

## Peap Configuration Guide v1.20

Written for AP 12.02T1, ACS Windows 3.1 and up, ACS SE, Windows 2000 (SP3 and SP4) or XP w/ACU v6 (if using ACS 3.2 the ACU is not required)

This guide was originally written to accommodate certificates created with a Microsoft CA but has been updated to add steps for using a self-signing certificate which is supported as of ACS 3.3. Using a self-signing certificate streamlines initial PEAP installation considerably since no external CA is required. **However, it is very important to note that, at this time, the default expiration period of the self-signing cert is only one year and cannot be changed.** This is fairly standard when it comes to server certs, but since the self-signed cert also acts as the root CA cert, this can mean installing the new cert on every client every year unless you do not check the "Validate Server Certificate" option. I recommend using self-signing certificates only as a temporary measure until a traditional CA can be used. **If you wish to use a self-signing certificate, skip to the Self-signing certificates section.**

### Microsoft Certificate Services Installation

- A. Click start > Settings > Control Panel
- B. Inside the Control Panel, open Add/Remove Programs
- C. In Add/Remove Programs, select Add/Remove Windows Components
- D. Check "Certificate Services" and click Next (click yes to the IIS message)
- E. Select a Stand-alone (or Enterprise) root CA and click Next
- F. Give the CA a name\* (all the other boxes are optional) and click Next
- G. The database default is fine... click Next
- H. Finish

#### **Note!!!**

IIS must be installed before you install the CA.

\*Avoid giving the CA the same name as an ACS server. Doing so may 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.

## ACS for Windows Certificate Setup

**If you are configuring the ACS appliance, skip to step 6**

### 1. Create a Server Certificate

- A. From your ACS server, browse to the CA - [http://IP\\_of\\_CA\\_server/certsrv/](http://IP_of_CA_server/certsrv/)
- B. Select the "Request a certificate" option, and click Next
- C. Select Advanced request, and click Next
- D. Select "Submit a certificate request to this CA using a form", click Next
- E. Type something in the name (CN) box
- F. For Intended Purpose select "Server Authentication Certificate"\*
- G. Under Key Options:
  - I. CSP = "Microsoft Base Cryptographic Provider v1.0"
  - II. Key Size = 1024\*\*
  - III. Check "Mark keys as Exportable"\*\*\*
  - IV. Check "Use Local Machine Store" (Software ACS only)
  - V. Leave everything else as default and click Submit
- H. You should get a message that states "Your certificate request has been received..."

#### **Note!!!**

Certificates created with a key size greater than 1024 will not work.

\*If you are using the Enterprise CA, choose "Web Server" on the first drop down box.

\*\* The Windows 2003 Enterprise CA allows key sizes greater than 1024, but using a key larger than 1024 does not work with PEAP. Authentication might appear to pass in ACS, but the client will just hang while attempting authentication.

\*\*\*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 will be greyed out. Unfortunately, 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 will be available in the dropdown, so we have to create a new template that does so. Here are the steps:

1. Start > Run > certmpl.msc
2. Right-click Web Server template and choose Duplicate Template
3. Name the template something easy to identify like ACS.
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" and 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.

The new template will be included in the Certificate Template dropdown.

Certificate services may also give a "Failed to create 'CertificateAuthority.Request' object" error when attempting to create a new certificate. Here are the steps to correct this:

1. 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 and then OK.
8. Restart IIS.

It should also be noted that using a 2003 CA in a 2000 domain whose schema has not been prepared for 2003 compatibility with adprep/forestprep/domainprep will not work with EAP.

If your browser locks with a "Downloading ActiveX Control" message, you will need to run the fix discussed in the following URL:

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B330389>

If the CSP field just says "Loading..." make sure you are not running a software firewall on the machine submitting the request. ZoneLabs' ZoneAlarm causes this pretty much every time. There may be other software that can cause this, but I have not identified any.

## **2. Approve the Certificate from the CA**

---

- A. Open the CA (click on Start > Programs > Administrative Tools > Certificate Authority)
- B. On the left, expand the certificate, then click "Pending Requests"
- C. Right-click on the certificate, select all tasks, then select "Issue"

## **3. Download the Server Certificate to the ACS Server**

---

- A. From your ACS server, browse to the CA - [http://IP\\_of\\_CA\\_server/certsrv/](http://IP_of_CA_server/certsrv/)
- B. Select "Check on a Pending Certificate", and click Next
- C. Select the certificate and click Next
- D. Click Install

#### 4. Install the CA Certificate on the ACS Server

(this step is not required if ACS and the CA are installed on the same server)

- A. From your ACS server, browse to the CA - [http://IP\\_of\\_CA\\_server/certsrv/](http://IP_of_CA_server/certsrv/)
- B. Select "Retrieve the CA certificate or certificate revocation list", and click Next
- C. Select "Base 64 encoded" and click "Download CA certificate"
- D. Click Open, and click "Install certificate"
- E. Click Next
- F. Select "Place all certificates in the following store" and click Browse
- G. Check the "Show physical stores" box
- H. Expand "Trusted root certification authorities", select Local Computer, and click Ok
- I. Click Next, FINISH, and click Ok for "The import was successful" box

#### 5. Setup ACS to use the Server Certificate

- A. On the ACS server click System Configuration on the left
- B. Select ACS Certificate Setup and then Install ACS certificate
- C. Select "Use certificate from storage"
- D. Type in the CN name (from step 2 e) and click Submit
- E. On the ACS server click system configuration on the left
- F. Select ACS Certificate Setup and then Edit Certificate Trust List
- G. Check the box for the CA (from step 1 f) and click Submit

### ACS Appliance Certificate Setup

If you are configuring ACS for Windows, skip to step 12

#### 6. Create a Certificate Signing Request

- A. Go to System Configuration > ACS Certificate Setup > Generate Certificate Signing Request
- B. Enter a name in the Certificate subject field using the cn=name format
- C. Enter a name for the private key file\*
- D. Enter the private key password and confirm it
- E. Choose a key length of 1024\*\*
- F. Click Submit
- G. Copy the CSR output on the right-hand side for submittal to the CA

\*Note that the path to the private key will be cached in this field so if "submit" is pressed a second time after the CSR is created the private key will be overwritten and will not match the original CSR. This will result in a "private key does not match" error when you attempt to install the server certificate.

\*\*while ACS can generate key sizes greater than 1024, using a key larger than 1024 does not work with PEAP. Authentication might appear to pass in ACS, but the client will just hang while attempting authentication.

## 7. Create a Server Certificate using your CSR

- A. From your FTP server, browse to the CA - [http://IP\\_of\\_CA\\_server/certsrv/](http://IP_of_CA_server/certsrv/)
- B. Select the "Request a certificate" option, and click Next
- C. Select Advanced request, and click Next
- D. Select "Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file"
- E. Paste the output from step 6 G into the Base64 Encoded Certificate Request field and click Submit.
- F. Click "Download CA certificate"
- G. Click "Save", name the certificate something useful, and save it to your FTP directory

## 8. Download CA Certificate to your FTP Server\*

- A. From your FTP server, browse to the CA - [http://IP\\_of\\_CA\\_server/certsrv/](http://IP_of_CA_server/certsrv/)
- B. Select "Retrieve the CA certificate or certificate revocation list", and click Next
- C. Select "Base 64 encoded" and click "Download CA certificate"
- D. Click "Save", name the certificate something useful, and save it to your FTP directory

## 9. Install CA Certificate on your Appliance\*

- A. Go to System Configuration > ACS Certificate Setup > ACS Certification Authority Setup
- B. Click "Download CA certificate file"
- C. Type the IP address or hostname of the FTP server in the FTP Server field
- D. Type a valid username that Cisco Secure ACS can use to access the FTP server in the Login field
- E. Type the above user's password in the Password field
- F. Type the relative path from the FTP server root directory to the directory containing the CA certificate file in the Remote FTP Directory field
- G. Type the name of the CA certificate file in the Remote FTP File Name field
- H. Click Submit
- I. Verify the filename in the field and click Submit
- J. Restart the ACS services in System Configuration > Service Control

\*Skipping these steps will result in either not being able to enable PEAP in step 12 and getting an error that the server certificate is not installed even though it is or getting an "EAP type not configured" failure in failed attempts even though the EAP type IS configured.

Also note that, if your server cert was created using an intermediate CA, you will need to repeat these steps for every CA in the chain between the root CA and the server cert (including the root CA cert, of course).

## 10. Install Server Certificate on your Appliance

- A. Go to System Configuration > ACS Certificate Setup
- B. Click Install ACS Certificate
- C. Select the Read certificate from file option and then click the Download certificate file link
- D. Type the IP address or hostname of the FTP server in the FTP Server field
- E. Type a valid username that Cisco Secure ACS can use to access the FTP server in the Login field
- F. Type the above user's password in the Password field
- G. Type the relative path from the FTP server root directory to the directory containing the server certificate file in the Remote FTP Directory field
- H. Type the name of the server certificate file in the Remote FTP File Name field
- I. Click Submit
- J. Enter the path to the private key from step 6 C
- K. Enter the password for the private key from step 6 D
- L. Click Submit

### Self-signed Certificate Setup Only if not using an external CA\*

## 11. Create and Install the Certificate

- A. On the ACS server click System Configuration on the left
- B. Click ACS Certificate Setup
- C. Click Generate Self-signed Certificate
- D. Type something into the Certificate subject field preceded by cn=  
**i.e. cn=ACS33**
- E. Type the full path\*\* and name of the certificate to be created  
**i.e. c:\acscerts\acs33.cer**
- F. Type the full path\*\* and name of the private key file to be created  
**i.e. c:\acscerts\acs33.pvk**
- G. Enter and confirm the private key password
- H. Choose 1024 from the key length dropdown\*\*\*
- I. I left the digest to sign with at SHA1
- J. Check "Install generated certificate"
- K. If you are using the appliance, enter the FTP server information in the "Export certificate and private key to:" section
- L. Click Submit

\*Testing in the lab with self-signed certs resulted in a longer authentication time the **first** time a client authenticates with the Microsoft supplicant. I believe this has to do with the MS supplicant getting confused about a server cert with the same name as the root CA cert. All subsequent authentications were fine.

\*\*Path is not necessary with the appliance.

**\*\*\***while ACS can generate key sizes greater than 1024, using a key larger than 1024 does not work with PEAP. Authentication might appear to pass in ACS, but the client will just hang while attempting authentication.

## 12. Configure Global Authentication Settings

- A. On the ACS server click System Configuration on the left
- B. Click Global Authentication Setup

---

---

FOR ACS v3.2 and up

- I. Check Allow EAP-MSCHAPv2 if using Microsoft PEAP
- II. Check Allow EAP-GTC if using Cisco PEAP
- III. Check Allow MS-CHAP Version 1 Authentication
- IV. Check Allow MS-CHAP Version 2 Authentication
- V. Click Submit and Restart

---

---

FOR ACS v3.1

- I. Check Allow PEAP
- II. Check Allow MS-CHAP Version 1 Authentication
- III. Check Allow MS-CHAP Version 2 Authentication
- IV. Click Submit and Restart

## 13. Setup the AP on the ACS

- A. On the ACS server click Network Configuration on the left.
- B. To add a AAA client click Add Entry
- C. Fill in the boxes:
  - I. AAA Client IP Address = "IP\_of\_your\_AP"
  - II. Key = Make up a key, and make sure this matches on the AP shared secret.
  - III. Authenticate Using = RADIUS (Cisco Aironet)
  - IV. Submit and Restart

### **Note!!!**

I didn't change any of the defaults on the AAA client setup.

## 14. Configure the AP

---

---

With VxWorks:

---

---

- A. Open the AP and go to Setup > Security > Authentication Server
    - I. Enter the ACS IP address
    - II. Enter the shared secret (Must match the 'KEY' in ACS)
    - III. Use server for: check "EAP Authentication"
    - IV. The default should work for everything else... click Ok
  
  - B. Go to Setup > Security > Radio Data Encryption
    - I. For Accept Authentication Type check "Open" and "Network-EAP"
    - II. For Require EAP check "Open"
    - III. If you are not using broadcast key rotation, set WEP key 1 and select 128bit
    - IV. Change Use of Data Encryption by Stations to "full Encryption"  
(if you can't change the use of data encryption Click apply first)
    - V. Click Ok
- 
- 

With IOS AP web interface:

---

---

- A. Open the AP and go to Security > Server Manager
  - I. Choose RADIUS from the Current Server List dropdown
  - II. Enter the ACS IP address
  - III. Enter the shared secret (Must match the 'KEY' in ACS)
  - IV. Use server for: check "EAP Authentication"
  - V. Click OK on the warning dialogue and then click Apply
  
- B. Go To Security > SSID Manager\*
  - I. Choose the SSID from the Current SSID List or enter a new SSID in the SSID field
  - II. Check Open Authentication and choose "with EAP" from the dropdown
  - III. Check Network EAP
  - IV. All other values can be left at default and click Apply
  
- C. Go to Security > Encryption Manager\*
  - I. Place the radio button in WEP Encryption and choose Mandatory from the dropdown
  - II. Place the radio button in Encryption Key 1, enter the key in the field
  - III. Choose 128 bit from the Key Size dropdown
  - IV. Click Apply

### **Note!!!**

The network-eap is required if you are installing the ACU.

If you are using broadcast key rotation, you don't need to set a key as the key should



already be set. If it not, go to Setup > Radio Advance and set a value for the broadcast key rotation. You probably don't need to set this any lower then 5 minutes (300 secs). Once the value is set, click OK and go back into the radio data encryption page.

\*Configuration will differ if using WPA. See WPA Key Management supplement at the end of this document for details.

## 15. Install the ACU v6 (only if using ACS 3.1 or if EAP-GTC is needed)

### **Note!!!**

You need to select CUSTOM install as the Cisco PEAP supplicant is not installed by the express setup. You can tell if the Cisco supplicant is installed by looking at the EAP type in the Authentication tab of your network connection properties. If it shows up as "Protected EAP (PEAP)", this is the Microsoft PEAP supplicant. If it shows up as just PEAP, then you are using the Cisco PEAP supplicant.

## 16. Install the Root CA Certificate for the Client

---

---

### If Using Certificate From Microsoft CA

---

---

- A. From the client PC, browse to the CA - [http://IP\\_of\\_CA\\_server/certsrv/](http://IP_of_CA_server/certsrv/)
- B. Select Retrieve a CA certificate and click Next
- C. Select Base64 Encoding and "Download CA certificate"
- D. Click open and click "Install Certificate"
- E. Click Next
- F. Select "Place all certificates in the following store" and then click Browse
- G. Check the "Show physical stores" box
- H. Expand "Trusted root certification authorities", select local computer, and click Ok.
- I. Click Next, FINISH, and click Ok for "The import was successful" box

---

---

### If Using Self-signed Certificate From ACS

---

---

- A. Copy the certificate from its location as specified in step 11E (or K for the appliance) to the client
- B. Right-click the .cer file and click "install certificate"
- C. Click Next
- D. Select "Place all certificates in the following store" and then click Browse
- E. Check the box "show physical stores"
- F. Expand "Trusted Root Certification Authorities", select Local Computer, and click OK
- G. Click Next, FINISH, and click Ok for "The import was successful" box

**Note!!!**

This step is REQUIRED for EACH client if you have the "Validate server certificate" box checked in Windows' PEAP properties.

**17. Setup the Client for PEAP**

---

---

**Setup XP SP1 or SP2 for PEAP\***

---

---

- A. Open Network Connections on the control panel (click Start -> Control Panel)
- B. Right-click the wireless network and select Properties
- C. On the wireless network tab, make sure "use windows to configure..." is checked
- D. If you see the SSID in the list click Configure. If NOT, click Add.
- E. Put in the SSID and check the WEP and "Key is provided for me automatically" boxes
- F. Select authentication tab, make sure "enable network-access control using..." is checked
- G. For EAP type select "Protected EAP" and click Properties
- H. Under "Trusted root certificate" check the box for the CA
- I. click Ok, Ok, and OK

**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.

\*Configuration will differ if using WPA. See WPA Key Management supplement at the end of this document for details.

---

---

**Setup XP for the Certificate (without SP1)**

---

---

- A. Open Network Connections on the Control Panel (Start -> Control Panel)
- B. Right-click the wireless network and select Properties
- C. On the wireless network tab, make sure "use windows to configure..." is checked
- D. Select the Authentication tab and make sure "enable network-access control using..." is checked
- E. For EAP type select PEAP and click Properties
- F. Under "Trusted root certificate" check the box for the CA
- G. click Ok, Ok, and OK

---

---

**Setup Windows 2000 for PEAP**

---

---

- A. If you are running SP3, download and install the 802.1x hotfix discussed at the following URL (this is not required for SP4):  
<http://support.microsoft.com/default.aspx?kbid=313664>
- B. Go to Start > Control Panel > Network and Dial-up Connections

- C. Right click your wireless connection and choose properties
- D. Click on the Authentication tab
- E. Check "Enable network access control using IEEE 802.1x"
- F. Choose PEAP from the EAP type dropdown and Click OK

**Note!!!**

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

- I. Right-click My Computer, and then click Manage.
- II. Click Services and Applications, and then click Services.
- III. Set the Startup value for the service to Automatic, and then start the service.

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 linked above or the vendor's website for supported drivers.

---

---

If you are using the ACU:

---

---

- A. Open the ACU
- B. Select Manage Profile and create a profile (or edit one)
- C. Put in client name and SSID of the AP
- D. Go to the Network Security tab
- E. For Network Security Type, select Host-based EAP
- F. For WEP, select "Use Dynamic WEP Keys"
- G. Click Ok and Ok
- H. Select the profile you created

**Note!!!**

If you are using the Cisco supplicant, on the authentication tab you'll have just "PEAP". If you are using the Microsoft supplicant, it will say "Protected EAP (PEAP)".

There is a very long delay before the client tries to associate to the AP (about a minute) which may be partially alleviated with the following patch from Microsoft <http://support.microsoft.com/?id=826942> (This patch may re-install the EAP-MSCHAPv2 supplicant which will prevent EAP-GTC compatible database types from functioning!).

If you are not getting associated at all, try disabling and then re-enabling the card.

---

---

## Set up Windows 2003 Mobile for PEAP

---

---

Note that this section was written to support the Cisco PEAP (EAP-GTC) supplicant. I have no experience with non-Cisco PEAP supplicants for Windows CE.

- A. Install the latest release of the Cisco ACU for Windows CE (be sure to install the PEAP supplicant during the install)
- B. Open the ACU and select <External Settings> from the Active Profile dropdown
- C. Insert your Cisco, click on the network icon on the taskbar, click on Settings > Advanced > Network Card.
- D. Click on your SSID if available or Add New Settings
- E. Verify the SSID in the Network Name field and the network to connect to
- F. Click on the Authentication tab
- G. Place a check in Data encryption (WEP) and “The key is provided for me...”
- H. Place a check in “Enable network access...802.1x” and choose Cisco PEAP
- I. Click properties and place a check in “Validate server certificate” (optional)\*
- J. Click OK until you are back at the Configure Wireless Networks screen
- K. Connect

### **Note!!!**

\*Checking this option requires that the root CA certificate be installed on the PocketPC. Unfortunately, Windows Mobile does not include a good method for importing/managing certificates. There are a number of utilities available like the one discussed on the following URL which I have used successfully:

[http://www.petri.co.il/adding\\_root\\_certificates\\_to\\_windows\\_mobile\\_2003\\_ppc.htm](http://www.petri.co.il/adding_root_certificates_to_windows_mobile_2003_ppc.htm)

These utilities are not supported by Cisco, obviously. Importing a root CA cert manually is not required when using the ACU, however, since the Cisco PEAP supplicant conveniently imports it for you. No version of Pocket PC operating system supports self-signed certificates at the time of this writing so you cannot import self-signed certificates into Pocket PC for validation. You can still use a self-signed certificate if you uncheck the “Validate server certificate” option.

## 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 may run and a user can log onto a domain. Domain membership is REQUIRED for machine credentials to be established and authentication to take place.

### 1. Setup ACS to Allow Machine Authentication

- A. Go to External User Databases > Database Configuration
- B. Click Windows Database and then Configure
- C. Place a check in "Enable PEAP machine authentication"
- D. Submit

### 2. Setup the Client for Machine Authentication

---

---

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

---

---

- A. Log into Windows with an account that has administrator privileges
- B. Right-click on My Computer and choose Properties
- C. Select the Computer Name tab and click Change
- D. Enter the host-name in the Computer name field
- E. Select Domain, enter the name of the domain, and Click OK
- F. To join the domain, a login dialog will be displayed. Login with an account that has permission to join the domain
- G. Once the computer has successfully joined the domain, restart the computer. The machine will be a member of the domain, and have authentication credentials negotiated with the domain which are only known by the OS. In ACS, the username will appear as *host/hostname*

---

---

Setup PEAP supplicant for machine authentication

---

---

- A. Open Network Connections on the control panel (click Start > Control Panel)
- B. Right-click the network connection and select Properties
- C. Select the Authentication tab and check "Authenticate as computer..."

## WPA Key Management Supplement

Written for IOS AP 12.02(13)JA1, ACS 3.2, and XP SP1 with WPA hotfix

### Note!!!

According to the following documentation (close to the bottom), Windows 2000 clients do not natively support WPA key management and you must use the vendor's client software in order to get this support:

<http://support.microsoft.com/?kbid=815485>

Unfortunately, the Cisco ACU does not support WPA key management for host-based EAP (EAP-TLS and PEAP) at this time and you must install a third party client such as the Funk Odyssey client or Meetinghouse AEGIS client. Further information on WPA support for Cisco products can be found here:

[http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo\\_350/350cards/windows/wizardrn/wiz12new.htm#82435](http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/windows/wizardrn/wiz12new.htm#82435)

The above information is true for Windows Mobile 2003 (Pocket PC) clients as well.

**WPA key management is basically the same with only the following changes:**

### 1. Configure the AP

- A. Go to Security > Encryption Manager
  - I. Place the radio button in WEP Cipher and choose TKIP from the dropdown
  - II. Click Apply
- B. Go To Security > SSID Manager
  - I. Choose the SSID from the Current SSID List or enter a new SSID in the SSID field
  - II. Check Open Authentication and choose "with EAP" from the dropdown
  - III. Check Network EAP
  - IV. Under "Authenticated Key Management" select "Mandatory" from the drop down menu and click "WPA"
  - V. Click Apply

### 2. Setup the XP SP1 (with KB826942 installed) or SP2 Client for PEAP and WPA

- A. Open Network Connections on the control panel (click Start -> Control Panel)
- B. Right-click the wireless network and select Properties
- C. On the wireless network tab, make sure "use windows to configure..." is checked

- D. If you see the SSID in the list click Configure. If NOT, click Add.
- E. Put in the SSID and choose "WPA" for Network Authentication and TKIP for Data Encryption
- F. Select authentication tab, make sure "enable network-access control using..." is checked
- G. For EAP type select "Protected EAP" and click Properties
- H. Under "Trusted root certificate" check the box for the CA
- I. click Ok, Ok, and OK