Security Backbone Configuration

For:
HX2 with Windows® CE 5.0
HX3 with Windows® CE 5.0
MX3Plus with Windows® CE 5.0
Marathon with Windows® XP, Windows® 7 or Windows® Embedded Standard 2009
MX7 Tecton with Windows® CE 6.0 or Windows Mobile® 6.5
MX7 with Windows® CE 5.0
MX8 with Windows® CE 5.0 or Windows Mobile® 6.1
MX9 with Windows® CE 5.0 or Windows Mobile® 6.5
Thor VM1 with Windows® CE 6.0 or Windows® Embedded Standard 2009
VX3 Plus with Windows® CE 5.0
VX6 with Windows® CE 5.0
VX7 with Windows® CE 5.0
Thor VX8 with Windows® XP, Windows® 7 or Windows® Embedded Standard 2009
Thor VX9 with Windows® XP, Windows® 7 or Windows® Embedded Standard 2009

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

Web Address: www.honeywellaidc.com

Acrobat® Reader © 2012 with express permission from Adobe Systems Incorporated.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

Patents

For patent information, please refer to www.honeywellaidc.com/patents.

Limited Warranty

Refer to www.honeywellaidc.com/warranty_information for your product’s warranty information.

Table of Contents

Chapter 1: Introduction

Overview

Note: Some of the equipment described in this manual is obsolete. Screen displays may differ based on the version of Cisco IOS you are using. However, to secure your wireless infrastructure the configuration process described remains the same.

Keeping a network secure is becoming quite a task. There are Internet based attacks making the news, thefts of PC's and especially laptops are common enough not to be news worthy and finally there is that mysterious subject of wireless security. Just how do you protect your computers and data from intrusion?

While this document contains a brief discussion of Internet and wired security procedures, the bulk of the information concerns wireless security.

Objectives

When you finish reading this guide, you should have a grasp of the types of security available to protect your network, especially the wireless portion. The purpose is not to explain the Honeywell components and systems themselves, but rather to give you the knowledge you need to read other, more detailed, documents on those subjects.

If you are a Honeywell employee or customer and you sometimes feel unsure of or intimidated by the security terminology you hear thrown about, then this document has been written for you. Rather than concentrating on developing detailed technical skills, this document is designed to give you an intuitive sense or feel for the security concepts and terms used.

Please refer to the appropriate mobile computer online Reference Guide for complete information on configuring security parameters for Honeywell mobile computers.

Also, please refer to documentation provided by other manufacturers (i.e.: Cisco documentation for the Access Point IOS) for other components in your network.

Principles of Network Security

Overview

In order to understand the threats to network security, we need to divide the attacks into different categories. There are many different ways to categorize attacks and we'll look at a few.

Later, as we begin to look at solutions, consider the type of attack when weighing the possible solutions.

We can divide attacks into two categories, structured and unstructured.

- An unstructured attack comes from a person (or persons) with limited technical ability, knowledge and resources. Examples include an outsider looking for free access to the Internet or to create network or Internet traffic to slow the system down. In many cases, these attacks are quite inconvenient but the attacker is not looking to steal information. Generally, even a minimal level of security discourages an unstructured attack. For example, simply changing wireless equipment settings from factory defaults and implementing security as basic as WEP may discourage an unstructured attack.
- Structured attacks are more sophisticated. The person (or persons) implementing the attack may have a deep understanding of network design and network and protocol weaknesses. These attackers will have some financial resources to devote to the attack. Attackers may be after banking, credit card or personal identity information. Your network could be the victim of industrial espionage from a competitor looking for confidential information. Other attacks may seek to destroy information. Competitors may hope to interrupt your business by deleting critical information from your network. You may find that WEP may not provide the security you desire when faced with a structured attack on your wireless devices. A structured attacker will be more familiar with the weaknesses built into an operating system, for example.

We can divide the attacks according to the source of the attack, internal or external.

- External threats originate from outside the users of your network. In many cases, the external attacks originating from the Internet are the ones you hear the most about. Other types of external threats include someone eavesdropping on your wireless network traffic.
- Internal threats originate from users on your network. The most common would be an employee, but could also be a contractor or vendor. An insider is authorized to be on the network and may know their way around the network fairly well. A common example is a disgruntled employee. Unintentional actions of employees may also pose an internal threat by downloading software containing viruses or worms.

We can also divide the threats into three categories, technology, configuration and policy weaknesses.

- Technology weaknesses include any weakness due to protocol, hardware or operating system. For example, TCP/IP protocol contains weaknesses because it was designed to be an open standard for communication. Many people are familiar with the workings of TCP/IP and how it can be exploited. Technology weaknesses also include operating system weaknesses. The most common examples are the security flaws (and related updates) announced for Microsoft® Windows®. Although problems with Windows operating systems get the most press due to the widespread use of Windows, any operating system should be considered a candidate for this type of attack.
- Configuration weaknesses arise when network equipment is left in its default configuration. A common mistake is failing to secure administrator accounts with a unique password, leaving no password (or the factory default password) to provide little security against attack. Another configuration weakness is using passwords that are easily guessed (common names, short passwords, common words).
- Policy weaknesses are the failure to implement and follow a policy on security. Policy should be written and include actions to be taken in the event of an attack. Another vital policy point is a recovery plan. Policy plans should include details on user privileges, passwords, Internet access, and hardware configuration. Common policy weaknesses are a lack of a policy plan or the failure to enforce the policy that is in place. Good policy includes strong passwords and a

regular password change policy. Good policy also includes removing user accounts when employees leave the company.

We can even divide the methodology into four categories as to how the attack is executed: reconnaissance attacks, unauthorized access, denial of service attacks, and data manipulation.

- Denial of service attacks attempt to disable network services for legitimate users. An example is sending a large number of PING requests, overwhelming devices in the network and slowing (if not stopping) service for legitimate users. Attacks may also be directed against CPU utilization, buffer memory or disk drive space as well as network resources.
- Reconnaissance attacks are unauthorized discovery, mapping or monitoring of the network. The attack may be to learn more about the network for additional attacks or to eavesdrop on network traffic for passwords or information theft.
- Unauthorized access occurs when an intruder gains access to information they should not access. It may be an outsider or it may be an employee viewing information they should not be able to access. Unauthorized access can occur when an intruder is able to find a user name and break a password. Once an intruder gains access, they can gain control of targeted devices or attempt to penetrate deeper into the network. The goal may be to gain “administrator” access to the network.
- Data manipulation is often referred to as a man in the middle attack. An intruder captures, manipulates and replays data. The attack may be made by IP spoofing (impersonating the identity of a trusted computer), session replay (interception and capture of data packets or commands which are then manipulated and rebroadcast), session hijacking (intruder takes over the session and inserts false data packets) and rerouting (intruder gains access to routers and spoofs identities, which can allow a remote host to pose as a local host on the network).

As we start to look at solutions, consider how these categories mentioned above come into play. If you expect unstructured attacks originating internally, you may find policy changes are all that is necessary. If you expect a structured attack from external sources, be aware of technology, configuration and policy weaknesses.

How do you protect your network from these types of attacks?

We’ll look at solutions by the portion of the network susceptible to the attack. The reason for this is because the commercially available security products seem to fit these three areas:

- Internet security risks
- Wired network security risks
- Wireless network security risks

Keep the distinctions made above in mind when considering the solutions provided.

Internet Security

Perhaps more has been written about Internet security than any other type of network security. Honeywell realizes most of its customers won’t use their mobile computers to browse the Internet. However, it is likely PC’s on the same network as the mobile computer may be used to browse the Internet. Once a virus enters the network, it may spread to other devices on the network.

There are many commercially available products to protect your computer or network from Internet based attacks. A firewall and anti-virus program should be considered the bare minimum. Types of attacks include:

- Trojan horse – A destructive program appearing as a benign application. An example is a virus removal program that introduces a new virus to the system rather than removing the virus as promised. Unlike a virus, a Trojan horse does not replicate itself. Instead the program stays in place doing its damage or allowing an outside person to take control of the computer.
- Virus – A piece of software code loaded onto your computer without your knowledge. The code is buried within an existing program. Once the code is executed, the code may be copied to other programs or other computers. Viruses may simply display a message or replicate to the point all available disk space or memory has been used. More malicious viruses may seek to destroy programs or data. Viruses may perform their action immediately or lay dormant until a certain date or time.
- Worm – A program or algorithm that replicates itself over a computer network. The worm replicates until the computer’s resources are used up, eventually taking the system down.
- Spyware – Software that sends information about your habits, such as web browsing, to a certain web site. Often, spyware is used to more directly target advertising on web sites to the user’s past browsing patterns. Spyware may also be used to gather e-mail addresses, passwords or credit card information.

There are numerous commercial and freeware antivirus and spyware blocking/removal programs available. Most of these providers maintain websites that provide details on the threats currently circulating. Please refer to these websites to determine the software packages that best suit your needs.

While Honeywell does not make specific recommendations on Internet security as Honeywell computers are generally not used to browse the Internet, you should consider implementing appropriate policies on Internet security on other portions of your network, such as

- Installing anti-virus programs on all computers that access the Internet.
- Scheduling of regular system virus scans.
- Regularly updating virus definitions.
- Computers with sensitive information should also be equipped with spyware detection tools.
- Implementation of software and/or physical firewalls to limit intrusion or damage should security be breached.

Wired Network Security

Providing a secure wired network can be accomplished by limiting physical access to wired network computers and setting up a “strong” password policy for user login.

- The strong password policy should include requiring the longest possible password (8 characters should be the minimum, 10 are better), and should enforce periodic password changes. If possible, passwords should include a mixture of letters, numbers and special characters.
- Policy should include regular password changes; especially to update any passwords an employee had access to when that employee leaves the company.
- As operating system security flaws are discovered, software updates should be implemented. This is especially important on computers with Microsoft Windows operating system simply because it is the most commonly deployed OS and is subject to more types of attacks.
- Implementation of software and/or physical firewalls to limit intrusion or damage should security be breached.

There are many commercially available publications dealing with networks and network security. Please refer to these guides for information on general network configuration.

Wireless Network Security

What type of wireless security is right for your network? Your choice will depend on many factors:

- Your network architecture – are there barriers between the wireless network and rest of the corporate network, is sensitive data available on the wireless network?
- The wireless client devices – what operating systems are used, what security options are available, etc?
- Your security infrastructure – what user database are you using, what authentication technology is being used, is a PKI in place, etc?
- How much administrative resource are you willing to commit to wireless security?
- What security policies can you reasonably expect your users to tolerate?

When to Upgrade?

If you are running a network of DOS computers and are concerned about security, when do you implement WPA (Wi-Fi Protected Access) since it requires an investment in new equipment? If your data is sensitive and you consider the probability of an attack likely, you may want to invest in WPA compliant equipment immediately. If you elect not to upgrade, use the strongest possible security available to you on the old equipment, for example, 128-bit WEP (as opposed to 40-bit) or Cisco’s LEAP if your equipment supports it.

Network Segmentation

If your DOS devices are used for a less critical purpose like transmitting inventory picks and moves, you may want to create network segments. Properly implemented, you can keep DOS devices running WEP or LEAP on their own network segment. If security of these older wireless devices were breached, only the information in the particular network segment would be in jeopardy.

If a building contains both office space and warehouse space, it certainly would make sense to create at least two network segments. The wireless inventory control computers could operate on WEP or LEAP. This would discourage most “casual” attackers. If a determined attacker did gain access to this network segment, they would be limited to the pick move data carried on this segment.

The office segment of the wireless network would likely carry much more sensitive data such as payroll information, employee data and business plans. Since the wireless computers in the office segment are likely going to be laptop computers running a Windows operating system, it makes sense to implement a WPA solution on this segment.

WEP

WEP (Wired Equivalent Privacy) is an IEEE standard security protocol that was introduced in 1997. The intent was to provide the same level of security to wireless networks that was possible in a wired environment. When WEP is used, data is encrypted as it is transmitted over the wireless network. Unlike WPA security methods, WEP does not provide for direct user authentication. However, since a client without the WEP key can only associate with an access point but cannot transmit data, WEP does provide a de facto user authentication.

WEP originally specified a 40-bit key. 128-bit keys (actually 104 bits plus a 24-bit initialization vector) were later specified. When possible, 128-bit keys should be specified as the longer key greatly increases security.

Advantages

- Available across DOS, Windows (98, 2000, XP) and Windows CE platforms.
- Can deter many less determined attackers such as “war drivers” looking for an open system to gain free access to the Internet.
- Dynamic WEP can be used to reduce the possibility of a security breech, where supported.

Disadvantages

- Requires the key to be entered on all access points and wireless devices. This makes regular changes to the WEP keys cumbersome.
- Encryption method used (RC4) is weak.

LEAP

Cisco’s LEAP may provide additional security as compared to WEP. However, LEAP is the oldest of the wireless oriented 802.1x protocols, and likely the most widely deployed. Recently published tools to exploit password vulnerabilities in the LEAP protocol have made it less attractive. LEAP should be deployed only if no other 802.1x protocol is supported, and then only if a strong password policy can be enforced.

LEAP authenticates users based on user names and passwords. LEAP does not require a Public Key Infrastructure (i.e. there is no certificate authority). While WEP only provides data encryption, LEAP authenticates users.

When deployed outside of WPA, LEAP can be used with Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC) to provide enhanced data encryption.

Advantages

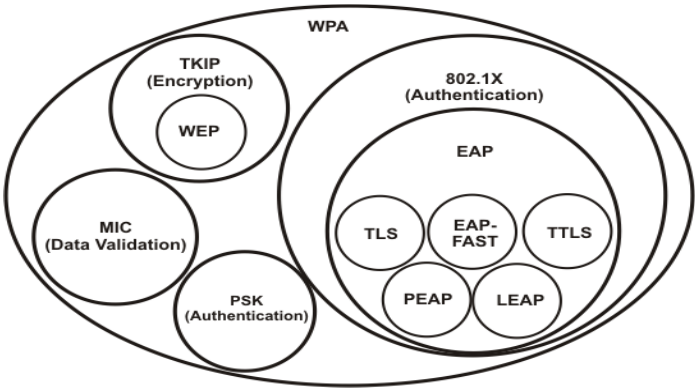
- Available across DOS, Windows (98, 2000, XP) and Windows CE platforms when Cisco radios are used.
- Can deter many less determined attackers such as “war drivers” looking for an open system to gain free access to the Internet.
- Is not vulnerable to published WEP attacks.

Disadvantages

- LEAP requires a RADIUS server.
- Requires Cisco or CCX certified radios and Access Points.
- Vulnerable to dictionary attack, meaning that enforcement of a strong password policy is required for security.

WPA

WPA contains two components – Encryption and Authentication. TKIP and MIC, both considered encryption components, are required. Authentication is also required, but there are many options available. WPA compatible devices for enterprise applications are required to support some form of 802.1x authentication – but not all of them. Devices intended for small office or home use can support WPA Pre-Shared Key PSK() instead of 802.1x. Many devices will support several forms of 802.1x authentication, as well as WPA-PSK.



If you are interested in the additional security provided by WPA, the first question you need to ask is “Does my equipment support WPA?”. Mobile computers that support WPA include all Honeywell computers with a Summit Client Utility (Windows XP, Windows CE and Windows Mobile operating systems), a Broadcom Client Utility (Windows XP operating system) or a Atheros Client Utility (Windows XP operating system). These utilities provide additional configuration options not available with the Windows Wireless Zero Config utility. If your mobile computer is not covered in the list above, please contact Technical Assistance for WPA support options. Complete instructions for using the wireless configuration utilities is covered in the device-specific Reference Guide.

If your equipment does not support WPA, is the additional security worth the upgrade costs? Upgrades may consist of new software or drivers for existing computers, a wireless radio upgrade or new mobile computers that support WPA. You’ll also want to check other wireless devices on your network. Many wireless printers, scanners and VoIP wireless telephones, for example, do not support WPA security. Also, older models of wireless Access Points may not support WPA.

If your equipment supports WPA, the next question is “What type of WPA should I implement on my network?”. Do you want to implement EAP-TLS, PEAP/MSCHAP or some other 802.11x protocol? Is WPA-PSK an option for you? The sections that follow provide some detail on the different WPA protocols available to you.

Advantages

- First truly ‘enterprise’ caliber security available for wireless networks.
- Improved data encryption using Temporal Key Integrity Protocol (TKIP).
- End user authentication is provided.
- Data validation ensures messages have not been altered during transmission.
- Different protocols allow flexibility to tailor security to your needs.

Disadvantages

- Requires more administrative effort than static WEP.
- May require hardware upgrades/replacement and additional network infrastructure.

EAP-TLS

This is probably the most secure of the 802.1x protocols in common use. But this security comes at a price. EAP-TLS requires PKI certificates on both the authentication server and on the client computers. These certificates provide identification (instead of a password). An asymmetric mathematical algorithm is used to verify certificates. Mutual authentication is supported (RADIUS server authenticates the client, client authenticates the RADIUS server) to eliminate rogue Access Point vulnerability. EAP-TLS requires more administrative attention than other 802.1x protocols.

Advantages

- Is available from all security supplicant vendors, such as Summit. It is included with Windows XP Service Pack 2 using Windows Wireless Zero Config.
- Provides strong authentication and security.

Disadvantages

- Costly, compared to password based systems, because of the required software and manpower for setup, training and maintenance.
- Is really practical only for device security. Especially in a warehouse environment, it is very difficult to use certificates to authenticate users.

PEAP/GTC

PEAP (Protected Extensible Authentication Protocol) is similar to EAP-TLS in that it is based on Transport Layer Security. PEAP, however, does not require user certificates on the client computers. PEAP establishes a protected tunnel to pass user credentials back to the authentication server.

There are two versions of PEAP available. This version uses credentials obtained from a Token Card to validate the user. PEAP/GTC could also be used to pass username and password credentials to any user database which expects clear text passwords.

Note that the password is not passed in clear text over the wireless link. On the wireless link, the password is encrypted inside the PEAP protected tunnel. Once it reaches the access point, and the PEAP tunnel is removed, it is placed in clear text on the Ethernet network.

Advantages

- Provides compatibility with a wide variety of user databases. Can be used with LDAP or other non-Microsoft user databases, as well as with all popular token card authentication engines.
- Does not require user or client device certificates, and is less difficult to administer than an EAP-TLS system.
- Provides strong authentication and security.

Disadvantages

- Not widely supported. It is not supported in Microsoft’s Windows XP WLAN security supplicant (the Zero Config utility).
- Token cards require additional hardware and are not typically suitable for warehouse deployment due to user and hardware considerations.
- One time passwords (OTP) complicate 802.11 mobility and are not recommended. One time passwords are common with token card systems.

PEAP/MSCHAP

PEAP (Protected Extensible Authentication Protocol) is similar to EAP-TLS in that it is based on Transport Layer Security. PEAP, however, does not require certificates on the client computers. PEAP establishes a protected tunnel to pass user credentials back to the authentication server.

There are two versions of PEAP available. This version uses MS-CHAP v2 to authenticate user names and passwords. PEAP/MSCHAP v2 is useful if the user database stores passwords hashed using MS-CHAP v2. This typically constrains PEAP/MSCHAPv2 to use by enterprises which deploy Active Directory to store user credentials. However, local RADIUS databases can use this protocol as well.

Advantages

- Commonly available. PEAP/MSCHAPv2 is supported by all supplicant vendors, and is one of three authentication methods supported natively by Windows XP Service Pack 2.
- Does not require user or client device certificates, and is less difficult to administer than an EAP-TLS system.
- Provides strong authentication and security.

Disadvantages

- Suitable only if user database stores passwords hashed with MSCHAP v2 (Active Directory or local RADIUS databases).

LEAP

LEAP (Lightweight Extensible Authentication Protocol) was developed by Cisco for deployment on wireless LANs with Cisco equipment.

Cisco’s LEAP may provide additional security as compared to WEP. However, LEAP is the oldest of the wireless oriented 802.1x protocols, and the most widely deployed. Recently published tools to exploit password vulnerabilities in the LEAP protocol have made it less attractive. LEAP should be deployed only if no other 802.1x protocol is supported, and if a strong password policy can be enforced.

It authenticates users based on user names and passwords. LEAP does not require a Public Key Infrastructure (i.e. there is no certificate authority).

Advantages

- Can deter many less determined attackers such as “war drivers” looking for an open system to gain free access to the Internet.
- Does not require any use of Certificates. LEAP is one of the easiest authentication protocols to administer.

Disadvantages

- Vulnerability to dictionary attacks means that enforcement of a strong password policy is a requirement.
- LEAP requires a RADIUS server.
- Requires Cisco radios, or CCX certified radios, and Cisco Access Points.

EAP-FAST

EAP-FAST was developed by Cisco to improve upon the security offered by LEAP. EAP-FAST uses shared secrets instead of certificates to establish an encrypted tunnel for exchanging user credebtials.

EAP-FAST occurs in three phases:

- Phase 0 is a method to provide a PAC (Protected Access Credential) key to the client. Alternatively, Phase 0 can be skipped and the PACs manually provided to the client.
- In Phase 1, the Cisco ACS and the user client establish a encrypted tunnel based on the PAC presented by the end user.
- In Phase 2, the Cisco ACS authenticates the user credentials with EAP-GTC which is protected by the encrypted tunnel created in the previous phase.

Advantages

- Does not require a strong password policy to be secure.
- Does not require any use of Certificates.

Disadvantages

- EAP-FAST requires a RADIUS server.
- Requires Cisco radios, or CCX certified radios, and Cisco Access Points.

PSK

WPA-PSK relies on a pre-shared secret key to establish the encrypted authentication and key exchange tunnel. Typically the Pre-Shared Key (PSK) is derived from a passphrase entered by the device administrator. The passphrase key is provisioned off-line (entered manually). Since the passphrase is manually entered into each device, it will rarely be changed. This makes it vulnerable to dictionary attacks. The IEEE 802 committee recommends that passphrases should be at least 20 characters long and follow the same rules as a strong password. This level of passphrase will deliver security equivalent of a 40-bit WEP key.

Honeywell does not recommend using WPA-PSK in enterprise applications. Some enterprises are tempted to use WPA-PSK to avoid the burden of establishing a RADIUS infrastructure. This should be chosen as a temporary solution only, with migration to 802.11x planned within the year.

Creating a Network Security Policy

It’s important to develop a network security policy. This should be a formal written statement detailing which people are given access to which network resources. The policy should be as specific as possible, detailing the scope of the policy, what constitutes authorized use and the technologies the organization will use to ensure only authorized users have access to the network and data.

As you start to formulate a network security policy, you will find that policies fall into three categories:

Open

- Permits everything that is not explicitly denied.
- Easy to configure and deploy.
- Transparent to network users.
- Lower cost.
- Least secure.

Restrictive

- A balanced approach between an open and a closed policy.
- Provides more security than an open policy at a greater cost and visibility.
- Provides less security than a closed policy at a lesser cost and visibility.

Closed

- Denies everything that is not expressly permitted.
- Most difficult to configure and administer.
- Highest impact and visibility to network user.
- Highest cost.
- Most secure.

What is right for you? Hopefully, the information presented in this document can help you determine the policies appropriate for your wireless network and provide some insight into security policies for the remainder of your network.

WPA Setup - A Backbone Case Study

Prerequisites

The equipment and configurations listed in this case study were tested by Honeywell. Other equipment and configuration options may be substituted however; these alternatives have not been tested by Honeywell.

Cisco AP1200 IOS

Internetwork Operating System (IOS)

Note: Configuration screens may appear slightly different depending on the version of IOS used.

Honeywell has also tested the Cisco 1242 and Cisco 1300 wireless bridges.

Cisco ACS Radius Server

Access Control Server (ACS) – ACS 3.2.3 or greater is required for EAP-FAST.

Remote Authentication Dial-In User System (Radius)

A Radius server is not necessary for TKIP.

Note: Configuration screens may appear different depending on the version of ACS used. ACS revision 3.3.2 was used for the illustrations in this document.

Windows 2003 Certificate Services

RSA ACE Server

The OTP server used.

Supplicant

The device must be equipped with the appropriate supplicant software. Please review the equipment requirements below to verify your device has the proper supplicant software installed.

Equipment Requirements

The Summit radio supplicant is available to support WPA for devices with Windows operating systems.

The VX8 and VX9 with an Atheros or Broadcom supplicant also support WPA.

For equipment not listed above, please contact Technical Assistance.

Configuration Process

1. Configure the Cisco AP for the appropriate authentication protocol. See Cisco AP / Bridge Configuration.
2. Configure the Cisco ACS RADIUS Server (not necessary for WPA-PSK). See Cisco ACS RADIUS Server Configuration to set up the RADIUS server for LEAP, PEAP/MSCHAP, PEAP/GTC and EAP-TLS.
3. Certificate administration (EAP/MS-CHAP, EAP/GTC, EAP/TLS) includes requesting certificate signing requests, requesting server and user certificates, exporting user certificates and installing certificates. See Certificate Administration.
4. RSA ACE Server Installation details the token server setup for PEAP/GTC. See RSA ACE Server Configuration.
5. Honeywell device configuration is covered in the online Reference Guide for the Honeywell device. Refer to the *Wireless Network Configuration* section in the Reference Guide.

Chapter 2: Cisco AP Bridge Configuration

The following equipment was tested by Honeywell:

Cisco AP1200 IOS

Alternative command line configuration for Cisco AP1200

Cisco 1242 Wireless Bridge

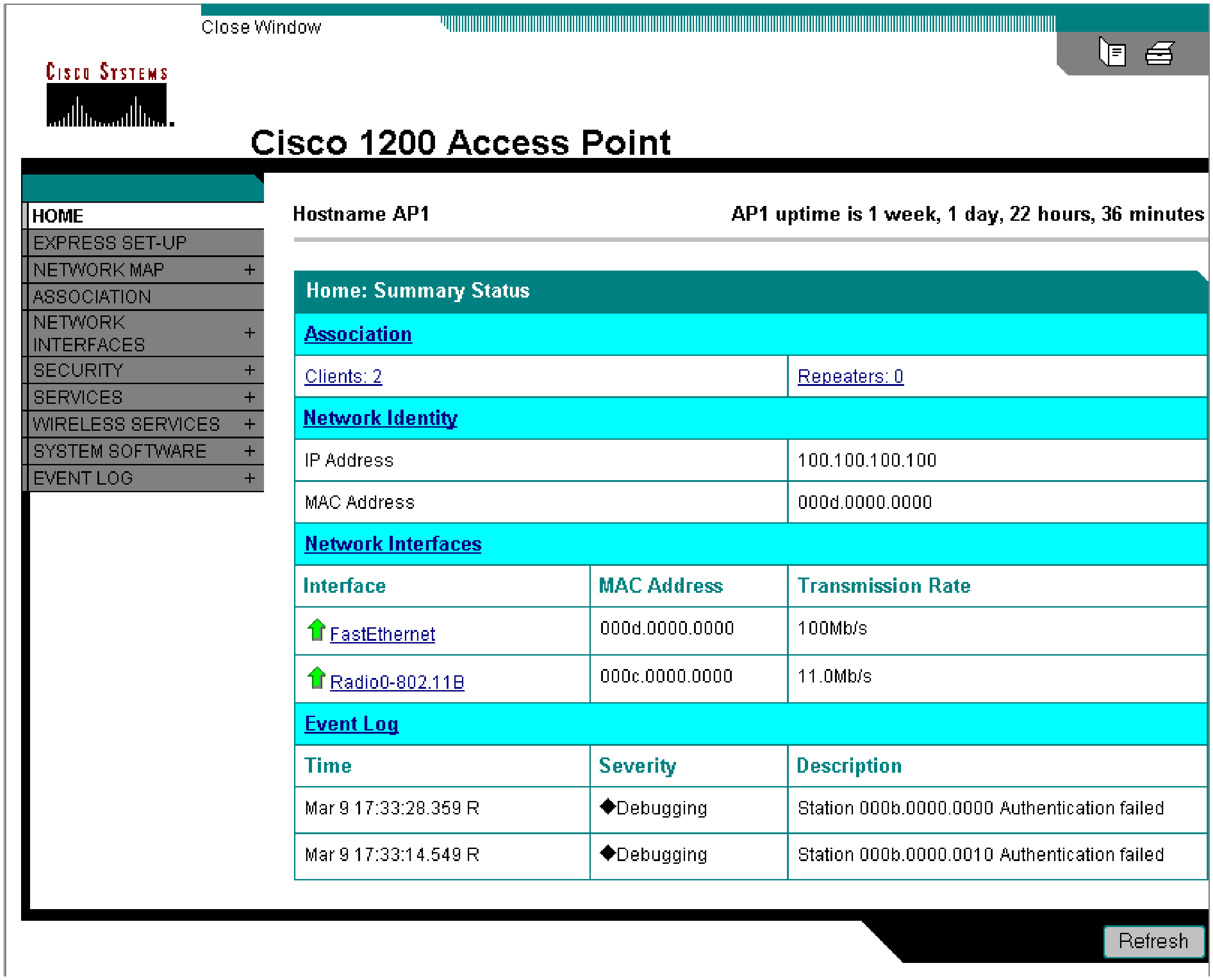
Cisco 1300 Wireless Bridge

Cisco AP1200 IOS Configuration

Web Browser Configuration

For browser configuration of the AP1200, open a browser to the main page of the AP by typing the IP address of the AP in the address bar. Enter the username and password when requested. The default is no username and Cisco for the password. Use the navigation bar on the left side of the screen to navigate to the following pages in this order:

Note: It is best to connect to the AP via the Ethernet port and not by radio. When configuration changes are made to the AP, the radio connection fails until the new configuration is made to the client radio as well.



Cisco 1200 Access Point

Hostname AP1

AP1 uptime is 1 week, 1 day, 22 hours, 36 minutes

Home: Summary Status		
Association		
Clients: 2		Repeaters: 0
Network Identity		
IP Address		100.100.100.100
MAC Address		000d.0000.0000
Network Interfaces		
Interface	MAC Address	Transmission Rate
↑ FastEthernet	000d.0000.0000	100Mb/s
↑ Radio0-802.11B	000c.0000.0000	11.0Mb/s
Event Log		
Time	Severity	Description
Mar 9 17:33:28.359 R	◆Debugging	Station 000b.0000.0000 Authentication failed
Mar 9 17:33:14.549 R	◆Debugging	Station 000b.0000.0010 Authentication failed

For more information on Cisco IOS, please refer to Cisco's on line help or product information available on Cisco's website.

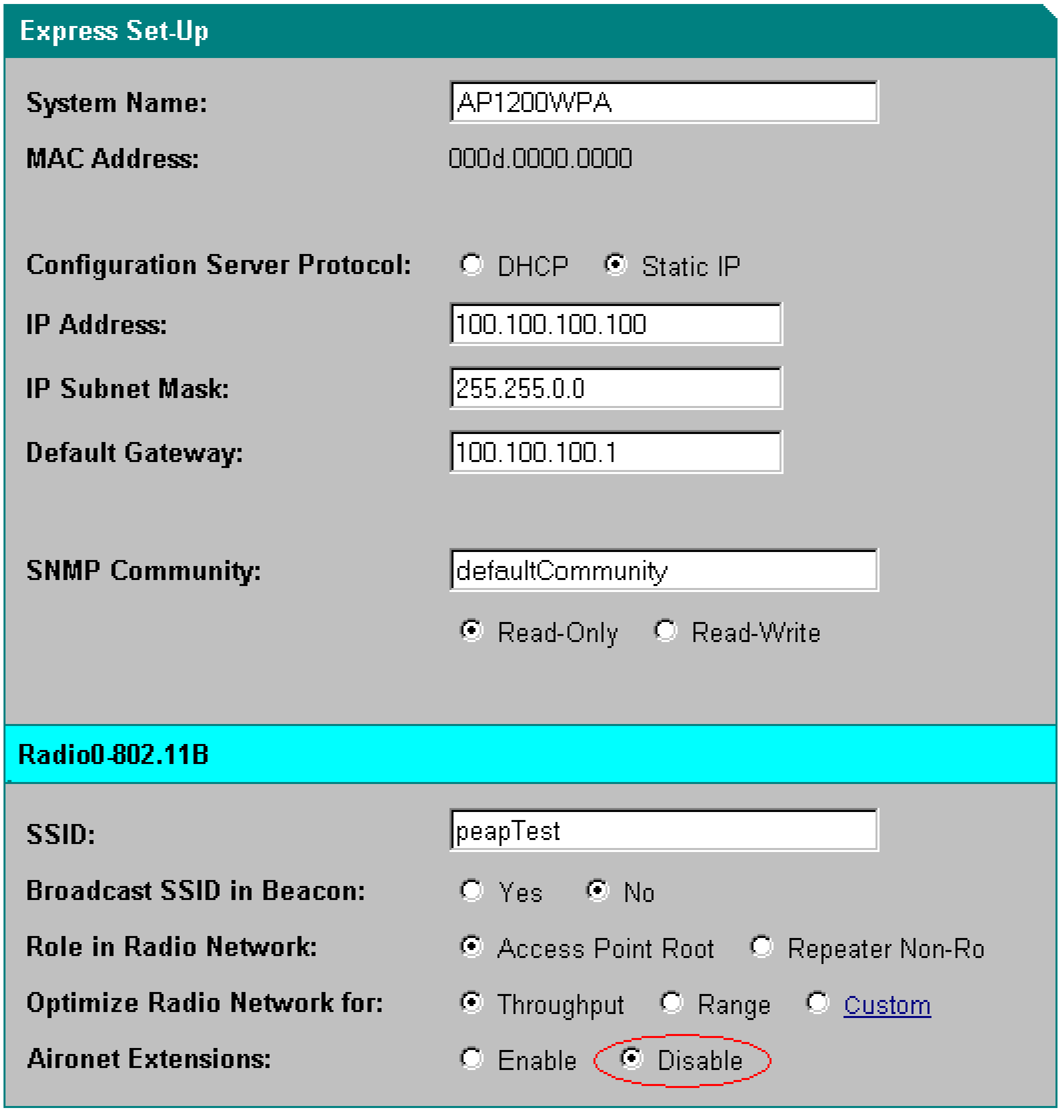
Screens shown throughout the remainder of this section are accessed from the navigation buttons shown displayed on the upper left hand corner of the screen.

Express Setup

Click **Express Setup**.

Set **Aironet Extensions** to disable.

Click **Apply**.



Express Set-Up

System Name:	AP1200WPA
MAC Address:	000d.0000.0000
Configuration Server Protocol:	○ DHCP ● Static IP
IP Address:	100.100.100.100
IP Subnet Mask:	255.255.0.0
Default Gateway:	100.100.100.1
SNMP Community:	defaultCommunity ● Read-Only ○ Read-Write

Radio0-802.11B

SSID:	peapTest
Broadcast SSID in Beacon:	○ Yes ● No
Role in Radio Network:	● Access Point Root ○ Repeater Non-Ro
Optimize Radio Network for:	● Throughput ○ Range ○ Custom
Aironet Extensions:	○ Enable [✓ ● Disable]

Server Manager

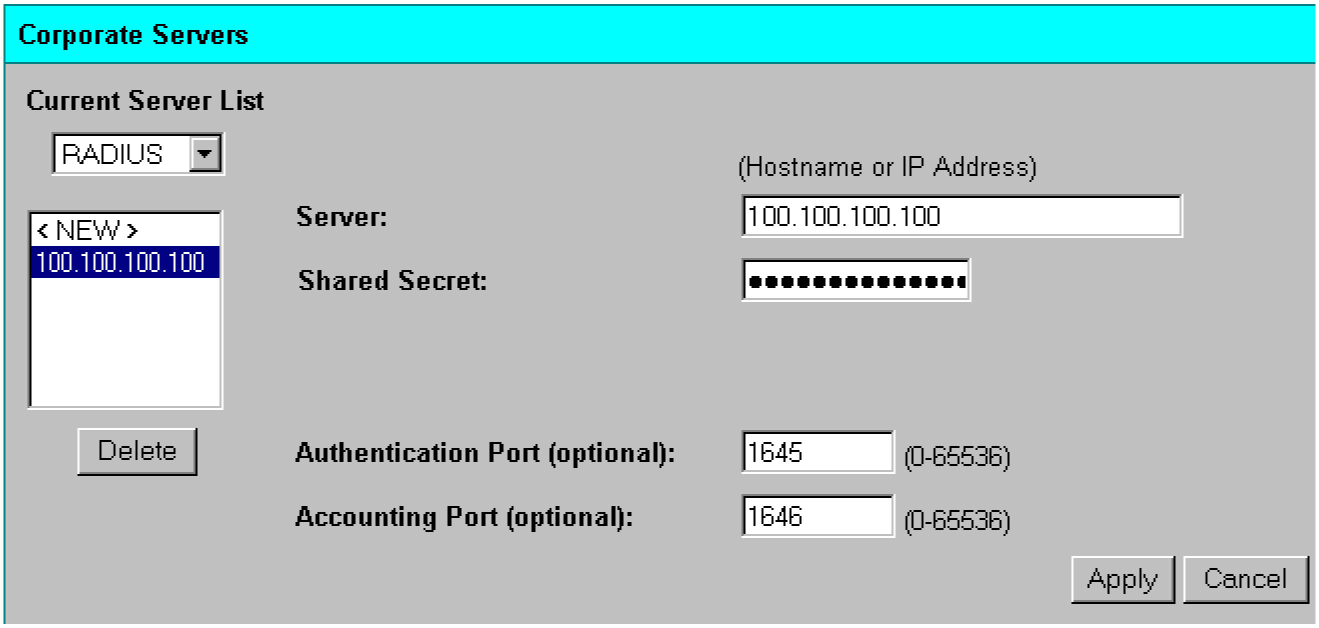
Click **Security**. Click **Server Manager** then scroll down.

This Server Manager configuration applies to all types of authentication except WPA-PSK. For WPA-PSK there is no server required, therefore this step is not applicable.

Scroll to the **Corporate Servers** area and with **<NEW>** highlighted in the Server list box enter the IP or hostname in the text box. Enter the shared secret used for that server and this AP.

Note: The shared secret is just a password used between the AP and the ACS server for that AP. Document the shared secret for each AP. The shared secret may be the same for each AP.

Scroll down and click the **Apply** button in the **Corporate Servers** area.



Corporate Servers

Current Server List

RADIUS

< NEW >
100.100.100.100

(Hostname or IP Address)

Server: 100.100.100.100

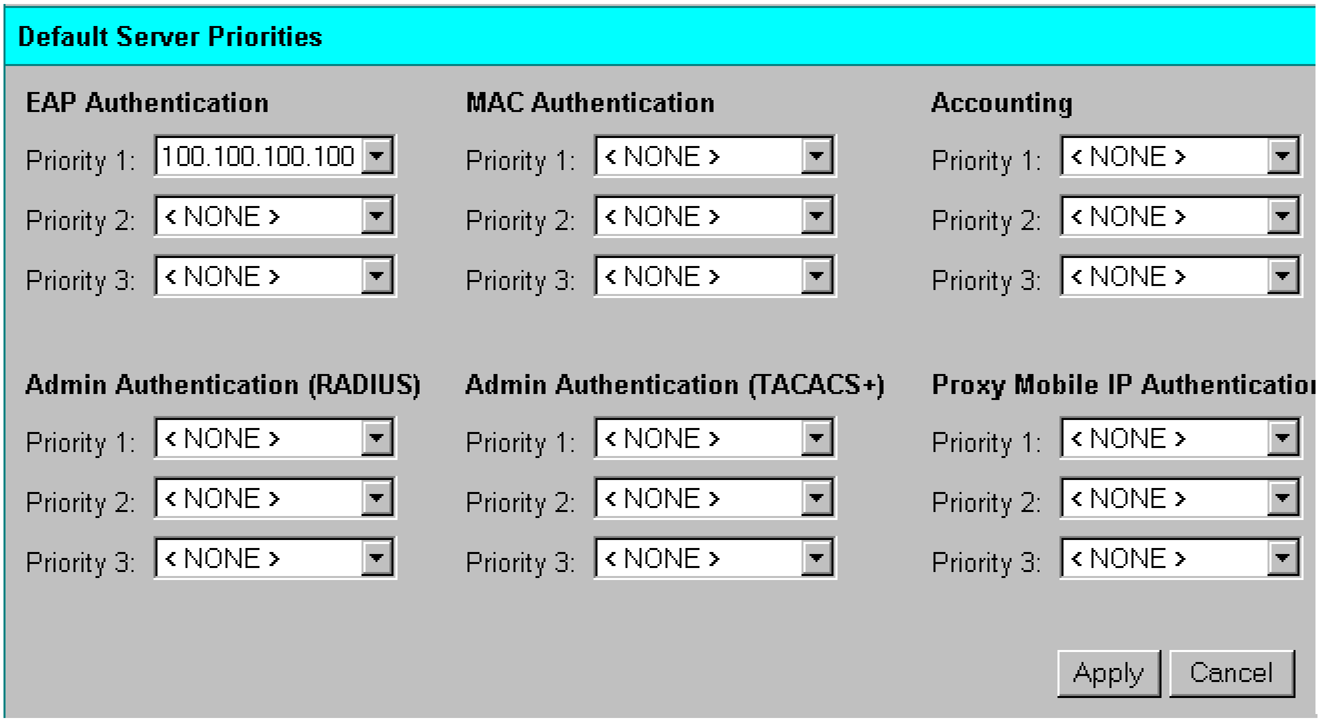
Shared Secret: ●●●●●●●●●●●●●●●

Authentication Port (optional): 1645 (0-65536)

Accounting Port (optional): 1646 (0-65536)

Navigate to the **Default Server Priorities** area and choose the server in the **EAP Authentication** scroll bar for **Priority 1**. If there are backup RADIUS servers you can put them in as well.

Scroll down and click the **Apply** button at the bottom of the screen.



Default Server Priorities

EAP Authentication

Priority 1: 100.100.100.100

Priority 2: < NONE >

Priority 3: < NONE >

MAC Authentication

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Accounting

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Admin Authentication (RADIUS)

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Admin Authentication (TACACS+)

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Proxy Mobile IP Authenticatio

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Encryption Manager

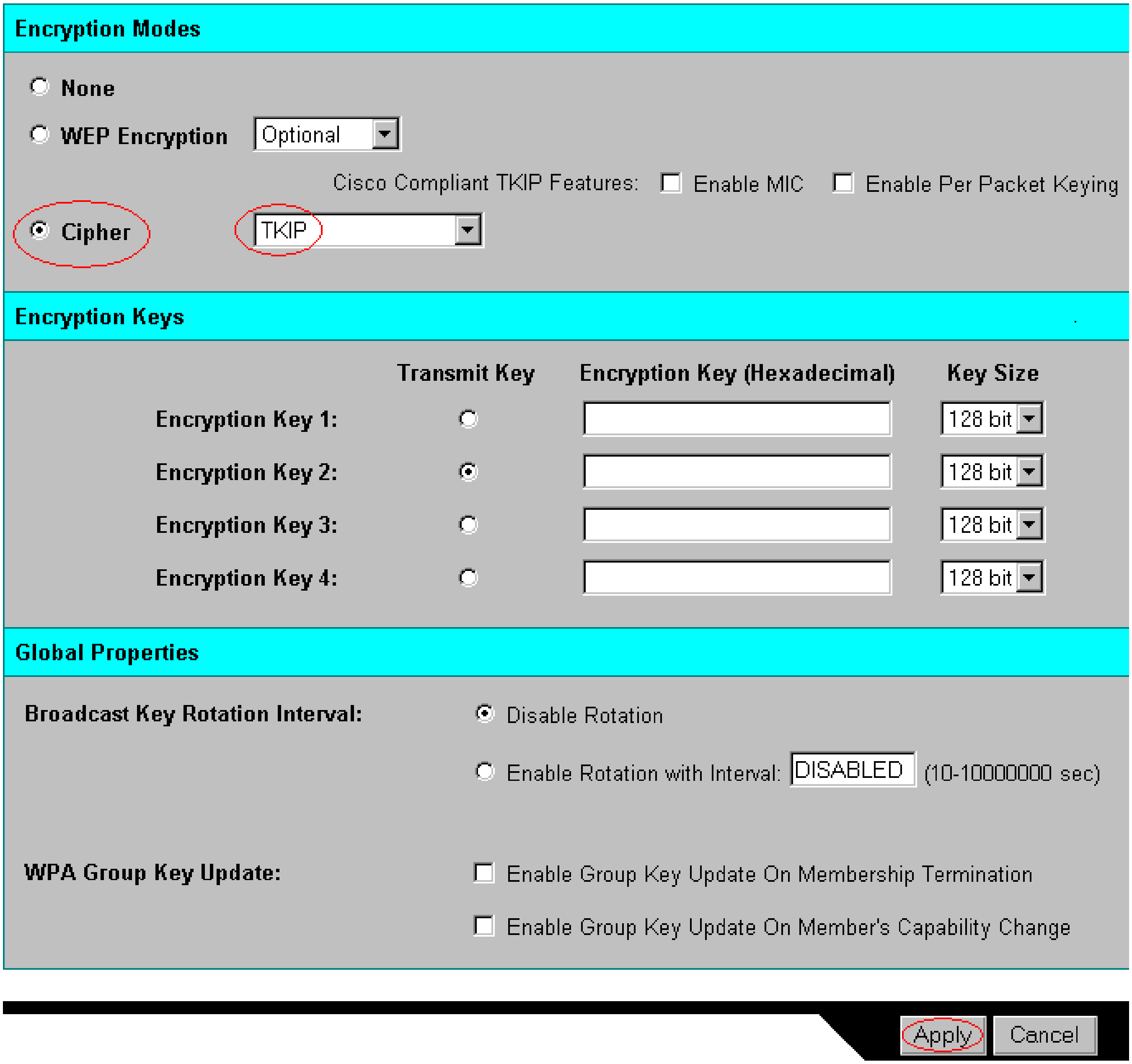
Click **Security**.

Using the navigation bar on the left, click on **Encryption Manager**.

This Encryption Manager configuration applies to all types of authentication with WPA and WPA-PSK. WPA requires the use of TKIP for both WPA and WPA-PSK.

In the Encryption Modes area click the radio button for **Cipher** and use the scroll bar to choose **TKIP**.

Scroll down and click the **Apply** button.



Encryption Modes

○ None

○ WEP Encryption Optional

Cisco Compliant TKIP Features: □ Enable MIC □ Enable Per Packet Keying

● Cipher TKIP

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	○		128 bit
Encryption Key 2:	●		128 bit
Encryption Key 3:	○		128 bit
Encryption Key 4:	○		128 bit

Global Properties

Broadcast Key Rotation Interval: ● Disable Rotation

○ Enable Rotation with Interval: DISABLED (10-10000000 sec)

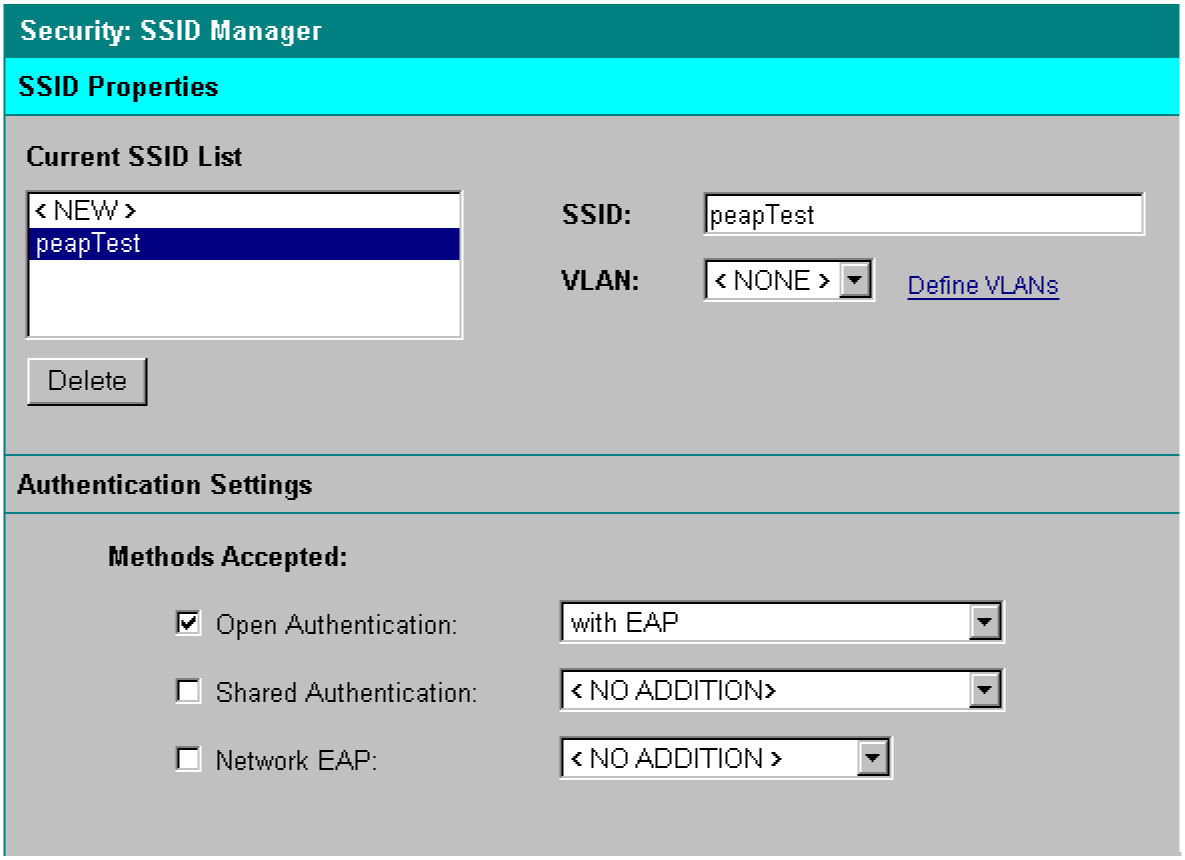
WPA Group Key Update: □ Enable Group Key Update On Membership Termination

□ Enable Group Key Update On Member's Capability Change

SSID Manager

Using the navigation bar on the left, click **SSID Manager**.

Create a SSID for the WPA system to use. Scroll down to **Authentication Settings** -> **Methods Accepted**.



Security: SSID Manager

SSID Properties

Current SSID List

< NEW >
peapTest

SSID: peapTest

VLAN: < NONE >

Authentication Settings

Methods Accepted:

☑ Open Authentication: with EAP

☐ Shared Authentication: < NO ADDITION>

☐ Network EAP: < NO ADDITION >

Note: AP configuration for PEAP/MS-CHAP, PEAP/GTC, EAP-TLS and EAP-FAST is the same. It does not matter which client supplicant is used. Configure the AP as shown in “PEAP, EAP-TLS”

LEAP

Check the box for **Open Authentication** and use the scroll bar to choose **with EAP**. Check the box for **Network EAP** and use the scroll bar to choose **No Addition**.

PEAP, EAP-TLS, EAP-FAST

Check the box for **Open Authentication** and use the scroll bar to choose **with EAP**.

WPA Configuration

Scroll down to **Authenticated Key Management**. Use the scroll bar to choose **Mandatory**. Check the box for **WPA**.

If configuring the system to authenticate to a RADIUS server do not put anything in the **WPA Pre-Shared Key** text box.

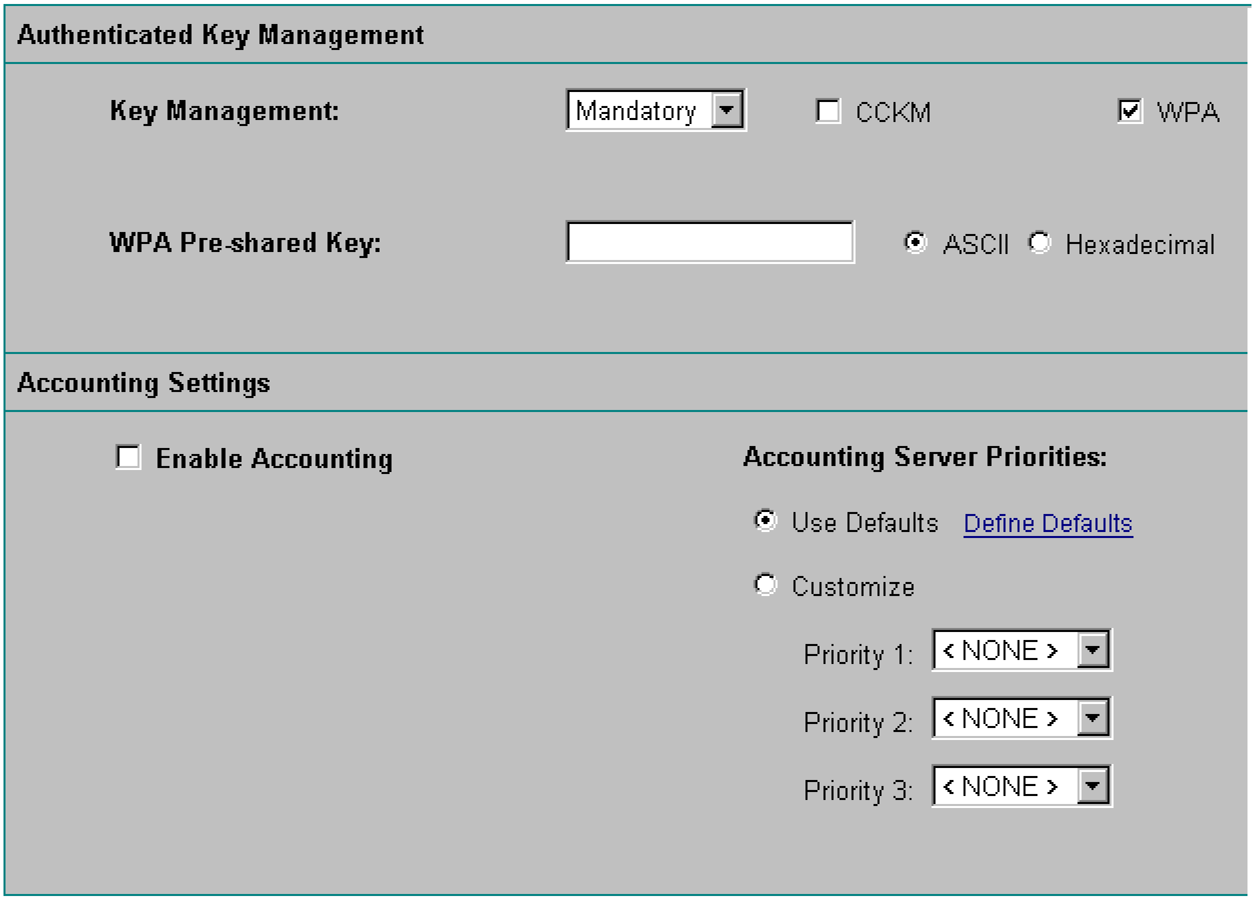
Scroll down and click the **Apply** button.

WPA-PSK Configuration

Click **Security**, click **SSID Manager** then scroll down.

If there is no RADIUS server and WPA-PSK is to be used, enter an ASCII key into the **WPA Pre-Shared Key** text box. Document what the key is so it can be entered into the client configuration. There is no authentication for WPA-PSK, so set method to **Open Authentication <NO ADDITION>**.

Scroll down and click the **Apply** button.



Authenticated Key Management

Key Management: Mandatory ▾ ☐ CCKM ☑ WPA

WPA Pre-shared Key: ● ASCII ○ Hexadecimal

Accounting Settings

☐ Enable Accounting

Accounting Server Priorities:

● Use Defaults Define Defaults

○ Customize

Priority 1: < NONE > ▾

Priority 2: < NONE > ▾

Priority 3: < NONE > ▾

The AP is now configured. By clicking the **Associations** link you can see which devices are EAP Authenticated. If a client is not authenticated the screen shows EAP pending.

AP Command Line Configuration

If using the command line to configure the AP1200 IOS instead of a browser, follow these commands.

Note: Check the Cisco documentation for these and other configuration settings.

Configure the access point normally then use these commands to turn on EAP and WPA.

Telnet into the AP on the LAN connection.

Parameter	Sub-parameter	Description	Example
hostname		Name of AP	AP1200WPA
aaa			new-model
aaa group server radius rad_eap	host	hostname or IP address of radius server	100.100.100.100
radius-server	host	Radius server IP address	100.100.100.100
	host key 0	Shared secret key with radius server	Secretkey
interface Dot11Radio0	encryption mode ciphers	Set encryption to ciphers and tkip	tkip
	authentication	Setting open with EAP	open eap eap_methods
	authentication	Setting WPA	key-management wpa

Example

Telnet into the AP, login (default is **Cisco** for username and password).

Type **en** for enable and **Cisco** for password. Enter **conf t**.

Paste the following data at this point to enter this configuration.

```
hostname AP1200WPA
aaa group server radius rad_eap
server 10.2.3.1 auth-port 1645 acct-port 1646
aaa group server radius rad_mac
aaa group server radius rad_acct
aaa group server radius rad_admin
aaa group server tacacs+ tac_admin
aaa group server radius rad_pmip
aaa group server radius dummy
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
bridge irb
interface Dot11Radio0
no ip address
no ip route-cache
ssid peapTest
authentication open eap eap_methods
authentication key-management wpa
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
interface BVI1
ip address 10.2.3.22 255.255.0.0
no ip route-cache
ip default-gateway 10.2.8.1
ip http server
ip http help-path http://www.cisco.com/war-
p/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip radius source-interface BVI1
radius-server host 10.2.3.1 auth-port 1645 acct-port 1646 key 7 13171117050B
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
end
```

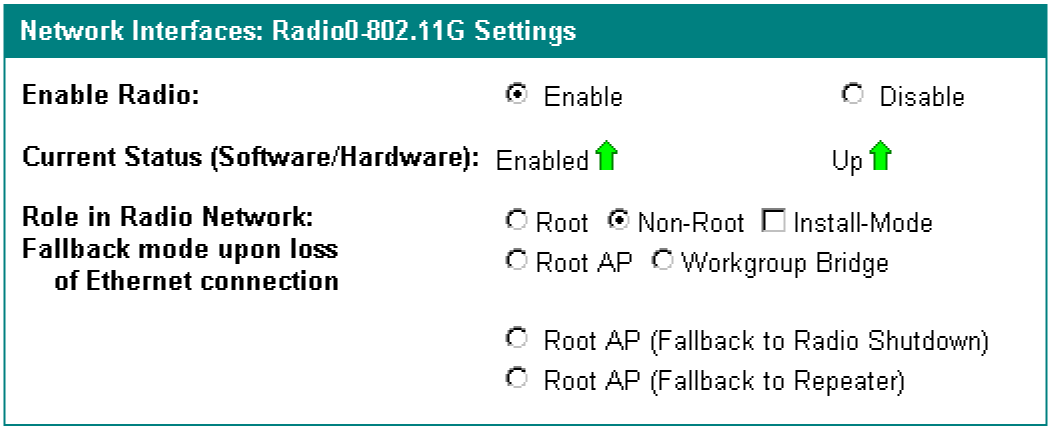
Cisco 1300 Wireless Bridge Configuration

The Cisco 1300 Wireless Bridge is WPA compliant both as an AP and as a wireless bridge. The wireless bridge was tested as a wireless bridge only, meaning there was a root and non-root bridge and an AP setup on the non-root bridge. No clients access was tested directly connecting to the wireless bridges. The root wireless bridge is configured as the 1200 AP shown above is configured. The non-root bridge is configured to authenticate to the root bridge just as a client is configured. The bridges were also tested as APs without bridging.

1300 Root Bridge

Configure the root wireless bridge as shown previously in the Web Browser Configuration section for the AP 1200. Configure the Server Manager, Encryption Manager and the SSID Manager for LEAP configuration.

Next navigate to the **Radio-802.11G** settings screen and set the **Role in Radio Network** setting.



Network Interfaces: Radio0-802.11G Settings

Enable Radio: ● Enable ○ Disable

Current Status (Software/Hardware): Enabled ↑ Up ↑

Role in Radio Network: ○ Root ● Non-Root □ Install-Mode

Fallback mode upon loss of Ethernet connection ○ Root AP ○ Workgroup Bridge

○ Root AP (Fallback to Radio Shutdown)

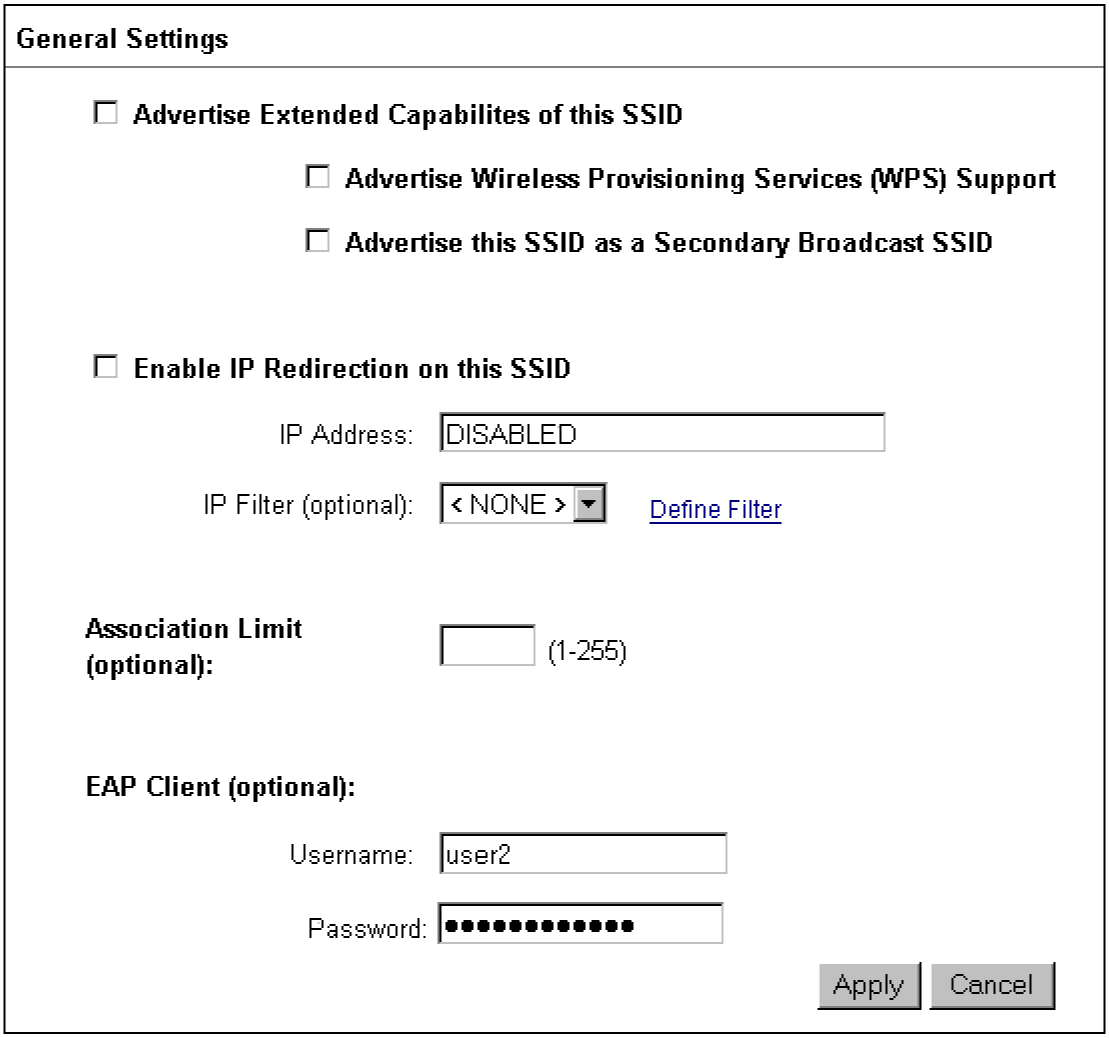
○ Root AP (Fallback to Repeater)

The root wireless bridge must be added to the RADIUS server just as an AP1200 is added.

The root wireless bridge is configured to authenticate any non-root wireless bridge via the RADIUS server.

1300 Non-Root Bridge

When configuring the non-root wireless bridge follow the exact same configuration as the root wireless bridge. Configure the Server Manager, Encryption Manager and the SSID Manager. The non-root will authenticate to the root using LEAP authentication.



General Settings

☐ Advertise Extended Capabilites of this SSID

☐ Advertise Wireless Provisioning Services (WPS) Support

☐ Advertise this SSID as a Secondary Broadcast SSID

☐ Enable IP Redirection on this SSID

IP Address: DISABLED

IP Filter (optional): < NONE > Define Filter

Association Limit (optional): (1-255)

EAP Client (optional):

Username: user2

Password: ●●●●●●●●●●●●●

To authenticate to the root wireless bridge the EAP client username and password must be entered as the authentication credentials. This is done on the SSID Manager configuration screen under **General Settings**.

The non-root wireless bridge appears on the root wireless bridge association table and the authentication state.

Now an access point can be connected to the non-root wireless bridge and all traffic will be secure.

1300 Bridges as APs

The 1300 Wireless Bridges may be configured as APs. The configuration is exactly as the 1200 AP configuration with the addition of configuring the 1300 as root AP on the 802.11G screen as shown in Root Bridge, earlier in this section.

Cisco 1242 Wireless Bridge Configuration

The Cisco 1242AG Wireless Bridge is WPA compliant both as an AP and as a wireless bridge. The root bridge was configured as an 802.11a bridge only. No clients access was tested directly connecting to the root wireless bridge. The non root wireless bridge was tested as an 802.11a wireless bridge and 802.11g AP. The root wireless bridge is configured as the 1200 AP shown in the previous section is configured. The non-root bridge is configured to authenticate to the root bridge just as a client is configured. The bridges were also tested as APs without bridging.

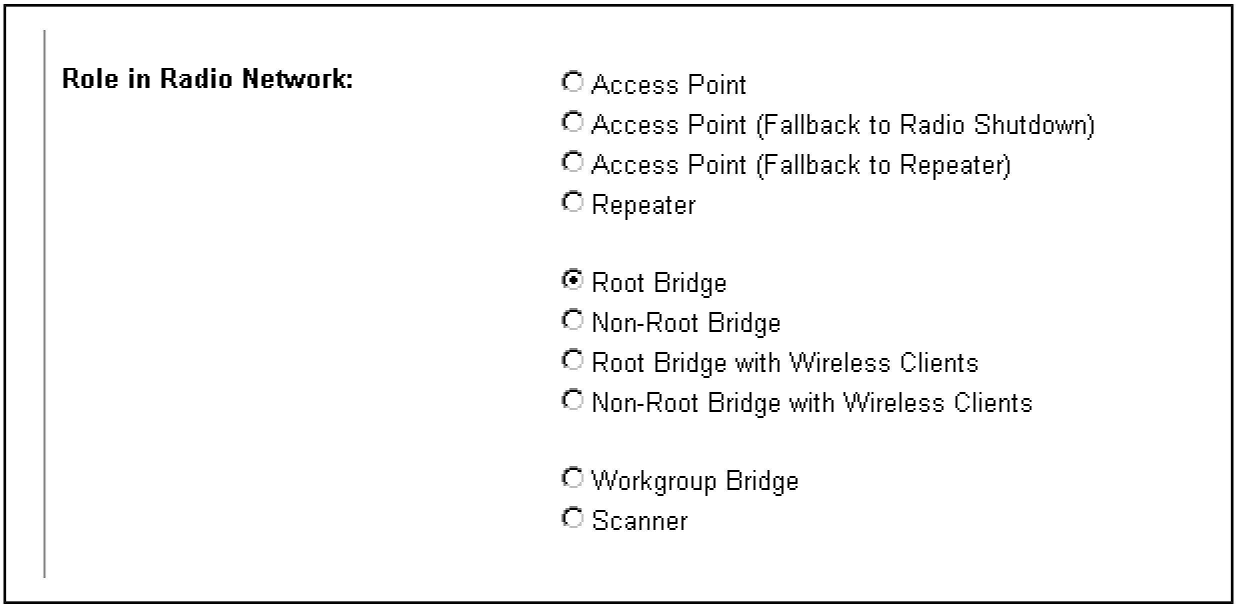
1242 Root Bridge

Configure the root wireless bridge as shown previously in the Web Browser Configuration section for the AP 1200. Configure the Server Manager, Encryption Manager and the SSID Manager for LEAP configuration.

Configure:

Server Manager	RADIUS Server
Encryption Manager	Cipher = TKIP
SSID Manager	Open authentication with EAP
	Network EAP
	Mandatory WPA

Next navigate to the **Radio-802.11G** settings screen and set the **Role in Radio Network** setting.



Role in Radio Network:

○ Access Point
○ Access Point (Fallback to Radio Shutdown)
○ Access Point (Fallback to Repeater)
○ Repeater

● Root Bridge
○ Non-Root Bridge
○ Root Bridge with Wireless Clients
○ Non-Root Bridge with Wireless Clients

○ Workgroup Bridge
○ Scanner

The root wireless bridge must be added to the RADIUS server just as an AP1200 is added.

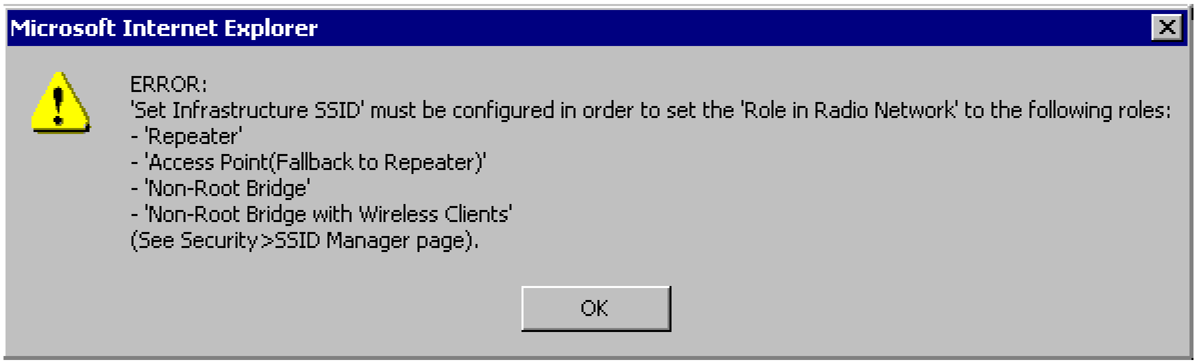
The root wireless bridge is configured to authenticate any non-root wireless bridge via the RADIUS server.

1242 Non-Root Bridge

When configuring the non-root wireless bridge follow the exact same configuration as the root wireless bridge as shown in the table in the previous section. Configure the Server Manager, Encryption Manager and the SSID Manager. Additional settings in the non root bridge include setting an Infrastructure SSID and AP authentication credentials.

The non root must have the infrastructure SSID set before configuring the 802.11a roll in network parameter.

If the SSID manager is not set first this error box will indicate this parameter must be set first.

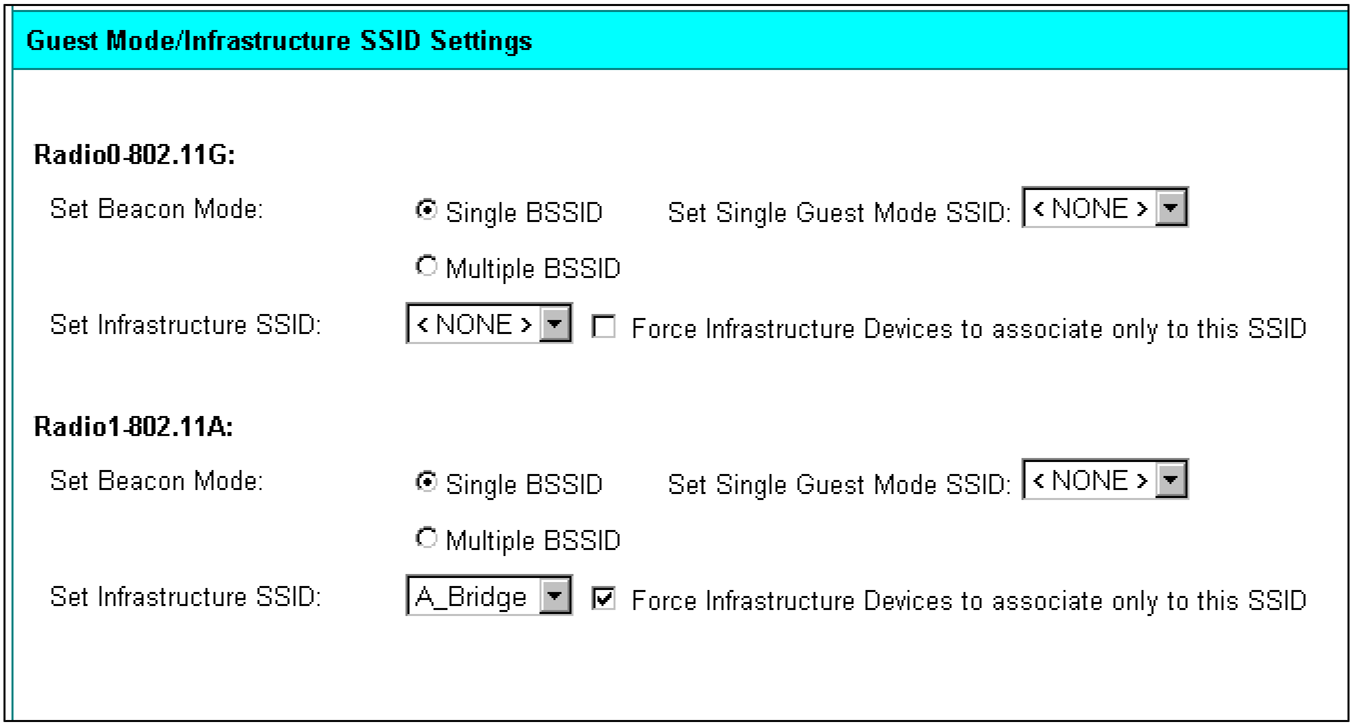


Microsoft Internet Explorer

ERROR:
'Set Infrastructure SSID' must be configured in order to set the 'Role in Radio Network' to the following roles:
- 'Repeater'
- 'Access Point(Fallback to Repeater)'
- 'Non-Root Bridge'
- 'Non-Root Bridge with Wireless Clients'
(See Security>SSID Manager page).

Set the correct SSID to connect to the root bridge and set the 'a' radio for this SSID.

Navigate to the bottom of the screen and set the **Infrastructure SSID** to the configured SSID setting as shown below.



Guest Mode/Infrastructure SSID Settings

Radio0-802.11G:

Set Beacon Mode: ● Single BSSID ○ Multiple BSSID

Set Single Guest Mode SSID: < NONE >

Set Infrastructure SSID: < NONE > □ Force Infrastructure Devices to associate only to this SSID

Radio1-802.11A:

Set Beacon Mode: ● Single BSSID ○ Multiple BSSID

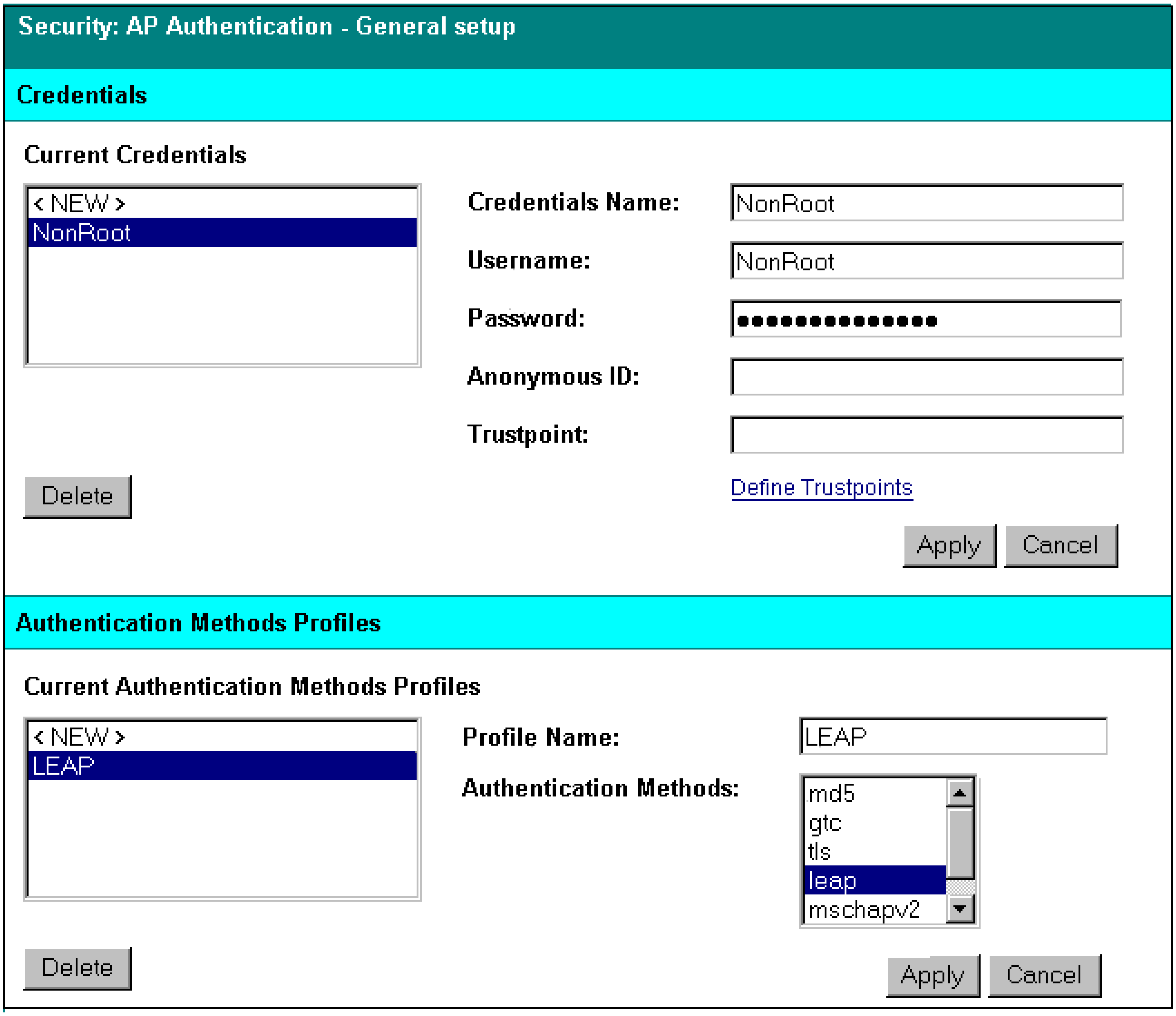
Set Single Guest Mode SSID: < NONE >

Set Infrastructure SSID: A_Bridge ☑ Force Infrastructure Devices to associate only to this SSID

Setting AP authentication credentials

- Enter valid client credentials from the RADIUS server to authenticate the non root bridge
- Enter the EAP method for authenticating to the root AP

After configuring the AP credentials navigate to the correct SSID in the SSID manager screen to use these credentials.



Security: AP Authentication - General setup

Credentials

Current Credentials

< NEW >
NonRoot

Credentials Name: NonRoot

Username: NonRoot

Password: ●●●●●●●●●●●●●●●

Anonymous ID:

Trustpoint:

Authentication Methods Profiles

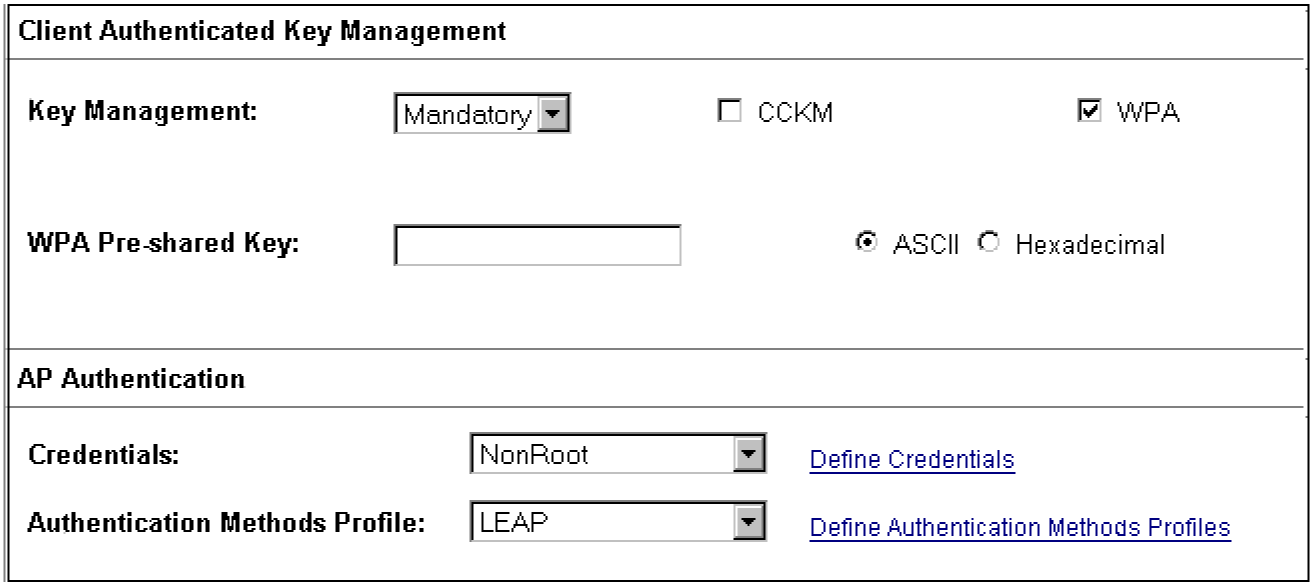
Current Authentication Methods Profiles

< NEW >
LEAP

Profile Name: LEAP

Authentication Methods: leap

After configuring the AP credentials navigate to the correct SSID in the SSID Manager screen to use these credentials.



Client Authenticated Key Management

Key Management: Mandatory ▾ ☐ CCKM ☑ WPA

WPA Pre-shared Key: ● ASCII ○ Hexadecimal

AP Authentication

Credentials: NonRoot ▾ Define Credentials

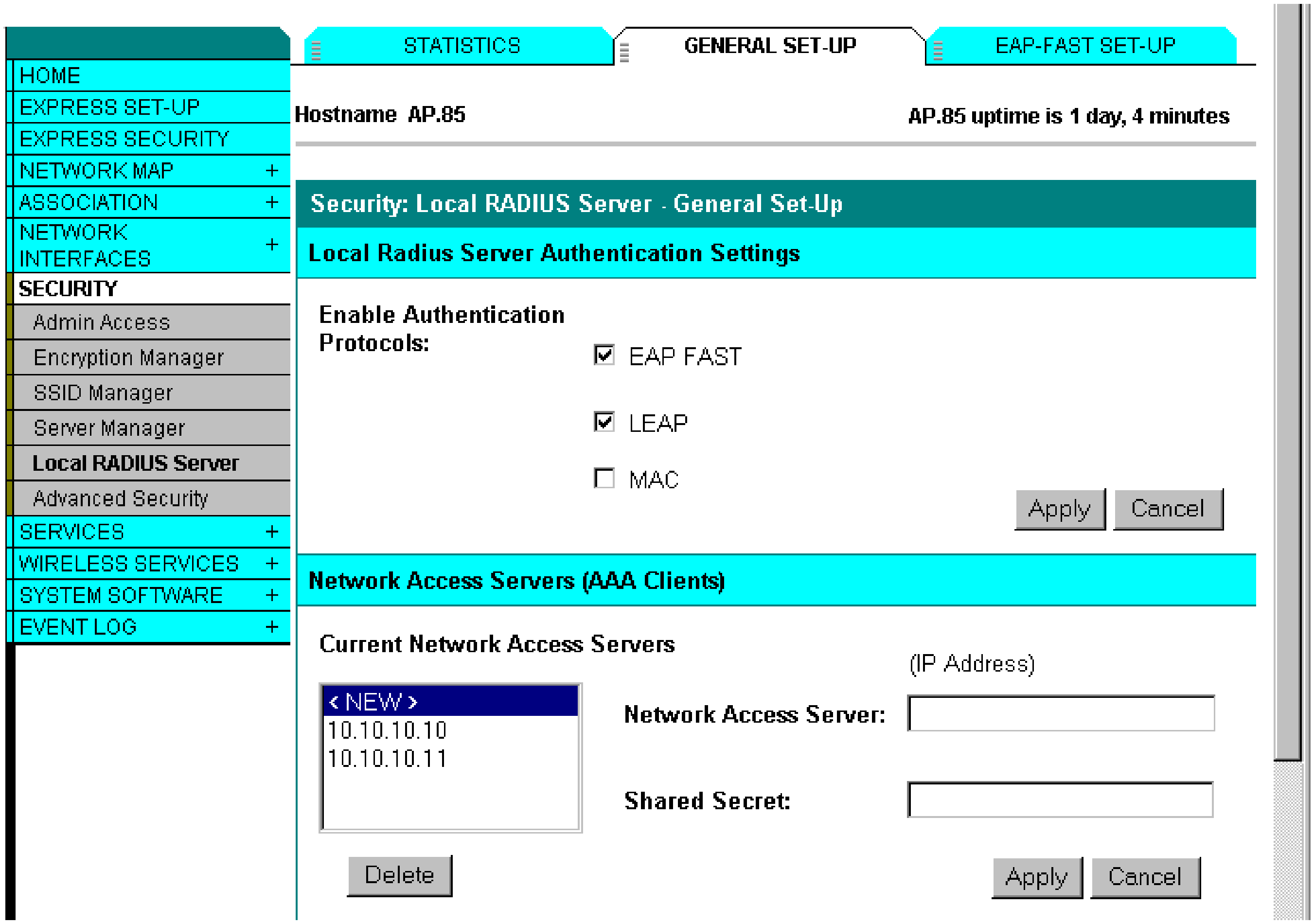
Authentication Methods Profile: LEAP ▾ Define Authentication Methods Profiles

1242 Bridges as APs

The 1242 Wireless Bridges may be configured as APs. The configuration is exactly as shown earlier for the 1200 AP configuration with the addition of configuring the 1242 as root AP on the 802.11G screen shown in Root Bridge earlier in this section.

AP Local RADIUS Server Configuration

To configure the AP as a local RADIUS server, click the **Security | Local RADIUS Server** navigation buttons.



Hostname AP.85

AP.85 uptime is 1 day, 4 minutes

Security: Local RADIUS Server - General Set-Up

Local Radius Server Authentication Settings

Enable Authentication Protocols:

☑ EAP FAST

☑ LEAP

□ MAC

Network Access Servers (AAA Clients)

Current Network Access Servers

< NEW >
10.10.10.10
10.10.10.11

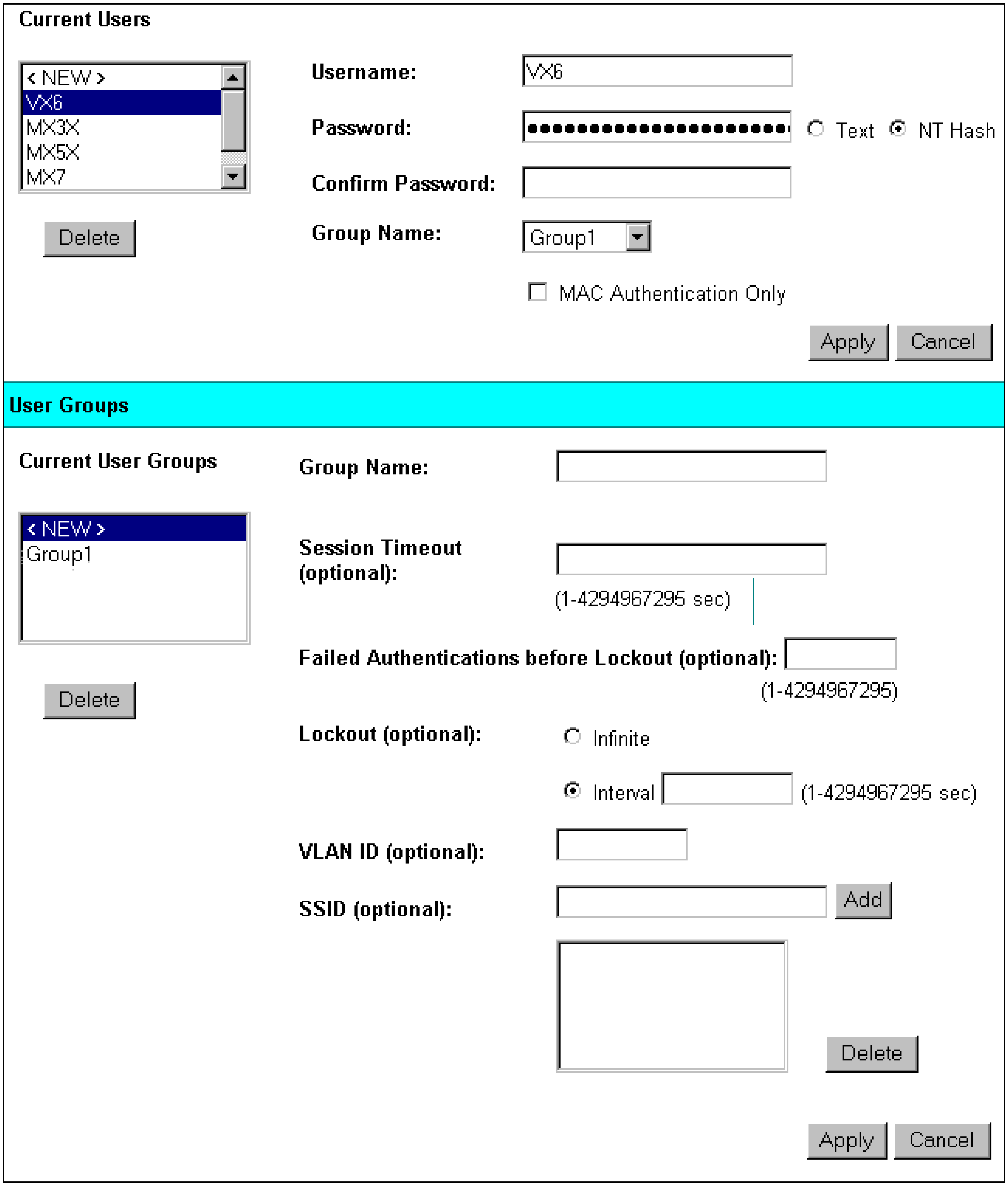
Network Access Server: (IP Address)

Shared Secret:

Click the **General Set-up** tab at the top of the page.

Enable the correct authentication type. Cisco APs only support the authentication settings shown.

Enter the APs that will use this RADIUS server under **AAA Clients**. Each AP must be entered with the shared secret, including the AP configured as the local RADIUS server if it is used to authenticate client radios.



Current Users

< NEW >
VX6
MX3X
MX5X
MX7

Delete

Username: VX6

Password: ●●●●●●●●●●●●●●●●●●●●●● ○ Text ● NT Hash

Confirm Password:

Group Name: Group1

□ MAC Authentication Only

Apply Cancel

User Groups

Current User Groups

< NEW >
Group1

Delete

Group Name:

Session Timeout (optional): (1-4294967295 sec)

Failed Authentications before Lockout (optional): (1-4294967295)

Lockout (optional): ○ Infinite

● Interval (1-4294967295 sec)

VLAN ID (optional):

SSID (optional): Add

Delete

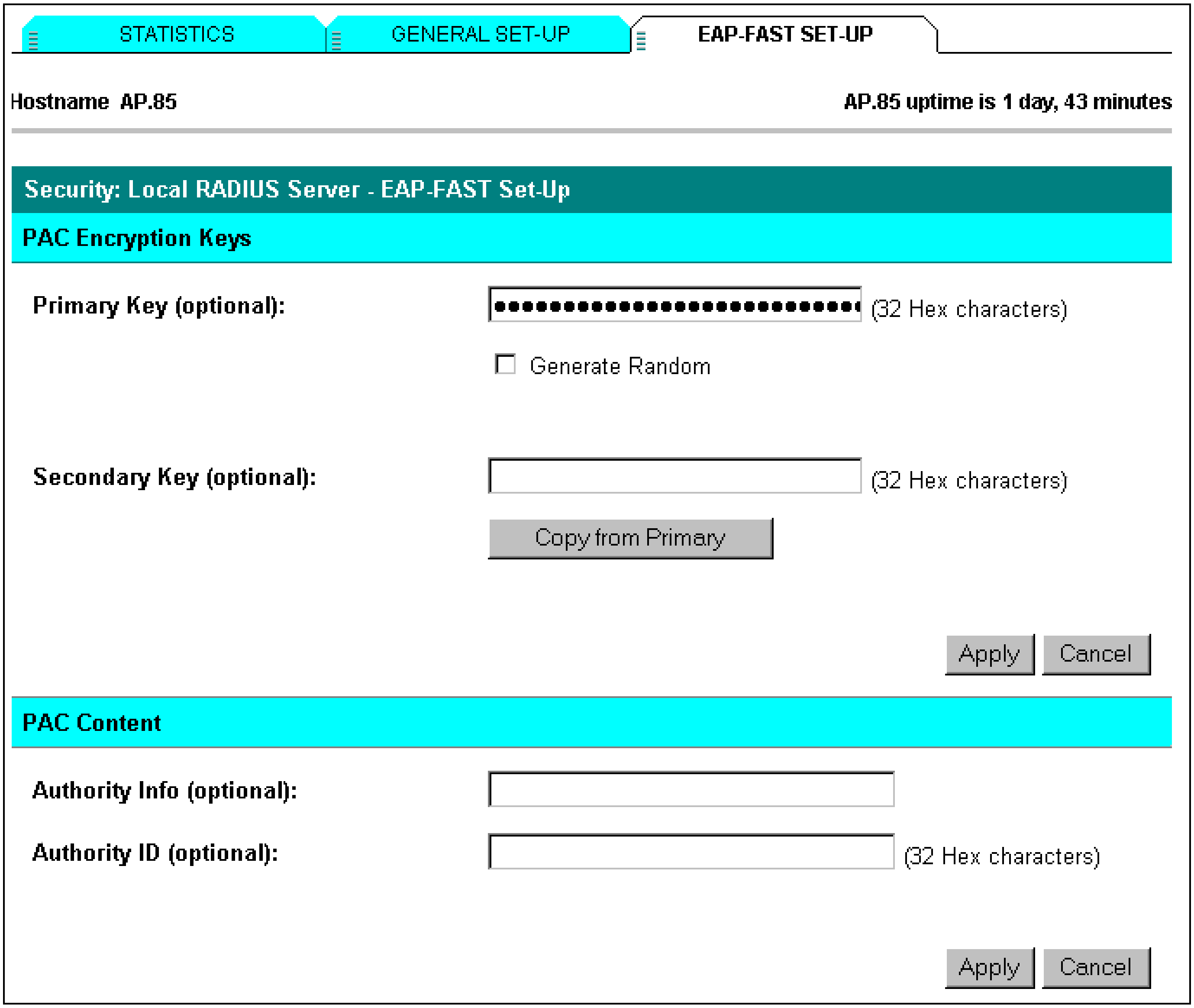
Apply Cancel

Add users for the RADIUS server by typing a **username** and **password** for each user.

If any group settings are required for session timeout or any of the other settings listed, add a group with your correct settings. After adding the group, make sure to change all the users to the correct group using the **Group Name** pull down listing in the **Current Users** box.

The AP local RADIUS server is now configured to authenticate LEAP clients. To continue configuration to authenticate EAP-FAST clients, click the **EAP-FAST Set-Up** tab at the top of the page.

Honeywell testing was completed with a Primary Key generated by clicking the **Generate Random** box and clicking **Apply**. This is optional per the AP setup screen shown.



Hostname AP.85

AP.85 uptime is 1 day, 43 minutes

Security: Local RADIUS Server - EAP-FAST Set-Up

PAC Encryption Keys

Primary Key (optional): ●●●●●●●●●●●●●●●●●●●●●●●●●●●● (32 Hex characters)

□ Generate Random

Secondary Key (optional): (32 Hex characters)

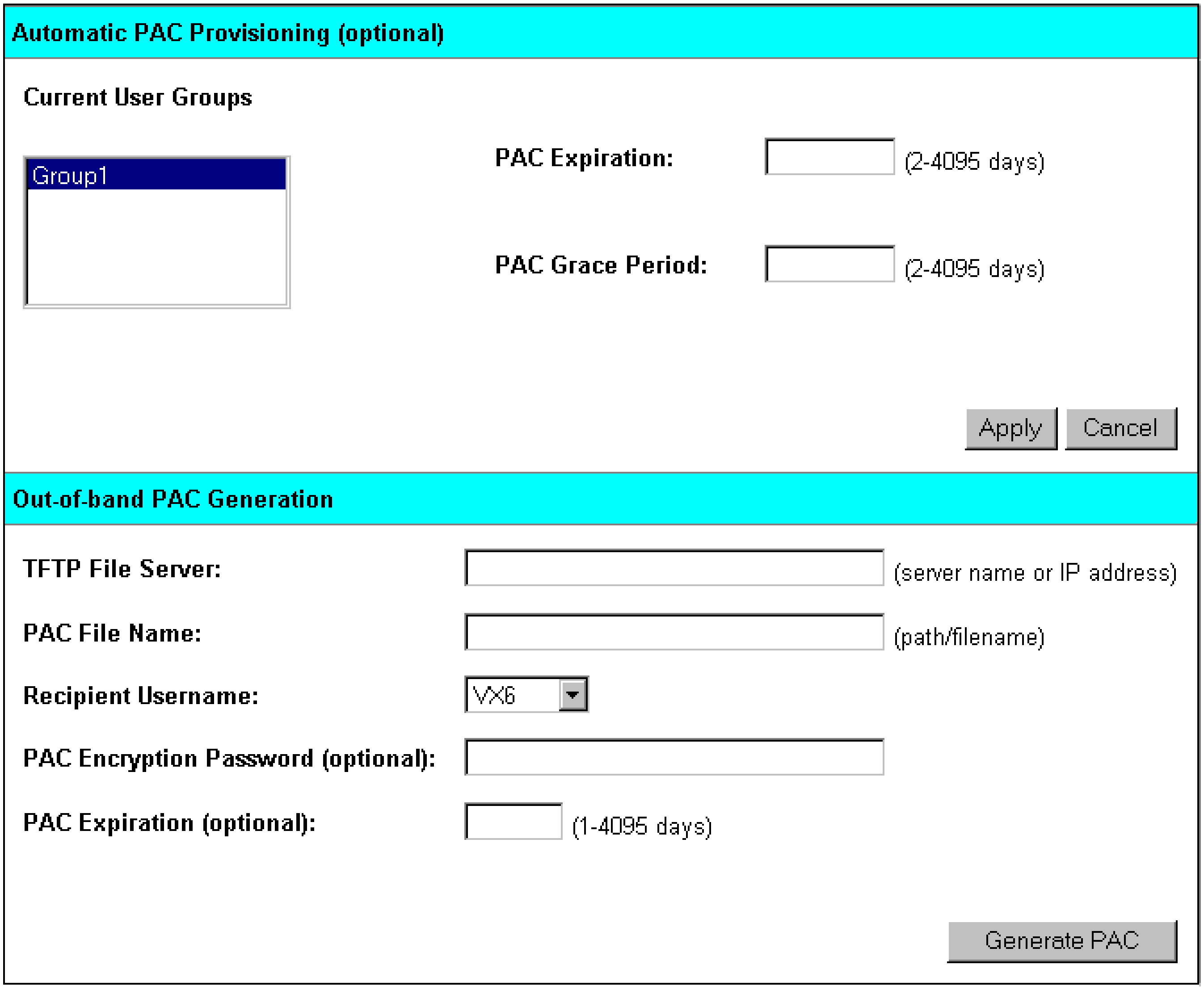
PAC Content

Authority Info (optional):

Authority ID (optional): (32 Hex characters)

No other options were changed.

Honeywell testing was done using automatic PAC Provisioning.



Automatic PAC Provisioning (optional)

Current User Groups

Group1

PAC Expiration: (2-4095 days)

PAC Grace Period: (2-4095 days)

Out-of-band PAC Generation

TFTP File Server: (server name or IP address)

PAC File Name: (path/filename)

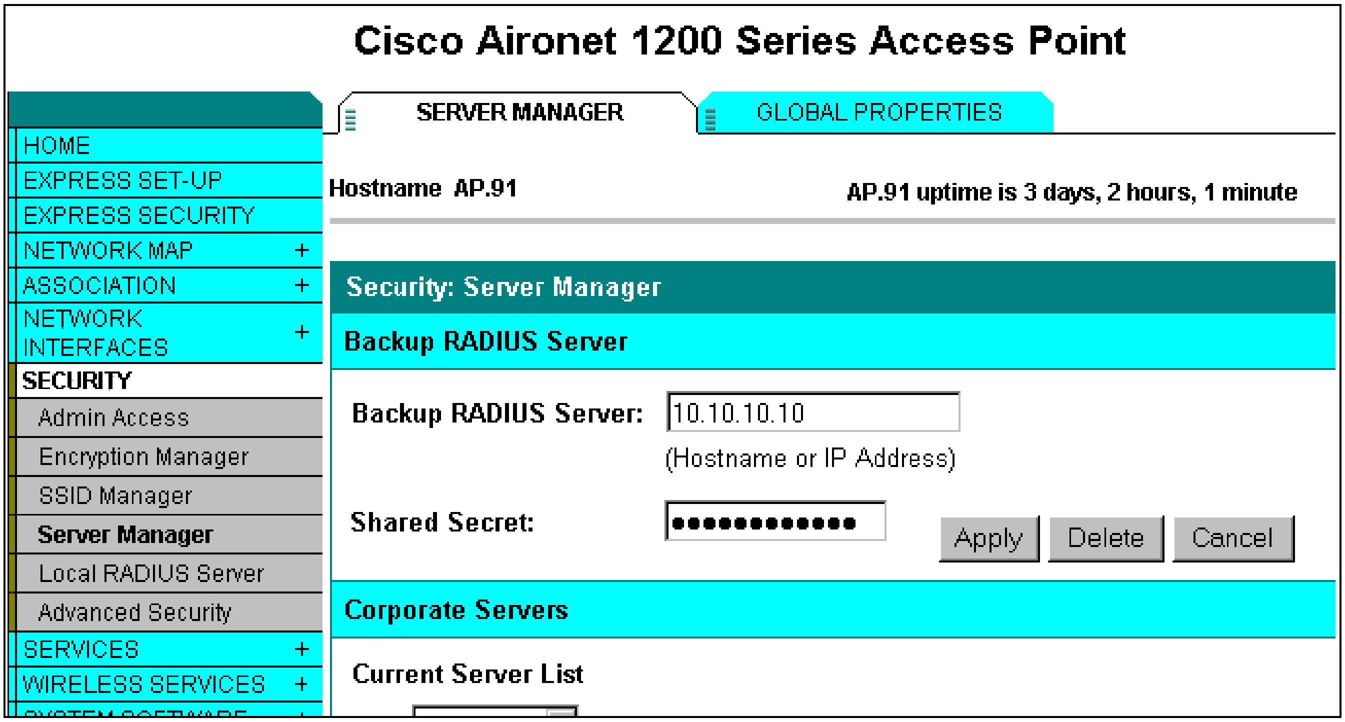
Recipient Username: VX6

PAC Encryption Password (optional):

PAC Expiration (optional): (1-4095 days)

No other options are required.

Navigate to the **Server Manager** of each AP on the network and enter the AP information configured for the local RADIUS server.



Cisco Aironet 1200 Series Access Point

Hostname AP.91

AP.91 uptime is 3 days, 2 hours, 1 minute

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: 10.10.10.10

(Hostname or IP Address)

Shared Secret: ●●●●●●●●●●●●●

Corporate Servers

Current Server List

This is configured in the **Backup RADIUS Server** box of each AP on the network as shown.

Enter the IP address and the shared secret configured above.

Do not configure Corporate Servers if using a local RADIUS server in an AP. Configuring a Corporate Server causes a delay in authentication as the Corporate Server must timeout before going to the Backup RADIUS Server.

Chapter 3: Cisco ACS RADIUS Server Configuration

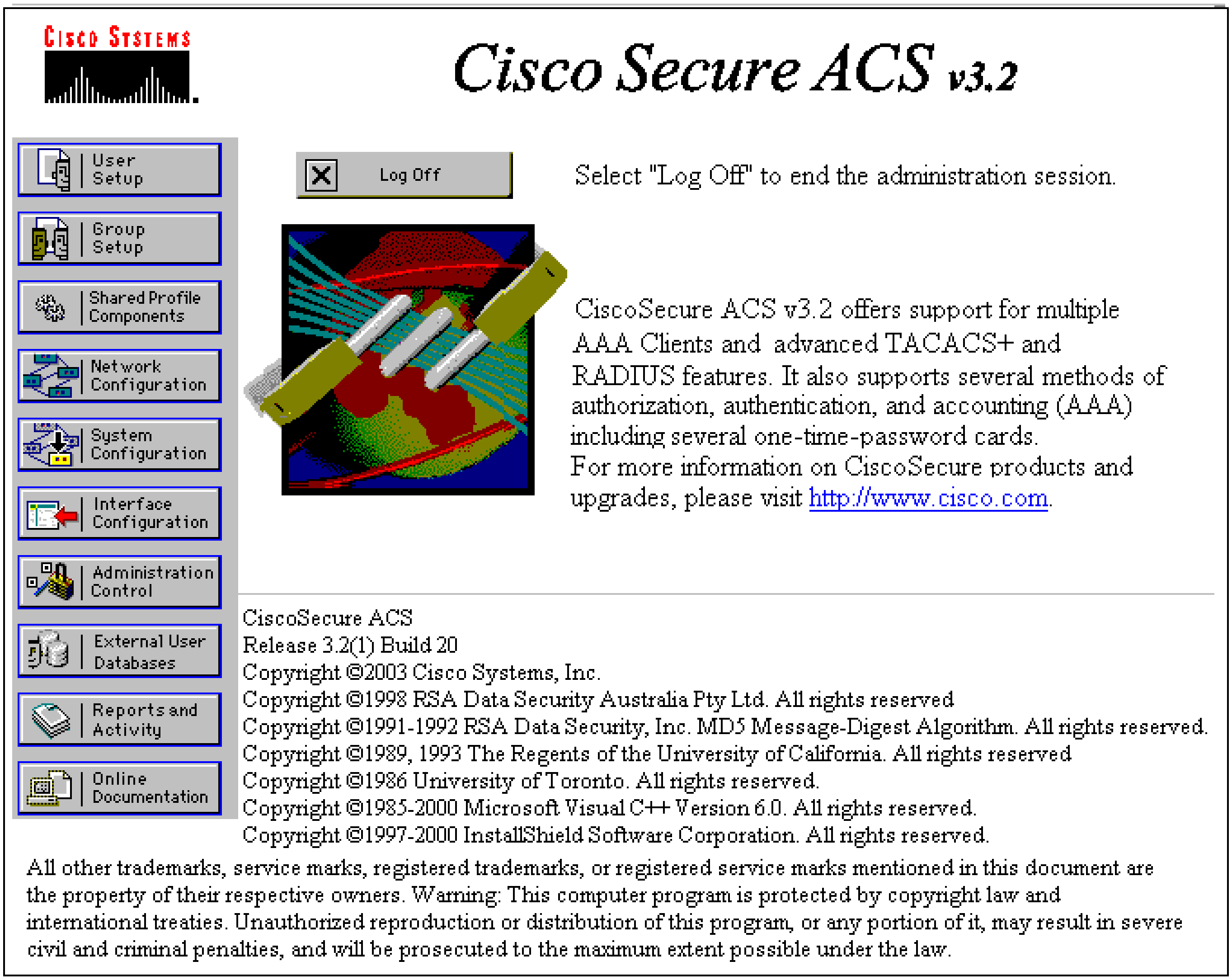
A user logging onto a network with the PEAP/MSCHAP, PEAP/GTC and EAP-TLS protocols is authenticated by a RADIUS server. Cisco ACS version tested was 3.2. After installation, navigate to the ACS by opening a browser to

http://<serverIP>:2002.

Follow the configuration steps in this order.

ACS Install

Install the Cisco ACS following the installation instructions on the CD. Start the ACS and log in.



Select "Log Off" to end the administration session.

CiscoSecure ACS v3.2 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.

CiscoSecure ACS
Release 3.2(1) Build 20
Copyright ©2003 Cisco Systems, Inc.
Copyright ©1998 RSA Data Security Australia Pty Ltd. All rights reserved
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.

All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

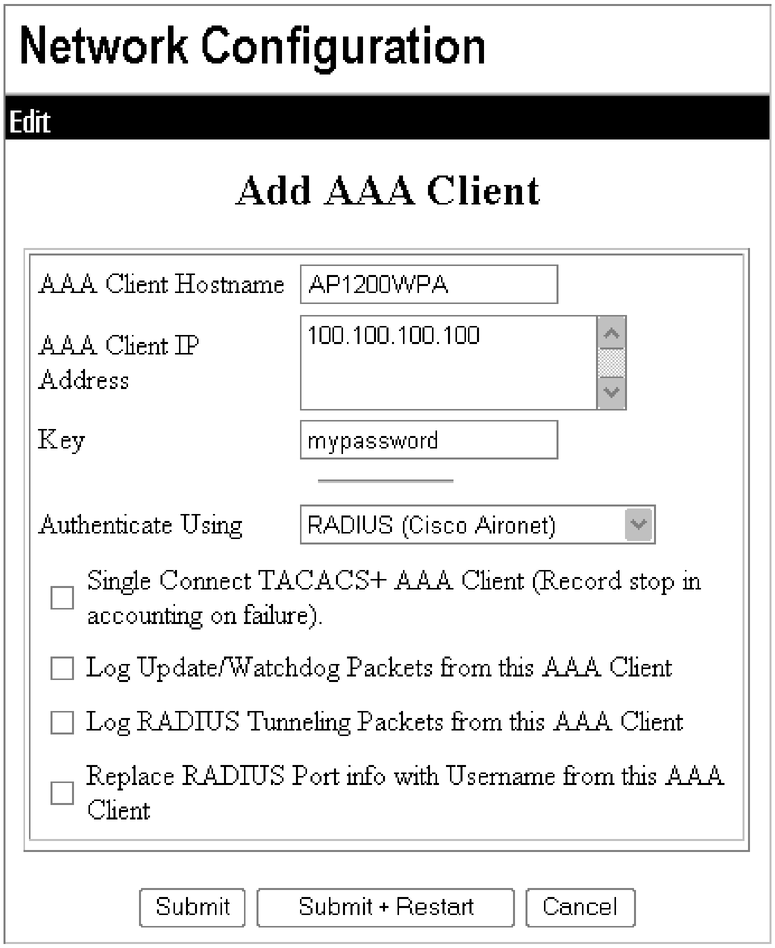
For more information on Cisco Secure ACS, please refer to Cisco's on line documentation and product information available on Cisco's web site.

Screens shown throughout the remainder of this section are accessed from the navigation buttons shown above, displayed on the left hand side of the screen.

Network Configuration

Click the **Network Configuration** button.

The Cisco ACS calls the AP to be used an AAA Client. Configure the AAA client with the same parameters as the AP1200. AAA Client Hostname is required to be the same as in the AP. The key is the same as entered in the AP Server configuration, called the shared secret.



Network Configuration

Edit

Add AAA Client

AAA Client Hostname	AP1200WPA
AAA Client IP Address	100.100.100.100
Key	mypassword
Authenticate Using	RADIUS (Cisco Aironet)

□ 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

- hostname,
- client IP,
- key and the
- Authenticate Using, by selecting **RADIUS (Cisco Aironet)** from the drop down box,

Click the **Submit + Restart** button.

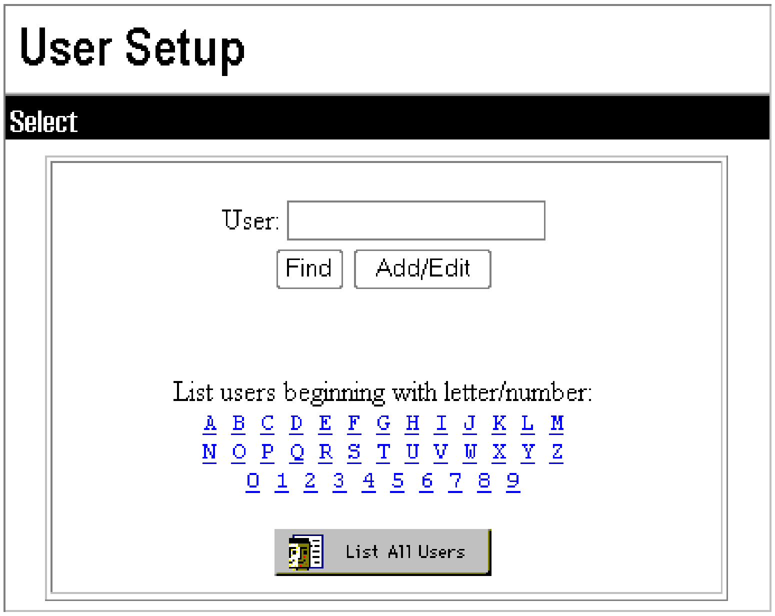
Note: AAA Clients are entered for each AP on the network.

User Setup

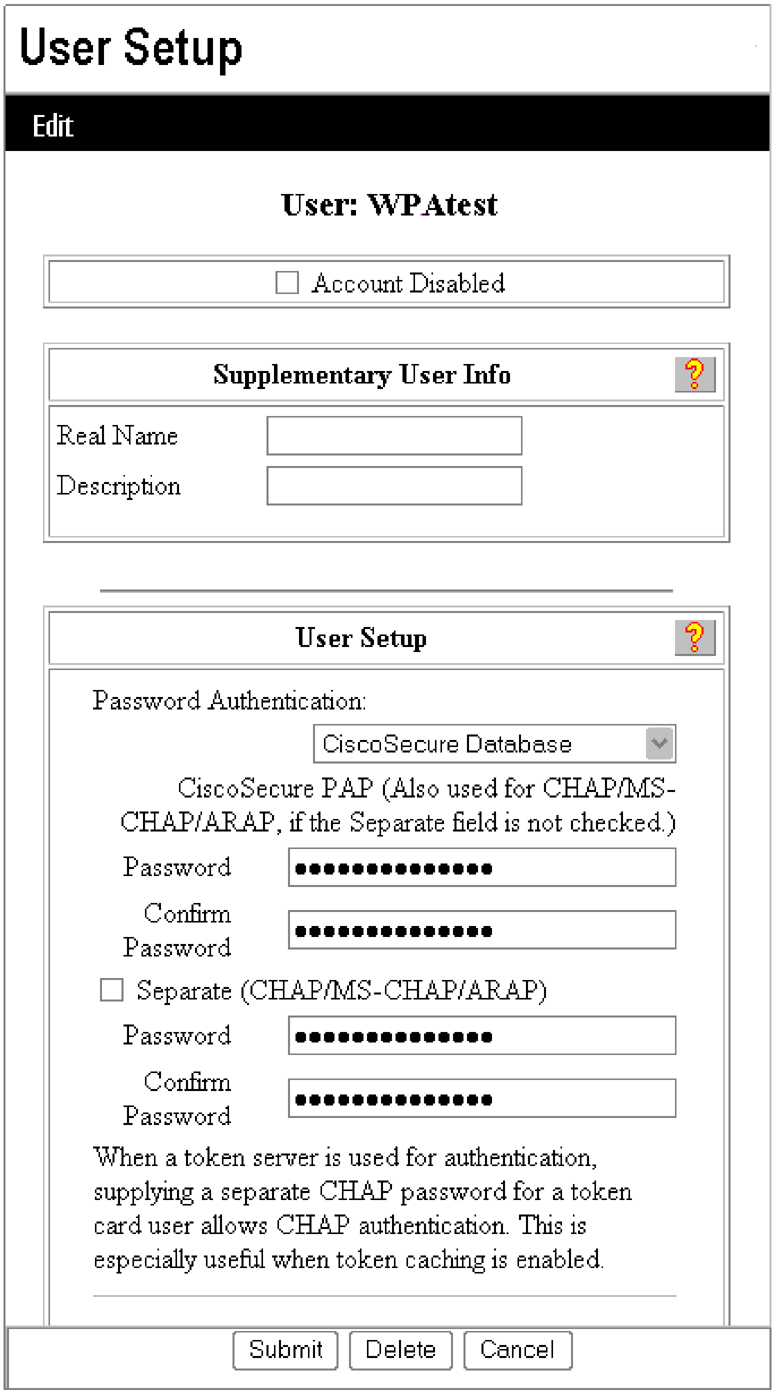
To authenticate users credentials with the Cisco ACS RADIUS server, that user must be setup in a user database. The Cisco ACS will check a user database in the ACS, or it will check any one of several possible external user databases.

CiscoSecure Database Authentication

Each user must be entered into the user database if no external user database is to be used. Sign on to the Cisco ACS web page and click the **User Setup** button.


User Setup
Select
User:
Find
Add/Edit
List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
List All Users

Enter the new username and click the **Add/Edit** button.



User Setup

Edit

User: WPAtest

☐ Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password ●●●●●●●●●●●●●●●

Confirm Password ●●●●●●●●●●●●●●●

☐ Separate (CHAP/MS-CHAP/ARAP)

Password ●●●●●●●●●●●●●●●

Confirm Password ●●●●●●●●●●●●●●●

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Make sure in the **User Setup** area that the **Password Authentication** box is set to **CiscoSecure Database**.

In the password boxes enter the password to be used for this username.

Scroll down and set the **Group** box to the group for this user if applicable.

Click the **Submit** button.

Repeat this process for each user to be added to the CiscoSecure User Database.

See the Cisco ACS online help for other user parameters that are available.

External User Database Setup

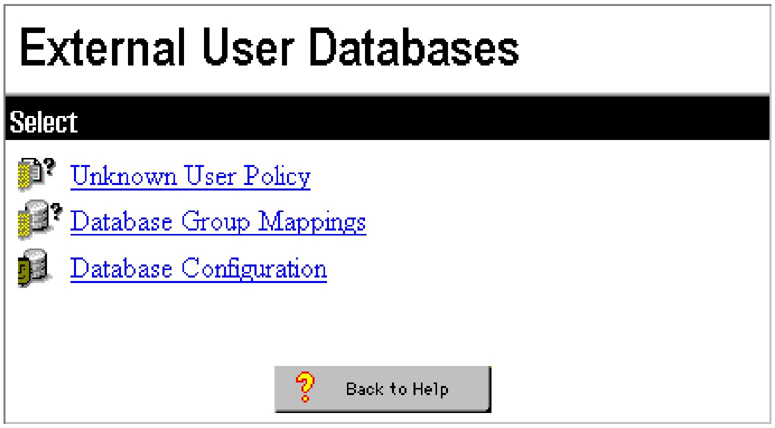
Click the **External User Databases** button.

It is possible to use other databases to get user credentials. Two that are explained here are the Windows Database for PEAP/MS-CHAP authentication and RSA ACE Server database for PEAP/GTC authentication. By checking these databases an administrator only has to configure a user at one place. For PEAP/GTC a token server must be used to authenticate the user token, this is not built into the Cisco ACS.

For Microsoft Windows database use the help screen of the server to find the procedure to add users to the active directory database. For RSA ACE server use the administrators guide that came with the RSA ACE server documentation.

To include these other databases to authenticate users follow the steps below:

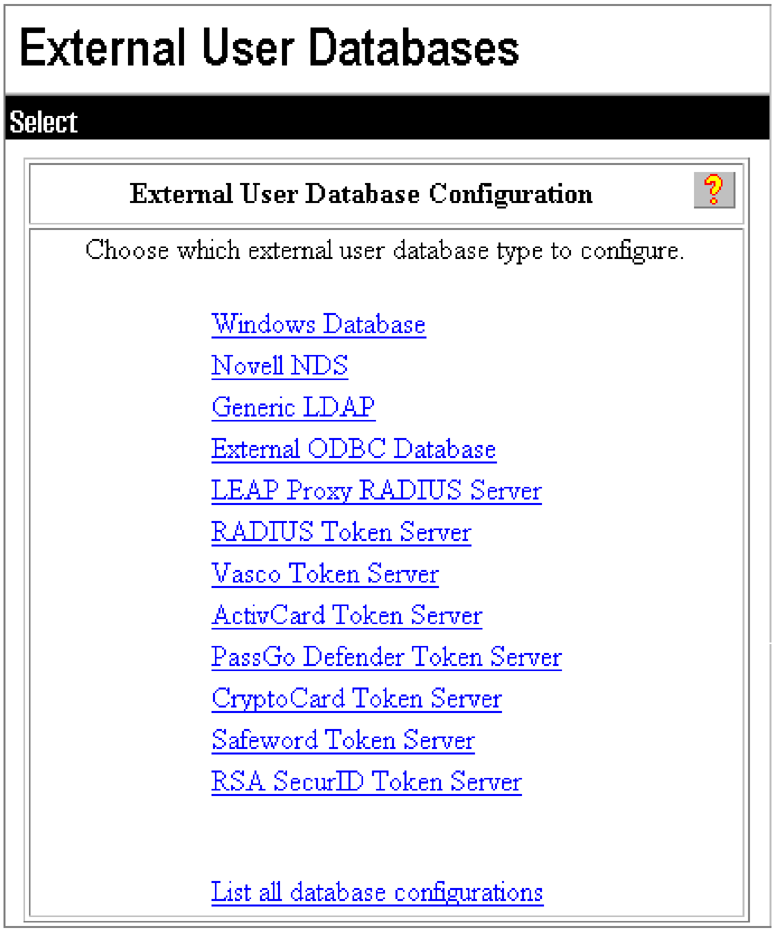
Click the **External Database** button.



External User Databases

Click **Database Configuration.**

Click on the databases that are to be added.



External User Databases

Select

External User Database Configuration

Choose which external user database type to configure.

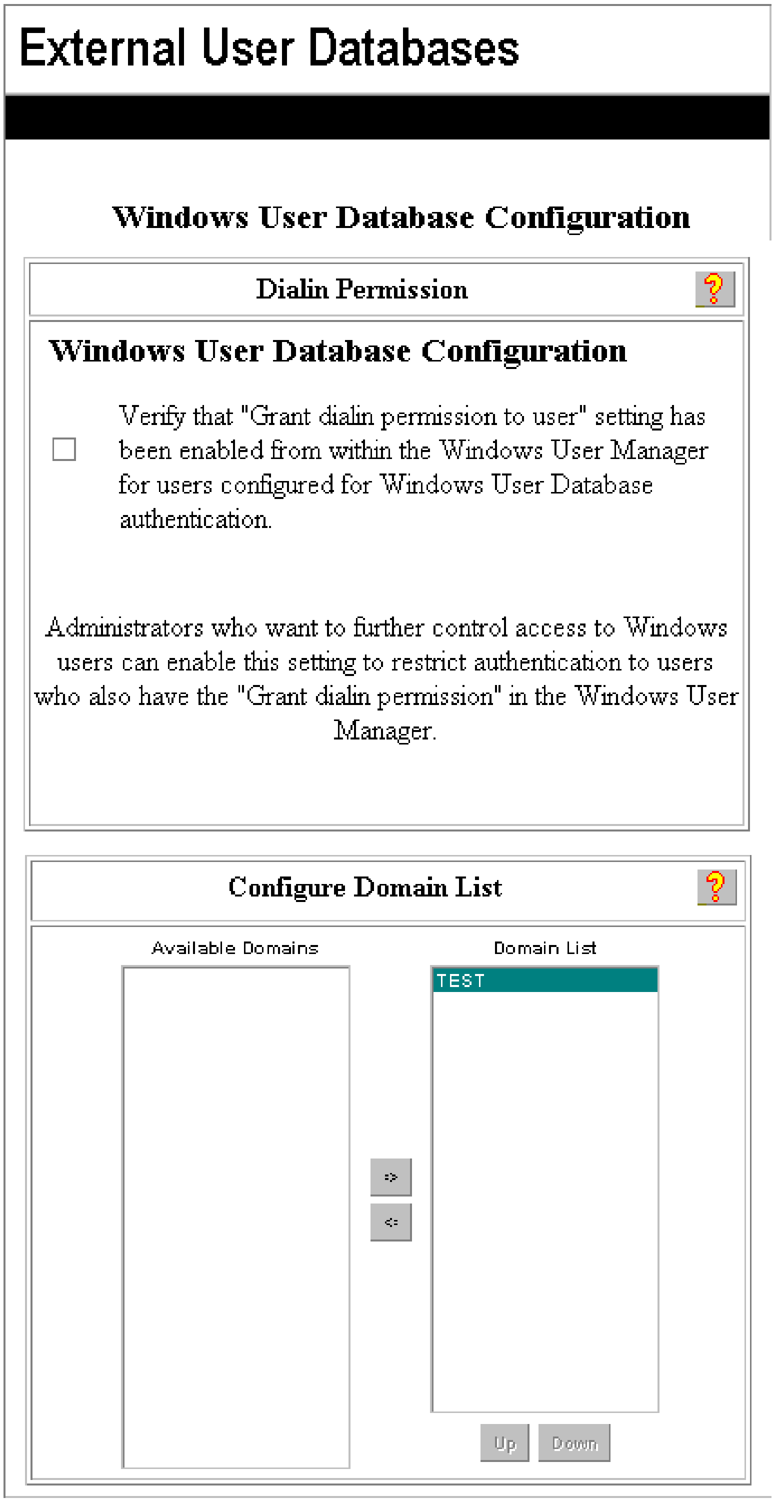
- Windows Database
- Novell NDS
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- RADIUS Token Server
- Vasco Token Server
- ActivCard Token Server
- PassGo Defender Token Server
- CryptoCard Token Server
- Safeword Token Server
- RSA SecurID Token Server

List all database configurations

Windows Database

Click **Windows Database**.

For testing purposes do not check the **Verify that “Grant dialin permission to user"...** button.



External User Databases

Windows User Database Configuration

Dialin Permission

Windows User Database Configuration

□ Verify that "Grant dialin permission to user" setting has been enabled from within the Windows User Manager for users configured for Windows User Database authentication.

Administrators who want to further control access to Windows users can enable this setting to restrict authentication to users who also have the "Grant dialin permission" in the Windows User Manager.

Configure Domain List

The available Windows domains found by the Cisco ACS will be listed on the left pane. Use the arrow button to move the correct domain to the box on the right (see Figure Below).

No other buttons need to be checked.

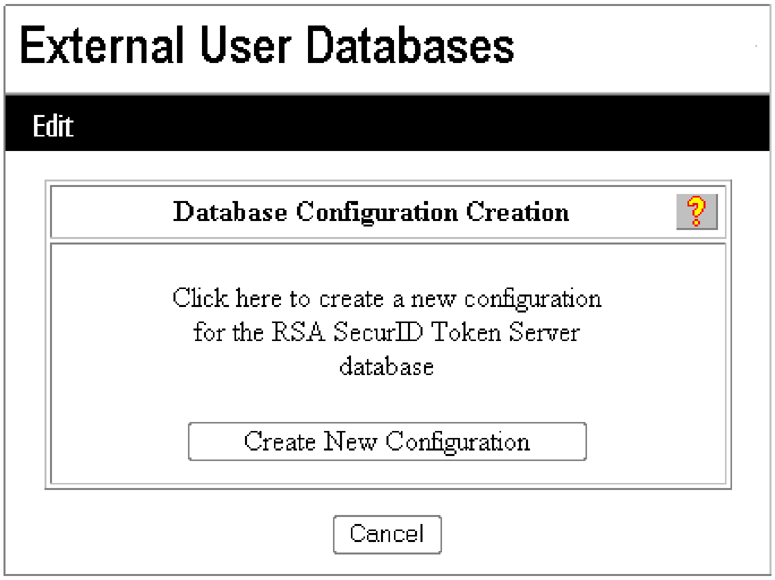
Click the **Submit** button at the bottom of the screen.

RSA ACE Server

The RSA ACE server must be installed before configuring the Cisco ACS to use the RSA ACE server. See RSA ACE Server Installation, later in this document.

Navigate back to the Cisco ACS External User Databases screen and click the **RSA SecurID Token Server** link. (see Figure: External User Database Configuration, below)

If no RSA database has been installed then click the **Create New Configuration** button.



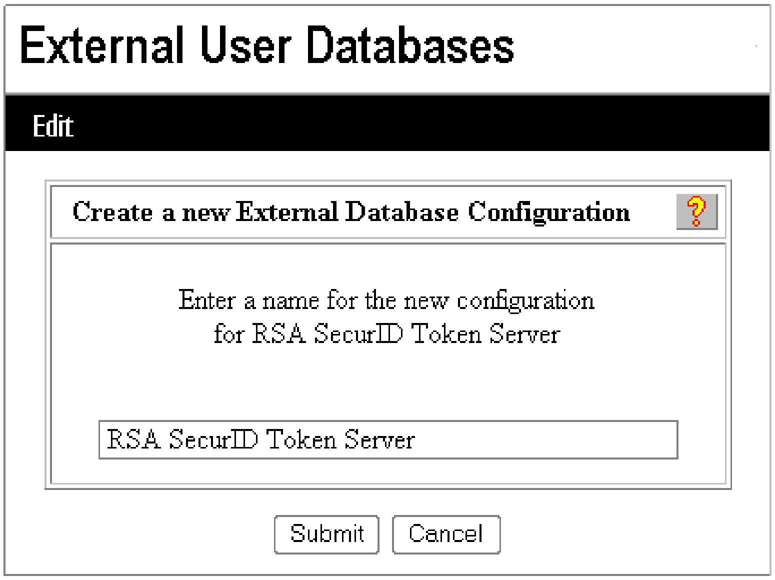
External User Databases

Edit

Database Configuration Creation

Click here to create a new configuration for the RSA SecurID Token Server database

The screen below is shown. Click the **Submit** button.



External User Databases

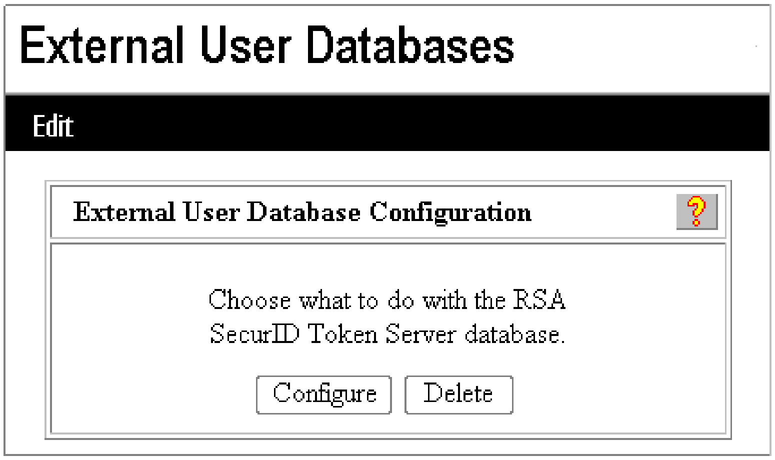
Edit

Create a new External Database Configuration

Enter a name for the new configuration for RSA SecurID Token Server

RSA SecurID Token Server

The following screen is shown.



External User Databases

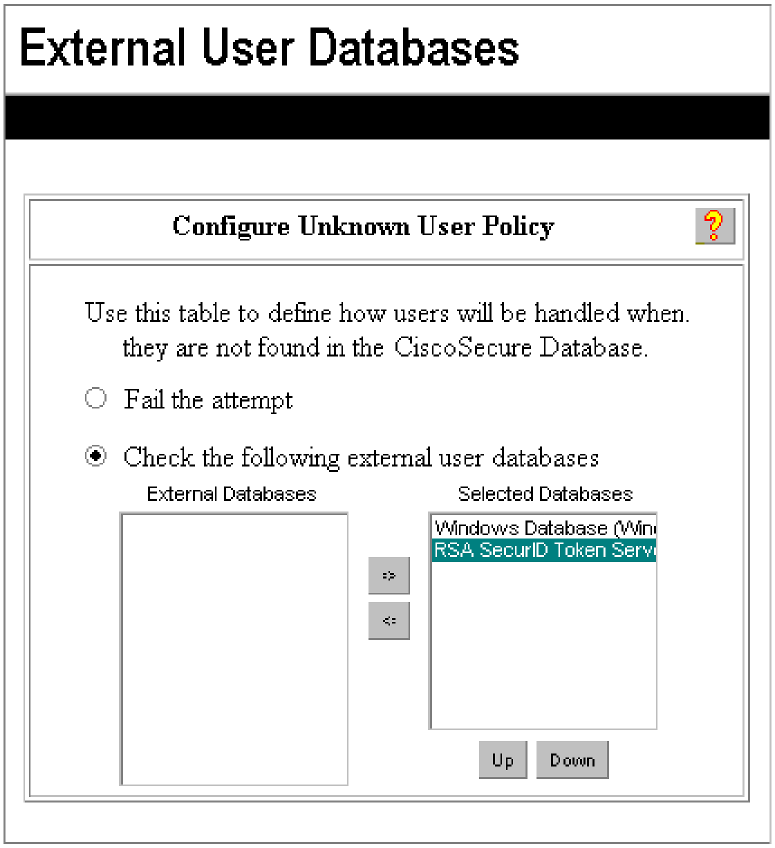
Edit

External User Database Configuration

Choose what to do with the RSA SecurID Token Server database.

There are no parameters in the Cisco ACS for the RSA ACE server.

The location of the RSA dll that the Cisco ACS finds is displayed.



External User Databases

Configure Unknown User Policy

Use this table to define how users will be handled when they are not found in the CiscoSecure Database.

○ Fail the attempt

● Check the following external user databases

External Databases

Selected Databases

Windows Database (Win

RSA SecurID Token Serv

Next, the Unknown User Policy must be configured so the Cisco ACS will check these new databases. Navigate to the External User Database screen and click the **Unknown User Policy** link.

The external databases configured will be displayed in the left pane. To have Cisco ACS check these databases highlight them and click the right arrow button.

Now when a username that the Cisco ACS does not know about is received it will check the databases list in the right pane (as shown above).

Click the **Submit** button and now a user can use the Active directory username and password or the RSA SecurID hardware token to authenticate.

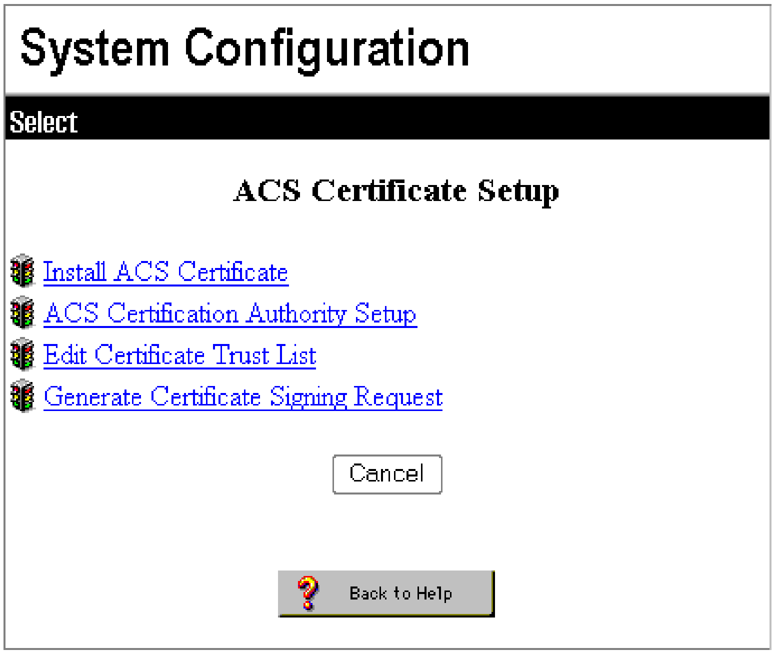
ACS Certificate Setup

In order to turn on PEAP (both versions) and EAP-TLS authentication a certificate must be first installed. Once a certificate is received from the CA install the certificate.

Note: For an example of getting a certificate see Server Certificate, later in this document.

Installing an ACS Certificate

Click the **System Configuration** button and then click the link to **ACS Certificate Setup**.



System Configuration

Select

ACS Certificate Setup

Install ACS Certificate

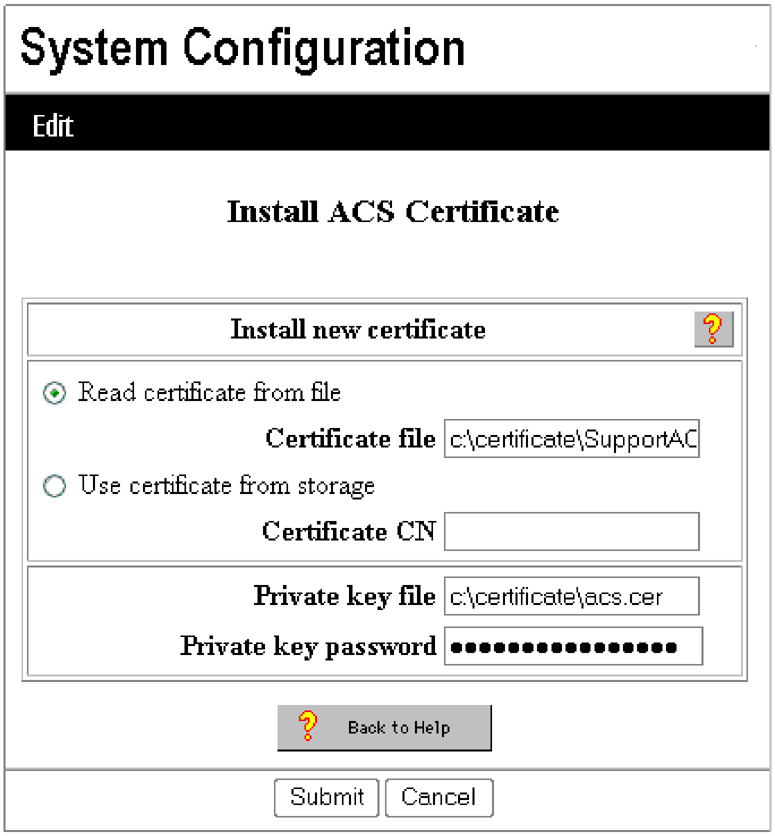
ACS Certification Authority Setup

Edit Certificate Trust List

Generate Certificate Signing Request

Install the certificate by clicking the **Install ACS Certificate** link.

Click the **Install New Certificate** link.



Install ACS Certificate

Install new certificate

● Read certificate from file

Certificate file: c:\certificate\SupportAC

○ Use certificate from storage

Certificate CN:

Private key file: c:\certificate\acs.cer

Private key password: ●●●●●●●●●●●●●●●●

The certificate is a file saved to a local drive.

Verify **Read certificate from file** button is checked.

Check that **certificate file** text box information is where the certificate is saved.

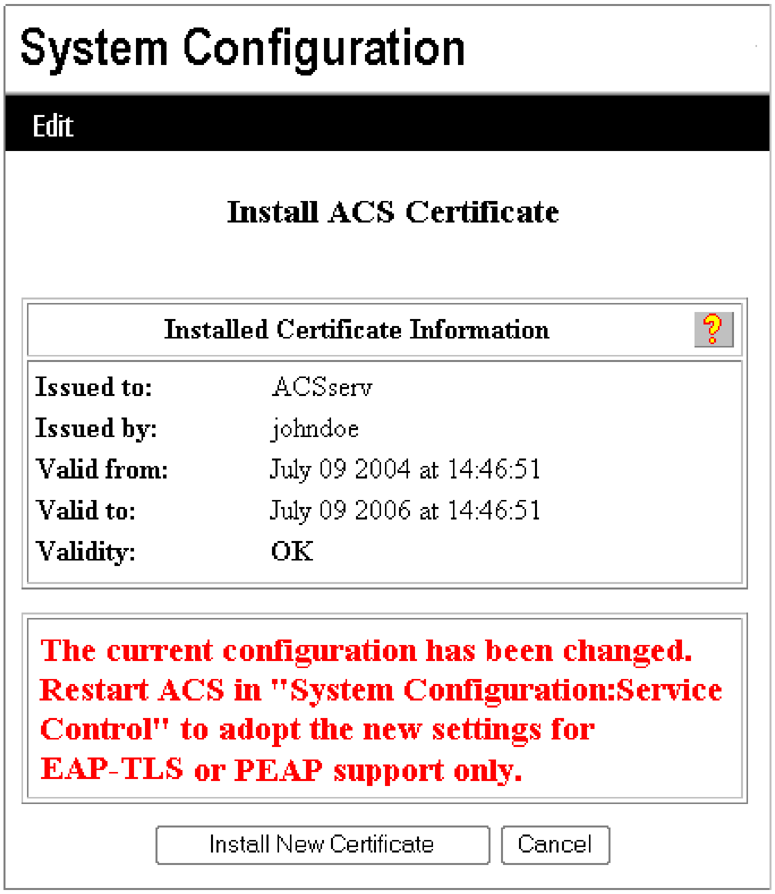
Verify **Private key file** data is correct.

Enter the **Private key password**.

Click the **Submit** button.

The ACS now has a certificate installed as shown in the Figure below.

The box at the bottom of the screen informs of the requirement to restart the ACS service.



System Configuration

Edit

Install ACS Certificate

Installed Certificate Information

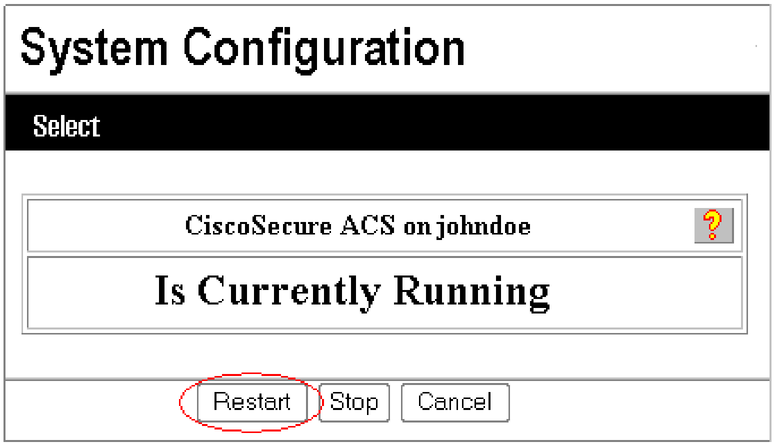
Issued to:	ACSserv
Issued by:	johndoe
Valid from:	July 09 2004 at 14:46:51
Valid to:	July 09 2006 at 14:46:51
Validity:	OK

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.

Click the **System Configuration** button.

Click the link to **Service Control**.

Click the **Restart** button.



System Configuration

Select

CiscoSecure ACS on johndoe

Is Currently Running

It is now time to configure authentication protocols as shown in the next section.

Global Authentication Setup

Make sure there is an ACS certificate installed before trying to configure Global Authentication for PEAP (both versions) and EAP-TLS. Use the **Install ACS Certificate** menu option to confirm installation of a certificate. DO NOT install a new certificate if a valid certificate is in place. If a certificate is currently installed then configuration can continue.

Using a browser navigate to the Cisco ACS.

Click the **System Configuration** button.

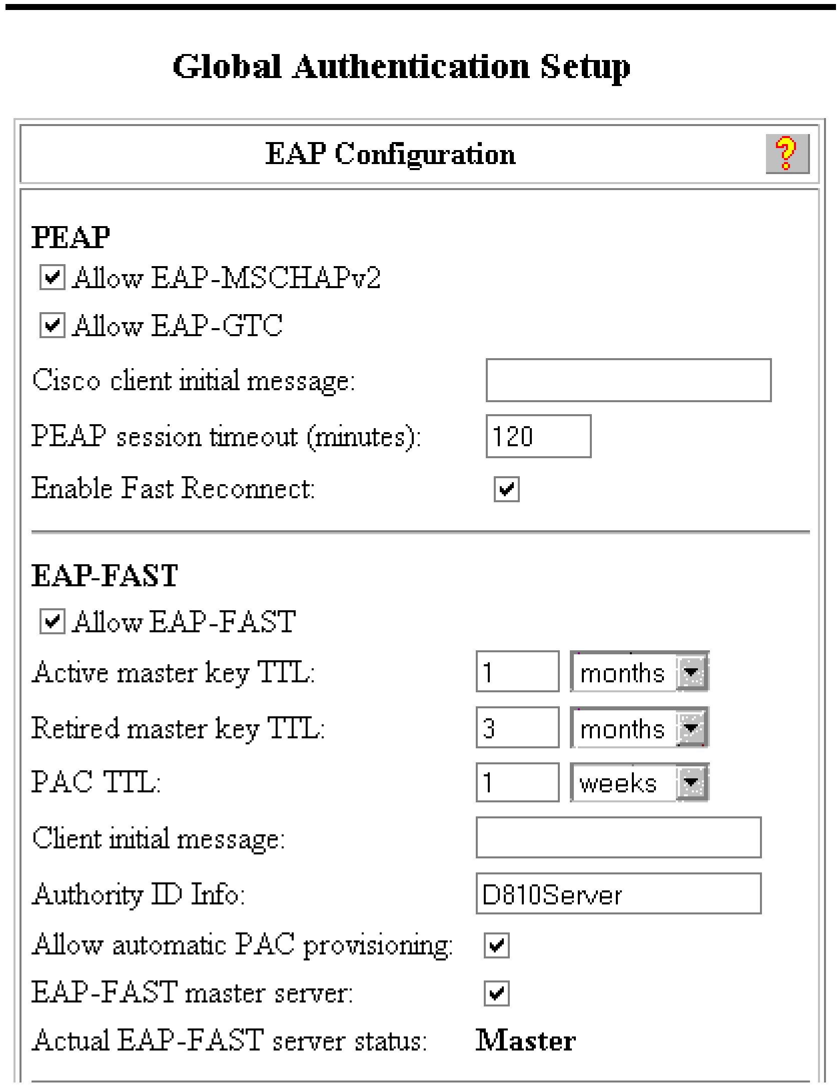
Choose the **Global Authentication Setup** menu option.

Check the boxes that will be used for authentication.

Including:

- PEAP/MSCHAPv2
- PEAP/EAP-GTC
- EAP-TLS
- EAP-FAST
- LEAP

Check the **Enable Fast Reconnect** box. This will allow the wireless devices to authenticate faster when they roam from one AP to another.



Global Authentication Setup

EAP Configuration

PEAP

☑ Allow EAP-MSCHAPv2

☑ Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes): 120

Enable Fast Reconnect: ☑

EAP-FAST

☑ Allow EAP-FAST

Active master key TTL: 1 months

Retired master key TTL: 3 months

PAC TTL: 1 weeks

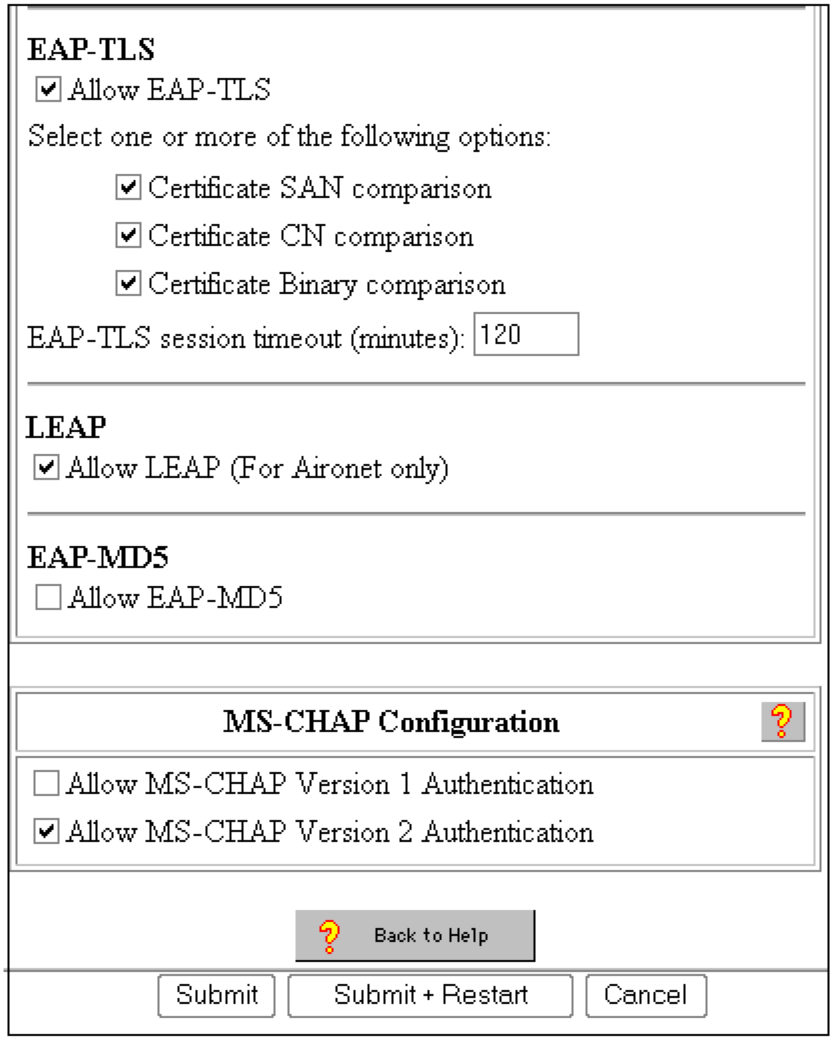
Client initial message:

Authority ID Info: D810Server

Allow automatic PAC provisioning: ☑

EAP-FAST master server: ☑

Actual EAP-FAST server status: **Master**



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): 120

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

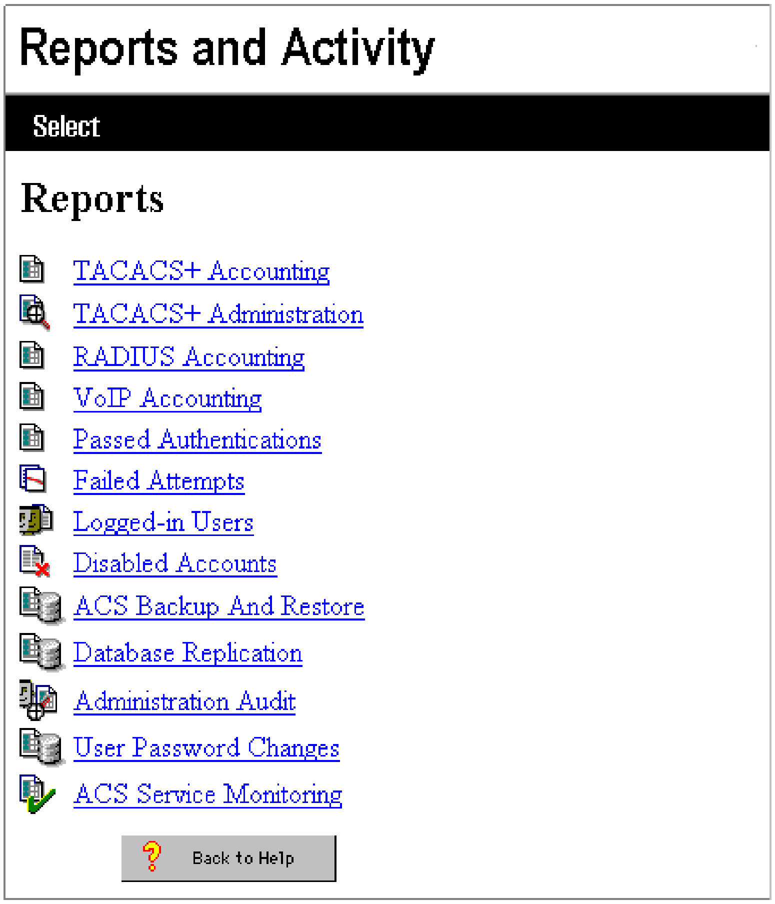
Click the **Submit + Restart** button.

The Cisco ACS is now ready to authenticate clients.

Authentication Help

If there is a problem getting authenticated one tool is the ACS logs.

Navigate to the Cisco ACS and click the **Reports and Activity** button.



Click the **Failed Attempt**s link.

Any authentication failures should display in the log with a brief description of the failure.

If no failures are shown or the failed mobile computer is not shown, then the failure did not come from the ACS. This could be a problem with the AP setup or something before the ACS in the authentication process.

Chapter 4: Certificate Administration

Introduction

Certificates are used to validate a server or user. By sending a certificate for validation there is no username and password sign on which simplifies the login process.

Administering user certificates however is time consuming. Each user has a certificate and must use that certificate to sign on, meaning they have to copy their certificate to each mobile device they are trying to login to.

The Server certificate is used to validate the Cisco ACS (or other RADIUS) server during phase 1 of the authentication process of EAP/MS-CHAP, EAP/TLS and EAP/GTC.

A User certificate is used to validate a user when authenticating with EAP-TLS.

Mobile Devices

Instructions for the Root Certificate and User Certificate generation and installation processes differ by equipment type and operating system. Refer to the *Wireless Network Configuration* section in the equipment specific Reference Guide.

In Brief:

1. Root Certificates are necessary for EAP-TLS, PEAP-GTC, and PEAP/MSCHAP.
    - Generate a Root Certificate.
    - Copy the certificate to the mobile device.
    - Install the Root CA Certificate.
2. User Certificates are necessary for EAP-TLS.
    - Generate a User Certificate.
    - Copy the certificate to the mobile device.
    - Install the User Certificate.

Server Certificate

The Cisco ACS requires a server certificate to be installed before it will allow any type of EAP authentication. The steps to get a certificate installed are

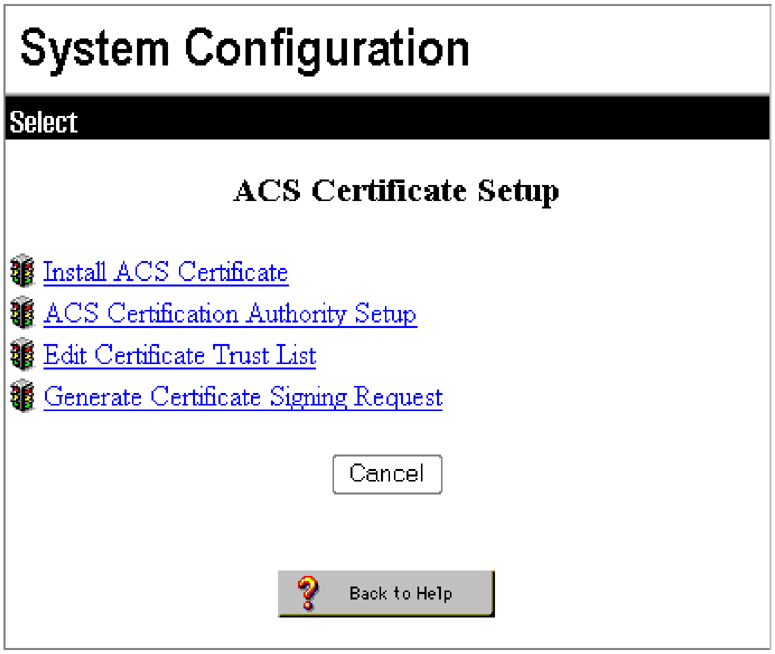
- Use the ACS Certificate setup page to generate a certificate signing request.
- Send the data from the request to a certificate authority to request a certificate.
- Copy the certificate to a file on the ACS.
- Install the certificate using the ACS certificate setup.
- Configure the ACS for EAP authentication.

Generating an ACS Certificate Signing Request

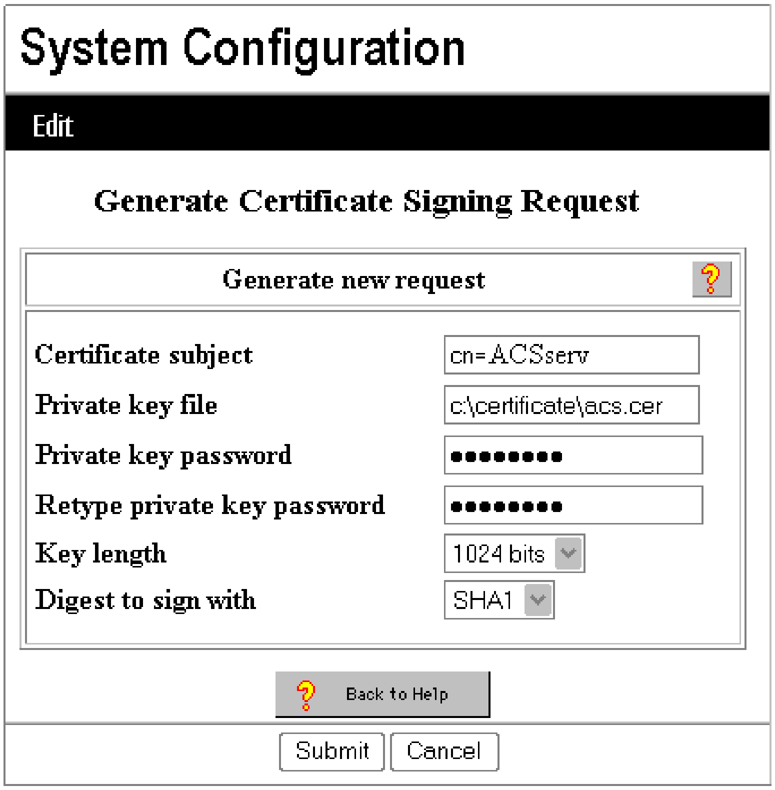
To configure PEAP on the Cisco ACS a certificate must be installed for the ACS server. Follow these steps to request a server certificate:

Log into the Cisco ACS.

From the main menu click the link to **System Configuration**, then the **ACS Certificate Setup** link


System Configuration
Select
ACS Certificate Setup
Install ACS Certificate
ACS Certification Authority Setup
Edit Certificate Trust List
Generate Certificate Signing Request
Cancel
Back to Help

Click the **Generate Certificate Signing Request** link.



System Configuration

Edit

Generate Certificate Signing Request

Generate new request

Certificate subject: cn=ACSserv

Private key file: c:\certificate\acs.cer

Private key password: ●●●●●●●●●

Retype private key password: ●●●●●●●●●

Key length: 1024 bits

Digest to sign with: SHA1

Certificate subject must be formatted as shown above:

(cn=<server cert name>)

The server certificate requires a private key. Type the path and filename for the key file.

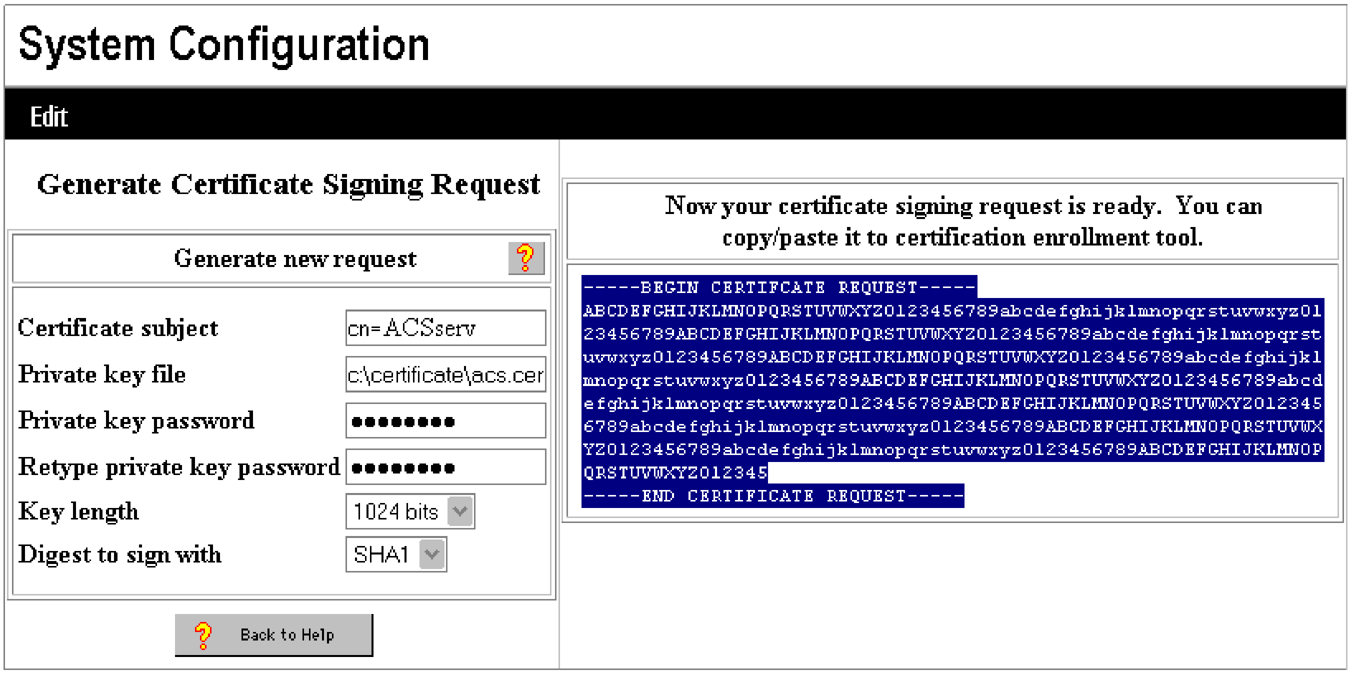
Enter the private key password in both boxes. This will be used to install the new certificate into the ACS.

Set the key length and Digest (or leave default).

Click the **Submit** button

The Cisco ACS will display the signing request in the right pane (as shown below).

Copy this data to the PC clipboard (highlight the data and press CTRL C). Use this data to request a certificate from your CA.



System Configuration

Edit

Generate Certificate Signing Request

Generate new request

Certificate subject	cn=ACSserv
Private key file	c:\certificate\acs.cer
Private key password	●●●●●●●●●
Retype private key password	●●●●●●●●●
Key length	1024 bits
Digest to sign with	SHA1

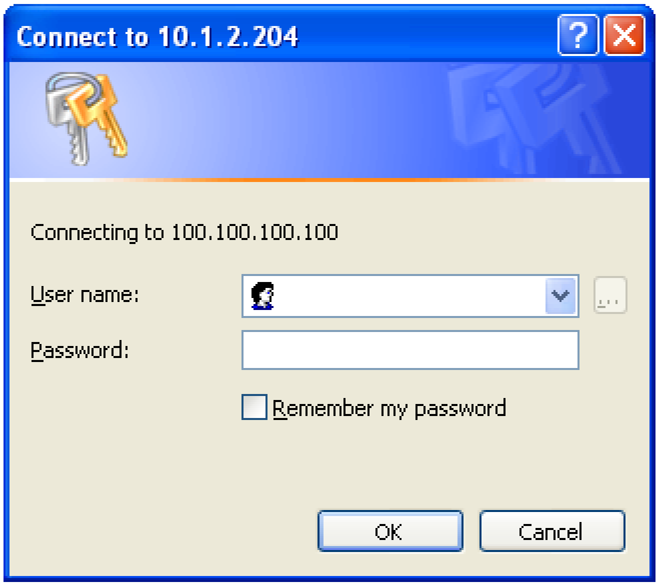
Now your certificate signing request is ready. You can copy/paste it to certification enrollment tool.

```
-----BEGIN CERTIFCATE REQUEST-----
ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz01
23456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrst
uvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijkl
mnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcd
efghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ012345
6789abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWX
YZ0123456789abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOP
QRSTUVWXYZ012345
-----END CERTIFICATE REQUEST-----
```

Requesting a Server Certificate from the CA

The certificate authority (CA) used for this configuration is Windows 2003 certificate services.

To request a certificate, open a browser to
http://<CA IP address>/certsrv.



Connect to 10.1.2.204

Connecting to 100.100.100.100

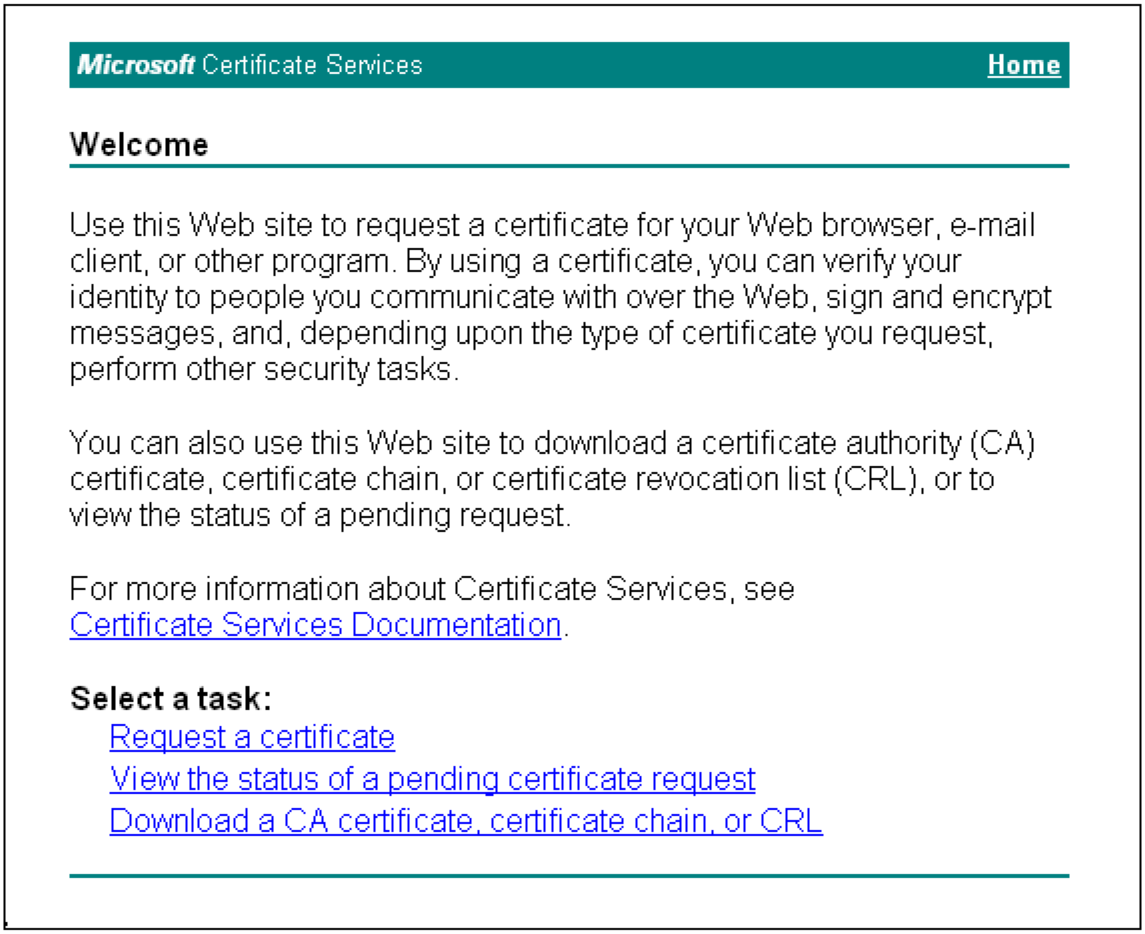
User name:

Password:

□ Remember my password

Sign into the CA with a username and password of an administrator.

Note: Signing on with non-administrator rights does not allow requesting the correct type of certificate.



Microsoft Certificate Services Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

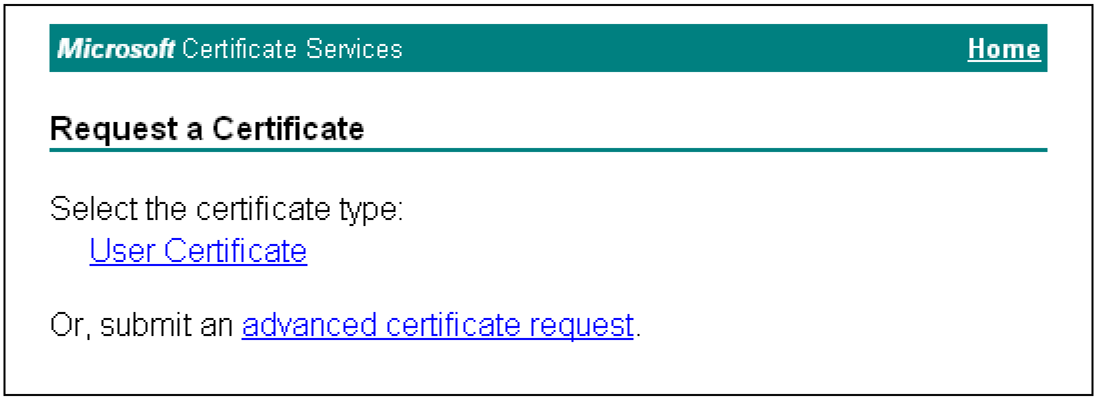
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Click the **Request a certificate** link



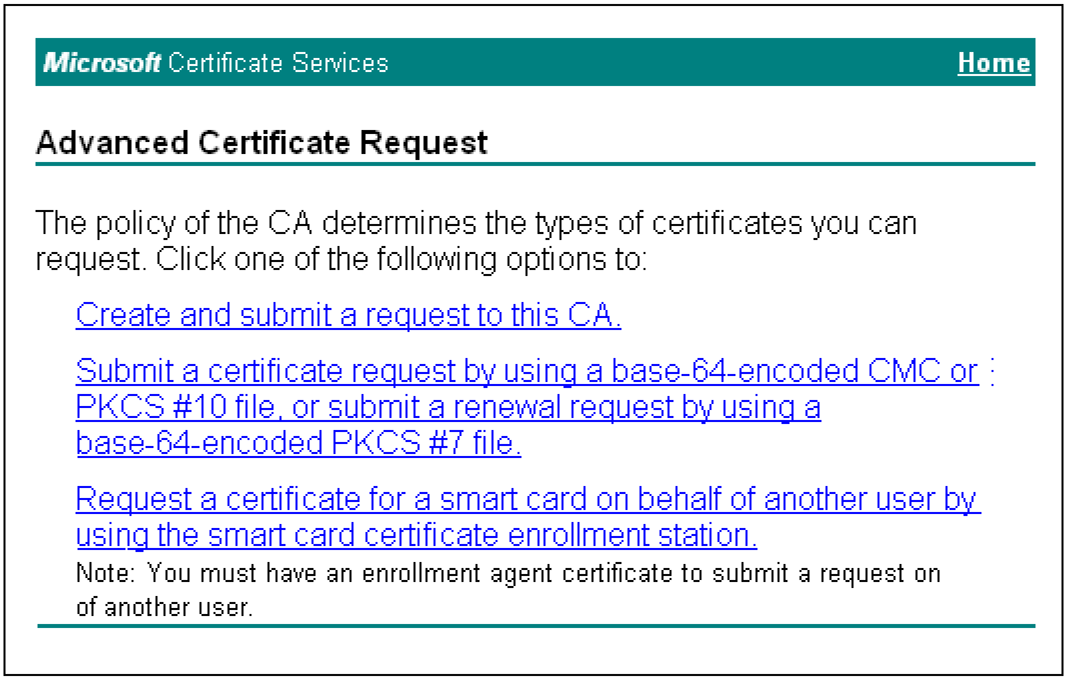
Microsoft Certificate Services Home

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Click the **advanced certificate request** link.



Microsoft Certificate Services

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

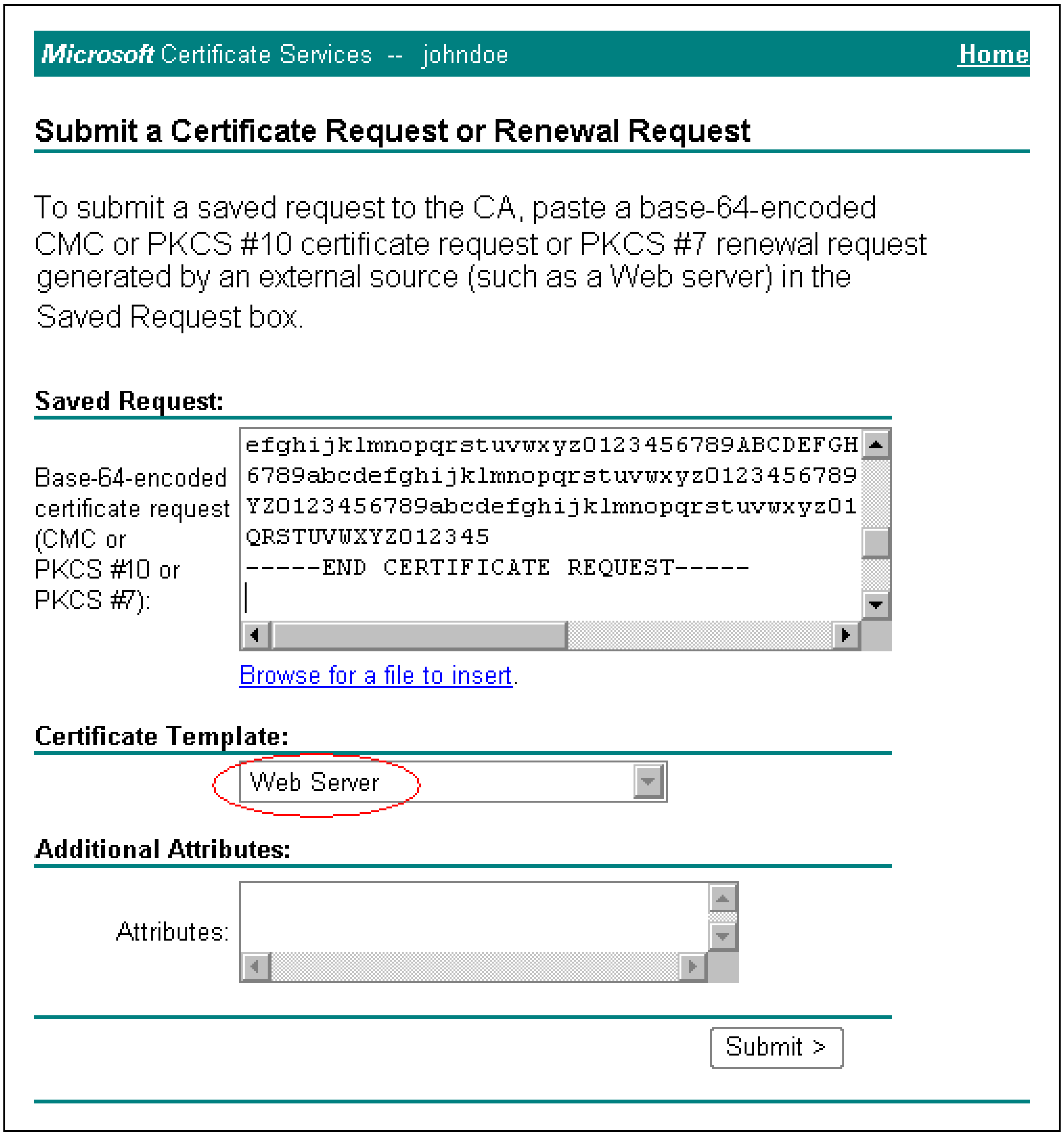
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

Note: You must have an enrollment agent certificate to submit a request on of another user.

Click the link for **Submit a certificate request by using a base-64-encoded CMC or PKCSA #10 file**.

Paste the generated request data from the Cisco ACS by pressing **Ctrl V**.

Set the certificate template to **Web Server**.



Microsoft Certificate Services -- johndoe

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
efghijklmnopqrstuvwxyz0123456789ABCDEFGH
6789abcdefghijklmnopqrstuvwxyz0123456789
YZ0123456789abcdefghijklmnopqrstuvwxyz01
QRSTUVWXYZ012345
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

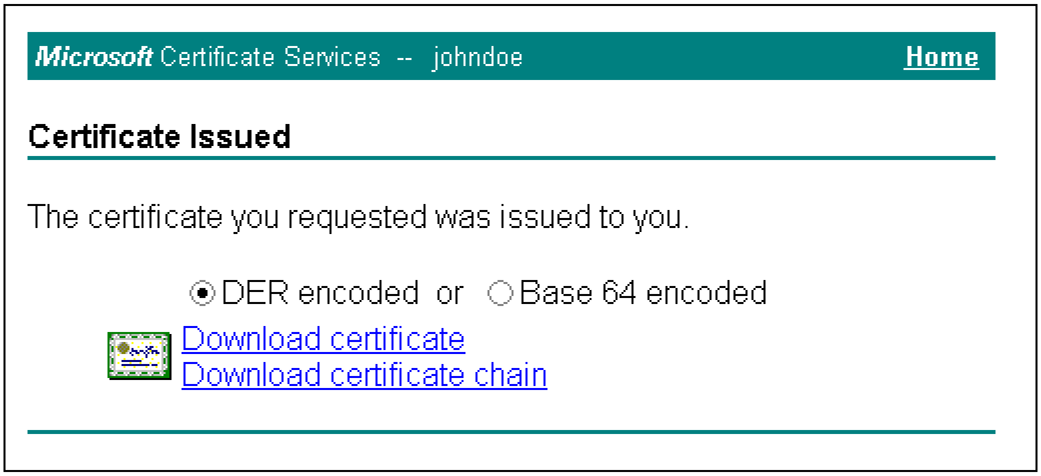
Additional Attributes:

Attributes:

Note: Signing on with non-administrator rights will not allow requesting the Web Server certificate.

Click the **Submit** button

The CA will issue a server certificate with the data provided to it.



Microsoft Certificate Services -- johndoe

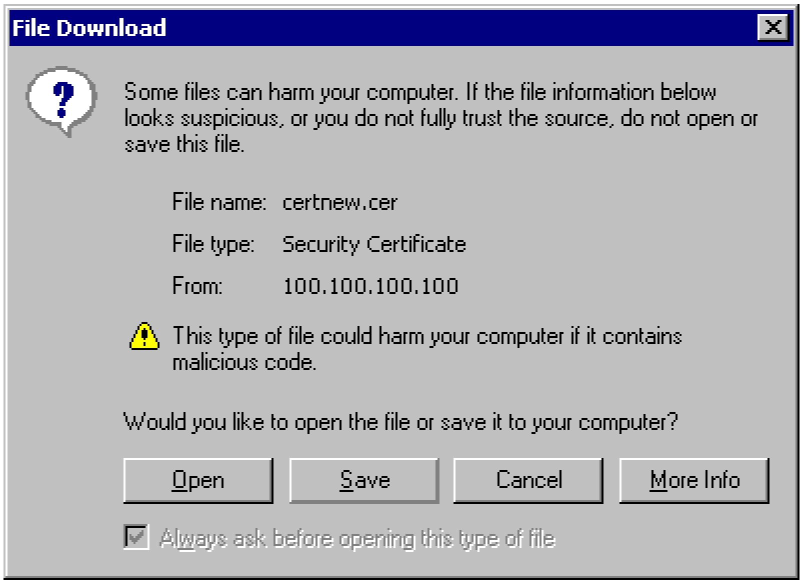
Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

When the CA issues the certificate click the link **Download certificate**.



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: certnew.cer

File type: Security Certificate

From: 100.100.100.100

This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

Save the certificate by clicking the **Save** button and save the certificate to a location on the hard disk.

Keep track of the certificate, as it is needed when installing it into the ACS.

Now the ACS certificate is saved on the ACS computer hard drive and is ready for installation.

To install the certificate go to Installing an ACS Certificate.

Chapter 5: RSA ACE Server Configuration

Introduction

To authenticate users using the EAP/GTC protocol a token server is required. Each user will have a hardware or software token that supplies a one-time password (OTP). To test this authentication Honeywell tested a RSA SecurID system consisting of hardware tokens and the RSA ACE server. The server was installed on the Windows Server 2003 with the Cisco ACS.

Server Installation

Install the RSA ACE server according to the directions in the documentation that comes with the server.

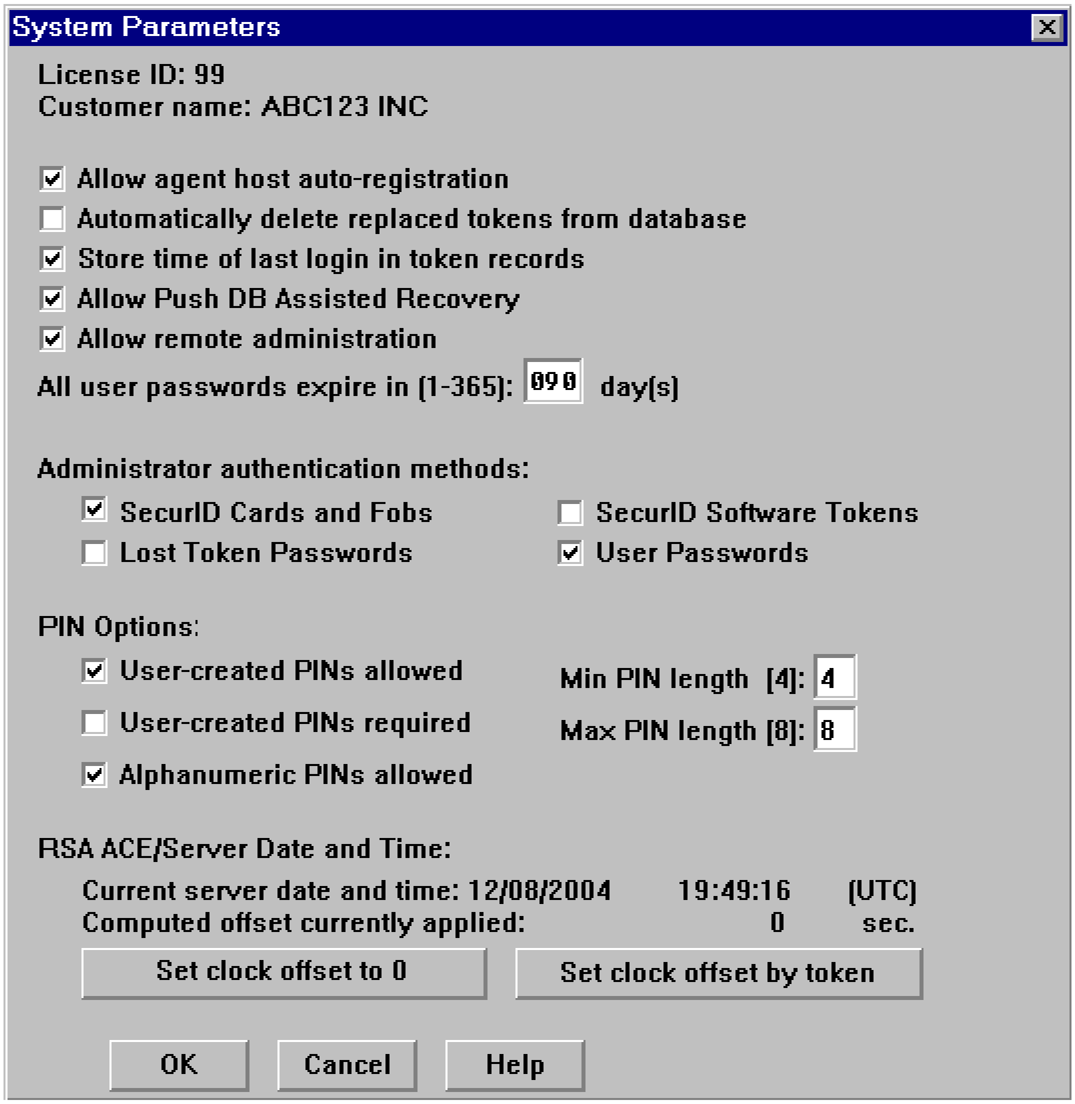
Import the token data once the server is installed.

Server Configuration

To configure the user database click **Start | Programs | RSA ACE Server | Database Administration – Host Mode**.

Click the **System** menu and make any changes required.

In the test case the **Allow agent host auto-registration** box was checked and the **Alphanumeric PINS allowed** box under **PIN options**.



System Parameters

License ID: 99
Customer name: ABC123 INC

☑ Allow agent host auto-registration
□ Automatically delete replaced tokens from database
☑ Store time of last login in token records
☑ Allow Push DB Assisted Recovery
☑ Allow remote administration

All user passwords expire in (1-365): 090 day(s)

Administrator authentication methods:

☑ SecurID Cards and Fobs
□ SecurID Software Tokens
□ Lost Token Passwords
☑ User Passwords

PIN Options:

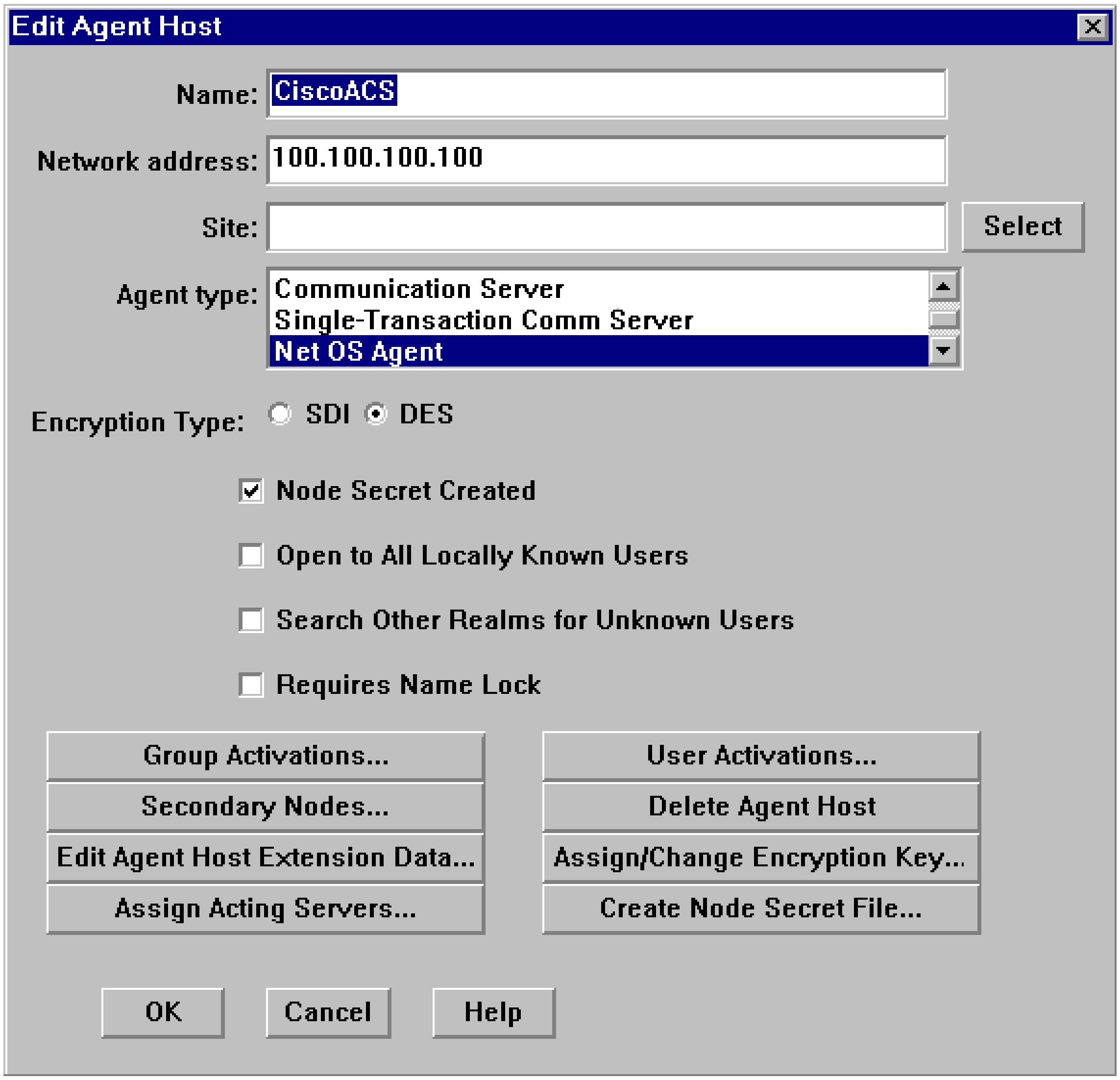
☑ User-created PINs allowed
□ User-created PINs required
☑ Alphanumeric PINs allowed

Min PIN length [4]: 4
Max PIN length [8]: 8

RSA ACE/Server Date and Time:

Current server date and time: 12/08/2004 19:49:16 (UTC)
Computed offset currently applied: 0 sec.

Click **OK**.



Edit Agent Host

Name: CiscoACS

Network address: 100.100.100.100

Site:

Agent type: Communication Server
Single-Transaction Comm Server
Net OS Agent

Encryption Type: ○ SDI ● DES

☑ Node Secret Created

□ Open to All Locally Known Users

□ Search Other Realms for Unknown Users

□ Requires Name Lock

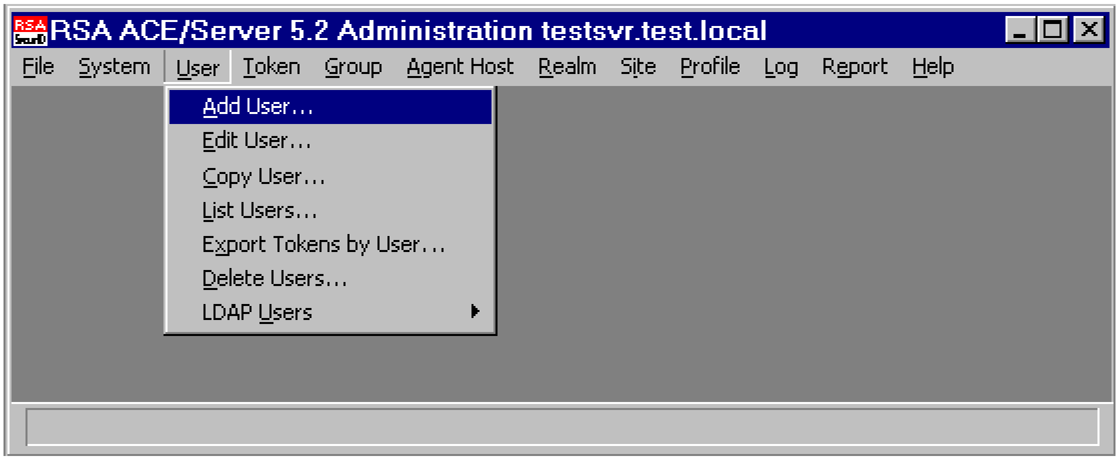
Next click **Agent Host** and click **Add Agent Host**.

The agent host is the Cisco ACS server. Enter a name and the IP address of the Cisco ACS.

Choose **Net OS Agent** and make the screen match the **Agent Host** figure above.

Adding Users

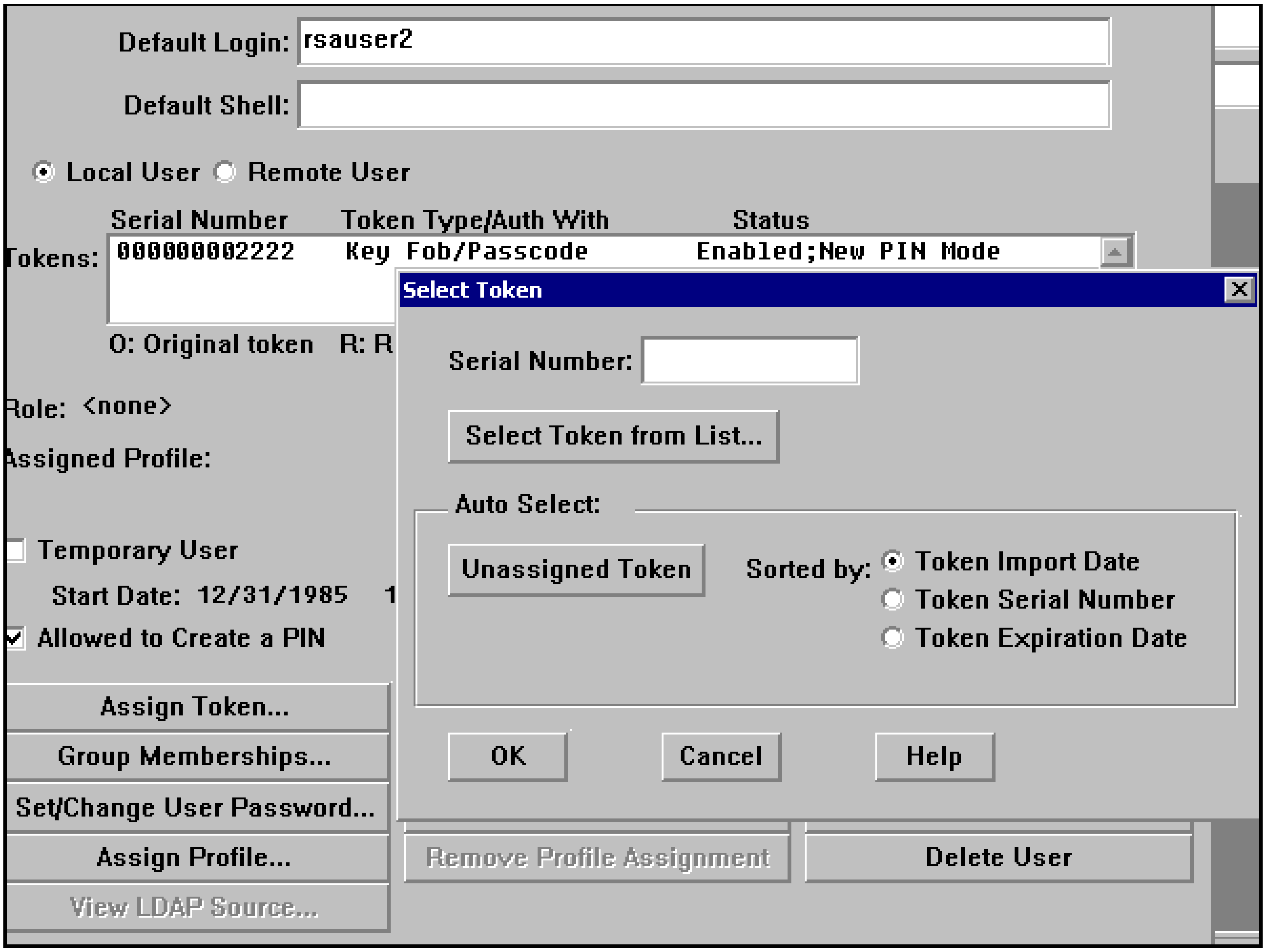
Now add users under the **User** menu.



Enter a user's last name and username and click the **Assign Token** button.

Click **yes** to add the user to the database.

The select token screen appears.



Default Login: rsauser2

Default Shell:

● Local User ○ Remote User

Tokens:

Serial Number	Token Type/Auth With	Status
000000002222	Key Fob/Passcode	Enabled;New PIN Mode

O: Original token R: R

Role: <none>

Assigned Profile:

□ Temporary User

Start Date: 12/31/1985 1

☑ Allowed to Create a PIN

Select Token

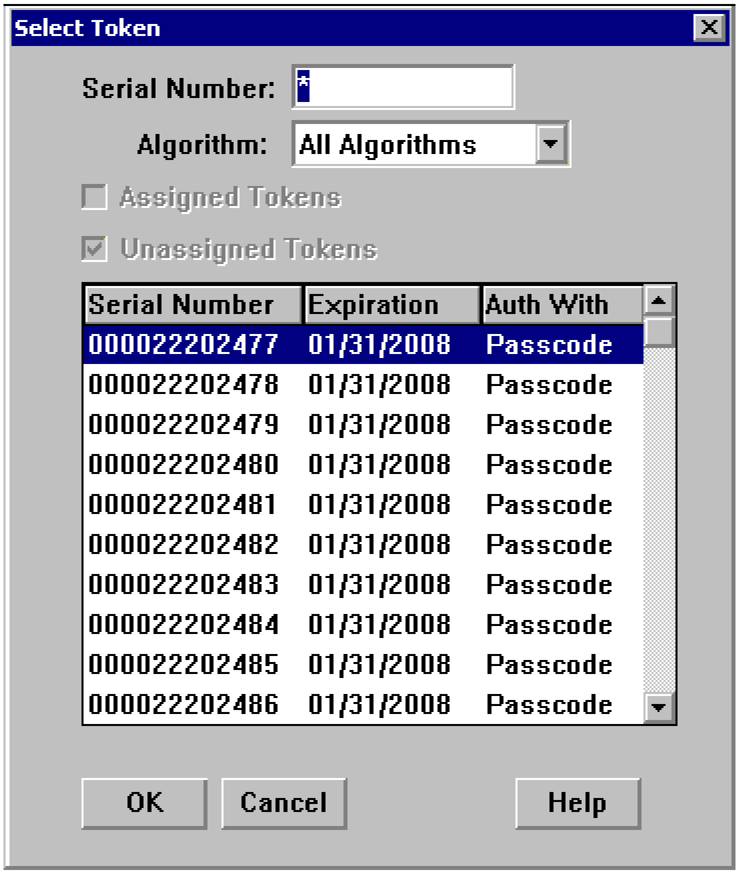
Serial Number:

Auto Select:

Sorted by: ● Token Import Date ○ Token Serial Number ○ Token Expiration Date

Click the **Select Token** from **List** button and choose the token for this user.

The numbers correspond with the number on the back of the tokens.



Serial Number: *

Algorithm: All Algorithms

□ Assigned Tokens

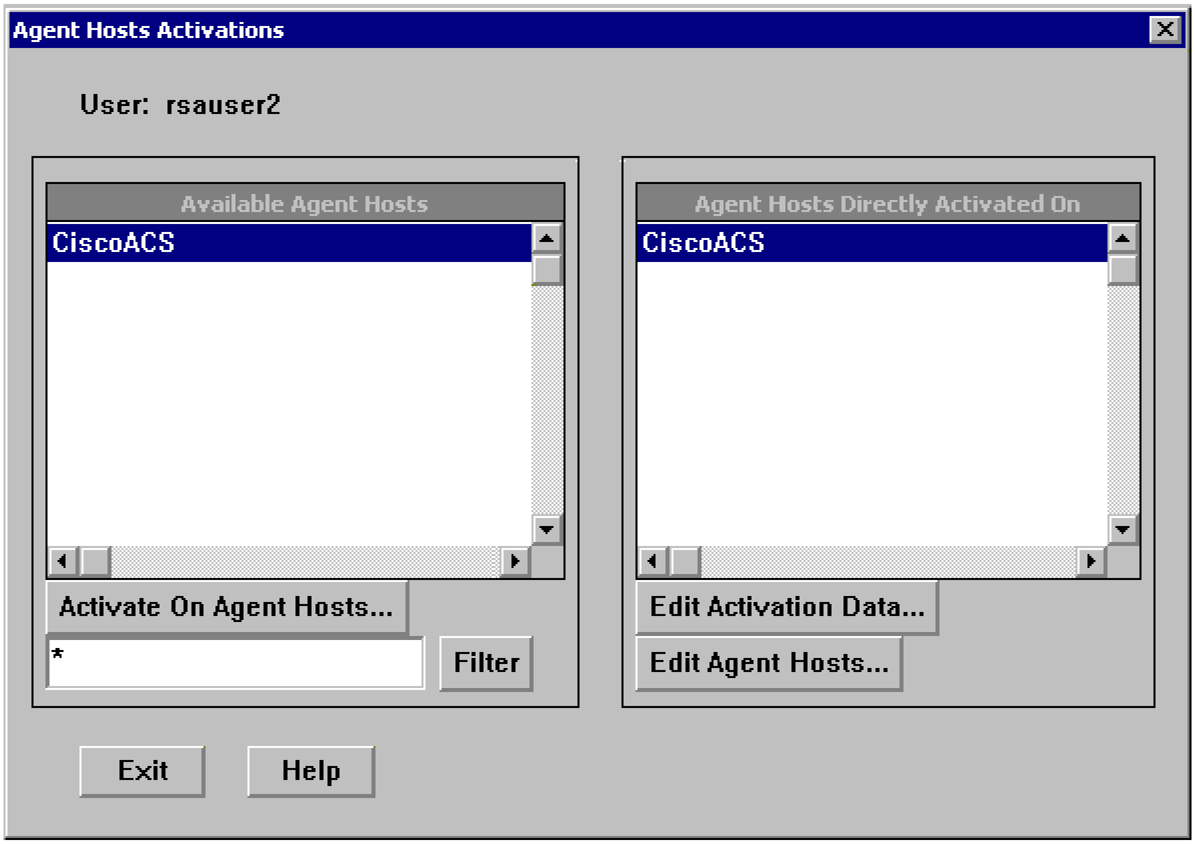
☑ Unassigned Tokens

Serial Number	Expiration	Auth With
000022202477	01/31/2008	Passcode
000022202478	01/31/2008	Passcode
000022202479	01/31/2008	Passcode
000022202480	01/31/2008	Passcode
000022202481	01/31/2008	Passcode
000022202482	01/31/2008	Passcode
000022202483	01/31/2008	Passcode
000022202484	01/31/2008	Passcode
000022202485	01/31/2008	Passcode
000022202486	01/31/2008	Passcode

Note: Write the username on the back of the token to keep track of which token goes with each username.

Now the user must be activated on the agent host by clicking the **Agent Host Activations** button on the user screen.

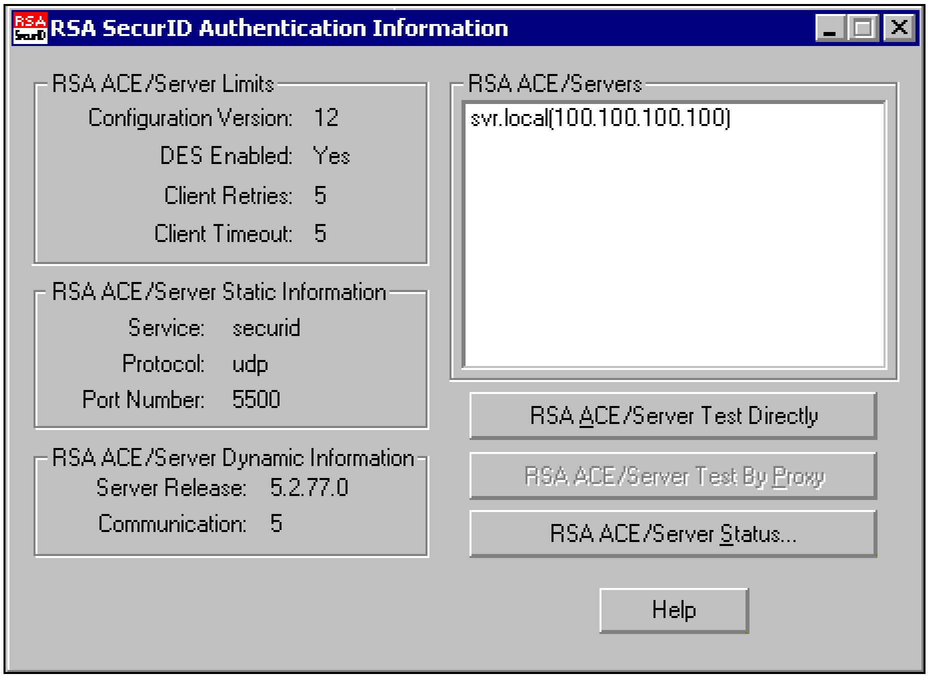
Double click the agent host name setup above to activate the user as shown below.



Agent Hosts Activations
User: rsauser2
Available Agent Hosts
CiscoACS
Agent Hosts Directly Activated On
CiscoACS
Activate On Agent Hosts...
*
Filter
Edit Activation Data...
Edit Agent Hosts...
Exit
Help

Testing Authentication

The user is now configured in the server and can be tested on the server. Navigate to **Start | All Programs | RSA ACE Agent | Test Authentication**.



RSA SecurID Authentication Information

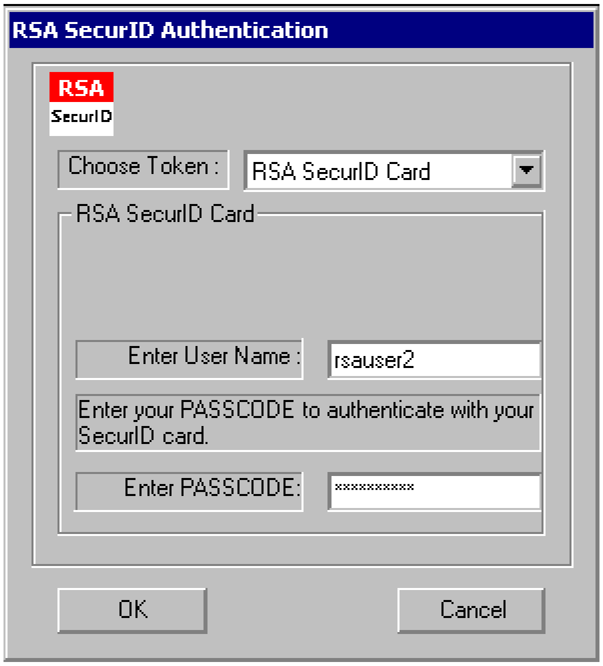
RSA ACE/Server Limits
Configuration Version: 12
DES Enabled: Yes
Client Retries: 5
Client Timeout: 5

RSA ACE/Server Static Information
Service: securid
Protocol: udp
Port Number: 5500

RSA ACE/Server Dynamic Information
Server Release: 5.2.77.0
Communication: 5

RSA ACE/Servers
svr.local(100.100.100.100)

Click the **RSA ACE/Server Test Directly** button.

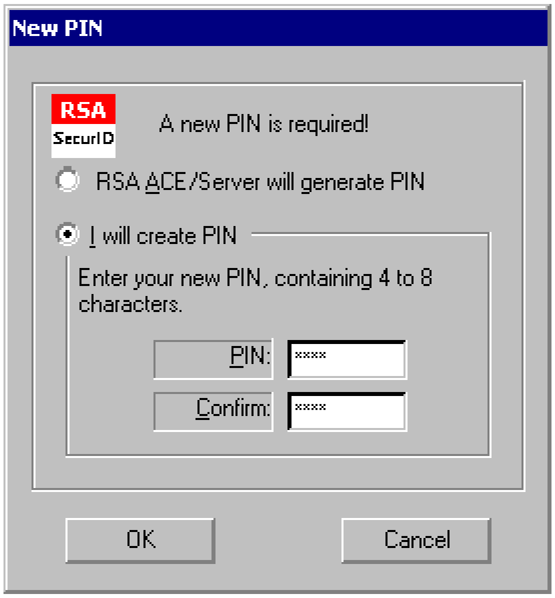


RSA SecurID Authentication

Choose Token : RSA SecurID Card

RSA SecurID Card
Enter User Name : rsauser2
Enter your PASSCODE to authenticate with your SecurID card.
Enter PASSCODE: ***********

Enter the new username and the current passcode from the hardware token.



New PIN

A new PIN is required!

○ RSA ACE/Server will generate PIN

● I will create PIN

Enter your new PIN, containing 4 to 8 characters.

PIN: ****

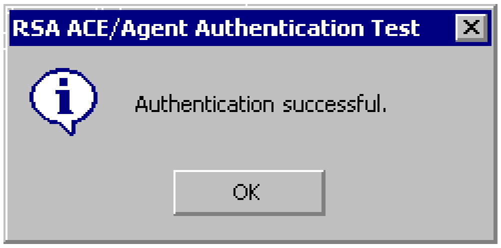
Confirm: ****

If this is the first time the username is used a new PIN will be created as shown.

After configuring the PIN it will ask to authenticate again.

Note: Using a PIN and passcode or only the passcode is configurable in the token screen for each token. The choices are Users authenticate with: passcode or tokencode only.

The username is already in the field. Now enter the PIN followed by the passcode.



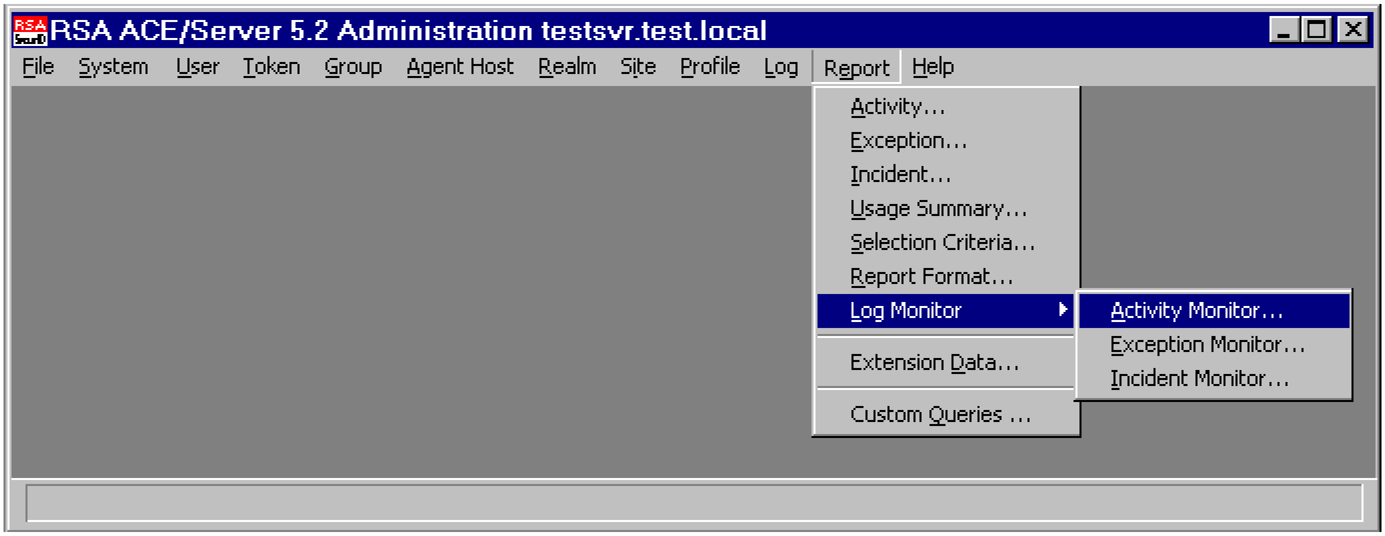
RSA ACE/Agent Authentication Test

Authentication successful.

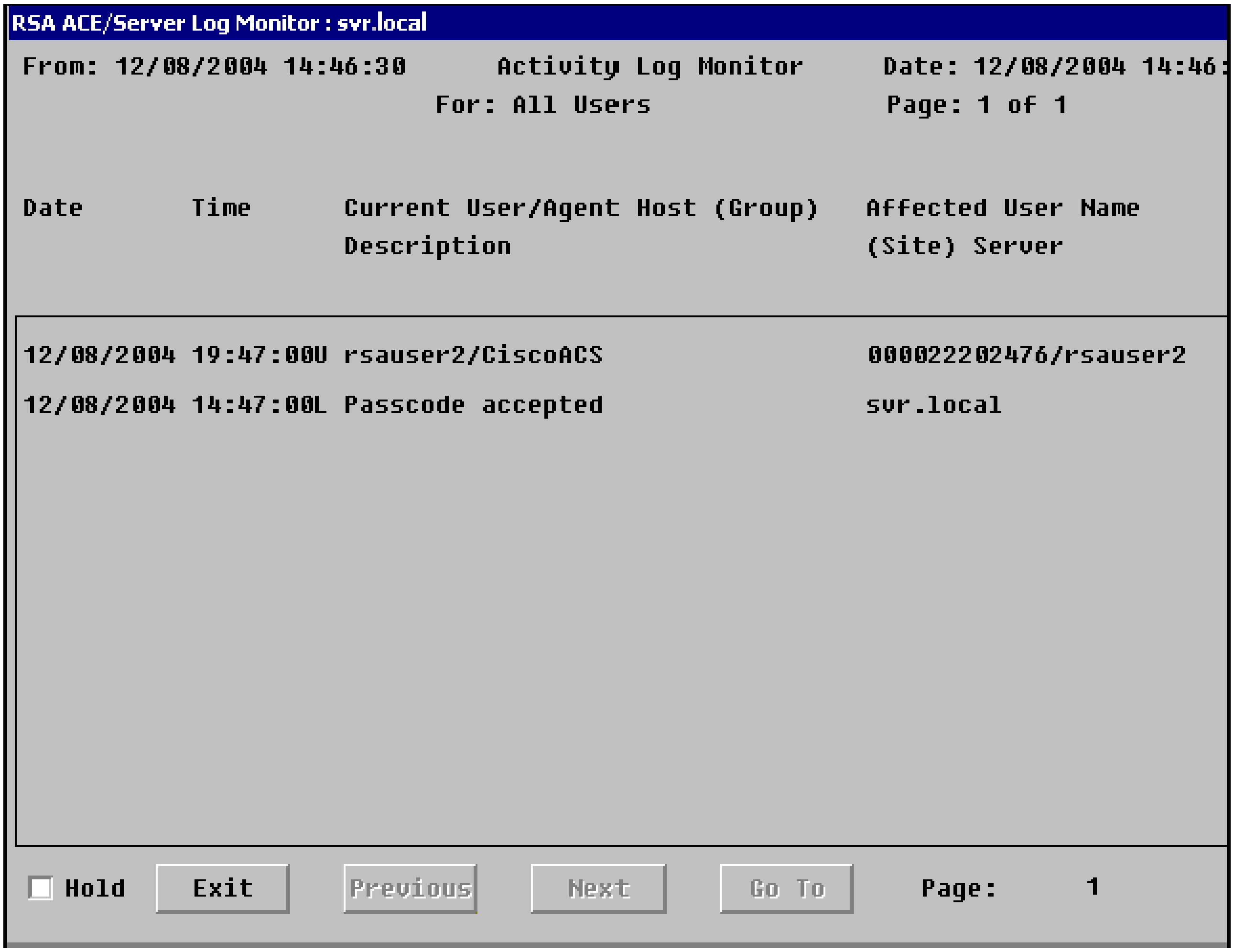
Once the test authentication works configure the mobile computer for EAP/GTC and use the same user credentials. Please refer to the appropriate Reference Guide for the mobile computer for details on configuring the computer for WPA.

Server Monitor Help

For diagnostic purposes there is a real time monitor that works very well.



Choose **Report | Log Monitor | Active Monitor**.



RSA ACE/Server Log Monitor : svr.local

```
From: 12/08/2004 14:46:30      Activity Log Monitor      Date: 12/08/2004 14:46:
                           For: All Users               Page: 1 of 1


Date        Time       Current User/Agent Host (Group)   Affected User Name
                       Description                       (Site) Server

12/08/2004 19:47:00U rsauser2/CiscoACS                 000022202476/rsauser2
12/08/2004 14:47:00L Passcode accepted                 svr.local
```

This screen displays each authentication attempt as tested with the Test authentication screen and the active monitor.

Additional Information

The documentation provided with the RSA ACE server is extensive. For additional parameters and configurations consult the documentation.

Links to additional help and implementation guides are available by typing "RSA ACE Server" into a browser search engine.

Chapter 6: Technical Assistance

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

Knowledge Base: www.hsmknowledgebase.com

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

Technical Support Portal: www.hsmsupportportal.com

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

Web form: www.hsmcontactsupport.com

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

Telephone: www.honeywellaidc.com/locations

For our latest contact information, please check our website at the link above.

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To obtain warranty or non-warranty service, please visit www.honeywellaidc.com and select **Support > Contact Service and Repair** to see your region’s instructions on how to obtain a Return Material Authorization number (RMA #). You should do this prior to returning the product.

Glossary

There are many terms and acronyms used when discussing security, especially when wireless security is the topic. The following terms and acronyms are used throughout this document.

ACS

Access Control Server.

AP

Access Point. Hardware and software product (essentially a computer) that performs an Ethernet to Radio Frequency bridging function over radios in the same frequency band.

CA

Certificate or Certification Authority. An organization that issues and manages security credentials and public keys for message encryption.

CKIP

Cisco Key Integrity Protocol.

CMIC

Cisco Message Integrity Check.

EAP-FAST

EAP - Extensible Authentication Protocol. FAST - Flexible Authentication via Secured Tunnel. EAP-FAST was developed by Cisco to improve upon the security offered by LEAP. Like LEAP, EAP-FAST relies on user names and passwords to authenticate individuals on the network. Authentication takes place within an encrypted tunnel that is based on a pre-shared secret, rather than on a certificate.

EAP-TLS

EAP - Extensible Authentication Protocol. TLS -Transport Layer Security. One of the possible 802.1x authentication protocols that can be used in WPA - Wi-Fi Protected Access. EAP-TLS uses client and server certificates (instead of passwords) through the use of PKI - Public Key Infrastructure.

Encryption

The translation of data into a secret code. Unencrypted data is often referred to as plain text. Encrypted data may be referred to as cipher text. To read encrypted data, you must have access to the secret key or password.

ICMP

Internet Control Message Protocol. The TCP/IP process that provides the set of functions used for network layer managment and control.

IEEE

Institute of Electrical and Electronics Engineers. Known among other things for developing standards for the computer industry. IEEE developed the 802.1x standards.

IOS

Internet Operating System.

LEAP

Lightweight Extensible Authentication Protocol. An 802.1x authentication protocol developed by Cisco. LEAP relies on user name and password to authenticate individuals on the network. LEAP was the first 802.1x protocol developed specifically for wireless applications. The LEAP protocol is proprietary to Cisco.

MIC

Message Integrity Check. MIC is a component of 802.11i and WPA that provides a mechanism for detecting changes to data that may have occurred in transit. MIC is more robust than the weaker CRC function in the original 802.11 specification.

OTP

One Time Password. A one time password is a password that can be used only once. Every login requires a unique password. An OTP is usually generated by a hardware ‘token’.

PC

Personal Computer. Usually considered a desktop or laptop computer.

PEAP

Protected Extensible Authentication Protocol. One of the possible 802.1x authentication protocols that can be used in WPA - Wi-Fi Protected Access.

PEAP/GTC

PEAP - Protected Extensible Authentication Protocol. GTC - Generic Token Card. One of the possible 802.1x authentication protocols that can be used in WPA. PEAP/GTC requires a certificate for authenticating the authentication server, but uses token card credentials for authenticating the user.

PEAP/MSCHAP

PEAP - Protected Extensible Authentication Protocol. MSCHAP - Microsoft Challenge Handshake Protocol. One of the possible 802.1x authentication protocols that can be used in WPA - Wi-Fi Protected Access. PEAP/MSCHAP requires a certificate for authenticating the authentication server, but relies on user name and password (encrypted with MSCHAPv2) to authenticate the user.

PING

Packet Internet Grouper. A program used to test reachability of destinations by sending them an Internet Control Message Protocol (ICMP) echo request and waiting for a reply.

PKI

Public Key Infrastructure. A PKI is required to issue and maintain digital certificates. The PKI is used to provide a highly reliable system for identifying users and/or devices on the network. A PKI consists of a Certificate Authority, along with certificate stores on network components.

PSK

Pre-Shared Key. The pre-shared key is a value or string known by all participants in a security conversation. The PSK is not distributed over the network. Normally, the PSK is manually entered into all devices where it is required.

RADIUS

Remote Authentication Dial-In User System. A common method for providing authentication, authorization and accounting services to the network. RADIUS was developed to support users dialing into the network, but is now commonly used for all types of network connections: Ethernet, dial-up, wireless, etc.

TCP/IP

TCP - Transmission Control Protocol. IP - Internet Protocol. The purpose of these two protocols is to allow computers to communicate over long distance networks. The TCP part has to do with verifying delivery of packets. The IP part refers to moving data packets between nodes. TCP/IP software is built into all major operating systems, such as Unix, Windows and the Mac OS.

TKIP

Temporal Key Integrity Protocol. TKIP is a data encryption protocol specified by the 802.11i standard as an improvement to the original 802.11 WEP encryption protocol.

WEP

Wired Equivalent Privacy. WEP is the encryption protocol specified by the original 802.11 specification. WEP was intended to provide privacy for wireless communication equivalent to that enjoyed by unencrypted wired line users.

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707
www.honeywellaidc.com