



CHAPTER 7

PEAP/EAP-TLS Configuration Scenario

You can select EAP-TLS as an inner method that is used within the tunnel that ACS establishes for PEAP authentication. If you select EAP-TLS, ACS can use it not only to encrypt the initial data sent through the PEAP protocol; but, once a secure tunnel is established between ACS and the NAD, to encrypt (for a second time) the data that is transmitted within the secure tunnel.

This enhanced encryption method greatly enhances the security of communications between ACS and the NAD.

Most customers who will use this feature are customers who use Microsoft supplicants.

Summary of Configuration Steps

To configure PEAP-TLS:

-
- Step 1** Configure security certificates.
See [Step 1: Configure Security Certificates, page 7-1](#) for details.
 - Step 2** Configure global authentication settings.
See [Step 2: Configure Global Authentication Settings, page 7-5](#) for details.
 - Step 3** Specify EAP-TLS options.
See [Step 3: Specify EAP-TLS Options, page 7-6](#) for details.
-

The following sections provide more details about the previous steps.

Step 1: Configure Security Certificates

This section describes a simplified procedure for the ACS for Windows platform. For detailed information on installing certificates and for information on how to install certificates on the Cisco Secure ACS Solution Engine platform, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.2*, “Advanced Configuration: Authentication and Certificates.”

Obtain Certificates and Copy Them to the ACS Host

To use EAP-TLS, you must obtain and install security certificates.

To copy a certificate to the ACS host:

-
- Step 1** Obtain a security certificate.
- Step 2** Create a `\Certs` directory on the ACS server.
- Open a DOS command window.
 - To create a certificates directory, enter:

```
mkdir <selected_drive>:\Certs
```

where *selected_drive* is the currently selected drive.
- Step 3** Copy the following files to the `\Certs` directory:
- `server.cer` (server certificate)
 - `server.pvk` (server certificate private key)
 - `ca.cer` (CA certificate)
-

Run the Windows Certificate Import Wizard to Install the Certificate

To run the Windows Certificate Import wizard to install the certificate on the server:

-
- Step 1** Start Windows Explorer.
- Step 2** Go to `<selected_drive>:\Certs`.
where *selected_drive* is the currently selected drive.
- Step 3** Double-click the `\Certs\ca.cer` file.
The Certificate dialog appears.

- Step 4** Select **Install Certificate**.
The Windows Certificate Import wizard starts.
- Step 5** To install the certificate, follow the instructions that the wizard displays.
- Step 6** Accept the default options for the wizard.



Note Only perform this process once on a Windows 2000 Server.

Enable Security Certificates on the ACS Installation

To enable security certificates:

- Step 1** In the navigation bar, click **System Configuration**.
The System Configuration page opens.
- Step 2** Click **ACS Certificate Setup**.
- Step 3** Click **Install ACS Certificate**.
- Step 4** The Install ACS Certificate page opens, shown in [Figure 7-1](#).

Figure 7-1 *Install ACS Certificate Page*

Install ACS Certificate

Install new certificate

Read certificate from file
Certificate file

Use certificate from storage
Certificate CN

Private key file
Private key password

Back to Help

156380

- Step 5** Ensure that you click the **Read certificate from file** radio button.
- Step 6** In the Certificate file text box, enter the server certificate location (path and name); for example `c:\Certs\server.cer`.
- Step 7** In the Private Key File text box, type the server certificate private key location (path and name); for example: `c:\Certs\server.pvk`.
- Step 8** In the Private Key password text box, type `1111`.
- Step 9** Click **Submit**.

- Step 10** ACS displays a message indicating that the certificate has been installed and instructs you to restart the ACS services.
- Step 11** Do not restart the services at this time.
- Restart the services later, after you have completed the steps for adding a trusted certificate. See [Add a Trusted Certificate](#), page 7-4.

Install the CA Certificate

To install the CA Certificate:

- Step 1** Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.
- Step 2** The ACS Certification Authority Setup page appears, shown in [Figure 7-2](#).

Figure 7-2 ACS Certification Authority Setup Page



- Step 3** In the CA certificate file box, type the CA certificate location (path and name). For example:
`c:\Certs\ca.cer`
- Step 4** Click **Submit**.

Add a Trusted Certificate

After you add a server certificate and set up the certificate authority, install a trusted certificate.

To add a trusted certificate:

- Step 1** Choose **System Configuration > ACS Certificate Setup > Edit Certificate Trust List**.
- The Edit Certificate Trust List appears.
- Step 2** Locate the trusted certificate that you want to install and check the check box next to the certificate name.
- For example, find the **Stress** certificate and check the check box next to it.

Step 3 Click **Submit**.

Step 4 To restart ACS, choose **System Configuration > Service Control**, and then click and then click **Restart**.

Step 2: Configure Global Authentication Settings

To configure global authentication settings:

Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **Global Authentication Setup**.

The Global Authentication Setup page opens, as shown in [Figure 7-3](#).

Figure 7-3 Global Authentication Setup Page

Global Authentication Setup

EAP Configuration

PEAP

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

158448

- Step 3** Specify the protocols to use with the PEAP protocol. They are:
- EAP_MSCHAP2
 - EAP-GTC
- Step 4** If you want to enable posture validation on this ACS installation, check the **Enable Posture Validation** check box.
-

Step 3: Specify EAP-TLS Options

Specify one or more of the certificate comparison options for EAP-TLS:

- **Certificate SAN Comparison**—Based on the name in the Subject Alternative Name (SAN) field in the user certificate.
- **Certificate CN Comparison**—Based on the name in the Subject Common Name (CN) field in the user certificate.
- **Certificate Binary Comparison**—Based on a binary comparison between the user certificate in the user object in the LDAP server or Active Directory and the certificate that the user presents during EAP-TLS authentication. You cannot use this comparison method to authenticate users in an ODBC external user database.

Step 4: (Optional) Configure Authentication Policy

You can enable EAP-TLS when you set up an authentication policy in the protocols section of Network Access Profile configuration.

Figure 7-4 shows the modified EAP configuration section on the NAP Protocols page.

Figure 7-4 EAP Configuration Section of NAP Protocols Page

EAP Configuration	
PEAP	
<input type="checkbox"/>	Allow EAP-MSCHAPv2
<input type="checkbox"/>	Allow EAP-GTC
<input checked="" type="checkbox"/>	Allow Posture Validation
<input type="checkbox"/>	Allow EAP-TLS

158847