters, and version 5.00.03 is required for mini-PCI client adapters.
  - ACU version 2.3 or later is required for Windows CE (PPC 2002) devices, and version 2.5 is required for Windows CE (PPC 2003 or Windows CE .Net) devices.
- Cisco Aironet CB21AG client adapter with standard drivers and utility
- Cisco Aironet 350 and 340 series access point firmware version 11.10 or later
- Cisco IOS access point firmware version 12.2(11)JA or later is required to support WPA authenticated key management
- Cisco Secure Access Control Server
  a. Software version 3.1 is required for support of Cisco PEAP (EAP-TLS).
  b. Software version 3.2 is required for support of Microsoft’s PEAP (EAP-MSCHAP v2).
  c. Minimum hardware requirements for Windows 2000 servers and Windows NT servers:
    - A 550 MHz Pentium processor, 256M RAM, 250MB available disk space (or as required by the local ACS database), a VGA monitor, and a video card capable of 256 colors and 800 x 600 screen resolution.
PEAP Installation Special Notes

- The Microsoft EAP framework used in PEAP for the Cisco Aironet 350 series and CB20A client adapters permits only one EAP DLL per EAP type. This restriction allows only one PEAP supplicant to be installed on a single machine.

**Note** When installing or configuring client adapters, the administrator must be aware of this restriction.

- The version of the PEAP (EAP-MSCHAP v2) supplicant available in Windows XP Service Pack 1 and in Windows 2000 Hotfix Q313664 is not compatible with the Cisco PEAP (EAP-GTC) supplicant included in the ACU or with the Cisco Aironet Client Install Wizard (hereafter called the install wizard).

**Note** The installation of ACU version 5.05 replaces the Microsoft PEAP (EAP-MSCHAP v2) supplicant.

**Note** In ACU version 6.0 and later, the installation of the Cisco PEAP (EAP-GTC) supplicant is optional and not enabled by default.

- If you want to use only the Microsoft PEAP (EAP-MSCHAP v2) supplicant, **do not install** the Cisco PEAP (EAP-GTC) supplicant with the ACU or the install wizard.

**Note** If you inadvertently configure the Cisco PEAP (EAP-GTC) supplicant, you must uninstall the ACU or the install wizard and then re-install the appropriate Windows service pack on the client PC.

- The Cisco PEAP (EAP-GTC) supplicant is not invoked before a user logs into the system. This can prevent some forms of single-signon when using PEAP.

Installation and Configuration of the Cisco Secure Access Control Server

Cisco Secure Access Control Server (hereafter called ACS) version 3.1 is required for Cisco PEAP (EAP-GTC) because it provides support for the PEAP-GTC EAP type, Microsoft password change, and one-time password (OTP) password server communications. The Cisco PEAP software does not utilize all functions of ACS version 3.1. You can obtain more information on ACS version 3.1 at this URL: http://www.cisco.com/en/US/products/sw/secursw/ps2086/ps5011/index.html

ACS version 3.2 is required for the Microsoft PEAP (EAP-MSCHAP v2) supplicant, and it also provides additional EAP-TLS functions such as extra flexibility in the certificate comparison mechanism, session resume, and password grace within the Microsoft domain. You can obtain more information on ACS v3.2 at this URL: http://www.cisco.com/en/US/products/sw/secursw/ps2086/ps5340/index.html
ACS Installation Procedures

Step 1 Obtain the ACS software, and place it in a temporary location on your Windows NT or Windows 2000 server.

Step 2 Double-click on the ACS software self-extracting zip file to extract the installation and setup utility. Double-click setup.exe to install (or upgrade) the ACS software. For additional information, refer to the ACS (version 3.2) data sheet or installation guide at these URLs.

Data sheet:  

Installation guide:  

Step 3 Use the ACS and Cisco Aironet reference manuals to install (or upgrade) and configure the ACS software on your Windows NT or Windows 2000 server.

Step 4 The ACS install application requires an IP address of an access point that is used for client authentication. This access point serves as a Network Access Server (NAS) for forwarding client adapter PEAP authentications to the ACS.

Step 5 Under Network Configuration, perform the following operations:

a. Edit the Authentication, Authorization, and Accounting (AAA) client for the access point providing the NAS functions.

b. Enter the shared secret key (common to the access point) that is used between the AAA client and the ACS.

c. Select Authenticate Using > RADIUS (Cisco Aironet) for this AAA client.

Step 6 Under System Configuration, click ACS Certificate Setup, and configure the ACS with a certificate from a certification authority (CA) server.

Step 7 Use the Generate Certificate Signing Request (CSR) utility (see Figure 1) to generate a certificate. This utility generates a signing request which may be sent or copied to a Certificate Authority (hereafter called CA) for generation of a certificate (certificate file & private key file). When using this utility, you must perform the following operations during the configuration of the certificate:

a. Check Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file (see Figure 53).

b. Check Mark keys as exportable (see Figure 54).

For additional information on configuration of the certificate, refer to the “Appendix A: Configuration of the Digital Certificate on the ACS” section on page 51.
Step 8  The certificate can be installed using the Install ACS Certificate utility (see Figure 2) or manually installed (see Appendix A: Configuration of the Digital Certificate on the ACS, page 51).

Figure 1  Generate Certificate Signing Request from ACS Screen

Figure 2  ACS Certificate Installation Screen

Step 9  To install the certificate using the Install ACS Certificate utility, perform these operations from the ACS Certificate Installation screen (see Figure 2):

a. Check Read certificate from file.

b. Enter the path and filename for the certificate file in the Certificate file field.
c. Enter the path and filename for the private key file in the *Private key file* field.
d. Enter the password in the *Private key password* field.
e. To install the certificate, click **Submit**.

**Step 10**

After installing the certificate, you are prompted to restart the ACS services from the *ACS System Configuration > Service Control* menu (see **Figure 3**). After you verify the information on this screen, restart the ACS application as directed.

---

**Note**  
Do not click **Install New Certificate** on this screen (see **Figure 3**) because this removes the previously installed certificate and requires you to restart from **Step 6**.

---

**Figure 3  Confirmation of ACS Certificate Installation Screen**

![Confirmation of ACS Certificate Installation Screen](image)

---

**Note**  
A certificate for ACS can also be generated and installed manually (that is, not by using the CSR utility) on the server which runs the ACS application. (See the “Appendix A: Configuration of the Digital Certificate on the ACS” section on page 51 for instructions on generating and installing a certificate in the local machine certificate store).

---

**Step 11**

After installing the certificate and restarting the ACS application, you must set up the ACS Certificate Authority (CA) certificate that corresponds to the certificate just installed. Perform these operations to access the ACS Certification Authority Setup utility:
a. Click **System Configuration**.
b. Click **ACS Certificate Setup**.
c. Click **ACS Certification Authority Setup** (refer to **Figure 4**).
The file for the CA certificate can be obtained from the system administrator or generated from the CA server under Windows Administrative Services. For complete details on exporting the CA certificate file, refer to the “Appendix A: Configuration of the Digital Certificate on the ACS” section on page 51.

**Figure 4 ACS Certification Authority Setup**

![ACS Certification Authority Setup](image)

d. Enter the complete path and filename into the *CA certificate file* field.

e. Click **Submit**, and the Confirmation of ACS Certificate Installation Screen appears (see **Figure 5**).
Figure 5  ACS Certificate Authority File Setup Confirmation

Step 12  After you verify the information on this screen (Figure 5), restart ACS from the ACS System Configuration > Service Control menu.

Note  Do not click Submit on this screen (see Figure 5) because this will remove the previously entered certificate information and will require you to repeat Step 11.

Step 13  After restarting ACS, you should now enable PEAP authentication. Perform these steps:

a. Click System Configuration.

b. Click Global Authentication Setup, and the ACS Global Authentication Screen appears (see Figure 6).
c. Under PEAP, check the desired PEAP type authentication:
   - Allow EAP-GTC—the PEAP supplicant for Cisco client devices available in the ACU, the install wizard, and from Funk Software and Meetinghouse Data Communications.

d. Enter an initial message text string to be included in the Cisco client adapter (EAP-GTC) login window.

e. Enter the time-out value in the PEAP session time-out field. This value should be set to the desired interval at which a user is re-prompted to enter authentication credentials (typically 8 to 10 hours, or a single work period).

Note  The PEAP session time-out is not the same as the WEP session time-out, which is typically set to a shorter interval.

f. If needed, check Enable Fast Reconnect. This option enables a user to roam or reconnect to an access point without re-entering their user credentials. With fast reconnect, the first-phase authentication (TLS session) parameters (known only by the client adapter and EAP server) are used to negotiate security parameters when a client adapter resumes a session with an access point or roams to a different access point that uses the same EAP server for authentication. This is also known as PEAP session resume.

g. Click Submit.
Step 14 Click **External User Databases** to configure the databases (see Figure 7).

Figure 7 Configuring External Database in ACS

![Figure 7](image)

Step 15 Click **Windows NT/2000** to configure domain and MS-CHAP settings for Windows NT and Windows 2000 external user databases (see Figure 8).

*Note* For the domain to be visible under *Available Domains*, the ACS must be the domain controller or be a member server joined to a Microsoft domain. If the ACS is on a routed network, additional Netbios or DNS configuration is typically required to permit the ACS to authenticate users to the domain.
Step 16 Enter the appropriate domains into the Domain List field.

Step 17 You can configure additional authentication functions into the Windows database by performing these operations (see Figure 8 and Figure 9):

a. Check Permit password changes using MS-CHAP version 2 under the MS-CHAP Settings to enable server-initiated password changes to be passed to the client adapter.
b. Check **Permit password change inside PEAT** to enable password change messaging via PEAP.

c. Check **Permit PEAP machine authentication** to enable EAP-MSCHAP v2 for authentication of client adapters in a Microsoft domain.

d. Enter **host/** in the **EAP-TLS and PEAP machine authentication name prefix** field for client adapter authentication, as this is the default configuration in Microsoft client adapters. If another string is used by client adapters, that string must be specified in this field.

**Step 18**  
To configure Novell NDS or Generic LDAP databases, refer to **Figure 10**. Detailed information on configuring ACS for external databases can be found in the ACS user guide. In general, however, primary server, secondary/backup server, domain name filtering, port number, time-out parameter, and shared secret password for RADIUS protocol communication are configured on this screen.

**Figure 10**  
**Generic LDAP Configuration**
Step 19 To configure the Safeword token server, refer to Figure 11. You can configure appropriate parameters, including IP address of primary server, IP address of any secondary or backup server, port, time-out parameter, and shared secret password for RADIUS protocol communication on this screen. Configuration procedures for other RADIUS token servers, such as Vasco or ActivCard, use identical RADIUS configuration screens.

Figure 11 Safeword Token Server and RADIUS Token Server Configuration Screen

Step 20 For communication with RSA Computing SecurID token server, a Microsoft API is used on the ACS, which serves as a client to the RSA token server. You must ensure that the ACS has the appropriate RSA token-card client software installed and enabled.

Step 21 After configuration of external databases, Unknown User mapping (see Figure 12) is used to provide prioritization of authentication mechanisms for users not found in the local ACS database or the ACS user cache. Use the Up and Down buttons to check for unknown users and to prioritize multiple databases listed in the Selected Databases field.
ACS provides additional configuration of database mappings and authentication schemes, but these complex mappings and schemes are beyond the scope of this document and PEAP configuration. Refer to ACS documentation for a list of the supported features of ACS release 3.2.

**Note**

We recommend that you verify that your database configuration is working correctly with wired clients (if possible) before extending authentication through the PEAP protocol.

For instructions on issuing and installing a digital certificate for the ACS using the CA service available on a Windows server, refer to the “Appendix A: Configuration of the Digital Certificate on the ACS” section on page 51.
Cisco Aironet Access Point Software Installation and Configuration

For full support of PEAP authentication accounting, Cisco Aironet access points must be running the following operating system software:

- VxWorks release 11.23T or later
  - Available on Cisco Aironet 1200, 350, and 340 series access points
- Cisco IOS release 12.2(4)JA
  - Available on Cisco Aironet 1100 access points
- Cisco IOS release 12.2(8)JA
  - Available on Cisco Aironet 1200 and 1100 access points
- Cisco IOS release 12.3(13)JA or later
  - Available on Cisco Aironet 1200, 1100, and 350 access points

Because PEAP is a variation of EAP, the listed operating system software also supports other EAP types, including Cisco LEAP, EAP-Transport Layer Security (EAP-TLS), EAP-Subscriber Identity Module (EAP-SIM), and types that operate over EAP-TLS, such as EAP-Tunneled TLS (EAP-TTLS).

Cisco Aironet access points can be upgraded using a web browser, FTP, TFTP, or through the console port. The web browser interface is recommended for simplicity. Refer to your Cisco Aironet access point documentation for operating system upgrade instructions.

Configuration of Access Points Running Cisco IOS Software

This section describes the configuration procedures for Cisco Aironet 350, 1100, and 1200 series access points running Cisco IOS software. To configure the access points, perform these steps:

- **Step 1** Verify the operating system software release running on your access point using the System Software tab on the left menu bar of the main browser screen or using the Cisco IOS show version command.
- **Step 2** Click SECURITY to configure your access point security settings.
Step 3  Click Encryption Manager, and Figure 13 appears.

**Figure 13  Encryption Manager Configuration Screen**

![Encryption Manager Configuration Screen](image)

Step 4  Click WEP Encryption and select Mandatory or Optional using the drop-down arrow.

---

**Note** We do not recommend setting the optional encryption, which enables unencrypted client adapters to associate to the access point and renders the network behind the access point vulnerable.

Step 5  When using static WEP keys on your client adapters, you must enter a key in the appropriate Encryption Key field for your client adapters (see Figure 13); this key will also be used as the broadcast key for PEAP client adapters.

---

**Note** If you are using static WEP client adapters, you must enter a static WEP key. If you are using only dynamically keyed client adapters, you do not need to enter a WEP key. It is derived as part of the 802.1X authentication process.

---

**Note** Encryption Key 2 is selected by default for compatibility with WPA encryption (keys 1 and 4 are used by the WPA key authentication process). If you are not using WPA, keys 1 and 4 can be configured for your client adapters.

We recommend that you check the Cisco-Compliant TKIP Features (Enable MIC and Enable Per Packet Keying) when using Cisco Aironet or Cisco Compatible client devices or both types (see Figure 13).

---

**Note** You can also set the Broadcast key rotation and the interval from this screen.
Step 6 If you are using WPA encryption on your client adapters, check Cipher, and choose a TKIP cipher (or a combination of ciphers that include TKIP) using the drop-down arrow (see Figure 13).

Step 7 Click SSID Manager, and Figure 14 appears.

Figure 14 SSID Manager Configuration

Step 8 Choose the SSID to be configured in the Current SSID List or enter the desired value in the SSID field.

Step 9 Under Authentication Settings and Methods Accepted, perform one of these steps:

a. Check Network EAP if you are using Cisco Aironet or Cisco Compatible client adapters or both types with PEAP authentication.

b. Check Open Authentication, and choose with EAP using the Open Authentication drop-down arrow if you are using third party client adapters, such as Microsoft Zero Configuration and 802.1X.

Step 10 If you are using unique RADIUS (EAP) servers for each SSID, you can specify the server priorities in the Server Priorities section (see Figure 15). If you are not using multiple RADIUS servers, click Server Manager to configure the RADIUS server (see Figure 16).
Step 11  If you are using WPA encryption, you must configure the SSID for Authenticated Key Management. Under Authenticated Key Management, choose **Optional** or **Mandatory** using the Key Management drop-down arrow, and check **WPA**.

**Note**  Optional WPA key management (also called WPA Migration Mode) permits the coexistence of WPA and non-WPA client devices. Refer to Cisco Aironet client adapter and access point release notes for specific compatibility issues when using Migration Mode.

Step 12  Under Accounting Settings, check **Enable Accounting** to use the RADIUS server for RADIUS accounting of EAP and 802.11 authentication traffic.

Step 13  If you are using non-Cisco Aironet client adapters, you might have to choose the configured SSID using the **Set Guest Mode SSID** drop-down arrow for proper client 802.11 association behavior.

**Note**  Enabling guest mode causes the configured SSID to be broadcast in the access point beacons.
Step 14  To configure the RADIUS server for use with PEAP authentication, click **Server Manager**, and **Figure 16** appears. In the **Corporate Servers** section perform these steps:

a. Enter the server host name or IP address in the **Server** field.

b. Enter the RADIUS shared secret string in the **Shared Secret** field.

c. Optionally, you can enter a specific port number (1645 is the default value) for authentication traffic in the **Authentication Port** field.

*Figure 16  Server Manager Configuration*

Step 15  In the **Default Server Priorities** section, choose the configured RADIUS server using the **Priority 1** drop-down arrow in the **EAP Authentication** column. If you are using multiple servers, choose the appropriate servers using the drop-down arrows in the **Priority 1** and **Priority 2** fields.

Step 16  Click the **Global Properties** tab, and the Global Properties screen appears. On the Global Properties screen, you can configure the RADIUS time-outs, retransmissions, and the RADIUS accounting interval. If you are using multiple RADIUS servers, we recommend that you enable the **Dead RADIUS Server List** and enter the appropriate retry interval in the associated field.

---

**Configuration of Access Point Running VxWorks Software**

This section describes the configuration procedures for Cisco Aironet access points running VxWorks software (versions 11.23T or later). Perform these steps to configure the access points:

Step 1  Use your browser to identify the operating system software release running on your access point, which is listed on the left side of the Summary Status screen.

Step 2  Access your access point security settings from the main **Summary Status** screen by clicking **Setup > Security > Radio Data Encryption (WEP)**, and **Figure 17** appears. To enable the use of dynamic WEP keys on the specific SSID being configured, choose **Full Encryption** or **Optional Encryption** using the drop-down arrow in the **Use of Data Encryption by Stations** field.
We do not recommend the use of optional encryption because this enables unencrypted client adapters to associate to your access point and allows un-authenticated access to your wired network.

You must configure a WEP key or enable broadcast key rotation on your access point to support encryption.

Step 3  Under *Accept Authentication Type*, check *Open* and *Network EAP* if you are using Cisco Aironet client devices (or Cisco Compatible devices).

Step 4  Under *Require EAP*, check *Open* if you are using non-Cisco client devices such as, third party client adapters using Microsoft’s Zero Configuration and XP 802.1X configuration).

Step 5  Access the advanced root radio settings from the *Setup* screen by clicking *Advanced* under Network Ports and Root Radio. *Figure 18* appears. If you are using Cisco Aironet client devices or Cisco Compatible client devices, we recommend that you enable *Temporal Key Integrity Protocol* and *Enhanced MIC verification for WEP* to increase the security of the WEP encryption keys derived from the PEAP/ 802.1X authentication process. Perform these steps:

a. Choose *MMH* using the drop-down arrow in the *Enhanced MIC verification for WEP* field.

b. Choose *Cisco* using the drop-down arrow in the *Temporal Key Integrity Protocol* field.
Note These VxWorks access point settings are not compatible with the WPA version of TKIP supported in Cisco IOS access points.

Figure 18  Radio Advanced Configuration: TKIP, MIC, Broadcast Key Rotation

Step 6 If you are not using static WEP key client devices, we recommend that you enable broadcast key rotation by entering a value in the Broadcast WEP Key rotation interval (sec) field.

Step 7 Verify that the ACS server IP address, port number, and shared secret are properly configured. From the main Summary Status screen, click Setup > Security > Authentication Server, and Figure 19 appears.

Note These settings are standard for 802.1X-based authentication and do not differ from configurations used for other authentication types, such as LEAP or EAP-TLS.
Cisco Aironet Client Utility Installation and Configuration

Cisco Aironet Client Utility (ACU) software version 5.05 or later includes Cisco PEAP (EAP-GTC) supplicant functionality within the client software. When using ACU version 5.0x for PEAP, you must manually upgrade the client adapter drivers and firmware. For the required driver and software versions, refer to the “Prerequisites” section on page 2.

Note
All bundled Cisco client adapter software (InstallWizard version 1.0 and later) automatically upgrade the driver and firmware upon installation.

Note
The PEAP supplicant option must be selected from the InstallWizard upon initial installation.

When you are using non-Cisco EAP supplicants with PEAP authentication, such as Microsoft 802.1X EAP-MSCHAP v2 in Windows XP Service Pack 1, only the appropriate client driver and software must be installed, because the authentication is handled by the EAP supplicant software incorporated into the operating system. The ACU can still be installed and used for diagnostics, statistics, or both, but the client adapter must be configured using the Microsoft (or other) utility.

All versions of the ACU after version 5.05 includes support for several EAP types including LEAP, EAP-TLS, and types that operate over EAP-TLS, such as EAP-TTLS and PEAP. Refer to the Cisco Aironet Client Utility Release Notes for additional information.
ACU Installation Precautions

Observe these precautions when you are installing the ACU:

- PEAP client devices use the EAP 802.1X support provided in the Windows XP and Windows 2000 operating systems to enable authentication.

  **Note** You must use the operating system to configure the authentication parameters of the PEAP supplicant.

- Windows XP supports EAP 802.1X as a standard authentication type. Windows 2000 supports EAP 802.1X authentication with Service Pack 4, but does not provide a Zero Configuration for client adapters. Hence, the ACU (or equivalent) software must be used to configure the client adapter 802.11 operating parameters.

- When installing the ACU software, select PEAP support during the initial installation. The PEAP supplicant cannot be added or enabled incrementally after installation; the ACU software must be reinstalled with the PEAP support option selected.

PEAP Client First-Phase Configuration

ACS Configuration

Verify that the ACS is running software version 3.1 or later and that it is configured for Allow PEAP under Global Authentication Configuration in the System Configuration section. The configuration of the ACS for certificate-based, server-side authentication is necessary for PEAP operation. Refer the “Appendix A: Configuration of the Digital Certificate on the ACS” section on page 51 or to the ACS documentation for certificate setup information.

ACU Configuration for PEAP Operation

Because EAP 802.1X authentication is enabled by the Windows operating system, the ACU is not used to configure the user credentials for PEAP authentication.

When using the Windows XP Service Pack 1 (or with later service packs and patches), you must configure the operating system to control the wireless network settings of your client adapter. On the Wireless Network Connection Properties Screen, you must check **Use Windows to configure my wireless network settings** (see Figure 21). This is known as Microsoft Zero Config for wireless.

**Note** In Windows XP, the client adapter configuration and the authentication configuration are integrated together and cannot be separated. Even when using the ACU to configure your client adapter parameters (such as SSID, power savings, and client ID), you must configure the operating system to control the wireless network.

In Windows 2000 (Service Pack 4 or later), only the Authentication features of the client adapter are supported. With this operating system, you must use the ACU (or another utility) to configure the RF parameters of your wireless client adapter.

The **Network and Dial-up Connections** selection in the Windows Control Panel is used to configure the EAP parameters such as certificate, trusted server, and user authentication type.
Perform these steps to configure the ACU for PEAP operation:

**Step 1**
To enable PEAP support in the client adapter, you must select **PEAP** during installation of the ACU. To work with a 802.11 wireless system, you must use the ACU to configure a wireless profile for a specific SSID, security parameters, power savings, and other parameters used in the wireless network.

**Step 2**
You must configure the Security settings for the client adapter to use the operating system (or host client) EAP supplicant for authentication. Perform these steps:

- From the main ACU screen, click **Profile Manager**.
- Create a new profile by clicking **Add** and entering a profile name, or choose an existing profile using the drop-down arrow and clicking **Edit**.
- Click **Network Security**, and Figure 20 appears.

**Figure 20**   **PEAP Configuration Example within the Aironet Client Utility User Profile**

- On the Network Security screen, choose **Host Based EAP** using the drop-down arrow in the Network Security Type field.
- Under the WEP section, check **Use Dynamic WEP Keys**.

**Step 3**
You must use the Device Manager properties in Windows to configure the client adapter for the appropriate SSID, EAP authentication type, second-phase PEAP type, and trusted certificate for use in first-phase PEAP authentication.
Step 4  From the main ACU screen, click Select Profile, and enable auto-profile selection, with the Microsoft EAP profile, Static WEP, and non-WEP profiles, as applicable.

Note  Multiple 802.1X profiles, such as PEAP and EAP-TLS do not work with auto-profile switching. This is because the EAP authentication type configured in the operating system is not changed after switching to a different profile.

Windows Configuration for EAP Authentication

The first-phase PEAP authentication is managed between the PEAP supplicant and the authentication server. In this phase, the client authenticates the server using a TLS certificate-based mechanism. This establishes an encrypted tunnel through which the second-phase PEAP credentials may be securely exchanged.

The parameters used by the client in negotiating PEAP authentication are configured through the Windows Device Manager properties. Perform these steps:

Step 1  From the Windows Wireless Network Connection Properties screen (see Figure 21) for your client adapter, verify that Use Windows to configure my wireless network settings is checked.

Figure 21  Wireless Network Connection Properties
Step 2  Perform one of these steps:

a. Choose the desired SSID of the network to be used for PEAP authentication from the Available networks list, and click Configure.

Click Add in the Preferred networks section to configure a new network SSID.

Step 3  From the Wireless network properties screen (see Figure 22), perform these steps:

a. Verify that the correct SSID is displayed in the Network name (SSID) field.

b. Choose the appropriate Network Authentication and Data Encryption parameters using the drop-down arrows.

c. Ensure that The key is provided for me automatically is checked.

Figure 22  Wireless Network Connection Association Parameters

Step 4  You must configure the correct security key type appropriate for your client adapter and the network. Perform these steps:

a. If you are using WEP encryption with either IEEE 802.11 128-bit (or 40-bit) WEP, Cisco TKIP, or MIC, choose Open in the Network Authentication field, and choose WEP in the Data encryption field using the drop-down arrows.

b. If you are using WPA (IEEE 802.11i) encryption, choose WPA in the Network Authentication field, and choose TKIP in the Data encryption field using the drop-down arrows.

Note  Microsoft Windows XP patch KB826942 or Service Pack 2 is required for WPA support in the operating system.
Configuration for PEAP (EAP-GTC) Authentication

The Authentication tab on the Wireless network properties screen is used to configure the operating system 802.1X authentication mechanism for PEAP authentication. Perform these steps to configure PEAP (EAP-GTC) authentication:

**Step 1**  Click the **Authentication** tab on the Wireless network properties screen (see Figure 24).

**Step 2**  Check **Enable IEEE 802.1x authentication for this network**.

**Step 3**  Choose **PEAP** as the authentication type using the drop-down arrow in the EAP type field.

*Figure 23  Wireless Network Authentication Parameters*

When PEAP is selected as the EAP type on the Authentication tab of the Wireless network properties screen, you can use the Properties button to configure PEAP parameters. This additional configuration screen is specific to the PEAP supplicant installed and is used to specify the PEAP server, the PEAP server CA certificate, and the second-phase EAP type.
Step 4  Click Properties, and the PEAP configuration screen for the Cisco EAP-GTC supplicant appears (see Figure 24).

Figure 24  Cisco PEAP (EAP-GTC) Supplicant Properties Screen

Step 5  The PEAP configuration parameters used for the first-phase PEAP authentication are specified on this screen. Perform these steps to configure the Cisco PEAP (EAP-GTC) supplicant:

a. Check Validate server certificate to use the CA certificate to validate EAP server certificate. You should only uncheck this option for initial operational testing and verification.

b. Choose the certificate authority that issued the EAP (PEAP) server certificate using the drop-down arrow in the Trusted root certificate authority (CA) field.

c. Choose Generic Token Card using the drop-down arrow in the Second-Phase EAP Type field.

Note  This field is also used for EAP-SIM, which is another EAP type supported by the Cisco supplicant.

d. Check Always try to resume secure session. This allows client adapters to resume a PEAP session with an EAP server after roaming out-of-coverage or to connect to a new access point without reentry of user credentials.

Note  TLS session credentials are used to resume the secure session.

The first time that a configured client adapter associates using the Cisco EAP-GTC supplicant, the user is prompted with a pop-up dialog screen to accept (or reject) the server CA certificate offered by the EAP server.

Note  Manuall installation of the server CA certivicate is not required. You should instruct all users to accept this certificate.
After accepting the certificate, PEAP authentication continues (using the server CA certificate to protect the user credentials), and the user is prompted for the second-phase EAP credentials.

### Configuration for PEAP (EAP-MSCHAP v2) Authentication

The configuration of the Microsoft PEAP (EAP-MSCHAP v2) supplicant (available in Windows XP SP1 and later and in Windows 2000 SP4) is shown in Figure 25 and Figure 26.

**Note**

This supplicant uses the same mechanism for specifying the server certificate CA (with a slightly different user interface) as used with the Cisco EAP-GTC supplicant.

The Authentication tab on the PEAP properties screen (see Figure 25) is used to configure the operating system 802.1X authentication mechanism for PEAP authentication. Perform these steps to configure PEAP (EAP-MSCHAP v2) authentication:

1. **Step 1**
   
   Click the Authentication tab on the PEAP properties screen, and Figure 25 appears.

   ![Figure 25 Authentication Configuration for PEAP(MSCHAP v2)]

2. **Step 2**
   
   Check **Enable IEEE 802.1x authentication for this network**.

3. **Step 3**
   
   Choose **Protected EAP (PEAP)** as the authentication type using the drop-down arrow in the **EAP type** field.
Step 4 If you want to authenticate the computer (also called machine authentication) to a Microsoft domain in advance of user authentication, check Authenticate as computer when computer information is available.

Note For a computer to be successfully authenticated to a domain, the computer must be registered to the domain using a non-802.1X secured network (a wired connection) prior to attempting machine authentication with PEAP.

Step 5 Click Properties, and the PEAP configuration screen for the Microsoft (EAP-MSCHAP v2) supplicant appears (see Figure 26).

Figure 26 Microsoft (MSCHAPv2) PEAP Supplicant Configuration Screen

Step 6 Check Validate server certificate.

Note If you do not check Validate server certificate, user credentials are not protected by the EAP server certificate.

Step 7 Check the correct CA in the Trusted Root Certification Authorities list.

Step 8 Choose Secured password (EAP-MSCHAP v2) using the drop-down arrow in the Select Authentication Method field.

Step 9 Check Enable Fast Reconnect to enable client devices to perform a PEAP session resume with properly equipped and configured EAP servers. PEAP session resume enables client devices to re-authenticate with an EAP server after roaming to a new access point without submitting the second-phase PEAP credentials. The session is resumed using the cached TLS credentials.
Step 10  Click Configure, and the EAP MSCHAP V2 Properties screen appears (see Figure 27).

**Figure 27  Microsoft EAP-MSCHAPv2 Configuration**

![EAP MSCHAPv2 Properties](image)

Step 11  If desired, check **Automatically use my Windows logon name and password (and domain if any)** to enable the Microsoft PEAP supplicant to use the Windows logon name for PEAP authentication. This enables the user to log in to the wireless network using their Windows credentials.

**Note**  When this options is checked, the user credentials cannot be changed because they are stored in the user’s profile, whether using manually entered credentials or using Windows credentials.

The Microsoft PEAP supplicant supports two authentication options:

- **User authentication**—forces each user to authenticate before network access is allowed.

  **Note**  To support user authentication, the CA certificate *must* be installed in the user profile.

- **Machine authentication**—forces each machine (computer) to authenticate before network access is allowed. This allows multiple users to use a computer. To support machine authentication, the CA certificate must be installed in the Windows Local Computer store on each computer. This CA certificate can be pushed to client computers as part of the Group Policy Object upon registering to the Microsoft Active Directory domain.

### PEAP Client Second-Phase Configuration and Operation

There are two major authentication types used for second-phase PEAP:

- **One Time Password (OTP) authentication**
- **Static password authentication to an external database**

The Cisco PEAP supplicant (EAP-GTC) is able to support either OTP or static password authentication types. The Microsoft PEAP supplicant (MSCHAP v2) is only functional with Microsoft databases and uses only static password authentication.
OTP Configuration and Verification

Using PEAP with OTP servers, such as Secure Computing Safeword Server or RSA Computing SecureID, requires that you configure the type of token that is used with PEAP authentication. Perform these steps to configure OTP for PEAP:

**Step 1**  
On the Cisco PEAP (EAP-GTC) Supplicant Properties Screen (see Figure 24), choose **Generic Token Card** using the drop-down arrow in the Second-Phase EAP Type field.

**Step 2**  
Click **Properties**, and the Generic Token Card Properties Screen appears (see Figure 28).

**Figure 28  Generic Token Card Properties (OTP) Screen**

![](image)

**Step 3**  
Check **One Time Password**.

**Step 4**  
Check the token type used with PEAP:

a. **Support Hardware Token**—specifies the use of a hardware token device that generates an OTP for manual entry into a dialog window.

b. **Support Software Token**—specifies the use of a software token program to generate an OTP after a PIN number is entered.

**Step 5**  
If you are using a software token, perform these steps:

a. Choose **Secure Computing Softoken Version 1.3**, or **Secure Computing Softoken Version 2.0**, or **RSA SecureID version 2.5** using the drop-down arrow in the **Supported Type** field.

b. In the Program Path field, enter the full path to the software token application on the client computer. You can use the Browse button to locate the application.

**Step 6**  
Click **OK** when done. OTP configuration is complete.
When a wireless client device initially associates to your access point, a One Time Password screen appears (Figure 29) for authentication.

**Figure 29 OTP Authentication Dialog Box**

![OTP Authentication Dialog Box](image)

OTP authentication requires the entry of a username and the OTP password before a user is allowed access to the wireless network. Perform these steps for OTP authentication:

**Step 1** Enter your username in the User Name field.

**Step 2** Obtain the token password from your hardware token device or the software token application. Typically, when using a software token application, you must enter your username and a PIN before obtaining the token password.

**Step 3** Enter or paste the token password into the Password field.

**Step 4** Check **Hardware Token** or **Software Token**.

**Step 5** Click **OK**.

**PIN Change Prompt for OTP Client Devices**

The OTP server can be configured (based upon policy settings) for password expiration to force users to enter new passwords. When the password expires the OTP server initiates a message requiring the user enter a new PIN, and the PEAP supplicant displays the OTP Pin Change Screen (see Figure 30).
Static User Credentials Configuration and Verification for PEAP (EAP-GTC)

Static user credentials can be used for authentication to Microsoft domain databases or NDS/LDAP databases. Only the Cisco PEAP supplicant can be used with the NDS/LDAP databases, but either the Cisco PEAP or the Microsoft PEAP supplicants can be used to authenticate with Microsoft domains. However, only the Microsoft PEAP supplicant permits the use of Windows logon credentials to be used for PEAP authentication (single sign-on with Windows credentials).

Perform these steps to configure static user credentials for the Cisco PEAP supplicant:

**Step 1**
On the Cisco PEAP (EAP_GTC Supplicant Properties Screen (see Figure 24), click **Properties**, and the Generic Token Card Properties screen appears (see Figure 31).

**Step 2**
Click **Static Password (Windows NT/2000, LDAP)**.

**Step 3**
Click **OK**.
When the wireless client device is configured and associated to your access point, the Static Password Screen appears (see Figure 32).

![Static Password Dialog Box](image)

The users must enter their usernames and passwords. If the user is logging on to a Windows domain, the domain name might also be required.

**Static User Credentials Configuration and Verification (PEAP EAP-MSCHAP v2)**

Static user credentials can be used for authentication to Microsoft domain databases or NDS/LDAP databases. Only the Cisco PEAP supplicant can be used with the NDS/LDAP databases, but either the Cisco PEAP or the Microsoft PEAP supplicants can be used to authenticate with Microsoft domains. However, only the Microsoft PEAP supplicant permits the use of Windows logon credentials to be used for PEAP authentication (single sign-on with Windows credentials).

---

**Note**

After these credentials are entered for a Windows user profile, those credentials will be used for all subsequent PEAP authentications. If it is necessary to change the username associated with a Windows user profile, the username entry must be deleted in the registry, or the profile must be deleted from the machine and re-entered.

Perform these steps to configure static user credentials for the Microsoft PEAP (EAP-MSCHAP v2) supplicant:

**Step 1**

On the PEAP Properties Screen (see Figure 25 for the Microsoft PEAP (EAP-MSCHAP v2) supplicant, click **Properties**, and the Generic Token Card Properties screen appears (see Figure 31).

**Step 2**

Click **Static Password (Windows NT/2000, LDAP)**. Figure 33 appears.
Step 3  The only configurable parameter within the Microsoft PEAP (EAP-MSCHAP v2) supplicant is the option to use Windows credentials for wireless authentication. If desired, check **Automatically use my Windows logon name and password (and domain if any)**.

The user login credential entry screen is shown in Figure 34. When this screen displays, the wireless computer users must enter their usernames, passwords, and the wireless domain name. After a successful authentication, the user can access the wireless network.

**Figure 34  Microsoft Enter Credentials Screen for Users**

---

**Note**  Unlike the Cisco PEAP supplicant, the user is presented with the enter credentials screen at login, regardless of whether the client device can authenticate the server certificate.

---

**Password Change Prompt and GUI**

The PEAP supplicant supports Windows password changes as directed by the Windows NT/ AD database server. Based on the user password expiration policy as configured in the Microsoft domain, a password change message is sent to the client device, and a Password Change screen appears.
Note that the EAP server must be configured to permit password change messaging.

**Cisco PEAP (EAP-GTC) Password Change**

This section describes the password change operation when using the Cisco PEAP supplicant provided with the ACU version 5.05 and later. When the user password expires, the server sends a change password screen to the user (see Figure 35).

![Change Password Screen for Cisco PEAP (EAP-GTC)](image)

Note During the password change process, the new user password credentials for the Cisco PEAP supplicant are not updated in the local cache of the client computer. The new credentials are only updated on the Windows NT/AD database server.

To update the locally cached password for the PEAP supplicant, the user must perform an extra step to synchronize the local password and the Windows domain password. The user must perform one of these steps:

a. Connect to the Windows domain over a non-802.1X secured connection (a wired connection) to update the locally cached credentials.

b. Login to the local computer using the cached password and manually change the computer password (using Ctrl + Alt + Delete > Change Password).

**Microsoft PEAP (EAP-MSCHAP v2) Password Change**

This section describes the password change operation when using the Microsoft PEAP supplicant. When the user password expires, the server sends a change password screen to the user (see Figure 36).
Cisco Aironet Desktop Utility for CB21AG Client Adapter

The Cisco Aironet Desktop Utility (ADU) CB21AG client software, unlike the 350 Series and CB20A client software, includes an 802.1X supplicant, which is installed by default when the client adapter is installed on a PC. This supplicant includes LEAP, EAP-TLS, PEAP (GTC & MSCHAP v2), and WPA capabilities and is included by default with the ADU. Because the CB21AG client software includes 802.1X capability, you are not required to add patches or service packs to the Microsoft operating system or to rely on the Microsoft 802.1X framework in any way.

Note
Microsoft’s 802.1X control (as outlined in the previous sections) can be used with the CB21AG client adapter by disabling the CB21AG software utility or by electing not to install it.

Perform these steps to configure the CB21AG client adapter for PEAP:

Step 1  Create a new profile using the New button from the appropriate Profile Management tab to configure a profile for PEAP authentication with the ADU. On the initial Profile Management screen (see Figure 37), you can configure a profile name, client name, and SSID.
Click the **Security** tab (without clicking OK) and the ADU Security Configuration Screen appears (see Figure 38).

**Step 2**

Configure 802.1x, and select the appropriate 802.1x EAP Type using the drop-down arrow. The ADU provides the capability to configure profiles that support Cisco PEAP (EAP-GTC) or Microsoft PEAP (EAP-MSCHAP v2). This capability provides flexibility in using the client adapter with either Microsoft, OTP, or other external databases through the use of multiple profiles, rather than the installation of a different supplicant.
Step 4  After you have configured general profile settings and the 802.1X EAP Type, click Configure from the Security tab (do not click OK), and choose the appropriate options.

Note The Configure button provides selections by 802.1X EAP Type.

Cisco PEAP (EAP-GTC) Configuration

To configure Cisco PEAP (EAP-GTC) on the ADU, perform these steps:

Step 1  When PEAP (EAP-GTC) is chosen in the 802.1X EAP Type field on the ADU Security Configuration Screen (see Figure 38), click Configure, and Figure 39 appears.

Figure 39  ADU PEAP (EAP-GTC) Configuration

Step 2  Choose the desired CA that issues the EAP Server certificate using the drop-down arrow in the Network Certificate Authority field.

Note The certificate must be manually installed on the operating system of the client computer (or must be a public CA available natively in the operating system) in order to be in the Network Certificate Authority drop-down list.

The User Name field is populated with the PEAP clear username used in accounting.

Note In the initial ADU release (version 1.0.5), you must not check the Use Windows User Name if a Windows login domain is specified in the Windows login.

Step 3  Specify the type of second-phase authentication used with the supplicant in the Set Password section by performing one of these steps:

a. Click Token for use with a One-Time-Password server.

b. Click Static Password for use with username and password databases.
Step 4  Click Advanced, and Figure 40 appears.

**Figure 40  ADU PEAP Advanced Configuration**

[Image of Advanced Configuration window]

Step 5  Enter the Login Name that is used in the second-phase PEAP authentication. This might be the same as the username specified in Figure 39.

**Note**  The Login Name is the user credential that is protected with the server certificate in the PEAP authentication process.

**Note**  With the ADU v1.0.5, *do not* configure the Specific Server or Domain field. Login to multiple domains is not supported with ADU v1.0.5.
Cisco Aironet PEAP (EAP-MSCHAP v2) Configuration

To configure Cisco Aironet PEAP (EAP-MSCHAP v2) on the ADU, perform these steps:

**Step 1** When PEAP (EAP-MSCHAP v2) is chosen in the 802.1X EAP Type field on the ADU Security Configuration Screen (see Figure 38), click **Configure**, and Figure 41 appears.

![Figure 41 PEAP(EAP-MSCHAPv2) Configuration](image)

The PEAP (EAP-MSCHAP v2) configuration process is similar to the Cisco PEAP (EAP-GTC) configuration.

**Step 2** Choose the CA server used to issue the EAP server certificate for PEAP authentication using the drop-down arrow in the Server field.

- **Note** The certificate must be manually installed on the operating system of the client computer (or must be a public CA available natively in the operating system) to be available in the Server field list.

**Step 3** Enter the username and password in the appropriate fields.

Unlike the Cisco PEAP (EAP-GTC) configuration, the User Name and Password fields on the initial configuration screen must be populated by the username and password to be used to authenticate with the PEAP MSCHAP v2 database.

- **Note** In the initial ADU release (version 1.0.5), you must not check the *Use Windows User Name* if a Windows login domain is specified in the Windows login.

- **Note** Do not use the Login Name fields in the Advanced menu.
If you change the username or CA, you should disable and then re-enable the client adapter to re-initialize the supplicant with the new credentials.

Step 4

After configuration of either PEAP supplicant, click the Current Status tab to verify the operation of the client adapter (see Figure 42).

Figure 42  ADU Status screen

The authentication algorithm and authentication status are shown on this status screen.

ACU Installation and Configuration for Windows CE

This section describes the installation and configuration of ACU version 2.4 for Windows CE devices.

Windows CE Software Support for PEAP Operation

There are two major software components required on a Windows CE device for PEAP support:

1. ACU—enables user configuration of 802.11 parameters, such as SSID, power-save mode, network security type, and others.

2. Authentication Manager application—permits configuration of 802.1X parameters, such as a CA certificate with PEAP authentication or a certificate for use with EAP-TLS authentication.
Figure 43 illustrates the applications that are installed with the ACU for Windows CE on a PPC 2002 device.

*Figure 43  Cisco ACU v2.40 Programs*

These applications are used to configure PEAP:

- ACU
- AuthMgr (Authentication Manager)
- CertMgr (Certificate Manager)
ACU Configuration on Windows CE Devices

Perform these steps to configure the ACU:

**Step 1**  
To open the ACU profile manager, double-tap the ACU icon on your desktop, or tap Start > Programs > Cisco > ACU. The ACU Profiles screen appears.

**Step 2**  
From the Manage Profiles box, choose the PEAP profile and tap the Edit button or double-tap the PEAP profile. The ACU PEAP Profile Configuration screen appears (see Figure 44).

*Figure 44  ACU PEAP Profile Configuration*

**Step 3**  
You must configure the ACU for the appropriate SSID, power savings, and other settings to work with the desired wireless network.

**Step 4**  
For PEAP authentication, choose Network Security Type using the scroll bar in the Property field.

**Step 5**  
Choose Host Based EAP using the drop-down arrow in the Value field.

**Step 6**  
Tap OK to activate your settings, and close the ACU.
Certificate Manager Configuration

The CA certificate corresponding to the EAP server certificate must be initially installed on the CE device. You can use a flash memory card or use an ActiveSync connection to a PC. When the certificate is installed in the CE devices memory, perform these steps to configure the CA certificate using the Certificate Manager:

**Step 1** Select **Start > Programs > Cisco > CertMgr**. The Certificate Manager screen appears (see Figure 45).

**Figure 45 Certificate Manager**

![Certificate Manager](image)

**Step 2** Choose **Trusted Authorities** in the Certificate drop-down menu.

**Step 3** Tap the **Import** button to import the certificate file into the Windows certificate store.

**Step 4** The Certificate Manager Open screen appears.

**Step 5** Tap the appropriate CA (X.509) certificate file. The selected certificate file is imported into the Certificate Manager and can be referenced for 802.1X authentication.
Step 6  The Certificate Manager screen reappears with the name of the CA certificate server listed in the middle of the screen (see Figure 46).

**Figure 46  Certificate Manager Confirmation**

![Certificate Manager Confirmation](image)

Step 7  Tap **ok** to close the Certificate Manager.

---

**Authentication Manager Configuration**

Perform these steps for Authentication Manager configuration:

Step 1  Select **Start > Programs > Cisco > AuthMgr**, and Figure 47 appears.

**Figure 47  Authentication Manager Configuration**

![Authentication Manager Configuration](image)
Step 2  Choose Cisco PEAP using the drop-down arrow in the EAP Type field.

Step 3  Tap Properties to configure PEAP authentication parameters, and Figure 48 appears.

**Figure 48  Authentication Manager- PEAP Properties**

![Image of PEAP Properties](example.png)

Step 4  Tap Validate server certificate.

Step 5  Choose the appropriate certificate using the drop-down arrow in the Trusted root certificate field.

Step 6  Tap ok to complete configuration of PEAP properties.

To verify the operation of PEAP authentication perform these steps:

Step 1  Tap the Connect button to initiate 802.1X connection to the EAP server, and Figure 49 appears.

**Figure 49  PEAP Network Log On screen**

![Image of PEAP Network Log On](example.png)
Step 2  Tap the keyboard icon from tray, and enter the PEAP user credentials in the User Name, Password, and Domain fields.

Step 3  Select Start > Programs > Cisco > AuthMgr to display Authentication Manager screen (see Figure 47). You can check the authentication status on the bottom of the screen in the Status and IP Address fields.

Step 4  Click ok to close Authentication Manager screen.

Step 5  You can also check the authentication status using the Status tab on the ACU. To activate the ACU, tap Start > Programs > Cisco > ACU.

Step 6  Tap the Status tab on bottom menu bar, and Figure 50 appears.

Figure 50  ACU Status

Tap ok to close the ACU.

Troubleshooting PEAP Installations

If you experience problems with the operation or tests of PEAP software after installation, use these installation and diagnostic configuration checks. Successful PEAP operation requires 802.1X EAP support in the Microsoft wireless client (Windows XP operating system) and certificate installation and configuration on the Microsoft server where ACS is installed. Perform these steps:

1. Verify that the supplicant for 802.1X EAP has been installed on the PC. Make sure that PEAP is available in the EAP Type drop-down list on the Authentication tab of the Wireless Network Properties screen (see Figure 23).

2. Verify proper configuration of the profile settings in the ACU (see Figure 20). Host Based EAP must be selected in the Network Security Type field on the ACU Network Security Tab.
3. Verify that the client adapter is sending the proper authentication request to the access point. The Cisco Aironet 350 Series access point can send debugging information to a console (or virtual console) port. To see EAP authentication logs, enter `:eap_diag1_on` at the VxWorks access point console prompt.

4. Verify that the external user database in ACS is correctly configured with an Unknown User Policy that contains the appropriate priority in the Selected Databases field (see Figure 12). Also, check any error messages recorded in the ACS authorization log file that is located in:

   `<ACS base directory>\CSAuth\Logs\Auth.log`.
Appendix A: Configuration of the Digital Certificate on the ACS

The PEAP wireless local area network (WLAN) protocol uses TLS as the first-phase authentication mechanism. During phase 1 authentication, the client device authenticates the server with which it will negotiate a user session. To accomplish the TLS session, digital certificates are used (as in a Public Key Infrastructure (PKI)).

PEAP support in the ACS requires that a digital certificate is installed on the Microsoft server that runs ACS. This certificate must be accessible to the ACS application. The PEAP client devices also require the installation of a public key certificate that matches the ACS server certificate. Manual installation of this public certificate is not required. The user of the PEAP client device must accept (or reject) this certificate during initiation of the PEAP session.

This section describes the steps used to obtain and configure a server certificate on the Microsoft server (where the ACS application resides). The steps use a web browser interface.

Note
You can also manually issue a certificate using a local interface to the Microsoft CA.

Note
If the server running the ACS application has a Web Server certificate issued by a valid CA, you do not need to configure CA services on the local machine.

Perform these steps to generate and install a certificate on the ACS server:

Step 1
You must login to the local PC using administrative credentials and open a browser session using this address: http://<localmachine IP>/certsrv, where localmachine IP is the IP address of the local PC. Figure 51 appears.

Figure 51 Microsoft Certification Authority: Certification Request
Step 2  Check **Request a certificate**, and click **Next** to obtain a certificate for the ACS server. **Figure 52** appears.

*Figure 52  Microsoft Certification Authority: Selecting a Request Type*

![Image of Microsoft Certification Authority: Selecting a Request Type]

Step 3  Click **Advanced Request**, and click **Next**. **Figure 53** appears.

*Figure 53  Microsoft Certification Authority: Advanced Certificate Requests Choices*

![Image of Microsoft Certification Authority: Advanced Certificate Requests Choices]
Appendix A: Configuration of the Digital Certificate on the ACS

Step 4  Click **Submit a certificate request to this CA using a form**, and click **Next**. Figure 54 appears.

![Figure 54 Microsoft Certification Authority: Advanced Certificate Request Detail](image)

*Figure 54  Microsoft Certification Authority: Advanced Certificate Request Detail*

Step 5  Complete the advanced certificate request form by performing these steps:

a. Choose **Web Server** using the drop-down arrow in the Certificate Template field.

b. Enter appropriate information in all the fields of the **Identifying Information For Offline Template** section.

  - **Note**  You should record the information entered in the **Name** field for later use. The Name field is used to reference the Certificate Name (CN) within the ACS application.

c. Choose **Microsoft Base Cryptographic Provider v1.0** using the drop-down arrow in the CSP field.

d. Click **Both** in the Key Usage field.

e. Enter **1024** in the Key Size field.

f. Click **Create new Key set**.

g. Check **Mark Keys as exportable**.
h. Check **Use local machine store**.

i. Click **Submit**.

After you submit the Advanced Certificate Request form, the certificate is issued to your local PC (see Figure 55).

*Figure 55 Microsoft Certification Authority: Certificate Issued*

---

**Step 6**
Click **Install this certificate** to install the certificate in the local machine store on your PC.

**Step 7**
You can confirm the certificate installation by clicking **Start > Control Panel > Administrative Control > Certificate Authority**. Figure 56 appears.

*Figure 56 Microsoft Certification Authority: Certificate Installed*
Obtaining the CA Certificate from the Windows CA Server

After the server certificate is installed on the local machine, you must obtain the CA certificate for installation in the ACS application. These steps provide a guideline for obtaining the CA certificate:

**Step 1**
Click Start > Control Panel > Services > Administrative Control to activate the ACS application. Figure 57 appears.

*Figure 57 CA Server Certificate Location*

![CA Server Certificate Location](image)

**Step 1**
Right-click Certificate Authority (Local), and Figure 58 appears.

*Figure 58 Certification Authority Properties*

![Certification Authority Properties](image)
Step 2  
Click **View Certificate** to obtain CA certification information, and **Figure 59** appears.

*Figure 59  Certification Authority Main Screen*
Step 3  Click the **Details** tab to obtain specific parameters for the CA certificate and to access the utility used to copy the CA certificate to a file. Figure 60 appears.

**Figure 60  Certification Authority Details**
Step 4  Click **Copy to File**, and the Certificate Export Wizard helps you create a file copy of the CA certificate (see Figure 61).

**Figure 61  Certificate Export Wizard**
Step 5  Click the desired Export File Format, such as *Base-64 encoded X.509 (.CER)*, and Figure 62 appears.

**Figure 62  Certificate Export Wizard File Export**

![Certificate Export Wizard File Export](image)

Step 6  Enter the path and filename for the CA certificate file in the File name field, or use **Browse** to browse to the desired location. Click **Next**, and Figure 63 appears.

**Note** You should record the certificate filename and path for later use.

**Figure 63  Certificate Export Wizard Completion**

![Certificate Export Wizard Completion](image)
Appendix B: Example of a PEAP Configuration for an Access Point Running Cisco IOS Software

This section provides an example of a simple configuration file for PEAP authentication (or another EAP authentication method).

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AP1200
!
ip subnet-zero
!
aaa new-model
!
aaa group server radius rad_eap
  server <RADIUS_SERVER_IP> auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common

dot11 network-map

bridge irb
!
!
interface Dot11Radio0
  no ip address
  no ip route-cache
  !
  encryption mode wep mandatory mic key-hash
  !
```
ssid PEAP
authentications open eap eap_methods
authentication network-eap eap_methods
guest-mode
!
speed basic-11.0
rts threshold 2312
power local 1
power client 5
station-role root
dot1x client-timeout 45
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption mode wep mandatory mic key-hash
!
ssid PEAP
authentications open eap eap_methods
authentication network-eap eap_methods
guest-mode
!
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address <AP_IP_ADDR> <AP_NETMASK>
no ip route-cache
!
ip default-gateway <DEFAULT_GATEWAY_IP>
ip http server
ip http help-path
ip radius source-interface BVI1
radius-server host <RADIUS_SERVER_IP> auth-port 1645 acct-port 1646 key 7
001612020D4E180D0A38
radius-server attribute 32 include-in-access-req format th
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
!
```
!
line con 0
    exec-timeout 0 0
line vty 0 15
!
end
```