

PEAP under Unified Wireless Networks with ACS 5.1 and Windows 2003 Server

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Configure](#)

[Network Diagram](#)

[Windows Enterprise 2003 Setup with IIS, Certificate Authority, DNS, DHCP \(CA\)](#)

[CA \(democa\)](#)

[Cisco 1121 Secure ACS 5.1](#)

[Installation Using the CSACS-1121 Series Appliance](#)

[Install the ACS Server](#)

[Cisco WLC5508 Controller Configuration](#)

[Create the Necessary Configuration for WPAv2/WPA](#)

[PEAP Authentication](#)

[Install the Certificate Templates Snap-in](#)

[Create the Certificate Template for the ACS Web Server](#)

[Enable the New ACS Web Server Certificate Template](#)

[ACS 5.1 Certificate Setup](#)

[Configure Exportable Certificate for ACS](#)

[Install the Certificate in ACS 5.1 Software](#)

[Configure ACS Identity Store for Active Directory](#)

[Add a Controller to ACS as an AAA Client](#)

[Configure ACS Access Policies for Wireless](#)

[Create ACS Access Policy and Service Rule](#)

[CLIENT Configuration for PEAP using Windows Zero Touch](#)

[Perform a Basic Installation and Configuraiton](#)

[Install the Wireless Network Adapter](#)

[Configure the Wireless Network Connection](#)

[Troubleshoot Wireless Authentication with ACS](#)

[PEAP Authentication Fails with ACS Server](#)

[Related Information](#)

[Introduction](#)

This document describes how to configure secure wireless access using Wireless LAN controllers,

Microsoft Windows 2003 software and Cisco Secure Access Control Server (ACS) 5.1 via Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 2.

Note: For information about the deployment of secure wireless, refer to the [Microsoft Wi-Fi website](#) and [Cisco SAFE Wireless Blueprint](#).

Prerequisites

Requirements

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

For initial installation and configuration information for the Cisco 5508 Series Controllers, refer to the [Cisco 5500 Series Wireless Controller Installation Guide](#). For initial installation and configuration information for the Cisco 2100 Series Controllers, refer to the [Quick Start Guide: Cisco 2100 Series Wireless LAN Controller](#).

Microsoft Windows 2003 installation and configuration guides can be found at [Installing Windows Server 2003 R2](#).

Before you begin, install the Microsoft Windows Server 2003 with SP1 operating system on each of the servers in the test lab and update all Service Packs. Install the controllers and lightweight access points (LAPs) and ensure that the latest software updates are configured.

Windows Server 2003 with SP1, Enterprise Edition, is used so that auto-enrollment of user and workstation certificates for PEAP authentication can be configured. Certificate auto-enrollment and autorenewal make it easier to deploy certificates and improve security by automatically expiring and renewing certificates.

Components Used

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

- Cisco 2106 or 5508 Series Controller that runs 7.0.98.0
- Cisco 1142 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise with Internet Information Server (IIS), Certificate Authority (CA), DHCP, and Domain Name System (DNS) installed
- Cisco 1121 Secure Access Control System Appliance (ACS) 5.1
- Windows XP Professional with SP (and updated Service Packs) and wireless network interface card (NIC) (with CCX v3 support) or third party supplicant.
- Cisco 3750 Switch

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.

Configure

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

Note: Use the [Command Lookup Tool](#) ([registered](#) customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

Cisco Secure Wireless Lab Topology

The primary purpose of this document is to provide you the step-by-step procedure to implement the PEAP under Unified Wireless Networks with ACS 5.1 and the Windows 2003 Enterprise server. The main emphasis is on auto-enrollment of the client so that the client auto-enrolls and takes the certificate from the server.

Note: In order to add Wi-Fi Protected Access (WPA)/WPA2 with Temporal Key Integrity Protocol (TKIP)/Advanced Encryption Standard (AES) to Windows XP Professional with SP, refer to [WPA2/Wireless Provisioning Services Information Element \(WPS IE\) update for Windows XP with Service Pack 2](#) .

Windows Enterprise 2003 Setup with IIS, Certificate Authority, DNS, DHCP (CA)

CA (democa)

CA is a computer that runs Windows Server 2003 with SP2, Enterprise Edition, and performs these roles:

- A domain controller for the **demo.local** domain that runs IIS
- A DNS server for the **demo.local** DNS domain
- A DHCP server
- Enterprise root CA for the **demo.local** domain

Perform these steps in order to configure CA for these services:

1. [Perform a basic installation and configuration.](#)
2. [Configure the computer as a domain controller.](#)
3. [Raise the domain functional level.](#)
4. [Install and configure DHCP.](#)
5. [Install certificate services.](#)
6. [Verify Administrator permissions for certificates.](#)
7. [Add computers to the domain.](#)
8. [Allow wireless access to computers.](#)
9. [Add users to the domain.](#)

10. [Allow wireless access to users.](#)
11. [Add groups to the domain.](#)
12. [Add users to the wirelessusers group.](#)
13. [Add client computers to the wirelessusers group.](#)

Perform Basic Installation and Configuration

Perform these steps:

1. Install Windows Server 2003 with SP2, Enterprise Edition, as a stand-alone server.
2. Configure the TCP/IP protocol with the IP address of *10.0.10.10* and the subnet mask of *255.255.255.0*.

Configure the Computer as a Domain Controller

Perform these steps:

1. In order to start the Active Directory Installation wizard, choose **Start > Run**, type **dcpromo.exe**, and click **OK**.
2. On the Welcome to the Active Directory Installation Wizard page, click **Next**.
3. On the Operating System Compatibility page, click **Next**.
4. On the Domain Controller Type page, select **Domain Controller for a new Domain** and click **Next**.
5. On the Create New Domain page, select **Domain in a new forest** and click **Next**.
6. On the Install or Configure DNS page, select **No, just install and configure DNS on this computer** and click **Next**.
7. On the New Domain Name page, type **demo.local** and click **Next**.
8. On the NetBIOS Domain Name page, enter the Domain NetBIOS name as **demo** and click **Next**.
9. In the Database and Log Folders Locations page, accept the default Database and Log Folders directories and click **Next**.
10. In the Shared System Volume page, verify that the default folder location is correct and click **Next**.
11. On the Permissions page, verify that **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems** is selected and click **Next**.
12. On the Directory Services Restore Mode Administration Password page, leave the password boxes blank and click **Next**.
13. Review the information on the Summary page and click **Next**.
14. When you are done with the Active Directory installation, click **Finish**.
15. When prompted to restart the computer, click **Restart Now**.

Raise the Domain Functional Level

Perform these steps:

1. Open the **Active Directory Domains and Trusts** snap-in from the **Administrative Tools** folder (**Start > Programs > Administrative Tools > Active Directory Domains and Trusts**), and then right-click the domain computer **CA.demo.local**.

2. Click **Raise Domain Functional Level**, and then select **Windows Server 2003** on the Raise Domain Functional Level page.
3. Click **Raise**, click **OK**, and then click **OK** again.

[Install and Configure DHCP](#)

Perform these steps:

1. Install **Dynamic Host Configuration Protocol (DHCP)** as a **Networking Service** component by using **Add or Remove Programs** in the Control Panel.
2. Open the **DHCP** snap-in from the **Administrative Tools** folder (**Start > Programs > Administrative Tools > DHCP**), and then highlight the DHCP server, **CA.demo.local**.
3. Click **Action**, and then click **Authorize** in order to authorize the DHCP service.
4. In the console tree, right-click **CA.demo.local**, and then click **New Scope**.
5. On the Welcome page of the New Scope wizard, click **Next**.
6. On the Scope Name page, type **CorpNet** in the Name field.
7. Click **Next** and fill in these parameters: Start IP address - **10.0.20.1** End IP address - **10.0.20.200** Length - **24** Subnet mask - **255.255.255.0**
8. Click **Next** and enter *10.0.20.1* for the Start IP address and *10.0.20.100* for the End IP address to be excluded. Then click **Next**. This reserves the IP addresses in the range from 10.0.20.1 to 10.0.20.100. These reserve IP addresses are not allotted by the DHCP server.
9. On the Lease Duration page, click **Next**.
10. On the Configure DHCP Options page, choose **Yes, I want to configure these options now** and click **Next**.
11. On the Router (Default Gateway) page add the default router address of *10.0.20.1* and click **Next**.
12. On the Domain Name and DNS Servers page, type *demo.local* in the Parent domain field, type *10.0.10.10* in the IP address field, and then click **Add** and click **Next**.
13. On the WINS Servers page, click **Next**.
14. On the Activate Scope page, choose **Yes, I want to activate this scope now** and click **Next**.
15. When you finish with the New Scope Wizard page, click **Finish**.

[Install Certificate Services](#)

Perform these steps:

Note: IIS must be installed before you install Certificate Services and the user should be part of the Enterprise Admin OU.

1. In Control Panel, open **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
2. In the Windows Components Wizard page, choose Certificate Services, and then click Next.
3. On the CA Type page, choose Enterprise root CA and click Next.
4. In the CA Identifying Information page, type *democa* in the Common name for this CA box. You can also enter the other optional details. Then click **Next** and accept the defaults on the Certificate Database Settings page.
5. Click **Next**. Upon completion of the installation, click **Finish**.

6. Click **OK** after you read the warning message about installing IIS.

[Verify Administrator Permissions for Certificates](#)

Perform these steps:

1. Choose **Start > Administrative Tools > Certification Authority**.
2. Right-click **democa CA** and then click **Properties**.
3. On the Security tab, click **Administrators** in the Group or User names list.
4. In the Permissions for Administrators list, verify that these options are set to **Allow**: Issue and Manage Certificates, Manage CA Request Certificates. If any of these are set to Deny or are not selected, set the permissions to **Allow**.
5. Click **OK** to close the democa CA Properties dialog box, and then close Certification Authority.

[Add Computers to the Domain](#)

Perform these steps:

Note: If the computer is already added to the domain, proceed to [Add Users to the Domain](#).

1. Open the **Active Directory Users and Computers** snap-in.
2. In the console tree, expand **demo.local**.
3. Right-click **Computers**, click **New**, and then click **Computer**.
4. In the New Object – Computer dialog box, type the name of the computer in the Computer name field and click **Next**. This example uses the computer name *Client*.
5. In the Managed dialog box, click **Next**.
6. In the New Object – Computer dialog box, click **Finish**.
7. Repeat steps 3 through 6 in order to create additional computer accounts.

[Allow Wireless Access to Computers](#)

Perform these steps:

1. In the Active Directory Users and Computers console tree, click the **Computers** folder and right-click on the computer for which you want to assign wireless access. This example shows the procedure with computer **Client** which you added in step 7. Click **Properties**, and then go to the **Dial-in** tab.
2. In the Remote Access Permission, choose **Allow access** and click **OK**.

[Add Users to the Domain](#)

Perform these steps:

1. In the Active Directory Users and Computers console tree, right-click **Users**, click **New**, and then click **User**.
2. In the New Object – User dialog box, type the name of the wireless user. This example uses the name *wirelessuser* in the First name field, and *wirelessuser* in the User logon name field.

Click **Next**.

3. In the New Object – User dialog box, type a password of your choice in the Password and Confirm password fields. Clear the **User must change password at next logon** check box, and click **Next**.
4. In the New Object – User dialog box, click **Finish**.
5. Repeat steps 2 through 4 in order to create additional user accounts.

[Allow Wireless Access to Users](#)

Perform these steps:

1. In the Active Directory Users and Computers console tree, click the **Users** folder, right-click **wirelessuser**, click **Properties**, and then go to the **Dial-in** tab.
2. In the Remote Access Permission, choose **Allow access** and click **OK**.

[Add Groups to the Domain](#)

Perform these steps:

1. In the Active Directory Users and Computers console tree, right-click **Users**, click **New**, and then click **Group**.
2. In the New Object – Group dialog box, type the name of the group in the Group name field and click **OK**. This document uses the group name *wirelessusers*.

[Add Users to the wirelessusers Group](#)

Perform these steps:

1. In the details pane of Active Directory Users and Computers, double-click on the group *WirelessUsers*.
2. Go to the Members tab and click **Add**.
3. In the Select Users, Contacts, Computers, or Groups dialog box, type the name of the users that you want to add to the group. This example shows how to add the user *wirelessuser* to the group. Click **OK**.
4. In the Multiple Names Found dialog box, click **OK**. The wirelessuser user account is added to the wirelessusers group.
5. Click **OK** in order to save changes to the wirelessusers group.
6. Repeat this procedure to add more users to the group.

[Add Client Computers to the wirelessusers Group](#)

Perform these steps:

1. Repeat steps 1 and 2 in the [Add Users to the wirelessusers Group](#) section of this document.
2. In the Select Users, Contacts, or Computers dialog box, type the name of the computer that you want to add to the group. This example shows how to add the computer named *client* to the group.
3. Click **Object Types**, clear the **Users** check box, and then check **Computers**.

4. Click **OK** twice. The CLIENT computer account is added to the wirelessusers group.
5. Repeat the procedure to add more computers to the group.

Cisco 1121 Secure ACS 5.1

Installation Using the CSACS-1121 Series Appliance

The CSACS-1121 appliance is preinstalled with the ACS 5.1 software. This section gives you an overview of the installation process and the tasks that you must perform before installing ACS.

1. Connect the CSACS-1121 to the network and appliance console. See [Chapter 4, "Connecting Cables."](#)
2. Power up the CSACS-1121 appliance. See [Chapter 4, "Powering Up the CSACS-1121 Series Appliance."](#)
3. Run the **setup** command at the CLI prompt to configure the initial settings for the ACS server. See Running the Setup Program.

Install the ACS Server

This section describes the installation process for the ACS server on the CSACS-1121 Series appliance.

- [Run the Setup Program](#)
- [Verify the Installation Process](#)
- [Post-Installation Tasks](#)

For detailed information on the installation of the Cisco Secure ACS Server refer to [Installation and Upgrade Guide for the Cisco Secure Access Control System 5.1](#).

Cisco WLC5508 Controller Configuration

Create the Necessary Configuration for WPAv2/WPA

Perform these steps:

Note: The assumption is that the controller has basic connectivity to the network and IP reachability to the management interface is successful.

1. Browse to **https://10.0.1.10** in order to login to the controller.
2. Click **Login**.
3. Log in with the default user *admin* and default password *admin*.
4. Create a new Interface for VLAN mapping under the **Controller** menu.
5. Click **Interfaces**.
6. Click **New**.
7. In the Interface name field, enter *Employee*. (This field can be any value you like.)
8. In the VLAN ID field, enter *20*. (This field can be any VLAN that is carried in the network.)
9. Click **Apply**.
10. Configure the information as this Interfaces > Edit window shows: Interface IP Address -

10.0.20.2Netmask - **255.255.255.0**Gateway - **10.0.10.1**Primary DHCP - **10.0.10.10**

11. Click **Apply**.
12. Click the **WLANs** tab.
13. Choose **Create New**, and click **Go**.
14. Enter a Profile Name, and, in the WLAN SSID field, enter *Employee*.
15. Choose an ID for the WLAN, and click **Apply**.
16. Configure the information for this WLAN when the WLANs > Edit window appears.**Note:** WPAv2 is the chosen Layer 2 encryption method for this lab. In order to allow WPA with TKIP-MIC clients to associate to this SSID, you can also check the **WPA compatibility mode** and **Allow WPA2 TKIP Clients** boxes or those clients that do not support the 802.11i AES encryption method.
17. On the WLANs > Edit screen, click the **General** tab.
18. Make sure that the Status box is checked for **Enabled** and the appropriate **Interface** (employee) is chosen. Also, make sure to check the **Enabled** check box for Broadcast SSID.
19. Click the **Security** tab.
20. Under the Layer 2 sub-menu, check **WPA + WPA2** for Layer 2 Security. For WPA2 encryption, check **AES + TKIP** in order to allow TKIP clients.
21. Choose **802.1x** as the authentication method.
22. Skip the Layer 3 sub-menu as it is not required. Once the RADIUS server is configured, the appropriate server can be chosen from the Authentication menu.
23. The **QoS** and **Advanced** tabs can be left at default unless any special configurations are required.
24. Click the **Security** menu to add the RADIUS Server.
25. Under the RADIUS sub-menu, click **Authentication**. Then, click **New**.
26. Add the RADIUS server IP address (10.0.10.20) which is the ACS server configured earlier.
27. Make sure that the shared key matches the AAA client configured in the ACS server. Make sure that the **Network User** box is checked and click **Apply**.
28. The basic configuration is now complete and you can begin to test PEAP.

[PEAP Authentication](#)

PEAP with MS-CHAP version 2 requires certificates on the ACS servers but not on the wireless clients. Auto enrollment of computer certificates for the ACS servers can be used to simplify a deployment.

In order to configure CA server to provide auto-enrollment for computer and user certificates, complete the procedures in this section.

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 grayed 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 so you have to create a new template that does so.

Note: Windows 2000 allows for exportable keys and these procedures do not need to be followed if you use Windows 2000.

[Install the Certificate Templates Snap-in](#)

Perform these steps:

1. Choose **Start > Run**, enter *mmc*, and click **OK**.
2. On the File menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Under Snap-in, double-click **Certificate Templates**, click **Close**, and then click **OK**.
4. In the console tree, click **Certificate Templates**. All of the certificate templates appear in the Details pane.
5. In order to bypass steps 2 through 4, enter *certtmpl.msc* which opens the Certificate Templates snap-in.

[Create the Certificate Template for the ACS Web Server](#)

Perform these steps:

1. In the Details pane of the Certificate Templates snap-in, click the **Web Server** template.
2. On the Action menu, click **Duplicate Template**.
3. In the Template display name field, enter *ACS*.
4. Go to the **Request Handling** tab and check **Allow private key to be exported**. Also ensure that **Signature and Encryption** is selected from the Purpose drop-down menu.
5. Choose **Requests must use one of the following CSPs** and check **Microsoft Base Cryptographic Provider v1.0**. Uncheck any other CSPs that are checked, and click **OK**.
6. Go to the **Subject Name** tab, choose **Supply** in the request, and click **OK**.
7. Go to the **Security** tab, highlight the **Domain Admins Group**, and make sure that the **Enroll** option is checked under Allowed. **Note:** If you choose to build from this Active Directory information only check the **User principal name (UPN)** and uncheck the **Include email name** in subject name and E-mail name because an e-mail name was not entered for the Wireless User account in the Active Directory Users and Computers snap-in. If you do not disable these two options, auto-enrollment attempts to use e-mail, which results in an auto-enrollment error.
8. There are additional security measures if needed to prevent certificates from being automatically pushed out. These can be found under the Issuance Requirements tab. This is not discussed further in this document.
9. Click **OK** in order to save the template and move onto issuing this template from the Certificate Authority snap-in.

[Enable the New ACS Web Server Certificate Template](#)

Perform these steps:

1. Open the Certification Authority snap-in. Perform steps 1 through 3 in the [Create the Certificate Template for the ACS Web Server](#) section, choose the **Certificate Authority** option, choose **Local Computer**, and click **Finish**.
2. In the Certificate Authority console tree, expand **ca.demo.local**, and then right-click **Certificate Templates**.
3. Go to **New > Certificate Template to Issue**.
4. Click the **ACS Certificate Template**.

5. Click **OK** and open the **Active Directory Users and Computers** snap-in.
6. In the console tree, double-click **Active Directory Users and Computers**, right-click **demo.local**, and then click **Properties**.
7. On the Group Policy tab, click **Default Domain Policy**, and then click **Edit**. This opens the Group Policy Object Editor snap-in.
8. In the console tree, expand **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**, and then choose **Automatic Certificate Request Settings**.
9. Right-click **Automatic Certificate Request Settings**, and choose **New > Automatic Certificate Request**.
10. On the Welcome to the Automatic Certificate Request Setup Wizard page, click **Next**.
11. On the Certificate Template page, click **Computer**, and then click **Next**.
12. When you complete the Automatic Certificate Request Setup Wizard page, click **Finish**.
The Computer certificate type now appears in the details pane of the Group Policy Object Editor snap-in.
13. In the console tree, expand **User Configuration > Windows Settings > Security Settings > Public Key Policies**.
14. In the details pane, double-click **Auto-enrollment Settings**.
15. Choose **Enroll certificates automatically** and check **Renew expired certificates, update pending certificates and remove revoked certificates** and **Update certificates that use certificate templates**.
16. Click **OK**.

[ACS 5.1 Certificate Setup](#)

[Configure Exportable Certificate for ACS](#)

Note: The ACS server must obtain a server certificate from the enterprise root CA server in order to authenticate a WLAN PEAP client.

Note: Make sure that the IIS Manager is not open during the certificate setup process as causes problems with cached information.

1. Log in to the ACS server with an account Admin rights.
2. Go to **System Administration > Configuration > Local Server Certificates**. Click **Add**.
3. When you choose a server certificate creation method, choose **Generate Certificate Signing Request**. Click **Next**.
4. Enter a certificate subject and key length as the example, then click **Finish**:Certificate Subject - **CN=acs.demo.local**Key Length - **1024**
5. ACS will prompt that a certificate signing request has been generated. Click **OK**.
6. Under System Administration, go to **Configuration > Local Server Certificates > Outstanding Signing Requests**.**Note:** The reason for this step is that Windows 2003 does not allow for exportable keys and you need to generate a certificate request based on the ACS Certificate that you created earlier that does.
7. Choose the **Certificate Signing Request** entry, and click **Export**.
8. Save the ACS certificate **.pem** file to the desktop.

[Install the Certificate in ACS 5.1 Software](#)

Perform these steps:

1. Open a browser and connect to CA server URL **http://10.0.10.10/certsrv**.
2. The Microsoft Certificate Services window appears. Choose **Request a certificate**.
3. Click to submit an **advanced certificate request**.
4. In the advanced request, click **Submit a certificate request using a base-64-encoded...**
5. In the Saved Request field, if browser security permits, browse to the previous ACS certificate request file and insert.
6. The browser's security settings may not allow accessing the file on a disk. If so, click **OK** to perform a manual paste.
7. Locate the ACS *.pem file from the previous ACS export. Open the file using a text editor (for example, Notepad).
8. Highlight the entire content of the file, and click **Copy**.
9. Return to the Microsoft certificate request window. **Paste** the copied content into the Saved Request field.
10. Choose **ACS** as the Certificate Template, and click **Submit**.
11. Once the Certificate is Issued, choose **Base 64 encoded**, and click **Download certificate**.
12. Click **Save** in order to save the certificate to the desktop.
13. Go to **ACS > System Administration > Configuration > Local Server Certificates**. Choose **Bind CA Signed Certificate**, and click **Next**.
14. Click **Browse**, and locate the saved certificate.
15. Choose the ACS certificate that was issued by the CA server, and click **Open**.
16. Also, check the Protocol box for **EAP**, and click **Finish**.
17. The CA-issued ACS certificate will appear in the ACS local certificate.

[Configure ACS Identity Store for Active Directory](#)

Perform these steps:

1. Connect to ACS and log in with Admin account.
2. Go to **Users and Identity Stores > External Identity Stores > Active Directory**.
3. Enter the Active Directory Domain *demo.local*, enter the password of the server, and click **Test Connection**. Click **OK** in order to continue.
4. Click **Save Changes**. **Note:** For more information on ACS 5.x integration procedure refer to [ACS 5.x and later: Integration with Microsoft Active Directory Configuration Example](#).

Add a Controller to ACS as an AAA Client

Perform these steps:

1. Connect to ACS, and go to **Network Resources > Network Devices and AAA Clients**. Click **Create**.
2. Enter into these fields: Name - **wlcIP - 10.0.1.10RADIUS** checkbox - **Checked** Shared Secret - **cisco**
3. Click **Submit** when finished. The controller will appear as an entry in the ACS Network Devices list.

[Configure ACS Access Policies for Wireless](#)

Perform these steps:

1. In ACS, go to **Access Policies > Access Services**.
2. In the Access Services window, click **Create**.
3. Create an access service, and enter a name (for example WirelessAD). Choose **Based on service template**, and click **Select**.
4. In the Webpage Dialog, choose **Network Access – Simple**. Click **OK**.
5. In the Webpage Dialog, choose **Network Access – Simple**. Click **OK**. Once the template is selected, click **Next**.
6. Under Allowed Protocols, check the boxes for **Allow MS-CHAPv2** and **Allow PEAP**. Click **Finish**.
7. When ACS prompts you to activate the new service, click **Yes**.
8. In the new access service that was just created/activated, expand and choose **Identity**. For the Identity Source, click **Select**.
9. Choose **AD1** for Active Directory that was configured in ACS, click **OK**.
10. Confirm the Identity Source is AD1, and click **Save Changes**.

[Create ACS Access Policy and Service Rule](#)

Perform these steps:

1. Go to **Access Policies > Service Selection Rules**.
2. Click **Create** in the Service Selection Policy window. Give the new rule a name (for example, *WirelessRule*). Check the box for **Protocol** to match **Radius**.
3. Choose **Radius**, and click **OK**.
4. Under Results, choose **WirelessAD** for Service (created in previous step).
5. Once the new wireless rule is created, choose and **Move** this rule to the top, which will be the first rule to identify wireless radius authentication using Active Directory.

[CLIENT Configuration for PEAP using Windows Zero Touch](#)

In our example, CLIENT is a computer that runs Windows XP Professional with SP that acts as a wireless client and obtains access to Intranet resources through the wireless AP. Complete the procedures in this section in order to configure CLIENT as a wireless client.

[Perform a Basic Installation and Configuraiton](#)

Perform these steps:

1. Connect CLIENT to the Intranet network segment using an Ethernet cable connected to the hub.
2. On CLIENT, install Windows XP Professional with SP2 as a member computer named CLIENT of the demo.local domain.
3. Install Windows XP Professional with SP2. This must be installed in order to have PEAP support. **Note:** Windows Firewall is automatically turned on in Windows XP Professional with SP2. Do not turn the firewall off.

Install the Wireless Network Adapter

Perform these steps:

1. Shut down the CLIENT computer.
2. Disconnect the CLIENT computer from the Intranet network segment.
3. Restart the CLIENT computer, and then log on using the local administrator account.
4. Install the wireless network adapter. **Note:** Do not install the manufacturer's configuration software for the wireless adapter. Install the wireless network adapter drivers using the Add Hardware Wizard. Also, when prompted, provide the CD provided by the manufacturer or a disk with updated drivers for use with Windows XP Professional with SP2.

Configure the Wireless Network Connection

Perform these steps:

1. Log off and then log in using the **WirelessUser** account in the **demo.local** domain.
2. Choose **Start > Control Panel**, double-click **Network Connections**, and then right-click **Wireless Network Connection**.
3. Click **Properties**, go to the **Wireless Networks** tab, and make sure the **Use Windows to configure my wireless network settings** is checked.
4. Click **Add**.
5. Under the Association tab, enter *Employee* in the Network name (SSID) field.
6. Choose **WPA** for the Network Authentication, and make sure that Data encryption is set to **TKIP**.
7. Click the **Authentication** tab.
8. Validate that EAP type is configured to use **Protected EAP (PEAP)**. If it is not, choose it from the drop-down menu.
9. If you want the machine to be authenticated prior to login (which allows login scripts or group policy pushes to be applied), check **Authenticate as computer when computer information is available**.
10. Click **Properties**.
11. As PEAP involves authentication of the Server by the client, ensure that the **Validate server certificate** is checked. Also, make sure the CA that issued the ACS certificate is checked under the Trusted Root Certification Authorities menu.
12. Choose **Secured password (EAP-MSCHAP v2)** under Authentication Method as it is used for inner authentication.
13. Make sure the **Enable Fast Reconnect** check box is checked. Then, click **OK** three times.
14. Right-click the wireless network connection icon in systray, and then click **View Available Wireless Networks**.
15. Click the Employee wireless network, and then click **Connect**. The wireless client will show **Connected** if the connection is successful.
16. After authentication is successful, check the TCP/IP configuration for the wireless adapter by using Network Connections. It should have an address range of 10.0.20.100-10.0.20.200 from the DHCP scope or the scope created for the CorpNet wireless clients.
17. In order to test functionality, open up a browser and browse to **http://10.0.10.10** (or the IP address of the CA server).

Troubleshoot Wireless Authentication with ACS

Perform these steps:

1. Go to **ACS > Monitoring and Reports**, and click **Launch Monitoring & Report Viewer**.
2. A separate ACS window will open. Click **Dashboard**.
3. In the My Favorite Reports section, click **Authentications – RADIUS – Today**.
4. A log will show all RADIUS authentications as either Pass or Fail. Within a logged entry, click on the **magnifying glass icon** in the Details column.
5. The RADIUS Authentication Detail will provide much information about the logged attempts.
6. ACS Service Hit Count can provide an overview of attempts matching the rule(s) created in ACS. Go to **ACS > Access Policies > Access Services**, and click **Service Selection Rules**.

PEAP Authentication Fails with ACS Server

When your client fails PEAP authentication with an ACS server, check if you find the NAS duplicated authentication attempt error message in the **Failed attempts** option under the **Report and Activity** menu of the ACS.

You might receive this error message when Microsoft Windows XP SP2 is installed on the client machine and Windows XP SP2 authenticates against a third party server other than a Microsoft IAS server. In particular, Cisco RADIUS server (ACS) uses a different method to calculate the Extensible Authentication Protocol Type:Length:Value format (EAP-TLV) ID than the method Windows XP uses. Microsoft has identified this as a defect in the XP SP2 supplicant.

For a Hotfix, contact Microsoft and refer to the article [PEAP authentication is not successful when you connect to a third-party RADIUS server](#). The underlying issue is that on the client side, with windows utility, the Fast Reconnect option is disabled for PEAP by default. However, this option is enabled by default on the server side (ACS). In order to resolve this issue, uncheck the Fast Reconnect option on the ACS server (under Global System Options). Alternatively, you can enable the Fast Reconnect option on the client side to resolve the issue.

Perorm these steps in order to enable Fast Reconnect on the client that runs Windows XP using Windows Utility:

1. Go to **Start > Settings > Control Panel**.
2. Double-click the **Network Connections** icon.
3. Right-click the **Wireless Network Connection** icon, and then click **Properties**.
4. Click the **Wireless Networks** tab.
5. Choose the **Use Windows to configure my wireless network settings** option in order to enable windows to configure the client adapter.
6. If you have already configured an SSID, choose the SSID and click **Properties**. If not, click **New** in order to add a new WLAN.
7. Enter the SSID under the Association tab. Make sure that Network Authentication is **Open** and Data Encryption is set to **WEP**.
8. Click **Authentication**.
9. Choose the **Enable IEEE 802.1x authentication for this network** option.
10. Choose **PEAP** as the EAP Type, and click **Properties**.

11. Choose the **Enable Fast Reconnect** option at the bottom of the page.

Related Information

- [PEAP under Unified Wireless Networks with ACS 4.0 and Windows 2003](#)
- [Cisco Wireless LAN Controller \(WLC\) and Cisco ACS 5.x \(TACACS+\) Configuration Example for Web Authentication](#)
- [Installation and Upgrade Guide for the Cisco Secure Access Control System 5.1](#)
- [Technical Support & Documentation - Cisco Systems](#)