# RSA SecurID Ready Implementation Guide

Last Modified: December 15, 2004

## 1. Partner Information

| | |
|---|---|
| Partner Name | Cisco Systems Inc. |
| Web Site | www.cisco.com |
| Product Name | Cisco WLAN solution (w/ PEAP ) |
| Version & Platform | Cisco Aironet Access Point 350/1200,<br>Cisco Aironet 350 Wireless Client,<br>Cisco Aironet Client Utility 6.3<br>Cisco ACS 3.2.3 for Windows 2000/NT |
| Product Description | Wireless LANs enable users to establish and maintain a wireless network connection throughout or between buildings, without the limitations of wires or cables. Cisco provides a family of wireless LAN products that combine the mobility and flexibility users want from a wireless LAN product with the throughput and security they demand from a business LAN. |
| Product Category | Wireless |

## 2. Contact Information

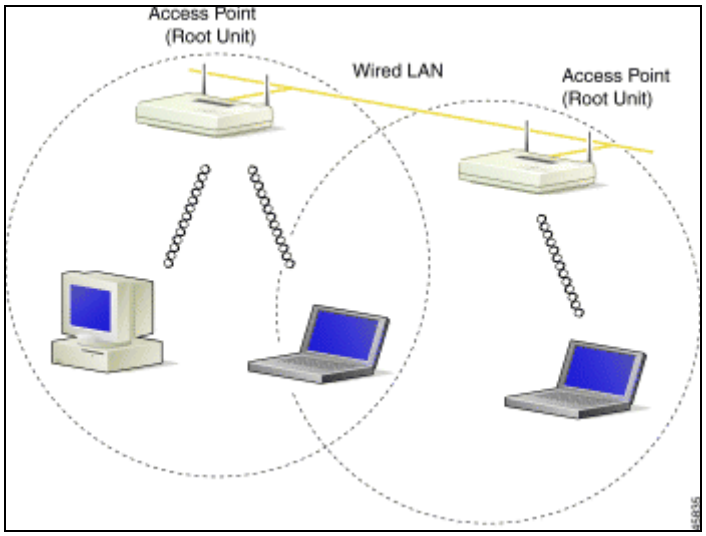
| | Sales Contact | Support Contact |
|---|---|---|
| E-mail | sales@cisco.com | tac@cisco.com |
| Phone | 1 800 553 6387 | 1 800 553 2447 |
| Web | www.cisco.com | www.cisco.com/public/support/tac/home.shtml |

## 3. Solution Summary

The scope of this guide is to show how to setup and configure Cisco ACS, Cisco Aironet AP and Cisco ACU on a wireless client for PEAP to be used in a SecurID authenticated, WLAN environment. Please reference the Implementation Guide for ACS for detailed steps on how to authenticate users via SecurID. For a more in depth explanation of how to configure your wireless hardware, please refer to the documentation provided by your hardware vendor.

The following table represents the ACE/Agent functionality of ACS 3.2.3:

| Feature | Details |
|---|---|
| Authentication Methods Supported | Native RSA SecurID |
| RSA Authentication Agent Library Version | Version # 5.2 [527] |
| RSA Authentication Manager Name Locking | Yes |
| RSA Authentication Manager Replica Support | Full Replica Support |
| Secondary RADIUS Server Support | N/A |
| Location of Node Secret on Client | In Registry |
| RSA Authentication Agent Host Type | Net OS |
| RSA SecurID User Specification | Designated users, all users, RSA SecurID as default. |
| Support for Download of Offline Day Files | No |
| RSA SecurID Protection of Partner Product Administrators | No |
| RSA Software Token API Integration | No |



## 4. Product Requirements

- ***Hardware requirements***

| Component Name: Cisco Secure ACS | |
|---|---|
| CPU make/speed required | Pentium III processor, 550 MHz or faster |
| Memory | 256 MB of RAM |
| HD space | At least 250 MB of free disk space. If you are running your database on the same machine, more disk space is required |
| Graphics resolution | Minimum 256 colors at 800 x 600 lines |
| | |

| Component Name: Cisco AP 1200/350 Series Access Points | |
|---|---|
| Firmware | 11.54T or higher |
| | |

**Misc:**

- For client connections, you will need a WiFi-compliant 802.11 wireless adaptor installed on a Windows XP/2000 PC.

- ***Software requirements***

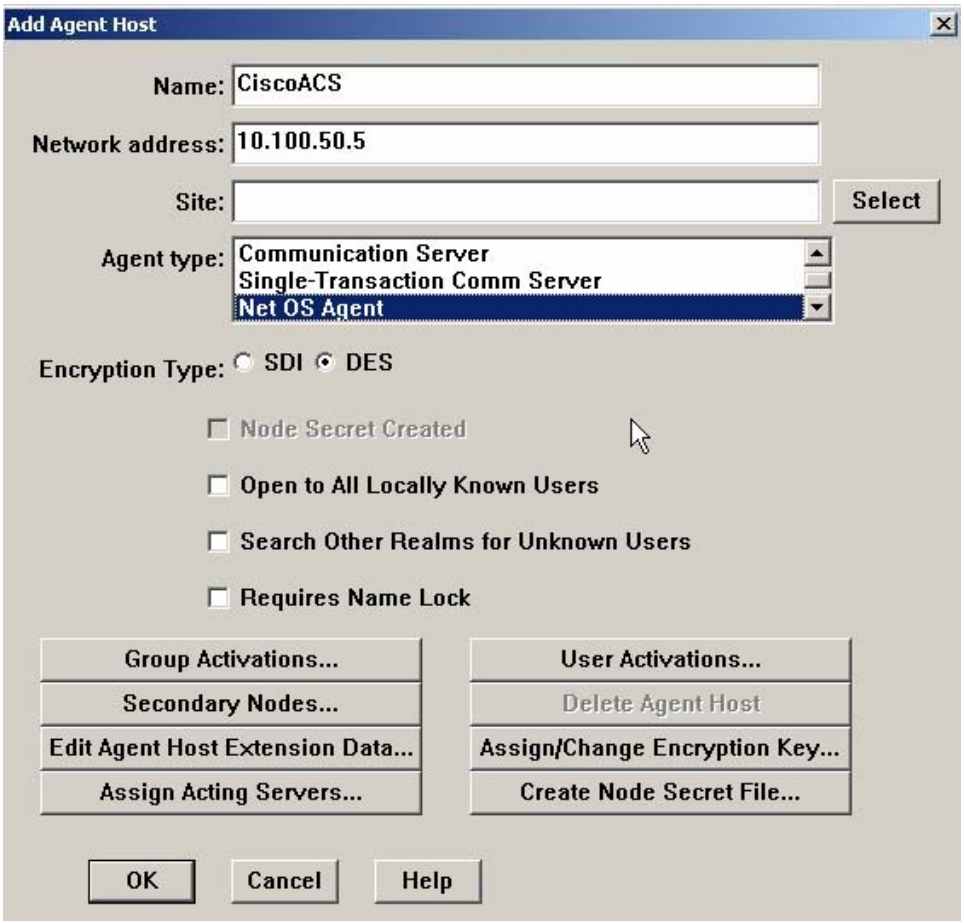
| Component Name: Cisco Secure ACS | |
|---|---|
| **Operating System** | **Version (Patch-level)** |
| **Operating System** | **Patch** |
| Windows NT Server 4.0 | Service Pack 6a |
| Windows 2000 Server | Service Pack 2 |
| | |
| **Web Browser** | **Version** |
| Microsoft Internet Explorer | 5.5 and 6.0 |
| Netscape Communicator | 6.2 |

## 5. RSA Authentication Manager configuration

Perform the following steps to set up the Cisco ACS Server as an Agent Host within the RSA Authentication Manager's database.

- On the RSA Authentication Manager computer, go to **Start > Programs > RSA ACE Server**, and then **Database Administration - Host Mode**.

1. On the **Agent Host** menu, choose **Add Agent Host…**.




   - In **Name**, type the hostname of the Cisco ACS Server.
   - In **Network address**, type the IP address of the Cisco ACS Server.
   - For **Agent Type**, select ***Net OS Agent***.

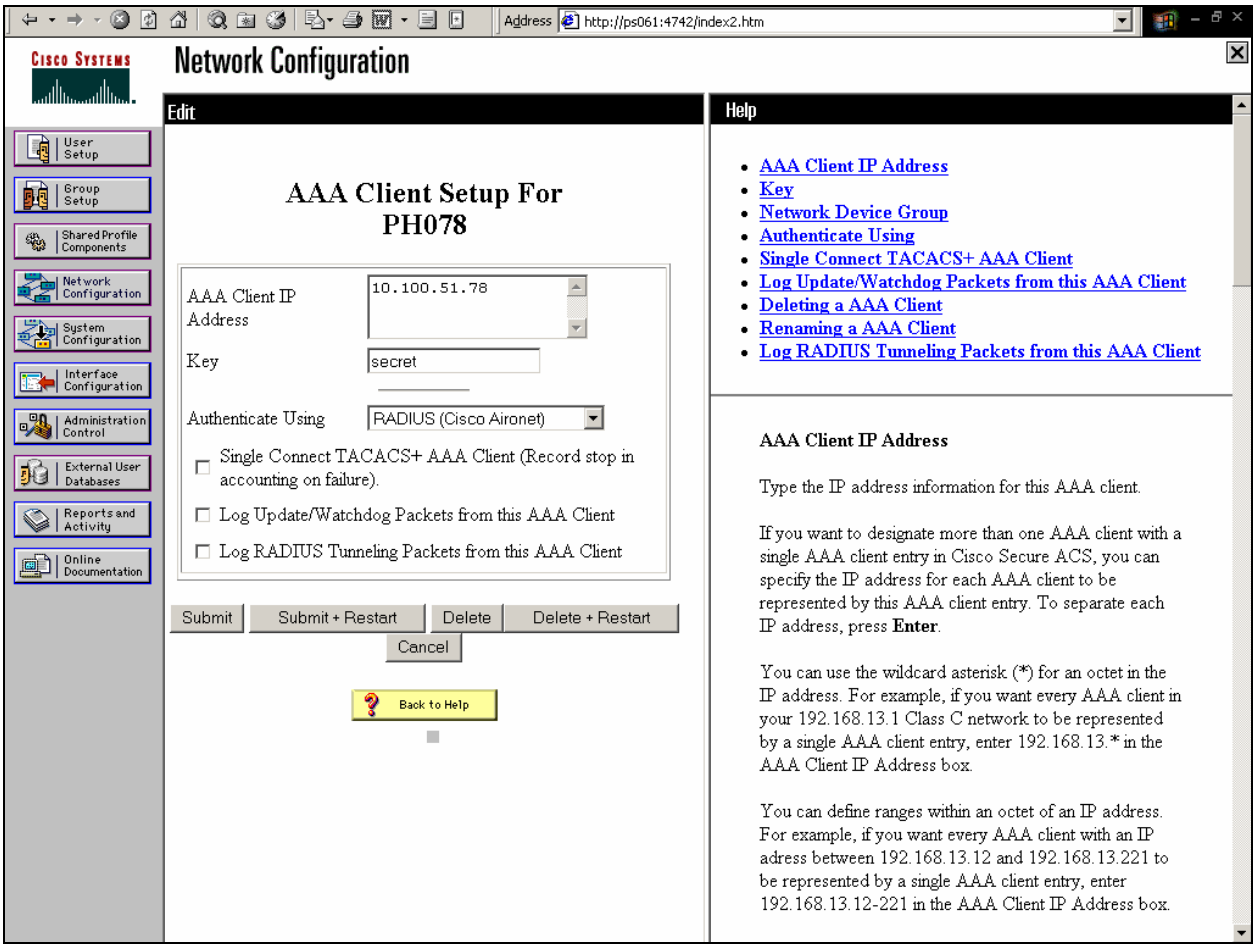
**Note**: It is important that all hostname and IP addresses resolve to each other. Please reference the RSA Authentication Manager documentation for detailed information on this and other configuration parameters within this screen. Subsequently, you can also select the 'Help' button at the bottom of the screen.

# 6. Partner RSA Authentication Agent configuration

## A. Configure ACS

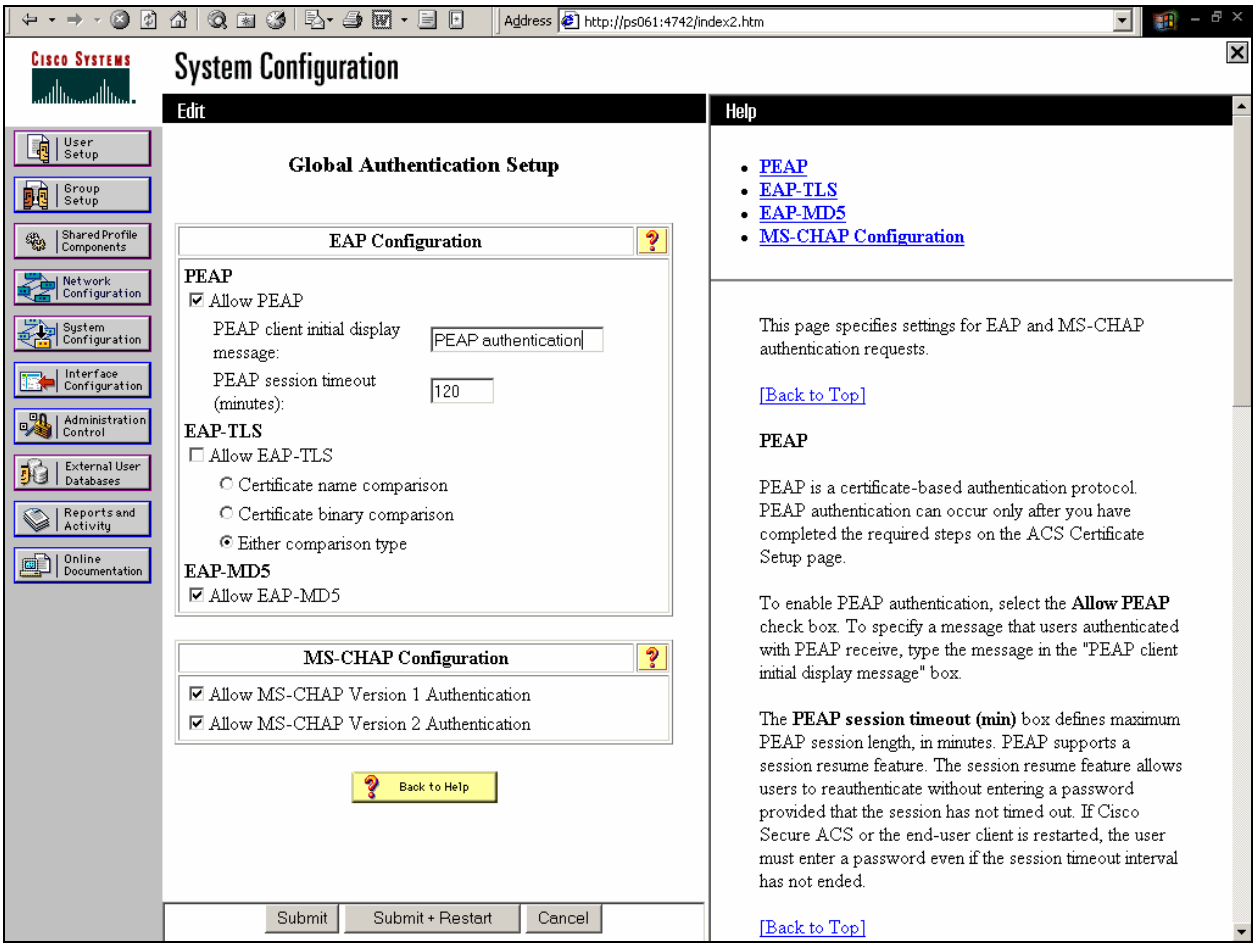
1. Configure ACS to authenticate users via SecurID. As noted in the Solution Summary in section 3 above, please reference the RSA Secured Implementation Guide for ACS for detailed steps on how to authenticate users via SecurID.

2. The ACS server install will need the IP addresses of the Access Point to serve as an NAS (Network Access Server) for forwarding client PEAP authentications to the ACS. Under Network Configuration, add/edit the AAA client for the Access Point that will be used. Enter the "shared secret" key (common to AP) that is used between AAA client and ACS. Select "Authenticate Using> RADIUS (Cisco Aironet)" for this AAA client. Click Submit + Restart.




3. Apply for and install a server certificate from a known, trusted Certificate Authority such as RSA Keon Certificate Authority. For detailed information on this process, please reference the documentation that ships with Cisco ACS 3.1. If you are using RSA Keon Certificate Authority you can view the RSA Keon Aironet implementation guide for additional help. You will need to successfully complete this task prior to continuing.

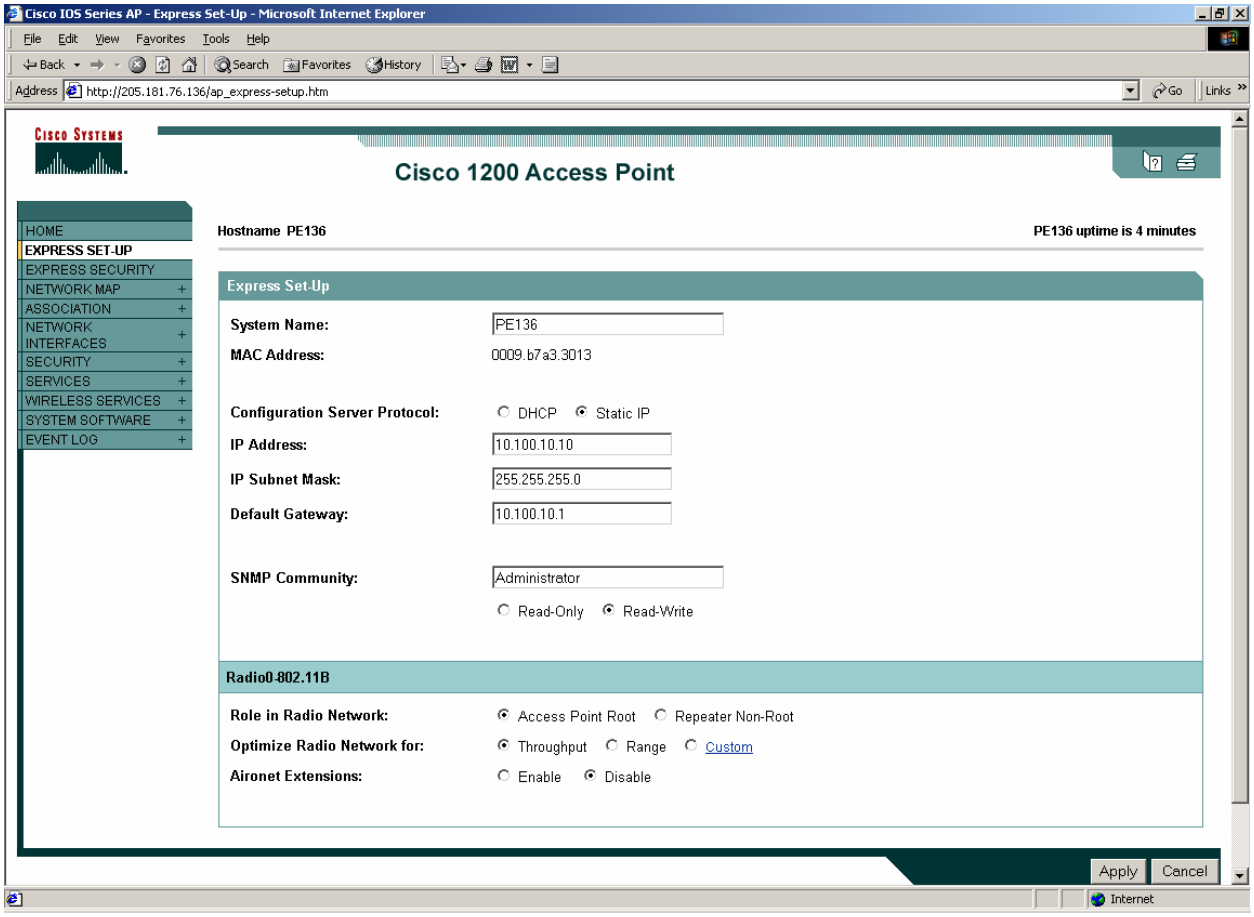
4. Under System Configuration> Global Authentication Setup, select the checkbox for “Allow PEAP” authentication.



## B. Configure Cisco Aironet Access Point for 802.1x security

1. Connect to the Access Point's web based configuration screen by pointing your browser to the IP address assigned to your access point.

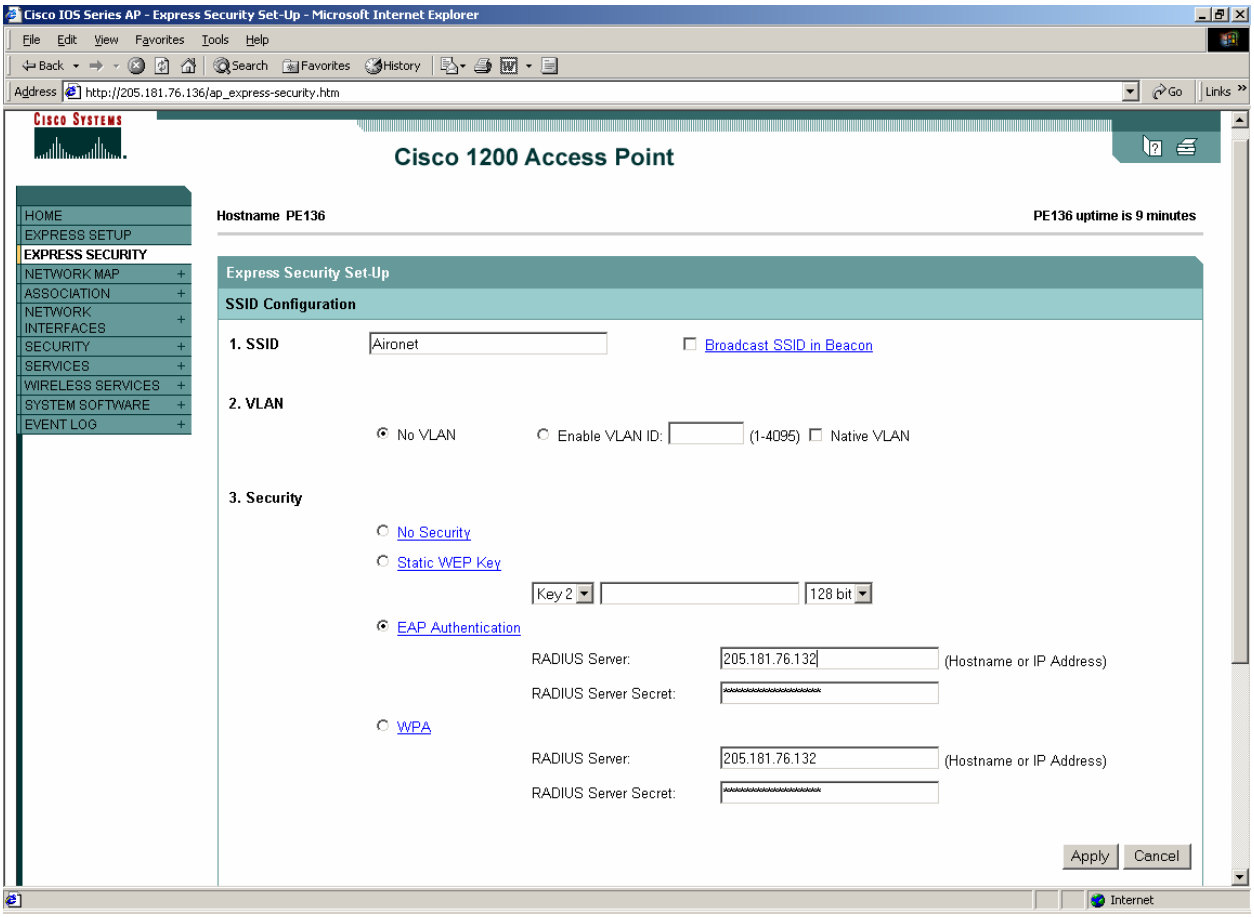
2. Press the "Express Setup" link:




- Choose a System name that will allow you to easily identify this particular access point on the network.

- Press the "Apply" button at the bottom of the screen to apply these changes.

3. Press the "Express Security" link:




- SSID: Change the Radio Service Set ID (SSID) from the Default setting to a unique string that will be used by all wireless access points and clients on your network.

- SSID: Check the box for Broadcast SSID in Beacon.

- Security: Select EAP Authentication. If this is your first time selecting this you will see a popup massage which is shown in figure1 below .

- RADIUS Server: If you don't have the Cisco ACS server defined as the default RADIUS Server, enter the IP Address for the Cisco ACS now.

- RADIUS Server Secret: The RADIUS Secret should match the secret entered in the Cisco ACS above.

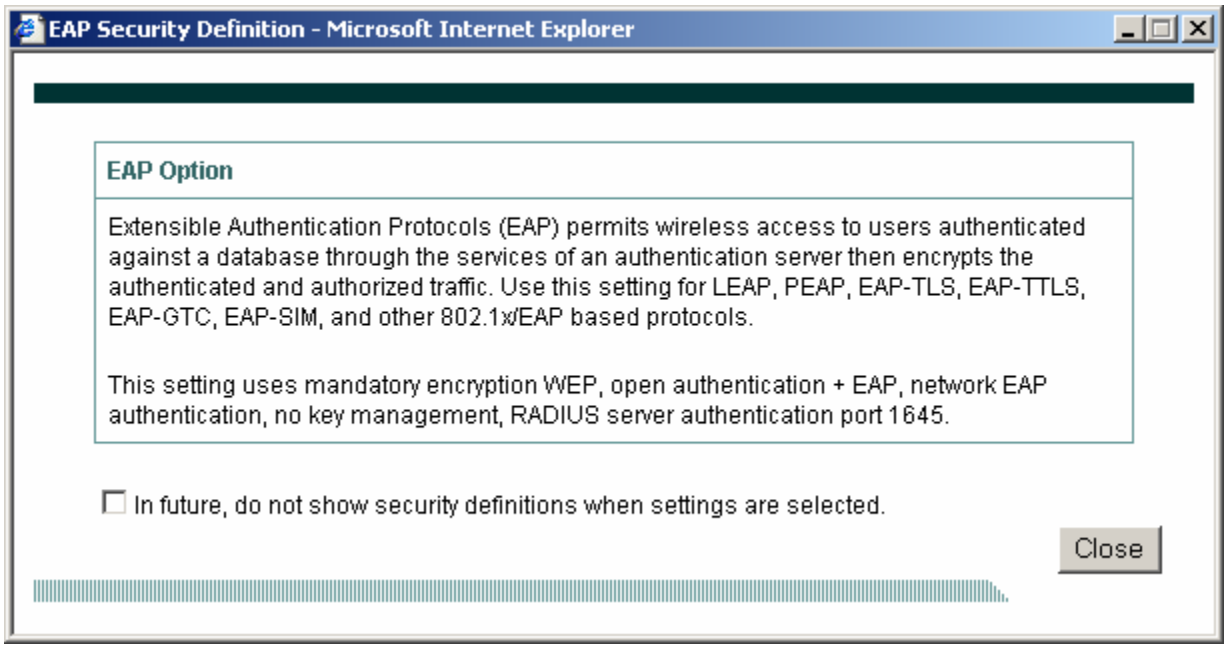



Figure1.

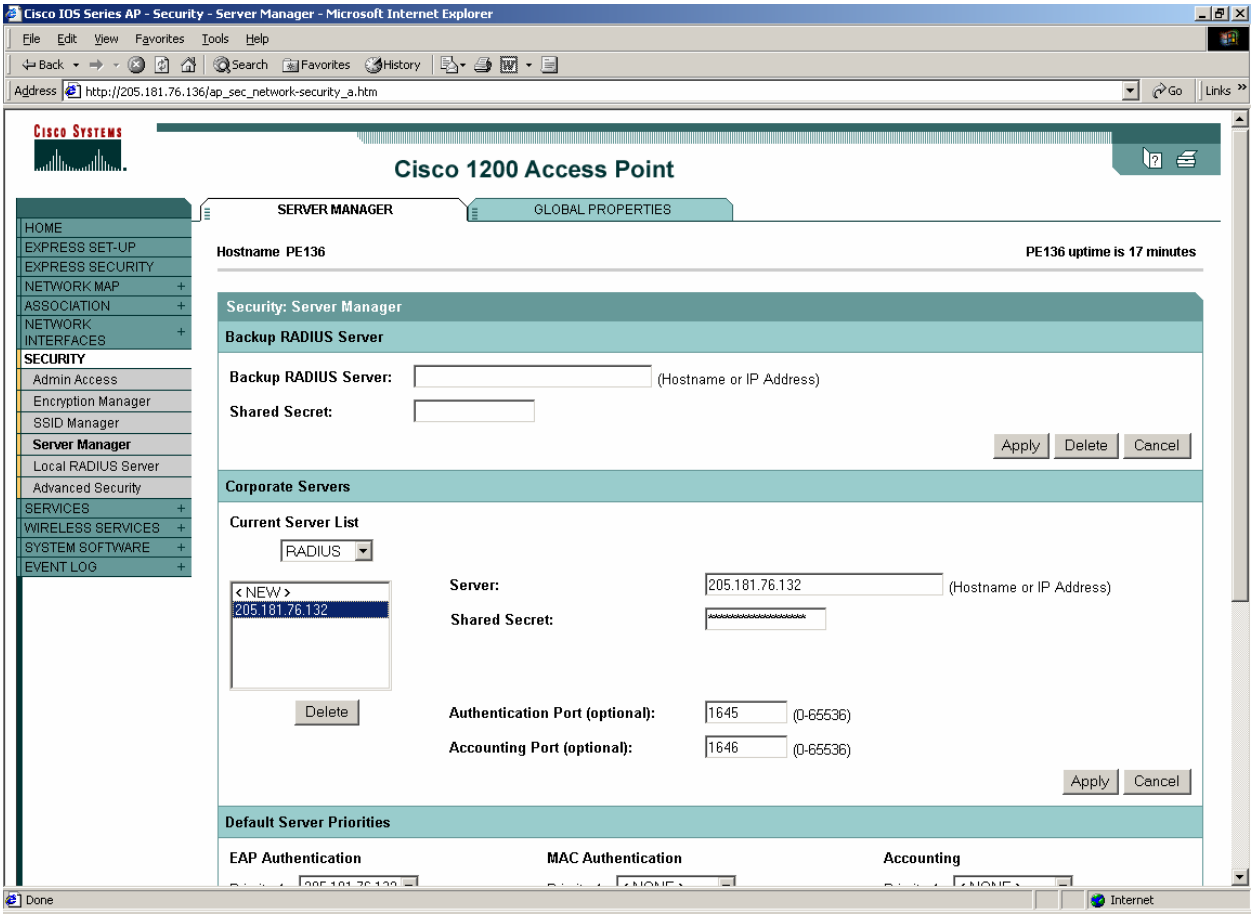
4. Click **Apply** for the Express Security setting to take affect.

5. You should now see an entry for your SSID on the SSID Table.

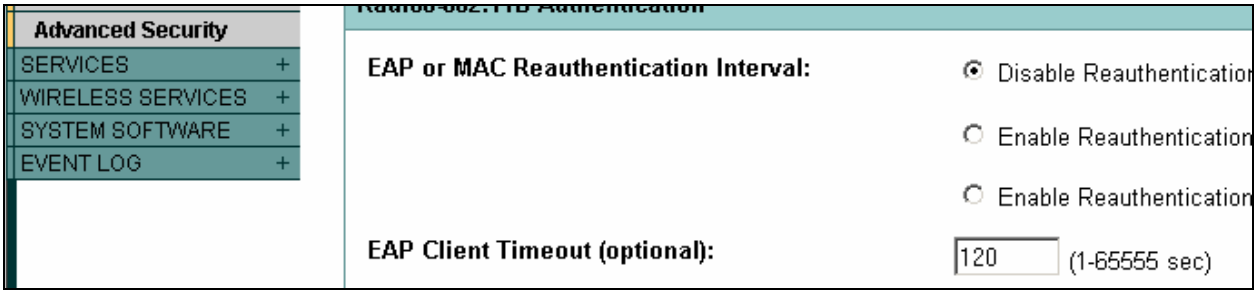
**SSID Table**

| Delete | SSID | VLAN | Encryption | Authentication | Key Management | Native VLAN | Broadcast SSID |
|---|---|---|---|---|---|---|---|
| ◉ | aironet | none | wep mandatory | open+EAP , network EAP | none | | ✓ |

6. Under the " Security – Server Manager " section verify that the RADIUS server address, port number, and “shared secret” are configured. These settings are “standard” and do not differ from those used in other authentication configurations, such as LEAP or EAP-TLS.



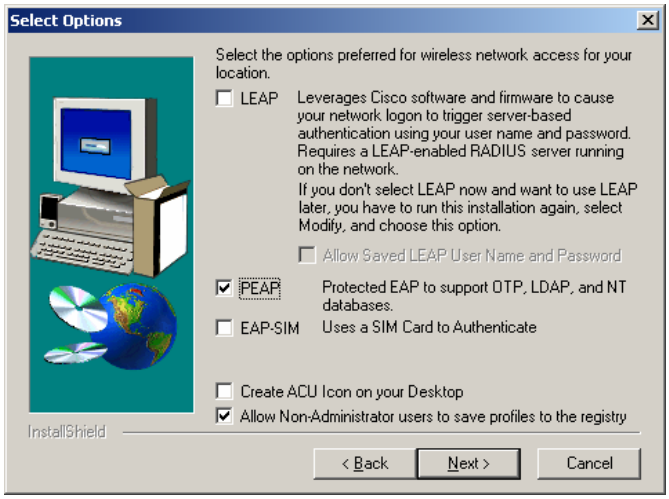

***Note***: *You will have to increase the default timeout value from 20. Testing was successful after increasing it to 120. This is also the default that RSA ACE/Server uses when authenticating users via RADIUS.* To do this go to Security - Advanced Security, click the Timers tab and set the EAP Client Timeout (optional).



## C. 802.11 wireless client configuration

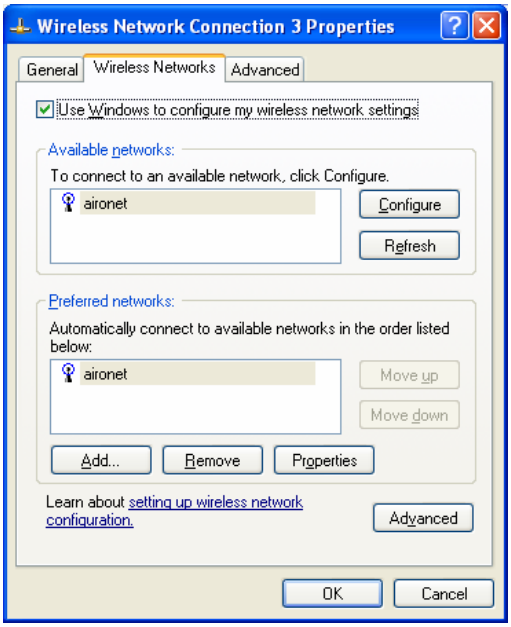
For a more in depth explanation of how to configure your wireless hardware, please refer to the documentation provided by your hardware vendor.

1. **Install Cisco Aironet Client Utility.** Choose appropriate PEAP option from "Select Options" screen:

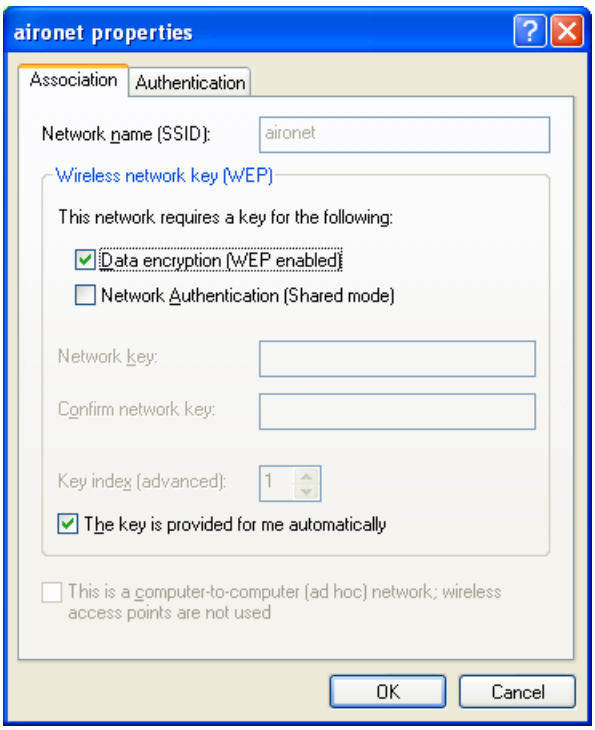


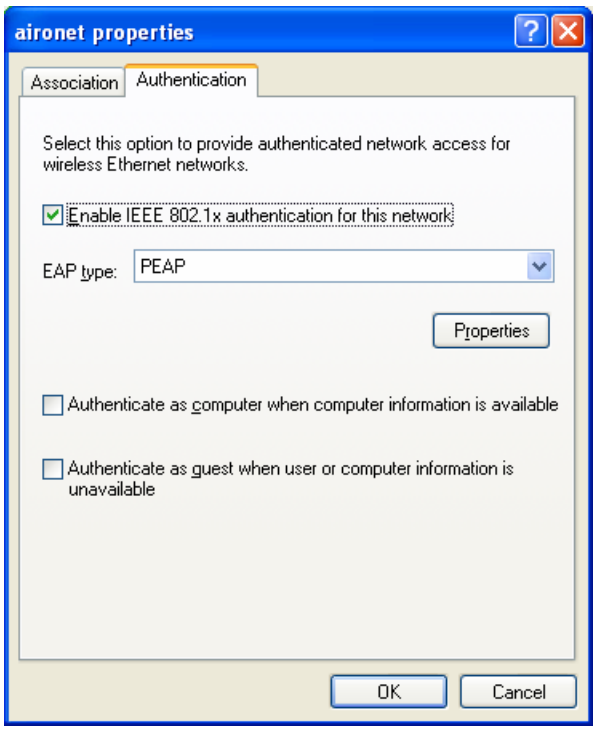

2. **Configure PEAP Client 1st Phase Operation.** 1st Phase PEAP authentication is handled between the PEAP supplicant and the authentication server (ACS 3.1). In this phase, the client authenticates the server using certificate-based mechanism. This establishes an encrypted tunnel over which the 2nd Phase PEAP transactions take place. Note: The screens will differ if you don't have SP1 installed on Windows XP.

   - Bring up your Wireless Network Connection Properties for your wireless card/connection

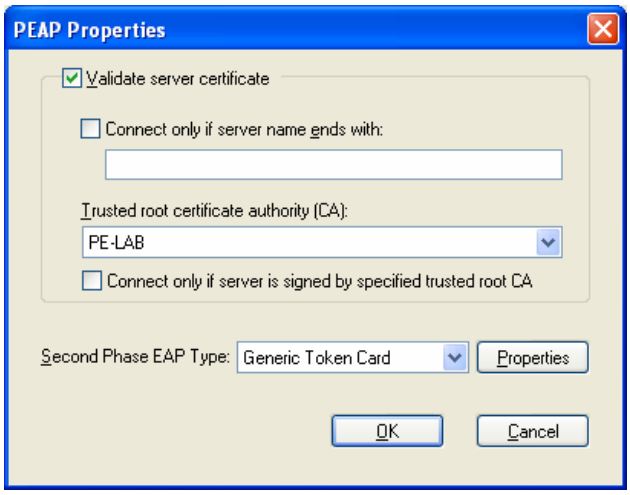


- Select the Wireless Networks tab.
- Select Use Windows to configure my wireless network settings.
- Click “Configure” under Available networks or “Properties” under Preferred networks.
- Under the Association tab, check the box for ‘Data encryption (WEP enabled)” and “The Key is provided for me automatically”.
- Under the Authentication Properties tab, check the box to ‘Enable IEEE 802.1x authentication for this network”. Then select PEAP under “EAP type”.



- When PEAP is selected as the EAP type, the Properties button just under the EAP type pull down menu allows configuration of PEAP parameters. This configuration screen for PEAP supplicant allows users to specify options for PEAP, EAP type & necessary parameters:




- From this configuration screen, the most important PEAP configuration parameters for the client are set. The 1st Phase PEAP settings are configured here- whether to validate server certificate (which should be "checked") as well as the Certificate Authority used to authenticate the server are selected on this screen. Please make sure that the certificate for the trusted root certificate authority for the server is installed on the client computer and is selected in the list of trusted CA's.

3. **Configure PEAP Client 2nd Phase Operation**. There are two major types of authentication used for 2nd Phase PEAP: One Time Password authentication and Static password authentication to external database. The following section details the operation of One Time Password (OTP) Configuration and Verification.

   - For user authentication using RSA Security's ACE/Server, configure the type of token to be used for One Time Password <EAP type> Authentication under the Generic Token Card Properties button found under the client's Windows Device Manager> Authentication> "EAP Type" Properties> PEAP Properties button.

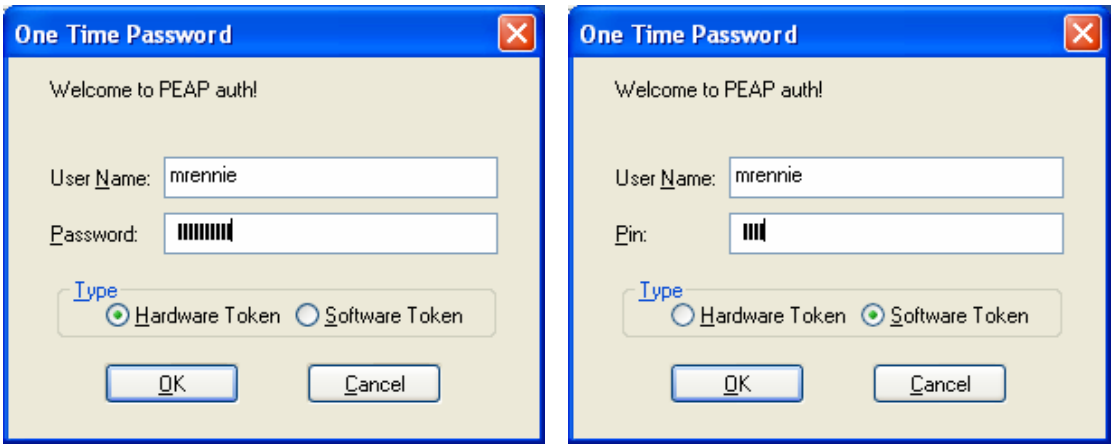
## Authentication Process

After configuration of the client for OTP operation and upon initialization and association of wireless client to the 802.1x-enabled Access Point, an authentication dialog box will be presented to the user. The user either enters their SecurID credentials as read from either their hardware token device or enters the PIN number from their RSA Software Token. The following steps walk you through the user experience:

**Step 1** A pop-up message appears above the Windows system tray informing you that you need to select a certificate or other credentials to access the network. **Click this message:**

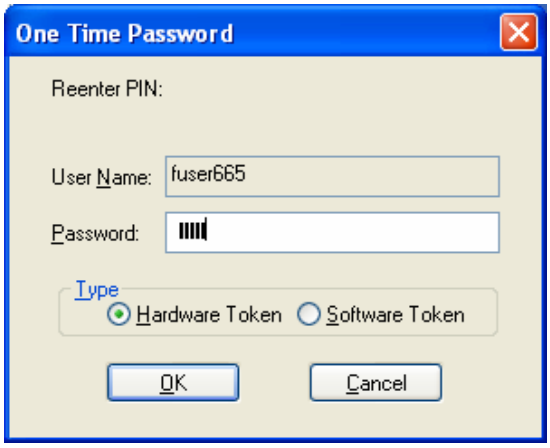

**Step 2** A pop-up message appears above the Windows system tray informing you that you need to enter your login credentials:


**Step 3** Enter your PEAP authentication username in the User Name field. Select either the **Hardware Token** or **Software Token** option. If you select the Software Token option, the Password field on the One Time Password screen changes to the PIN field. Enter either your hardware token password or your software token PIN:

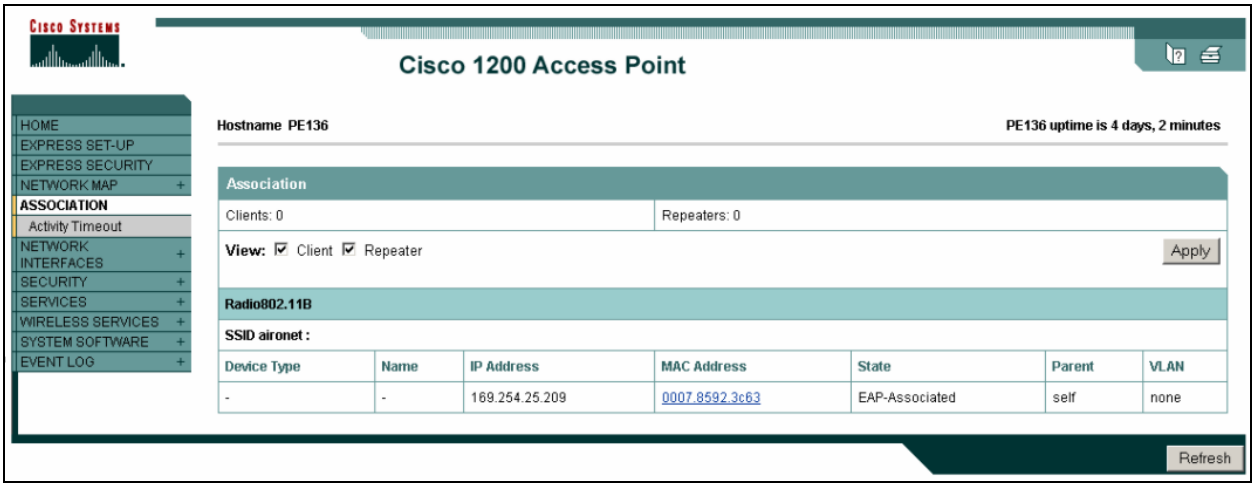



***Note**: When using the PEAP client software in conjunction with the RSA Software Token, the user is prompted for a PIN, but is not required to enter the entire PASSCODE (which is generated by the Software Token client application).*

**Step 4** Click **OK**. The client adapter will now EAP authenticate. Below are examples of a user in New Pin and Next Tokencode along with the client association on the access point.





## 7. Certification Checklist

Date Tested: August 31, 2004

| Tested Certification Environment | | |
|---|---|---|
| **Product** | **Platform (OS)** | **Product Version** |
| RSA Authentication Manager | Windows 2000 | 5.2 |
| RSA Authentication Agent | Windows 2000 | 5.2.0 (527) |
| RSA Software Token | Windows 2000 | 3.0.4 |
| Cisco AiroNet AP1200 | N/A | 12.2.15JA |
| Cisco AiroNet 350 Client card | N/A | Driver version 8.3.10 |
| Cisco AiroNet Client Utility | XP | 6.3 (installer v14) |

| Test | RSA Native Protocol | RADIUS Protocol |
|---|---|---|
| **1st time auth. (node secret creation)** | P | |
| **New PIN mode:** | | |
| **System-generated** | | |
| Non-PINPAD token | P | N/A |
| PINPAD token | P | N/A |
| **User-defined (4-8 alphanumeric)** | | |
| Non-PINPAD token | P | N/A |
| Password | P | N/A |
| **User-defined (5-7 numeric)** | | |
| Non-PINPAD token | P | N/A |
| PINPAD token | P | N/A |
| Software token | P (1) | N/A |
| Deny 4 digit PIN | P (2) | N/A |
| Deny Alphanumeric | P (2) | N/A |
| **User-selectable** | | |
| Non-PINPAD token | P | N/A |
| PINPAD token | P | N/A |
| **PASSCODE** | | |
| 16 Digit PASSCODE | P | P |
| 4 Digit Password | P | P |
| "Pin-less" TokenCode | P | P |
| **Next Tokencode mode** | | |
| Non-PINPAD token | P | N/A |
| PINPAD token | P | N/A |
| **Software Token API Authentication** | | |
| New PIN mode | N/A | N/A |
| 8 Digit PIN with 8 Digit TokenCode | N/A | N/A |
| **Failover** | P | N/A |
| **User Lock Test (RSA Name Lock Function)** | P | |
| **No RSA Authentication Manager** | P | P |

SWA

Pass, Fail or N/A (N/A=Non-available function)

## 8. Known Issues

- **RADIUS**. New Pin and Next Tokencode modes do not work via RADIUS. This is due to the fact that state is not kept during the challenge response. The RADIUS tests above were done by attempting to proxy the RADIUS request from a RADIUS client through Cisco Secure ACS to ACE/Server's RADIUS.

- **PEAP.** PEAP testing involved using a wireless client authenticating through an Access Point, which talked RADIUS to Cisco ACS 3.1, which talked Native SecurID to ACE/Server 5.0.

    - **(1) RSA Software Token.** New Pin mode and Next Tokencode modes are not supported when using this form of authentication with XP (Windows 2000 works as designed). This has been reported to Cisco and will be addressed in the next version of PEAP. The error you will receive is:


    - **(2) Deny 4 digit / Alphanumeric PINs.** If a user in New Pin mode goes against the PIN policy, the authentication process fails, and the user is unaware of how or why. Typically, if a user goes against the policy, they will be sent a message that the PIN was rejected and be prompted again while showing the user again what the PIN policy is (For example if the PIN policy is 5-7 digits, yet the user enters 4 digits).

    - Roaming between Access Points with SecurID is supported and handled by the ACS Server.

    - Service Pack 1 for Windows XP includes Microsoft's PEAP supplicant, which supports a Windows username and password only and does not interoperate with Cisco's PEAP supplicant. To use Cisco's PEAP supplicant, install ACU version 5.05.001 or greater ***after*** Service Pack 1 for Windows XP. Otherwise, it will be overwritten by Microsoft's PEAP supplicant. You can also install Cisco's PEAP supplicant separately.

    - Current Microsoft EAP framework currently only permits 1 EAP DLL per EAP type. This may cause conflict if multiple PEAP implementations are resident on the same machine.

    - As of November 2002, Windows XP and 2000 are the only operating systems supported for use with PEAP, EAP-TLS, EAP-MD5, and EAP-SIM authentication in conjunction with ACU. Windows 2000 requires a patch which is documented in TechNet article Q 313664 and can be downloaded @ http://support.microsoft.com/default.aspx?scid=kb;en-us;313664

## Appendix