

# Cisco Secure ACS for Windows v3.2 With PEAP-MS-CHAPv2 Machine Authentication

Document ID: 43486

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Background Theory
- Conventions
- Network Diagram

#### Configure Cisco Secure ACS for Windows v3.2

- Obtain a Certificate for the ACS Server
- Configure ACS to Use a Certificate From Storage
- Specify Additional Certificate Authorities That the ACS Should Trust
- Restart the Service and Configure PEAP Settings on the ACS
- Specify and Configure the Access Point as an AAA Client
- Configure the External User Databases
- Restart the Service

#### Configure the Cisco Access Point

#### Configure the Wireless Client

- Configure MS Certificate Machine Autoenrollment
- Join the Domain
- Manually Install the Root Certificate on the Windows Client
- Configure the Wireless Networking

#### Verify

#### Troubleshoot

#### Related Information

## Introduction

This document demonstrates how to configure Protected Extensible Authentication Protocol (PEAP) with Cisco Secure ACS for Windows version 3.2.

For more information on how to configure secure wireless access using Wireless LAN controllers, Microsoft Windows 2003 software, and Cisco Secure Access Control Server (ACS) 4.0, refer to PEAP under Unified Wireless Networks with ACS 4.0 and Windows 2003.

## Prerequisites

### Requirements

There are no specific prerequisites for this document.

### Components Used

The information in this document is based on the software and hardware versions below.

- Cisco Secure ACS for Windows version 3.2
- Microsoft Certificate Services (installed as Enterprise root certificate authority [CA])

**Note:** For more information, refer to [Step-by-Step Guide to Setting up a Certification Authority](#).

- DNS Service with Windows 2000 Server with Service Pack 3

**Note:** If you experience CA Server problems, install hotfix 323172. The Windows 2000 SP3 Client requires hotfix 313664 to enable IEEE 802.1x authentication.

- Cisco Aironet 1200 Series Wireless Access Point 12.01T
- IBM ThinkPad T30 running Windows XP Professional with Service Pack 1

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

## Background Theory

Both PEAP and EAP-TLS build and use a TLS/Secure Socket Layer (SSL) tunnel. PEAP uses only server-side authentication; only the server has a certificate and proves its identity to the client. EAP-TLS, however, uses mutual authentication in which both the ACS (authentication, authorization, and accounting [AAA]) server and clients have certificates and prove their identities to each other.

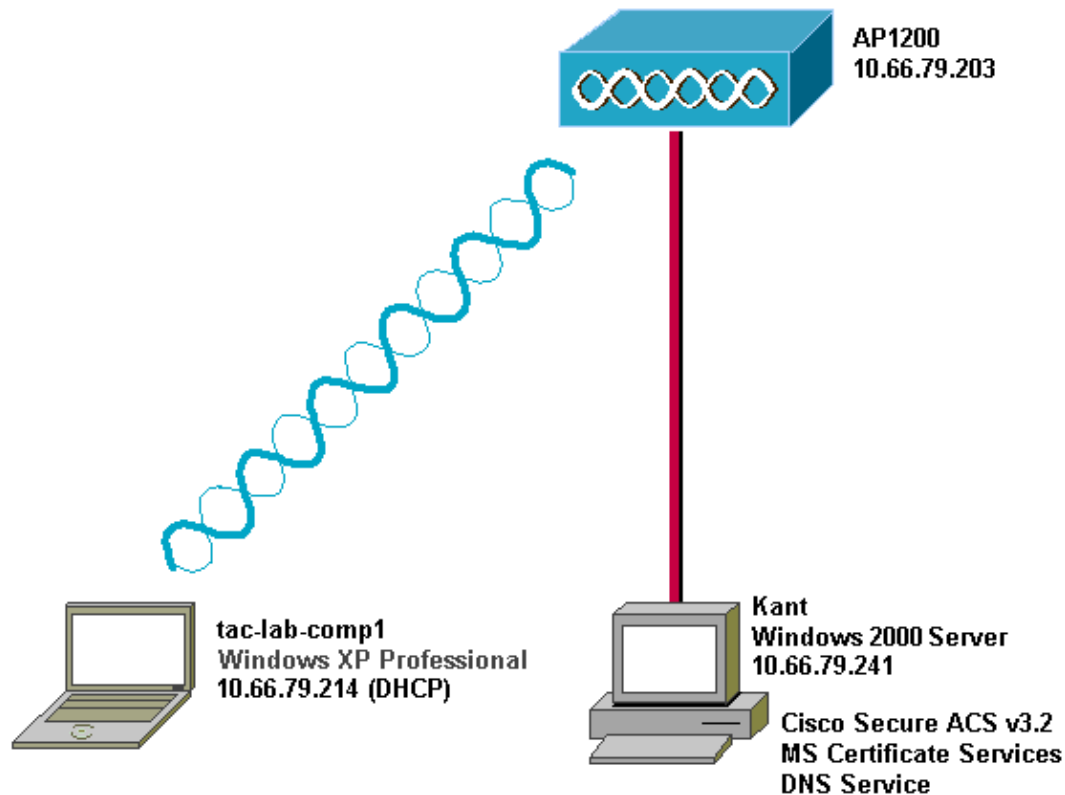
PEAP is convenient because clients do not require certificates. EAP-TLS is useful for authenticating headless devices, because certificates require no user interaction.

## Conventions

For more information on document conventions, see the [Cisco Technical Tips Conventions](#).

## Network Diagram

This document uses the network setup shown in the diagram below.



## Configure Cisco Secure ACS for Windows v3.2

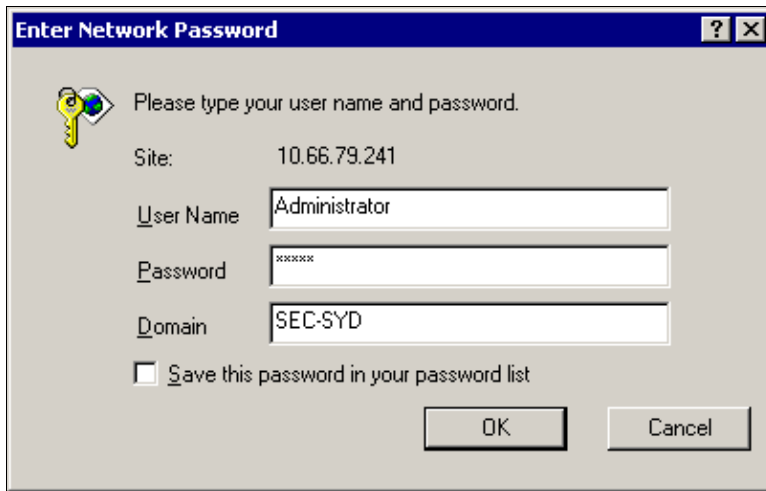
Follow these steps to configure ACS 3.2.

1. Obtain a certificate for the ACS server.
2. Configure ACS to use a certificate from storage.
3. Specify additional certificate authorities that the ACS should trust.
4. Restart the service and configure PEAP settings on the ACS.
5. Specify and configure the access point as an AAA client.
6. Configure the external user databases.
7. Restart the service.

### Obtain a Certificate for the ACS Server

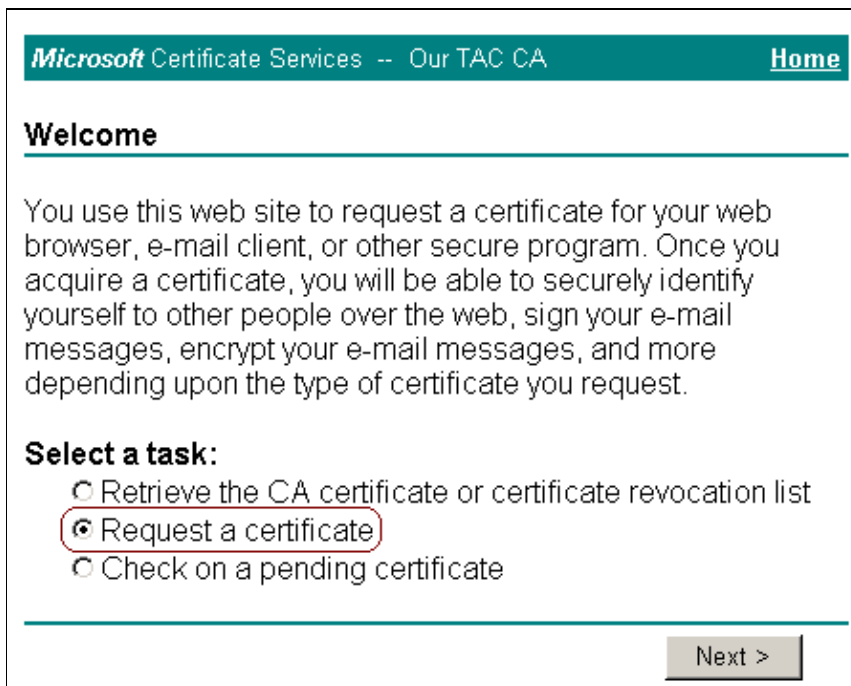
Follow these steps to obtain a certificate.

1. On the ACS server, open a web browser and browse to the CA server by entering **http://CA-ip-address/certsrv** in the address bar. Log in to the domain as Administrator.



The image shows a Windows dialog box titled "Enter Network Password". It contains a key icon and the text "Please type your user name and password." Below this, there are four input fields: "Site:" with the value "10.66.79.241", "User Name" with "Administrator", "Password" with "\*\*\*\*\*", and "Domain" with "SEC-SYD". There is a checkbox labeled "Save this password in your password list" which is unchecked. At the bottom right, there are "OK" and "Cancel" buttons.

2. Select **Request a certificate**, and then click **Next**.



The image shows a web page from Microsoft Certificate Services. The header includes "Microsoft Certificate Services -- Our TAC CA" and a "Home" link. The main content area has a "Welcome" heading followed by a paragraph explaining the purpose of the site. Below this, there is a "Select a task:" section with three radio button options: "Retrieve the CA certificate or certificate revocation list", "Request a certificate" (which is selected and circled in red), and "Check on a pending certificate". At the bottom right, there is a "Next >" button.

3. Select **Advanced request**, and then click **Next**.

**Microsoft** Certificate Services -- Our TAC CA [Home](#)

## Choose Request Type

Please select the type of request you would like to make:

User certificate request:

User Certificate

Advanced request

[Next >](#)

4. Select **Submit a certificate request to this CA using a form**, and then click **Next**.

**Microsoft** Certificate Services -- Our TAC CA [Home](#)

## Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

Submit a certificate request to this CA using a form.

Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.  
*You must have an enrollment agent certificate to submit a request for another user.*

[Next >](#)

5. Configure the certificate options.

- a. Select **Web Server** as the certificate template. Enter the name of the ACS server.

## Advanced Certificate Request

### Certificate Template:

### Identifying Information For Offline Template:

- b. Set the key size to **1024**. Select the options for **Mark keys as exportable** and **Use local machine store**. Configure other options as needed, and then click **Submit**.

### Key Options:

Key Usage:  Exchange  Signature  Both

Key Size:  Min: 384 Max: 1024 (common key sizes: [512](#) [1024](#))

 Create new key set Set the container name Use existing key set Enable strong private key protection Mark keys as exportable Export keys to file Use local machine store

*You must be an administrator to generate a key in the local machine store.*

### Additional Options:

Hash Algorithm:

*Only used to sign request.*

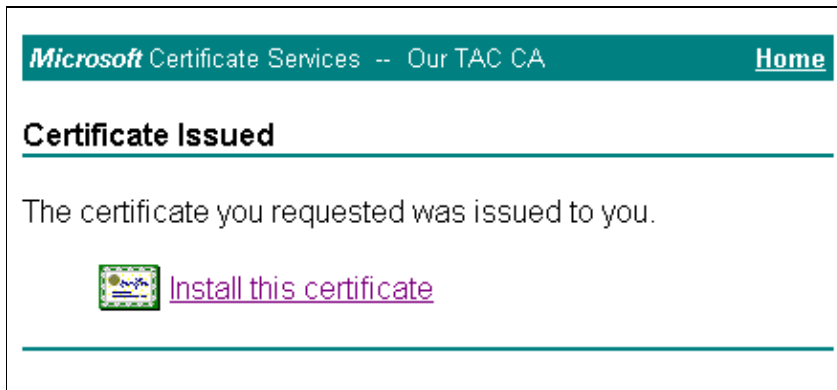
 Save request to a PKCS #10 file

Attributes:

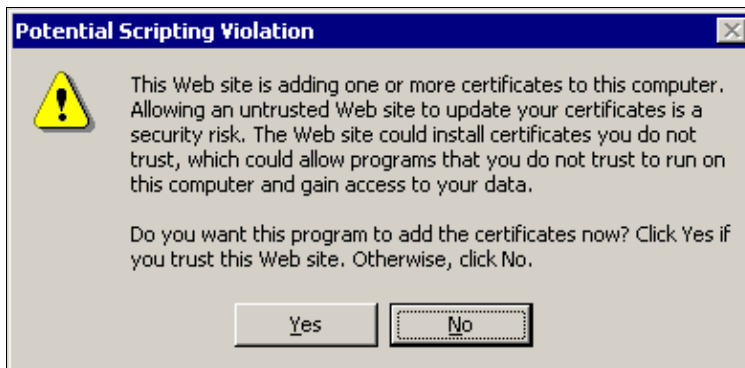
**Note:** If you see a warning window referring to a scripting violation (depending on your browser's security/privacy settings), click **Yes** to continue.



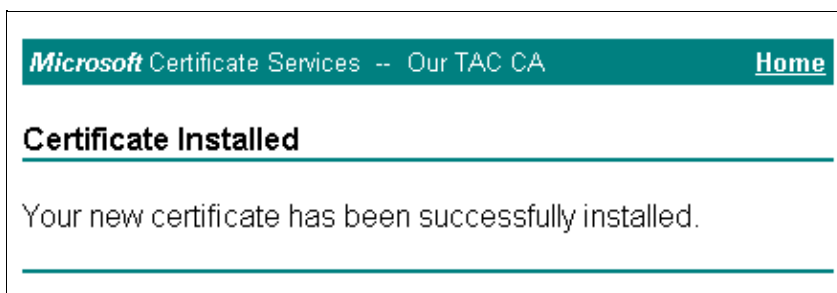
6. Click **Install this certificate**.



**Note:** If you see a warning window referring to a scripting violation (depending on your browser's security/privacy settings), click **Yes** to continue.



7. If the installation has been successful, you will see a confirmation message.



## Configure ACS to Use a Certificate From Storage

Follow these steps to configure ACS to use the certificate in storage.

1. Open a web browser and browse to the ACS server by entering **http://ACS-ip-address:2002/** in the address bar. Click **System Configuration**, and then click **ACS Certificate Setup**.
2. Click **Install ACS Certificate**.
3. Select **Use certificate from storage**. In the Certificate CN field, enter the name of the certificate that you assigned in step 5a of the section Obtain a Certificate for the ACS Server. Click **Submit**.

This entry must match the name that you typed in the Name field during the advanced certificate request. It is the CN name in the subject field of the server certificate; you can edit the server certificate to check for this name. In this example, the name is "OurACS". Do *not* enter CN name of issuer.

The screenshot shows the Cisco Systems System Configuration web interface. The page title is "System Configuration" and the sub-page is "Install ACS Certificate". The interface is in "Edit" mode. On the left is a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Install ACS Certificate" and contains the following fields and options:

- Install new certificate** (with a help icon)
- Read certificate from file
- Use certificate from storage
- Certificate file** (text input field)
- Certificate CN** (text input field containing "OurACS")
- Private key file** (text input field)
- Private key password** (text input field)

At the bottom of the form area is a "Back to Help" button. At the bottom of the page are "Submit" and "Cancel" buttons.

4. When the configuration is complete, you will see a confirmation message indicating that the configuration of the ACS server has been changed.

**Note:** You do not need to restart the ACS at this time.



**CISCO SYSTEMS**

# System Configuration

Edit

**Install ACS Certificate**

**Installed Certificate Information** ?

**Issued to:** OurACS  
**Issued by:** Our TAC CA  
**Valid from:** June 23 2003 at 02:19:56  
**Valid to:** June 18 2005 at 00:52:30  
**Validity:** OK

**The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.**

Install New Certificate    Cancel

## Specify Additional Certificate Authorities That the ACS Should Trust

The ACS will automatically trust the CA that issued its own certificate. If the client certificates are issued by additional CAs, then you need to complete the following steps.

1. Click **System Configuration**, and then click **ACS Certificate Setup**.
2. Click **ACS Certificate Authority Setup** to add CAs to the list of trusted certificates. In the field for CA certificate file, enter the location of the certificate, and then click **Submit**.

**CISCO SYSTEMS** System Configuration

**Edit**

**ACS Certification Authority Setup**

**CA Operations** ?

Add new CA certificate to local certificate storage

CA certificate file

[? Back to Help](#)

The screenshot shows the Cisco System Configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'ACS Certification Authority Setup' and features a 'CA Operations' section with a help icon. Below this, there is a text input field for 'CA certificate file' and a 'Back to Help' button.

3. Click **Edit Certificate Trust List**. Check all the CAs that the ACS should trust, and uncheck all the CAs that the ACS should not trust. Click **Submit**.

**CISCO SYSTEMS** System Configuration

**Edit**

**Edit Certificate Trust List**

**Edit the Certificate Trust List (CTL)**

**Display Name (Friendly Name)**

- ABA.ECOM Root CA  
(DST (ABA.ECOM) CA)
- Autoridad Certificadora de la Asociacion Na  
(Autoridad Certificadora de la Asociacion N)
- Autoridad Certificadora del Colegio Naciona
- Baltimore EZ by DST  
(DST (Baltimore EZ) CA)
- Belgacom E-Trust Primary CA
- C&W HKT SecureNet CA Class A  
(CW HKT SecureNet CA Class A)
- C&W HKT SecureNet CA Class B  
(CW HKT SecureNet CA Class B)

The screenshot shows the 'Edit Certificate Trust List' page in the Cisco System Configuration interface. The left navigation menu is the same as in the previous screenshot, with 'System Configuration' highlighted. The main content area is titled 'Edit Certificate Trust List' and contains a section 'Edit the Certificate Trust List (CTL)'. Below this, there is a list of CA entries with checkboxes for selection. The entries include various CA names and their friendly names, such as 'ABA.ECOM Root CA' and 'Autoridad Certificadora de la Asociacion Na'.

## Restart the Service and Configure PEAP Settings on the ACS

Follow these steps to restart the service and configure PEAP settings.

1. Click **System Configuration**, and then click **Service Control**.
2. Click **Restart** to restart the service.
3. To configure PEAP settings, click **System Configuration**, and then click **Global Authentication Setup**.
4. Check the two settings shown below, and leave all other settings as default. If you wish, you can specify additional settings, such as Enable Fast Reconnect. When you are finished, click **Submit**.

- ◆ **Allow EAP-MSCHAPv2**

- ◆ **Allow MS-CHAP Version 2 Authentication**

**Note:** For more information on Fast Connect, refer to "Authentication Configuration Options" in System Configuration: Authentication and Certificates.

**CISCO SYSTEMS**

# System Configuration

**Edit**

## Global Authentication Setup

### EAP Configuration

**PEAP**

- Allow EAP-MSCHAPv2
- Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

**EAP-TLS**

- Allow EAP-TLS

Select one or more of the following options:

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

EAP-TLS session timeout (minutes):

**LEAP**

- Allow LEAP (For Aironet only)

**EAP-MD5**

- Allow EAP-MD5

### MS-CHAP Configuration

- Allow MS-CHAP Version 1 Authentication
- Allow MS-CHAP Version 2 Authentication

**User Setup**

**Group Setup**

**Shared Profile Components**

**Network Configuration**

**System Configuration**

**Interface Configuration**

**Administration Control**

**External User Databases**

**Reports and Activity**

**Online Documentation**

## Specify and Configure the Access Point as an AAA Client

Follow these steps to configure the access point (AP) as an AAA client.

1. Click **Network Configuration**. Under AAA Clients, click **Add Entry**.

**CISCO SYSTEMS**

# Network Configuration

Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

**AAA Clients**

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

**AAA Servers**

AAA Server Name	AAA Server IP Address	AAA Server Type
<a href="#">kant</a>	10.66.79.241	CiscoSecure ACS

2. Enter the AP's hostname in the AAA Client Hostname field and its IP address in the AAA Client IP Address field. Enter a shared secret key for the ACS and the AP in the Key field. Select **RADIUS (Cisco Aironet)** as the authentication method. When you are finished, click **Submit**.

**CISCO SYSTEMS** Network Configuration

**Edit**

### Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

## Configure the External User Databases

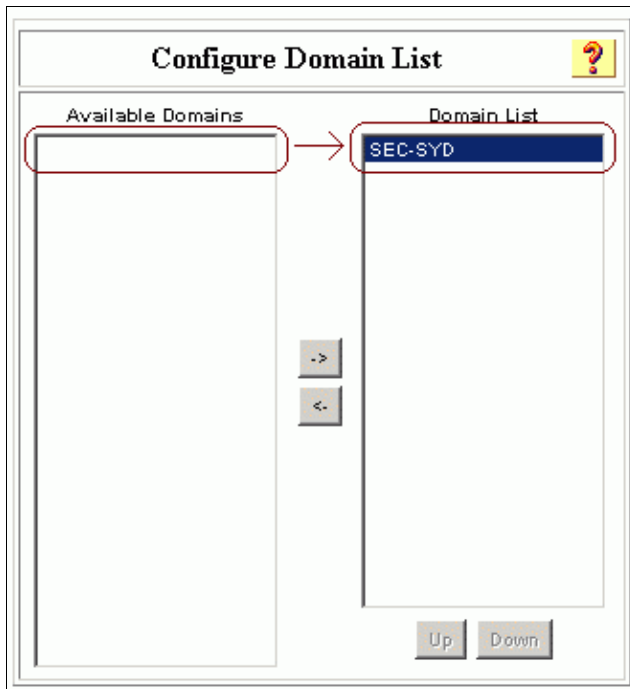
Follow these steps to configure the external user databases.

**Note:** Only ACS 3.2 supports PEAP-MS-CHAPv2 with machine authentication to a Windows database.

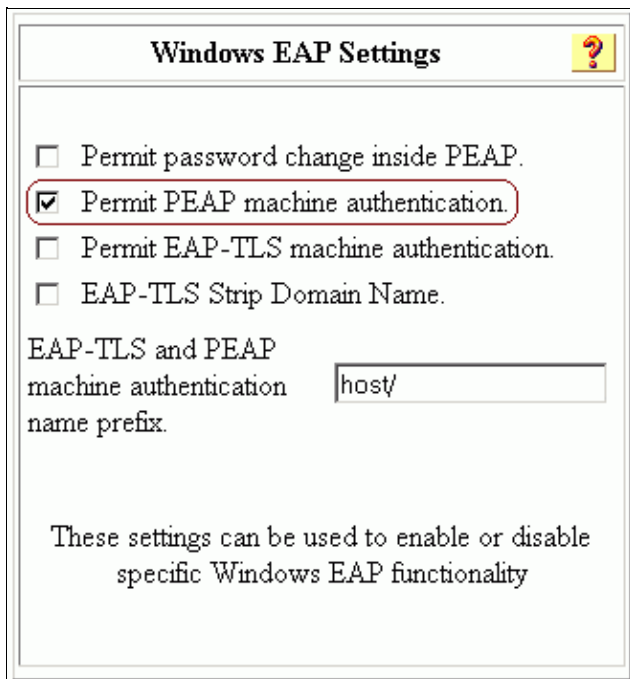
1. Click **External User Databases**, and then click **Database Configuration**. Click **Windows Database**.

**Note:** If there is no Windows database already defined, click **Create New Configuration**, and then click **Submit**.

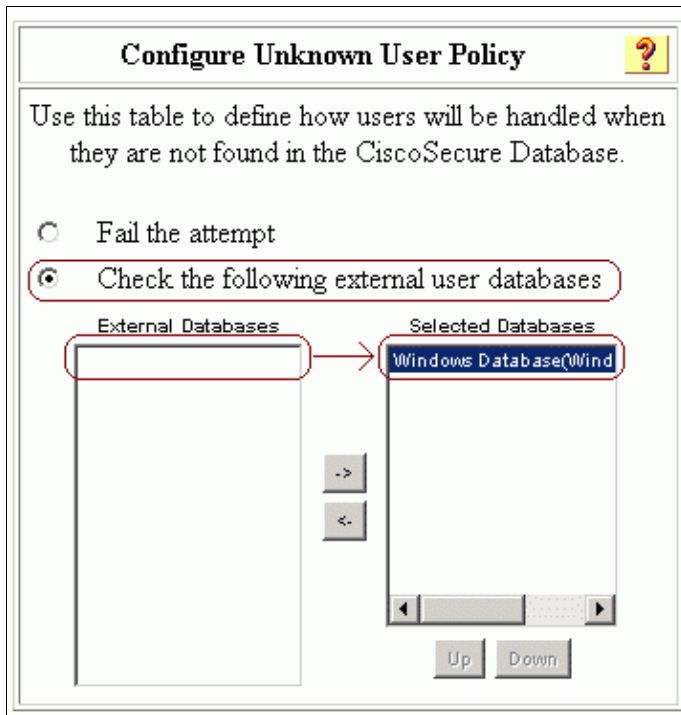
2. Click **Configure**. Under Configure Domain List, move the SEC-SYD domain from Available Domains to Domain List.



3. To enable machine authentication, under Windows EAP Settings check the option to **Permit PEAP machine authentication**. *Do not* change the machine authentication name prefix. Microsoft currently uses "/host" (the default value) to distinguish between user and machine authentication. If you wish, check the option for **Permit password change inside PEAP**. When you are finished, click **Submit**.



4. Click **External User Databases**, and then click **Unknown User Policy**. Select the option for **Check the following external user databases**, then use the right arrow button ( -> ) to move Windows Database from External Databases to Selected Databases. When you are finished, click **Submit**.



## Restart the Service

When you have finished configuring the ACS, follow these steps to restart the service.

1. Click **System Configuration**, and then click **Service Control**.
2. Click **Restart**.

## Configure the Cisco Access Point

Follow these steps to configure the AP to use the ACS as the authentication server.

1. Open a web browser and browse to the AP by entering **http://AP-ip-address/certsrv** in the address bar. On the toolbar, click **Setup**.
2. Under Services, click **Security**.
3. Click **Authentication Server**.

**Note:** If you have configured accounts on the AP, you will need to log in.

4. Enter the authenticator configuration settings.
  - ◆ Select **802.1x-2001** for the 802.1x Protocol Version (for EAP Authentication).
  - ◆ Enter the IP address of the ACS server in the Server Name/IP field.
  - ◆ Select **RADIUS** as the Server Type.
  - ◆ Enter **1645** or **1812** in the Port field.
  - ◆ Enter the shared secret key that you specified in step 2 of Specify and Configure the Access Point as an AAA Client.
  - ◆ Check the option for **EAP Authentication** to specify how the server should be used.

When you are finished, click **OK**.



### AP1200-eac9c4 Authenticator Configuration

Cisco 1200 Series AP 12.01T

Map Help

802.1X Protocol Version (for EAP Authentication):

Primary Server Reattempt Period (Min.):

Server Name/IP	Server Type	Port	Shared Secret
<input type="text" value="10.66.79.241"/>	<input type="text" value="RADIUS"/>	<input type="text" value="1645"/>	<input type="text" value="AAAAAAAA"/>

Use server for:  EAP Authentication  MAC Address Authentication  User Authentication

5. Click **Radio Data Encryption (WEP)**.

6. Enter the internal data encryption settings.

- ◆ Select **Full Encryption** to set the level of data encryption.

- ◆ Enter an encryption key and set the key size to **128 bit** to be used as a broadcast key.

When you are finished, click **OK**.

### AP1200-eac9c4 AP Radio: Internal Data Encryption

Cisco 1200 Series AP 12.01T

Map Help

Uptime: 4 days, 01:18:45

IF VLANs are *not* enabled, set Radio Data Encryption on this page. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

Use of Data Encryption by Stations is:

Accept Authentication Type:  Open  Shared  Network-EAP

Require EAP:

Transmit With Key	Encryption Key	Key Size
WEP Key 1: <input checked="" type="checkbox"/>	<input type="text" value="12345678901234567890abcdef"/>	<input type="text" value="128 bit"/>
WEP Key 2: <input type="checkbox"/>	<input type="text"/>	<input type="text" value="not set"/>
WEP Key 3: <input type="checkbox"/>	<input type="text"/>	<input type="text" value="not set"/>
WEP Key 4: <input type="checkbox"/>	<input type="text"/>	<input type="text" value="not set"/>

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).  
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).  
This radio supports Encryption for all Data Rates.

Apply OK Cancel Restore Defaults

7. Confirm that you are using the correct Service Set Identifier (SSID) by going to **Network > Service Sets >** Select the SSID Idx , and click **OK** when you are finished.

The example below shows the default SSID "tsunami."

AP1200-eac9c4 **AP Radio: Internal Data Encryption** **CISCO SYSTEMS**

Cisco 1200 Series AP 12.01T

Uptime: 4 days, 01:18:45

Map Help

Device: AP Radio: Internal

Service Set ID (Primary SSID): tsunami

Current Number of Associations: 0

Maximum Number of Associations: 0

Classify Workgroup Bridges as Network Infrastructure:  yes  no

Proxy Mobile IP is enabled:  yes  no

Default VLAN ID: [0] -None-

Default Policy Group ID: [0] -None-

Accept Authentication Type:  Open  Shared  Network-EAP

Require EAP:

Default Unicast Address Filter: Allowed Allowed Allowed

To require static or server-based MAC-Address authentication, set "Default Unicast Address Filter" to "Disallowed".

Apply OK Cancel Restore Defaults

## Configure the Wireless Client

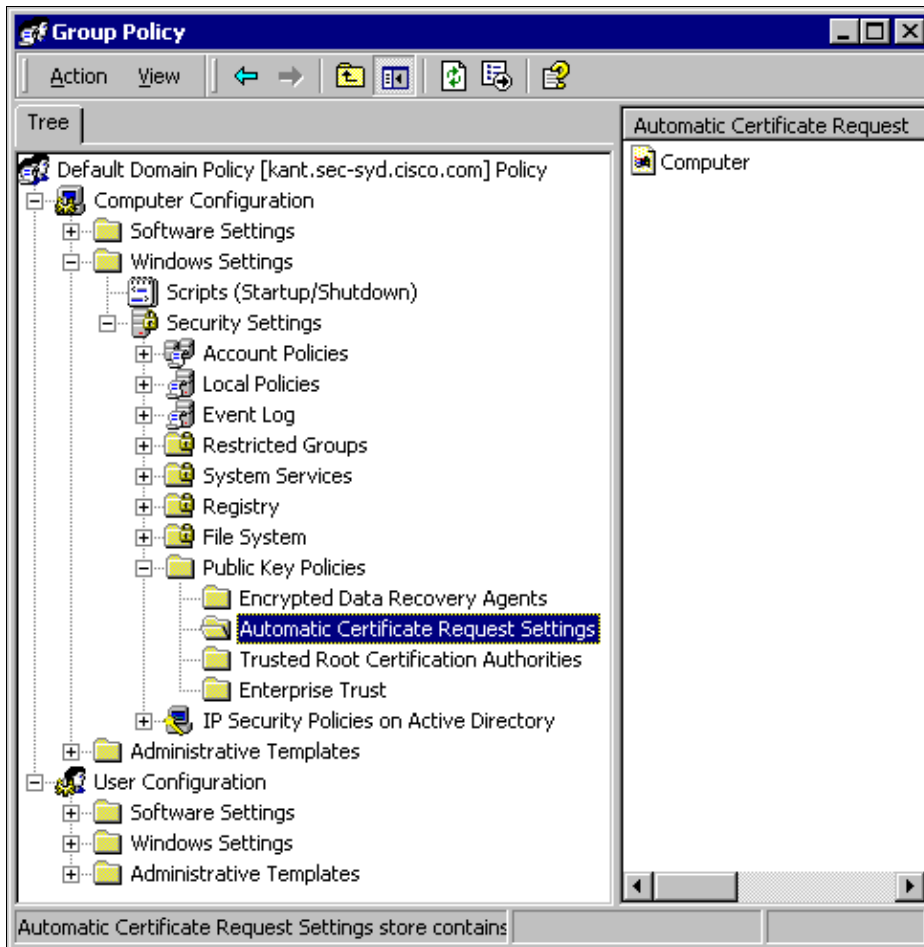
Follow these steps to configure ACS 3.2.

1. Configure MS certificate machine autoenrollment.
2. Join the domain.
3. Manually install the root certificate on the Windows client.
4. Configure the wireless networking.

## Configure MS Certificate Machine Autoenrollment

Follow these steps to configure the domain for automatic machine certificate enrollment on domain controller Kant.

1. Go to **Control Panel > Administrative Tools > Open Active Directory Users and Computers**.
2. Right-click on **domain sec-syd** and select **Properties** from the submenu.
3. Select the **Group Policy** tab. Click **Default Domain Policy**, and then click **Edit**.
4. Go to **Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Automatic Certificate Request Settings**.



5. On the menu bar, go to **Action > New > Automatic Certificate Request** and click **Next**.
6. Select **Computer** and click **Next**.
7. Check the CA.

In this example, the CA is named "Our TAC CA."

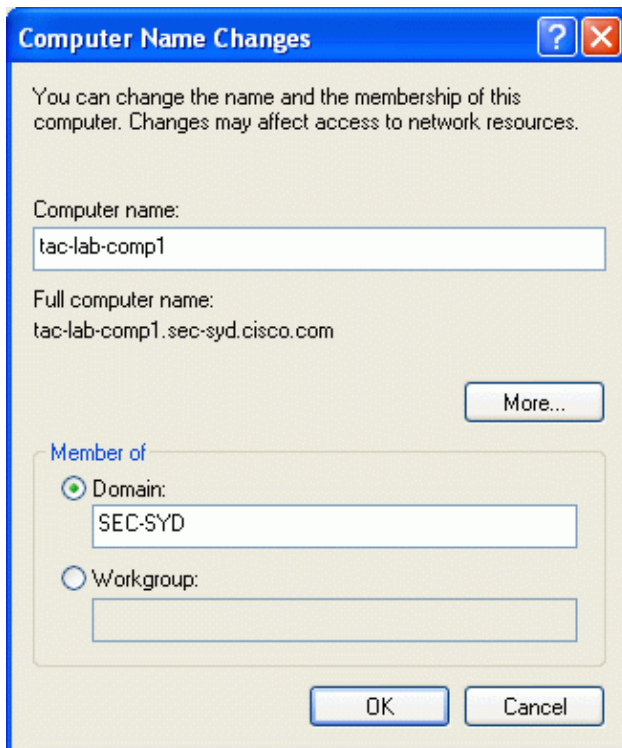
8. Click **Next**, and then click **Finish**.

## Join the Domain

Follow these steps to add the wireless client to the domain.

**Note:** To complete these steps, the wireless client must have connectivity to the CA, either through a wired connection or through the wireless connection with 802.1x security disabled.

1. Log in to Windows XP as local administrator.
2. Go to **Control Panel > Performance and Maintenance > System**.
3. Select the **Computer Name** tab, and then click **Change**. Enter the host name in the field for computer name. Select **Domain**, and then enter the name of the domain (SEC-SYD in this example). Click **OK**.



4. When a login dialog is displayed, join the domain by logging in with an account that has permission to join the domain.
5. When the computer has successfully joined the domain, restart the computer. The machine will be a member of the domain; since we have set up machine autoenrollment, the machine will have a certificate for the CA installed as well as a certificate for machine authentication.

## Manually Install the Root Certificate on the Windows Client

Follow these steps to manually install the root certificate.

**Note:** If you have already set up machine autoenrollment, you do not need this step. Please skip to Configure the Wireless Networking.

1. On the Windows client machine, open a web browser and browse to the Microsoft CA server by entering **http://root-CA-ip-address/certsrv** in the address bar. Log in to the CA site.

In this example, the CA's IP address is 10.66.79.241.



2. Select **Retrieve the CA certificate or certification revocation list** and click **Next**.

**Microsoft** Certificate Services -- Our TAC CA [Home](#)

---

## Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

**Select a task:**

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

3. Click **Download CA certificate** to save the certificate on the local machine.

**Microsoft** Certificate Services -- Our TAC CA [Home](#)

---

## Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

**Choose file to download:**

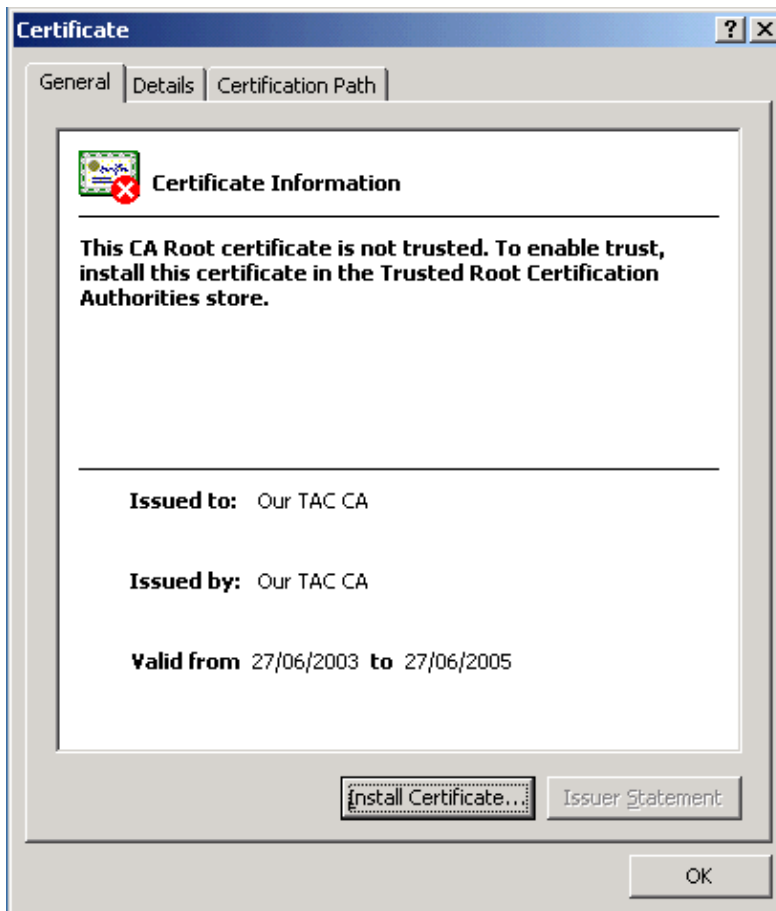
CA Certificate:

DER encoded or  Base 64 encoded

[Download CA certificate](#)  
[Download CA certification path](#)  
[Download latest certificate revocation list](#)

4. Open the certificate and click **Install Certificate**.

**Note:** In the example below, the icon at the top left indicates that the certificate is not yet trusted (installed).



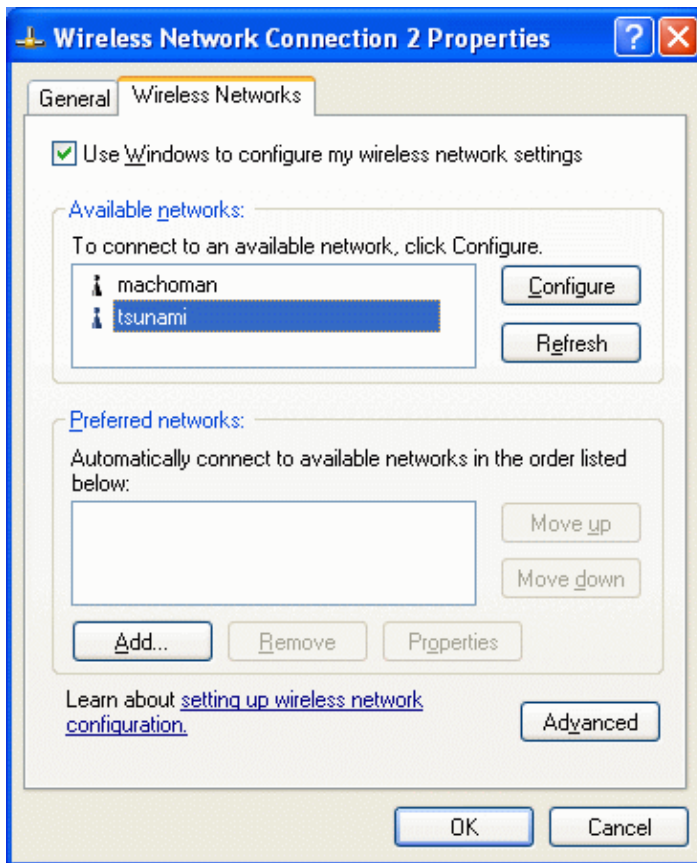
5. Install the certificate in Current User/ Trusted Root Certificate Authorities.

- a. Click **Next**.
- b. Select **Automatically select the certificate store based on the type of the certificate** and click **Next**.
- c. Click **Finish** to place the root certificate automatically under Current User/ Trusted Root Certificate Authorities.

## Configure the Wireless Networking

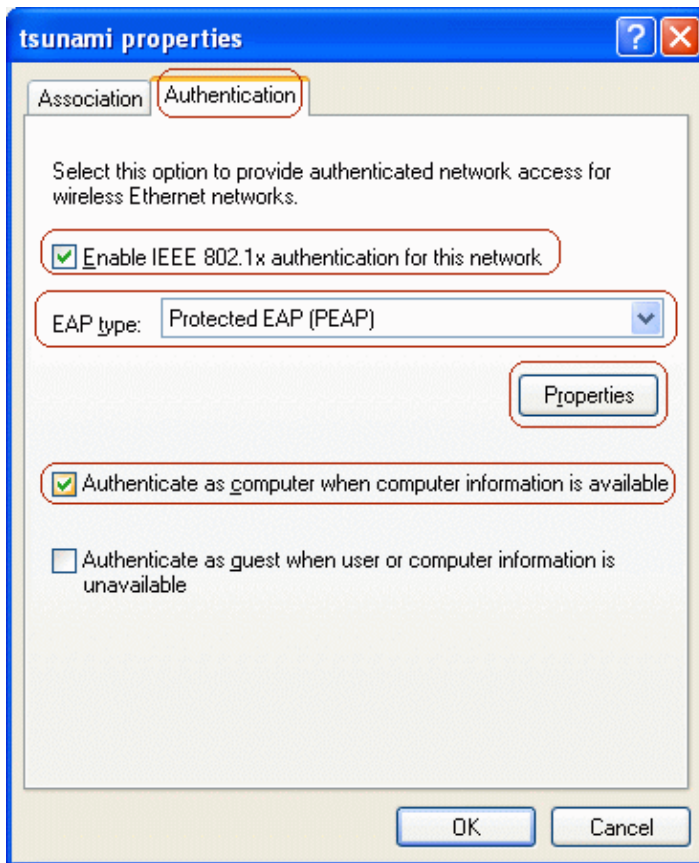
Follow these steps to set the options for wireless networking.

1. Log in to the domain as a domain user.
2. Go to **Control Panel > Network and Internet Connections > Network Connections**. Right-click on **Wireless Connection** and select **Properties** from the submenu that is displayed.
3. Select the **Wireless Networks** tab. Select the wireless network (displayed using the SSID name of the AP) from the list of available networks, and then click **Configure**.



4. On the Authentication tab of the network properties window, check the option for **Enable IEEE 802.1x authentication for this network**. For EAP type, select **Protected EAP (PEAP)** for EAP type, and then click **Properties**.

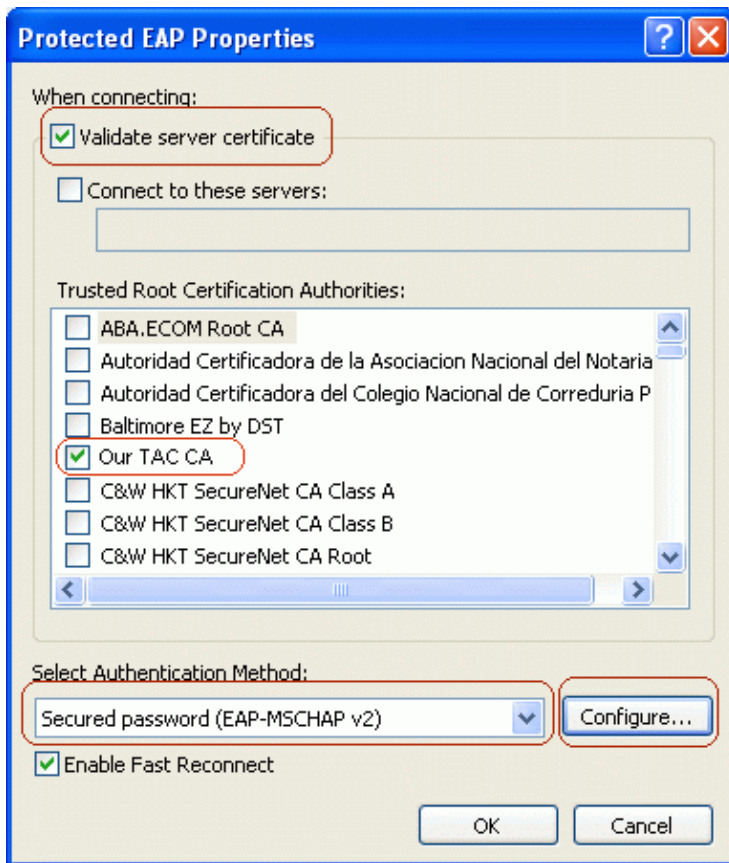
**Note:** To enable machine authentication, check the option for **Authenticate as computer when computer information is available**.



5. Check **Validate server certificate**, and then check the root CA for the enterprise used by PEAP clients and ACS devices. Select **Secure password (EAP-MSCHAP v2)** for the authentication method, and then click **Configure**.

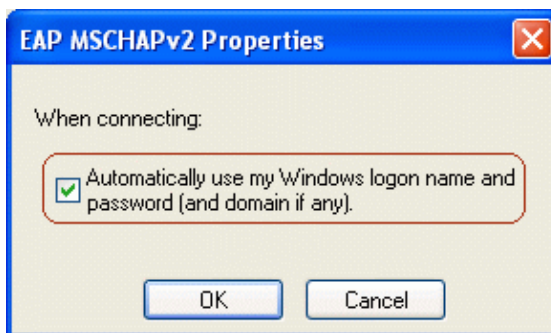
In this example, the root CA is named "Our TAC CA."



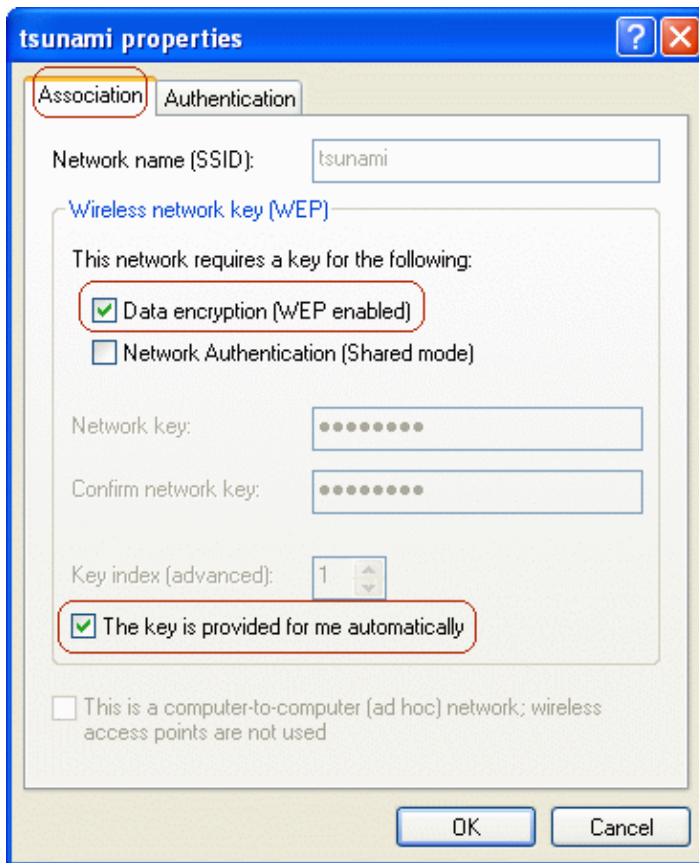


6. To enable single sign-on, check the option for **Automatically use my Windows logon name and password (and domain if any)**. Click **OK** to accept this setting, and then click **OK** again to return to the network properties window.

With single sign-on for PEAP, the client uses the Windows logon name for the PEAP authentication, so the user does not need to enter the password a second time.



7. On the Association tab of the network properties window, check the options for **Data encryption (WEP enabled)** and **The key is provided for me automatically**. Click **OK**, and then click **OK** again to close the network configuration window.



## Verify

This section provides information you can use to confirm your configuration is working properly.

- To verify that the wireless client has been authenticated, on the wireless client go to **Control Panel > Network and Internet Connections > Network Connections**. On the menu bar, go to **View > Tiles**. The wireless connection should display the message "Authentication succeeded."
- To verify that wireless clients have been authenticated, on the ACS web interface go to **Reports and Activity > Passed Authentications > Passed Authentications active.csv**.

## Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- Verify that MS Certificate Services have been installed as an Enterprise root CA on a Windows 2000 Advanced Server with Service Pack 3. Hotfixes 323172 and 313664 must be installed *after* MS Certificate Services are installed. If MS Certificate Services are reinstalled, hotfix 323172 must also be reinstalled.
- Verify that you are using Cisco Secure ACS for Windows version 3.2 with Windows 2000 and Service Pack 3. Ensure that hotfixes 323172 and 313664 have been installed.
- If machine authentication fails on the wireless client, there will be no network connectivity on the wireless connection. Only accounts that have their profiles cached on the wireless client will be able to log in to the domain. The machine will need to be plugged in to a wired network or set for wireless connection with no 802.1x security.
- If automatic enrollment with the CA fails when joining the domain, check Event Viewer for possible reasons. Try checking the DNS settings on the laptop.
- If the ACS's certificate is rejected by the client (which depends on the certificate's valid "from" and "to" dates, the client's date and time settings, and CA trust), then the client will reject it and

authentication will fail. The ACS will log the failed authentication in the web interface under **Reports and Activity > Failed Attempts > Failed Attempts XXX.csv** with the Authentication Failure–Code similar to "EAP–TLS or PEAP authentication failed during SSL handshake." The expected error message in the CSAuth.log file is similar to the following.

```
AUTH 06/04/2003 14:56:41 E 0345 1644 EAP: buildEAPRequestMsg:
other side probably didn't accept our certificate
```

- In the logs on the ACS web interface, under both **Reports and Activity > Passed Authentications > Passed Authentications XXX.csv** and **Reports and Activity > Failed Attempts > Failed Attempts XXX.csv**, PEAP authentications are shown in the format <DOMAIN>\<user-id>. EAP–TLS authentications are shown in the format <user-id>@<domain>.
- To use PEAP Fast Reconnect, you must enable this feature on both the ACS server and the client.
- If PEAP Password Changing has been enabled, you can change the password only when an account's password has aged or when the account is marked to have its password changed on the next log in.
- You can verify the ACS server's certificate and trust by following the steps below.

1. Log in to Windows on the ACS server with an account that has administrator privileges. Open Microsoft Management Console by going to **Start > Run**, typing **mmc**, and clicking **OK**.
2. On the menu bar, go to **Console > Add/Remove Snap–in**, and then click **Add**.
3. Select **Certificates** and click **Add**.
4. Select **Computer account**, click **Next**, and then select **Local computer (the computer this console is running on)**.
5. Click **Finish**, click **Close**, and then click **OK**.
6. To verify that the ACS server has a valid server–side certificate, go to **Console Root > Certificates (Local Computer) > ACSCertStore > Certificates**. Verify that there is a certificate for the ACS server (named OurACS in this example). Open the certificate and verify the following items.

- ◇ There is no warning about the certificate not being verified for all its intended purposes.
- ◇ There is no warning about the certificate not being trusted.
- ◇ "This certificate is intended to – Ensures the identity of a remote computer."
- ◇ The certificate has not expired and has become valid (check for valid "from" and "to" dates).
- ◇ "You have a private key that corresponds to this certificate."

7. On the Details tab, verify that the Version field has the value V3 and that the Enhanced Key Usage field has Server Authentication (1.3.6.1.5.5.7.3.1).
8. To verify that the ACS server trusts the CA server, go to **Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**. Verify that there is a certificate for the CA server (named Our TAC CA in this example). Open the certificate and verify the following items.

- ◇ There is no warning about the certificate not being verified for all its intended purposes.
- ◇ There is no warning about the certificate not being trusted.
- ◇ The certificate's intended purpose is correct.
- ◇ The certificate has not expired and has become valid (check for valid "from" and "to" dates).

If the ACS and client did not use the same root CA, then verify that the whole chain of CA servers' certificates have been installed. The same applies if the certificate was obtained from a subcertificate authority.

- You can verify the client's trust by following the steps below.

1. Log in to Windows on the wireless client with the client's account. Open Microsoft

- Management Console by going to **Start > Run**, typing **mmc**, and clicking **OK**.
2. On the menu bar, go to **Console > Add/Remove Snap-in**, and then click **Add**.
  3. Select **Certificates** and click **Add**.
  4. Click **Close**, and then click **OK**.
  5. To verify that the client's profile trusts the CA server, go to **Console Root > Certificates – Current User > Trusted Root Certification Authorities > Certificates**. Verify that there is a certificate for the CA server (named Our TAC CA in this example). Open the certificate and verify the following items.

- ◇ There is no warning about the certificate not being verified for all its intended purposes.
- ◇ There is no warning about the certificate not being trusted.
- ◇ The certificate's intended purpose is correct.
- ◇ The certificate has not expired and has become valid (check for valid "from" and "to" dates).

If the ACS and client did not use the same root CA, then verify that the whole chain of CA servers' certificates have been installed. The same applies if the certificate was obtained from a subcertificate authority.

- Verify the ACS settings as described in the section on Configuring Cisco Secure ACS for Windows v3.2.
- Verify the AP settings as described in the section on Configuring the Cisco Access Point.
- Verify the wireless client settings as described in the section on Configuring the Wireless Client.
- Verify that the user account exists in the internal database of the AAA server or on one of the configured external databases. Ensure that the account has not been disabled.

## Related Information

- [Cisco Secure ACS for Windows Support Page](#)
- [Documentation for Cisco Secure ACS for Windows](#)
- [EAP-TLS Deployment Guide for Wireless LAN Networks](#)
- [Obtaining Version and AAA Debug Information for Cisco Secure ACS for Windows](#)
- [Technical Support – Cisco Systems](#)

---

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

© 2013 – 2014 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Feb 02, 2006

Document ID: 43486

---