

Install Certificate on the Cisco Secure ACS Appliance for PEAP Clients

Document ID: 64067

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Microsoft Certificate Service Installation

Cisco Secure ACS for Window Certificate Setup

- Step 1: Create a Server Certificate
- Step 2: Approve the Certificate from the CA
- Step 3: Download the Server Certificate to the Cisco Secure ACS Server
- Step 4: Install the CA Certificate on the Cisco Secure ACS Server
- Step 5: Set up Cisco Secure ACS to use the Server Certificate

Cisco Secure ACS Appliance Certificate Setup

- Step 1: Create a Certificate Signing Request
- Step 2: Create a Server Certificate with your CSR
- Step 3: Download CA Certificate to your FTP Server
- Step 4: Install CA Certificate on your Appliance
- Step 5: Install the Server Certificate on your Appliance

Self-signed Certificate Setup (only if you do not use an external CA)

- Configure Global Authentication Settings
- Set up the AP on the Cisco Secure ACS
- Configure the AP
- Install ACU Version 6 (only if you use Cisco Secure ACS 3.1 or if you require EAP-GTC)
- Install the Root CA Certificate for the Client (only for EAP-MSCHAP-V2)
- Set up the Client for PEAP

Machine Authentication Supplement

- Set up ACS to Allow Machine Authentication
- Set up the Client for Machine Authentication

WPA Key Management Supplement

- Configure the AP
- Set up the Windows XP SP1 (with KB826942 installed) or SP2 Client for PEAP and WPA

Verify

Troubleshoot

- Problem 1
- Solution
- Problem 2
- Solution
- Problem 3
- Solution
- Problem 4
- Solution

Related Information

Introduction

This guide describes certificates created with a Microsoft CA and also contains steps for when you use a self-signing certificate, which is supported as of Cisco Secure Access Control Server (ACS) 3.3. The use of a self-signing certificate streamlines the initial Protected Extensible Authentication Protocol (PEAP) installation considerably since no external CA is required. However, at this time, the default expiration period of the self-signing certificate is only one year and cannot be changed. This is standard when it comes to server certificates. However, because the self-signed certificate also acts as the root CA certificate, this can mean the installation of the new certificate on every client every year when you use the Microsoft supplicant unless you do not check the **Validate Server Certificate** option. Cisco recommends that you use self-signing certificates only as a temporary measure until you can use a traditional CA. If you wish to use a self-signing certificate, proceed to the self-signing certificates section.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco IOS® Access Point (AP) 12.02T1
- Cisco Secure ACS for Windows 3.1 and later
- Cisco Secure ACS Solution Engine (SE).
- Microsoft Windows 2000 (SP3 and SP4) or XP with ACU version 6 (if you use Cisco Secure ACS 3.2 the ACU is not required)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Microsoft Certificate Service Installation

Complete these steps:

1. Choose **Start > Settings > Control Panel**.
2. Inside the Control Panel, open **Add/Remove Programs**.
3. In Add/Remove Programs, choose **Add/Remove Windows Components**.
4. Check **Certificate Services** and click **Next**. Click **yes** to the IIS message.
5. Choose a Stand-alone (or Enterprise) root CA and click **Next**.
6. Give the CA a name and click **Next**. All the other boxes are optional.

Note: Do not give the CA the same name as an Cisco Secure ACS server. This can cause PEAP clients to fail authentication because they get confused when a root CA certificate is found with the same name as the server certificate. This problem is not unique to Cisco clients.

7. Click **Next**.

8. Click **Finish**.

Note: You must install IIS before you install the CA.

Cisco Secure ACS for Window Certificate Setup

Step 1: Create a Server Certificate

Complete these steps in order to create a server certificate.

1. From your Cisco Secure ACS server, browse to the CA **http://IP_of_CA_server/certsrv/**.
2. Choose the **Request a certificate** option and click **Next**.
3. Choose **Advanced request** and click **Next**.
4. Choose **Submit a certificate request to this CA using a form** and click **Next**.
5. Type something in the name (CN) box.
6. Choose **Server Authentication Certificate** for Intended Purpose.

Note: Choose **Web Server** on the first drop-down box if you use the Enterprise CA.

- ◆ **CSP** Microsoft Base Cryptographic Provider v1.0
- ◆ **Key Size** 1024**

Note: The Windows 2003 Enterprise CA allows key sizes greater than 1024. However, the use of a key larger than 1024 does not work with PEAP. Authentication might appear to pass in the ACS, but the client just hangs while it attempts authentication.

- ◆ Check **Mark Keys as Exportable** .
- ◆ Check **Use Local Machine Store** (Software ACS only).
- ◆ Leave everything else as default and click **Submit**.

A message appears that states `Your certificate request has been received....`

Note: Certificates created with a key size greater than 1024 do not work.

Note 2

Note: Microsoft has changed the Web Server template with the release of the Windows 2003 Enterprise CA so that keys are no longer exportable and the option is greyed out. There are no other certificate templates supplied with certificate services that are for server authentication and give the ability to mark keys as exportable that are available in the drop-down. Therefore, you need to create a new template that does so.

Complete these steps:

1. Choose **Start > Run > certtmpl.msc**.
2. Right-click the **Web Server** template and choose **Duplicate Template**.
3. Name the template with a name that is easy to identify.
4. Go to the Request Handling tab and check **Allow private key to be exported**.
5. Click on the **CSPs** button and check **Microsoft Base Cryptographic Provider v1.0**. Click **OK**.
6. All other options can be left at default.
7. Click **Apply** and **OK**.
8. Open the CA MMC snap-in.
9. Right-click **Certificate Templates** and choose **New > Certificate Template to Issue**.
10. Choose the new template you created and click **OK**.
11. Restart the CA.

Certificate services can also give a Failed to create 'CertificateAuthority.Request' object error when an attempt is made to create a new certificate. Complete these steps in order to correct this issue:

1. Choose **Start > Administrative Tools > IIS**.
2. Expand **Web Sites > Default Web Site**.
3. Right-click **CertSrv** and choose **Properties**.
4. Click the **Configuration** button in the Application settings section of the Virtual Directory tab.
5. Go to the Options tab and check **Enable session state**.
6. Everything else can be left alone.
7. Click **OK** twice.
8. Restart IIS.

If your browser locks with a Downloading ActiveX Control message, run the fix discussed in the Microsoft document Internet Explorer Stops Responding at "Downloading ActiveX Control" Message When You Try to Use a Certificate Server . If the CSP field only states Loading . . . , make sure you do not run a software firewall on the machine that submits the request.

Step 2: Approve the Certificate from the CA

Complete these steps:

1. Open the CA and choose **Start > Programs > Administrative Tools > Certificate Authority**.
2. On the left, expand the certificate, then click **Pending Requests**.
3. Right-click on the certificate, choose **all tasks**, and choose **Issue**.

Step 3: Download the Server Certificate to the Cisco Secure ACS Server

Complete these steps:

1. From your Cisco Secure ACS server, browse to the CA –**http://IP_of_CA_server/certsrv/** directory.
2. Choose **Check on a Pending Certificate** and click **Next**.
3. Select the certificate and click **Next**.
4. Click **Install**.

Step 4: Install the CA Certificate on the Cisco Secure ACS Server

Complete these steps:

Note: This step is not required if Cisco Secure ACS and the CA are installed on the same server.

1. From your Cisco Secure ACS server, browse to the CA –**http://IP_of_CA_server/certsrv/** directory.
2. Choose **Retrieve the CA certificate or certificate revocation list** and click **Next**.
3. Choose **Base 64 encoded** and click **Download CA certificate**.
4. Click **Open** and choose **Install certificate**.
5. Click **Next**.
6. Choose **Place all certificates in the following store** and click **Browse**.
7. Check the **Show physical stores** box.
8. Expand **Trusted root certification authorities**, choose **Local Computer**, and click **OK**.
9. Click **Next**, **Finish**, and click **OK** for **The import was successful** box.

Step 5: Set up Cisco Secure ACS to use the Server Certificate

Complete these steps:

1. On the Cisco Secure ACS server, click **System Configuration**.
2. Choose **ACS Certificate Setup** and **Install ACS certificate**.
3. Choose **Use certificate from storage**.
4. Type in the CN name and click **Submit**.
5. On the Cisco Secure ACS server, click **System Configuration**.
6. Choose **ACS Certificate Setup** and **Edit Certificate Trust List**.
7. Check the box for the CA and click **Submit**.

Cisco Secure ACS Appliance Certificate Setup

Step 1: Create a Certificate Signing Request

Complete these steps:

1. Choose **System Configuration > ACS Certificate Setup > Generate Certificate Signing Request**.
2. Enter a name in the Certificate subject field with the `cn=name` format.
3. Enter a name for the private key file.

Note: The path to the private key is cached in this field. If you press **submit** a second time after the CSR is created, the private key is overwritten and does not match the original CSR. This result in a `private key does not match` error message when you attempt to install the server certificate.

4. Enter the private key password and confirm it.
5. Choose a key length of 1024.

Note: While Cisco Secure ACS can generate key sizes greater than 1024, the use of a key larger than 1024 does not work with PEAP. Authentication might appear to pass in Cisco Secure ACS, but the client hangs while authentication is attempted.

6. Click **Submit**
7. Copy the CSR output on the right-hand side for submittal to the CA.

Step 2: Create a Server Certificate with your CSR

Complete these steps.

1. From your FTP server, browse to the **CA –`http://IP_of_CA_server/certsrv/`** directory.
2. Choose the **Request a certificate** option and click **Next**.
3. Choose **Advanced Request** and click **Next**.
4. Choose **Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**.
5. Paste the output from the Certificate Signing Request into the Base64 Encoded Certificate Request field and click **Submit**.
6. Click **Download CA certificate**.
7. Click **Save**, name the certificate, and save it to your FTP directory.

Step 3: Download CA Certificate to your FTP Server

Complete these steps:

Note: If you skip these steps, it results in either not being able to enable PEAP. You also receive an error that the server certificate is not installed even though it is or you receive an EAP type not configured failure in failed attempts even though the EAP type is configured.

Note: Also note that if your server certificate is created using an intermediate CA, you need to repeat these steps for every CA in the chain between the root CA and the server certificate, which includes the root CA certificate.

1. From your FTP server, browse to the CA –**http://IP_of_CA_server/certsrv/** directory.
2. Choose **Retrieve the CA certificate or certificate revocation list** and click **Next**.
3. Choose **Base 64 encoded** and click **Download CA certificate**.
4. Click **Save** and name the certificate. Save it to your FTP directory.

Step 4: Install CA Certificate on your Appliance

Complete these steps:

Note: If you skip these steps, it results in either not being able to enable PEAP. You also receive an error that the server certificate is not installed even though it is or you receive an EAP type not configured failure in failed attempts even though the EAP type is configured.

Note: Also note that if your server certificate is created using an intermediate CA, you need to repeat these steps for every CA in the chain between the root CA and the server certificate, which includes the root CA certificate.

1. Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.
2. Click **Download CA certificate file**.
3. Type the IP address or hostname of the FTP server in the FTP Server field.
4. Type a valid username that Cisco Secure ACS can use in order to access the FTP server in the Login field.
5. Type the password of the user in the Password field.
6. Type the relative path from the FTP server root directory to the directory that contains the CA certificate file in the Remote FTP Directory field.
7. Type the name of the CA certificate file in the Remote FTP File Name field.
8. Click **Submit**.
9. Verify the filename in the field and click **Submit**.
10. Restart the ACS services in **System Configuration > Service Control**.

Step 5: Install the Server Certificate on your Appliance

Complete these steps:

1. Choose **System Configuration > ACS Certificate Setup**.
2. Click **Install ACS Certificate**.
3. Choose the **Read certificate** from file option and then click the **Download certificate file** link.
4. Type the IP address or hostname of the FTP server in the FTP Server field.
5. Type a valid username that Cisco Secure ACS can use in order to access the FTP server in the Login field.
6. Type the password of the user in the Password field.
7. Type the relative path from the FTP server root directory to the directory that contains the server certificate file in the Remote FTP Directory field.
8. Type the name of the server certificate file in the Remote FTP File Name field.
9. Click **Submit**.

10. Enter the path to the private key.
11. Enter the password for the private key.
12. Click **Submit**.

Self–signed Certificate Setup (only if you do not use an external CA)

Note: When you test in the lab with self–signed certificates, it results in a longer authentication time the first time a client authenticates with the Microsoft supplicant. All subsequent authentications are fine.

Complete these steps:

1. On the Cisco Secure ACS server, click **System Configuration**.
2. Click **ACS Certificate Setup**.
3. Click **Generate Self–signed Certificate**.
4. Type something into the Certificate subject field preceded by **cn=**, for example, **cn=ACS33**.
5. Type the full path and name of the certificate that you want to create, for example, **c:\acsert\acs33.cer**.
6. Type the full path and name of the private key file that you want to create, for example, **c:\acsert\acs33.pvk**.
7. Enter and confirm the private key password.
8. Choose **1024** from the key length drop–down menu.

Note: While Cisco Secure ACS can generate key sizes greater than 1024, the use of a key larger than 1024 does not work with PEAP. Authentication might appear to pass in ACS, but the client hangs while authentication is attempted.

9. Check **Install generated certificate**.
10. Click **Submit**.

Configure Global Authentication Settings

Complete these steps.

1. On the Cisco Secure ACS server, click **System Configuration**.
2. Click **Global Authentication Setup**.

For Cisco Secure ACS Version 3.2 and Later

- a. Check **Allow EAP–MSCHAPv2** if you use Microsoft PEAP.
- b. Check **Allow EAP–GTC** if you use Cisco PEAP.
- c. Check **Allow MS–CHAP Version 1 Authentication**.
- d. Check **Allow MS–CHAP Version 2 Authentication**.
- e. Click **Submit** and **Restart**.

For Cisco Secure ACS Version 3.1

- a. Check **Allow PEAP**.
- b. Check **Allow MS–CHAP Version 1 Authentication**.
- c. Check **Allow MS–CHAP Version 2 Authentication**.
- d. Click **Submit** and **Restart**.

Set up the AP on the Cisco Secure ACS

Complete these steps:

1. On the Cisco Secure ACS server, click **Network Configuration**.
2. Click **Add Entry** in order to add an AAA client.
3. Fill in these boxes:
 - ◆ **AAA Client IP Address** IP_of_your_AP
 - ◆ **Key** Make up a key, and make sure this matches on the AP shared secret.
 - ◆ **Authenticate Using RADIUS** (Cisco Aironet)
4. Click **Submit** and **Restart**.

Note: None of the defaults on the AAA client setup were changed.

Configure the AP

With VxWorks

Complete these steps:

1. Open the AP and choose **Setup > Security > Authentication Server**.
 - a. Enter the Cisco Secure ACS IP address.
 - b. Enter the shared secret, which must match the **KEY** in Cisco Secure ACS.
 - c. Check **EAP Authentication**.
 - d. Click **OK**.
2. Choose **Setup > Security > Radio Data Encryption**.
 - a. Check **Open** and **Network–EAP** for Accept Authentication Type.
 - b. Check **Open** for Require EAP.
 - c. Set **WEP key 1** and choose **128 bit** if you do not use broadcast key rotation.
 - d. Change Use of Data Encryption by Stations to **full Encryption**. If you cannot change the use of data encryption, click **Apply** first.
 - e. Click **OK**.

With the Cisco IOS AP Web Interface

Complete these steps:

1. Open the AP and choose **Security > Server Manager**.
 - a. Choose **RADIUS** from the Current Server List drop–down.
 - b. Enter the Cisco Secure ACS IP address.
 - c. Enter the shared secret, which must match the 'KEY' in Cisco Secure ACS.
 - d. Check **EAP Authentication**.
 - e. Click **OK** on the warning dialogue and then click **Apply**.
2. Choose **Security > SSID Manager**.

Note: The configuration differs if you use WPA. See the WPA Key Management supplement at the end of this document for details.

- a. Choose the SSID from the Current SSID List or enter a new SSID in the SSID field.

- b. Check **Open Authentication** and choose **with EAP** from the drop-down menu.
 - c. Check **Network EAP**.
 - d. Leave all other values at their defaults and click **Apply**.
3. Choose **Security > Encryption Manager**.

Note: The configuration differs if you use WPA. See the WPA Key Management supplement at the end of this document for details.

- a. Click the **WEP Encryption** radio button and choose **Mandatory** from the drop-down.
- b. Click the **Encryption Key 1** radio button and enter the key in the field.
- c. Choose **128 bit** from the Key Size drop-down.
- d. Click **Apply**.

Note: The network EAP is required if you install the ACU.

Note: If you use broadcast key rotation, you do not need to set a key since the key should already be set. If the key is not set, choose **Setup > Radio Advance** and set a value for the broadcast key rotation. There is no need to set this any lower than five minutes (300 seconds). Once the value is set, click **OK** and go back into the radio data encryption page.

Install ACU Version 6 (only if you use Cisco Secure ACS 3.1 or if you require EAP-GTC)

You need to select CUSTOM install because the Cisco PEAP supplicant is not installed by the express setup. You can tell if the Cisco supplicant is installed when you look at the EAP type in the Authentication tab of your network connection properties. If it shows up as PEAP, this is the Microsoft PEAP supplicant. If it shows up as just PEAP, then you use the Cisco PEAP supplicant.

Install the Root CA Certificate for the Client (only for EAP-MSCHAP-V2)

If You Use the Certificate From Microsoft CA

Complete these steps:

1. From the client PC, browse to the CA –http://IP_of_CA_server/certsrv/.
2. Choose **Retrieve a CA certificate** and click **Next**.
3. Choose **Base64 Encoding** and **Download CA certificate**.
4. Click **Open** and select **Install Certificate**.
5. Click **Next**.
6. Choose **Place all certificates in the following store** and then click **Browse**.
7. Check the **Show physical stores** box.
8. Expand **Trusted root certification authorities**, choose the local computer, and click **OK**.
9. Click **Next**, click **Finish**, and click **OK** for **The import was successful** box.

If you use a Self-signed Certificate from Cisco Secure ACS

Complete these steps:

1. Copy the certificate from its location to the client.
2. Right-click the **.cer** file and click **install certificate**.
3. Click **Next**.
4. Choose **Place all certificates in the following store** and click **Browse**.
5. Check **show physical stores**.

6. Expand **Trusted Root Certification Authorities**, select **Local Computer**, and click **OK**.
7. Click **Next**, click **Finish**, and click **OK**.

Note: Set up the AP for the Cisco Secure ACS is required for each client if you use EAP-MSCHAP-V and have the **Validate server certificate** box checked in Windows' PEAP properties.

Set up the Client for PEAP

Set up Windows XP SP1 or SP for PEAP

Complete these steps:

Note: This configuration differs if you use WPA. See the WPA Key Management section of this document for details.

Note: Windows XP SP2 currently has problems with PEAP authentication to RADIUS servers other than IAS. This is documented in KB885453 and Microsoft has a patch available upon request.

1. Open Network Connections on the control panel and choose **Start > Control Panel**).
2. Right-click the wireless network and choose **Properties**.
3. On the wireless network tab, make sure **use windows to configure...** is checked.
4. If you see the SSID in the list, click **Configure**. If not, click **Add**.
5. Put in the SSID and check **WEP** and **Key is provided for me automatically**.
6. Choose the Authentication tab and make sure **enable network-access control using...** is checked.
7. Choose **Protected EAP** and click **Properties** for the EAP type.
8. Check the box for the **CA** under Trusted root certificate.
9. Click **OK** three times.

Set up Windows XP for the Certificate (without SP1)

Complete these steps:

1. Open Network Connections on the Control Panel and choose **Start > Control Panel**).
2. Right-click the wireless network and choose **Properties**.
3. On the Wireless Network tab, make sure **use windows to configure...** is checked.
4. Choose the Authentication tab and make sure **enable network-access control using...** is checked.
5. Choose **PEAP** and click **Properties** for the EAP type.
6. Check the box for the **CA** under Trusted root certificate.
7. Click **OK** three times.

Set up Windows 2000 for PEAP

Complete these steps:

1. If you run SP3, download and install the 802.1x hotfix from Microsoft. This is not required for SP4.
2. Choose **Start > Control Panel > Network and Dial-up Connections**.
3. Right-click your wireless connection and choose **Properties**.
4. Click on the Authentication tab.

Note: If there is no Authentication tab the 802.1X service is installed in a disabled state. In order to solve this, you must enable the **Wireless Configuration service** in the list of services:

- a. Right-click **My Computer** and click **Manage**.

- b. Choose **Services > Applications** and click **Services**.
 - c. Set the Startup value for the service to **Automatic**, and then start the service.
- Note:** If the Authentication tab is present but is unavailable, this indicates that the network adapter driver does not support 802.1x correctly. Check the list at the bottom of the 802.1x hotfix page or the vendor website for supported drivers.
5. Check **Enable network access control using IEEE 802.1x**.
 6. Choose **PEAP** from the EAP type drop-down menu and click **OK**.

If you use the ACU

Complete these steps:

1. Open the ACU.
2. Choose **Manage Profile** and create a profile or edit one.
3. Put in the client name and SSID of the AP.
4. Choose the Network Security tab.
5. Choose **Host-based EAP** for Network Security Type.
6. Choose **Use Dynamic WEP Keys** for WEP.
7. Click **OK** twice.
8. Choose the profile you created.

Note: If you use the Cisco supplicant, on the Authentication tab you only have PEAP. If you use the Microsoft supplicant, it states Protected EAP (PEAP).

Note: There is a very long delay before the client tries to associate to the AP (about a minute), which can be partially alleviated with the Wireless update rollup package for Windows XP is available patch from Microsoft. This patch can potentially re-install the EAP-MSCHAPv2 supplicant which prevents the EAP-GTC compatible database types from functioning.

Note: If you do not get associated, try to disable and then re-enable the card.

Set up Windows 2003 Mobile for PEAP

Complete these steps:

1. Install the latest release of the Cisco ACU for Windows CE and be sure to install the PEAP supplicant during the install.
2. Open the ACU and choose **<External Settings>** from the Active Profile drop-down menu.
3. Insert your Cisco network card, click on the network icon on the taskbar, and choose **Settings > Advanced > Network Card**.
4. Click on your SSID (if available) or **Add New Settings**.
5. Verify the SSID in the Network Name field and the network to connect to.
6. Click on the Authentication tab.
7. Check **Data encryption (WEP)** and **The key is provided for me....**
8. Check in **Enable network access...802.1x** and choose **Cisco PEAP**.
9. Click **Properties** and check **Validate server certificate** (optional).

Note: When you check this option, it requires that you install the root CA certificate on the PocketPC. Windows Mobile does not include a good method you can use to import/manage certificates. There are a number of utilities available. These utilities are not supported by Cisco. Importing a root CA certificate manually is not required when you use the ACU, since the Cisco PEAP supplicant imports it for you. No version of the PocketPC operating system supports self-signed certificates at this time so you cannot import self-signed certificates into PocketPC for validation. You can still use a self-signed certificate if you uncheck the **Validate server certificate** option.

10. Click **OK** until you are back at the Configure Wireless Networks screen.
11. Click **Connect**.

Machine Authentication Supplement

The purpose of machine authentication is to allow EAP authentication and network connectivity to be established before user authentication so that logon scripts can run and a user can log onto a domain. Domain membership is required for machine credentials to be established and authentication to take place.

Set up ACS to Allow Machine Authentication

Complete these steps:

1. Choose **External User Databases > Database Configuration**.
2. Click **Windows Database** and choose **Configure**.
3. Check **Enable PEAP machine authentication**.
4. Click **Submit**.

Set up the Client for Machine Authentication

Join the Domain (if not already a member of the domain)

Complete these steps:

1. Log into Windows with an account that has administrator privileges.
2. Right-click on **My Computer** and choose **Properties**.
3. Choose the Computer Name tab and click **Change**.
4. Enter the host-name in the Computer name field.
5. Choose **Domain**, enter the name of the domain, and click **OK**.
6. In order to join the domain, a login dialog displays. Login with an account that has permission to join the domain.
7. Once the computer successfully joins the domain, restart the computer. The machine is a member of the domain, and has authentication credentials negotiated with the domain which are only known by the OS. In Cisco Secure ACS, the username appears as host/hostname.

Set up PEAP Supplicant for Machine Authentication

Complete these steps:

1. Choose **Start > Control Panel** in order to open Network Connections on the control panel.
2. Right-click the network connection and choose **Properties**.
3. Choose the Authentication tab and check **Authenticate as computer**.

WPA Key Management Supplement

Written for Cisco IOS AP 12.02(13)JA1, Cisco Secure ACS 3.2, and Windows XP SP1 with the WPA hotfix.

Note: Windows 2000 clients do not natively support WPA key management . You must use the client software of the vendor in order to get this support:

Note: The Cisco ACU does not support WPA key management for host-based EAP (EAP-TLS and PEAP) at this time. You must install a third party client such as the Funk Odyssey client or Meetinghouse AEGIS client.

Refer to WPA Support for more information on WPA support for Cisco products.

Note: Also note that the drivers installed for Cisco cards by the Pocket PC version of the ACU do not support WPA at this time. WPA does not work for Cisco clients on a PocketPC even with a Third party supplicant.

Configure the AP

Complete these steps:

1. Choose **Security > Encryption Manager**.
 - a. Choose **WEP Cipher** and choose **TKIP** from the drop-down.
 - b. Click **Apply**.
2. Choose **Security > SSID Manager**.
 - a. Choose the SSID from the Current SSID List or enter a new SSID in the SSID field.
 - b. Check **Open Authentication** and choose **with EAP** from the drop-down menu.
 - c. Check **Network EAP**.
 - d. Under Authenticated Key Management, choose **Mandatory** from the drop-down menu and click **WPA**.
 - e. Click **Apply**.

Set up the Windows XP SP1 (with KB826942 installed) or SP2 Client for PEAP and WPA

Complete these steps:

1. Choose **Start > Control Panel** in order to open Network Connections on the control panel.
2. Right-click the wireless network and choose **Properties**.
3. On the Wireless Network tab, make sure **use windows to configure...** is checked.
4. If you see the SSID in the list, click **Configure**. If not, click **Add**.
5. Put in the SSID and choose **WPA** for Network Authentication and **TKIP** for Data Encryption.
6. Choose the Authentication tab and make sure that **enable network-access control using...** is checked.
7. Choose **Protected EAP** and click **Properties** for the EAP type.
8. Check the box for the **CA** under Trusted root certificate.
9. Click **OK** three times.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Problem 1

This error occurs during the certificate installation/authentication with ACS.

```
Unsupported private key file format
Failed to initialize PEAP or EAP-TLS authentication protocol because ACS certificate is
not installed
```

Solution

The error occurs because peap certificate is not installed properly. Remove the certificate and install the new self-signed certificate in order to resolve the problem.

Problem 2

This error occurs during the certificate installation/authentication with ACS.

```
Failed to initialize PEAP or EAP-TLS authentication protocol because CA certificate is not installed.
```

Solution

In order to resolve the error, install the CA certificate using ACS Certification Authority Setup. This error occurs due to incorrect CA certificate if the self-signed certificate is not used.

Problem 3

This error occurs when the ACS upgrade is done.

```
A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file. (800B0101)
```

Solution

This error occurs when the ACS software upgrade is done if you do not upgrade the Management Software. Perform the Management software upgrade and then the ACS software upgrade in order to resolve the problem. Refer to the Upgrading the Appliance section of Administering the Cisco Secure ACS Appliance for more information on how to upgrade ACS.

Problem 4

This error occurs during the certificate installation with ACS.

```
Private key you've selected doesn't fit to this certificate
```

Solution

The most common cause of this is accidentally overwriting the private key by generate a new CSR.

Verify this information:

1. You load the correct certificate as the ACS certificate.
2. The RSA pub key length is 1024 bits during the creation of the request.
3. You use the complete CN=string when you generate CSR.

Related Information

- [Cisco Secure ACS for UNIX Support Page](#)
- [Security Products Field Notices \(including CiscoSecure UNIX\)](#)
- [Documentation for Cisco Secure Access Control Server for Unix](#)

- **Cisco Secure ACS for Windows Support Page**
 - **Documentation for Cisco Secure ACS for Windows**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 13, 2007

Document ID: 64067
