Table of Contents

EAP−TLS Version 1.01 Configuration Guide

Document ID: 64064

Introduction

This document provides a sample configuration for Extensible Authentication Protocol−Transport Layer Security (EAP−TLS) Version 1.01.

Note: This document assumes that you use Microsoft Certificate Authority (CA). While you can use a self−signed certificate, Cisco highly discourages this practice, and this document does not cover self−signed certificates. The default expiration period of the self−signed certificates is only one year, and you cannot change this setting. This is fairly standard for server certificates. However, the self−signed certificate also acts as the root CA certificate. Therefore, you need to install the new certificate on every client every year unless you do not check the Validate Server Certificate option. A real CA must be available to obtain the client certificates anyway, and so, there is really no reason to employ self−signed certificates with EAP−TLS.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Access Point (AP) 12.02T1
- Access Control Server (ACS) 3.1, 3.2, and 3.3
- Windows 2000 and XP
- Enterprise Root Certificate Authority (CA)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

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

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

Install the Microsoft Certificate (CA) Server

Complete these steps:

1. Choose **Start > Settings > Control Panel**.
2. Click **Add/Remove Programs** in the Control Panel.
3. Select **Add/Remove Windows Components**.
4. Select Certificate Services.
5. Click **Next**.
6. Click **Yes** to the IIS message.
7. Select a stand−alone (or Enterprise) root CA.
8. Click **Next**.

9. Name the CA.

   Note: All the other boxes are optional.

   Note: Do not use the same name for the CA as the ACS server, because this can cause the PEAP clients to fail authentication. A root CA certificate with the same name as the server certificate confuses the PEAP clients. This problem is not unique to Cisco clients. Of course, if you do not plan to use PEAP, this does not apply.
10. Click **Next**.

    The database default is correct.
11. Click **Next**.

    IIS must be installed before you install the CA.

Create a Server Certificate

Complete these steps:

1. Browse to the CA (**http://IP_of_CA_server/certsrv/**) from your ACS server.
2. Check the **Request a certificate** box.
3. Click **Next**.
4. Select **Advanced request**.
5. Click **Next**.
6. Select **Submit a certificate request to this CA using a form**.
7. Click **Next**.
8. Type a name in the name (CN) box.
9. Check the **Server Authentication Certificate** box for Intended Purpose.

   Note: If you use the Enterprise CA, select **Web Server** on the first list.
10. Select these options under Key Option to create a new template:

    - **CSP Microsoft Base Cryptographic Provider v1.0**
    - **Key Size¡024**

      Note: Certificates created with a key size greater than 1024 can work for HTTPS but not for PEAP.

      Note: The Windows 2003 Enterprise CA allows key sizes greater than 1024, but a key larger than 1024 does not work with PEAP. Authentication can appear to pass in ACS, but the client just hangs at the authentication attempt.
    - Check the **Mark Keys as Exportable** option

      Note: Microsoft has changed the Web Server template with the release of the Windows 2003 Enterprise CA. With this template change, you can no longer export keys, and the option is greyed out. There are no other certificate templates supplied with certificate services that are for server authentication, or that give the ability to mark keys as exportable. In order to create a new template that does so, see the Create a New Certificate Template section.
    - Check the **Use Local Machine Store** option

    Note: Retain the default selections for all other options.
11. Click **Submit**.

You must receive this message: **Your certificate request has been received**.

Create a New Certificate Template

Complete these steps:

1. Choose **Start** > **Run**.
2. Type **certmpl.msc** in the Run dialog box, and press ENTER.
3. Right−click **Web Server template**, and select **Duplicate Template**.
4. Name the template, for example, ACS.
5. Select the **Request Handling** tab.
6. Check the **Allow private key to be exported** option.
7. Select the **CSPs** button.
8. Check the **Microsoft Base Cryptographic Provider v1.0** option.
9. Click **OK**.

   Note: Retain the default selections for all other options.
10. Click **Apply**.
11. Click **OK**.
12. Open the CA MMC snap−in.
13. Right−click **Certificate Templates**, and choose **New** > **Certificate Template to Issue**.
14. Choose the new template you created.
15. Click **OK**.
16. Restart the CA.

    The new template is included in the Certificate Template list.

Sometimes, a "`Failed to create 'CertificateAuthority.Request' object`" error occurs when you attempt to create a new certificate.

Complete these steps in order to correct this error:

1. Choose **Start** > **Administrative Tools** > **IIS**.
2. Expand **Web Sites** > **Default Web Site**.
3. Right−click **CertSrv**, and choose **Properties**.
4. Click the **Configuration** button in the Application settings section of the Virtual Directory tab.
5. Select the **Options** tab.
6. Check the **Enable session state** option.

   Note: Retain the default selections for all other options.
7. Click **OK** twice.
8. Restart IIS.

Note: A 2003 CA in a 2000 domain whose schema has not been prepared for 2003 compatibility with adprep/forestprep/domainprep does not work with EAP. If your browser locks with a "`Downloading ActiveX Control`" message, you need to run the fix in this URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben−us%3B330389 .

Note: If the CSP field just displays "`Loading....`" ensure that you do not have a software firewall on the machine that submits the request. ZoneLabs' ZoneAlarm causes this error pretty much every time. Certain other software can also cause this error.

Approve the Certificate from the CA

Complete these steps:

1. Choose **Start > Programs > Administrative Tools > Certificate Authority**.
2. Expand the certificate on the left pane.
3. Select **Pending Requests**.
4. Right−click on the certificate.
5. Select all tasks.
6. Select **Issue**.

Install the Certificate on a Windows Server

Download the Server Certificate to the ACS Server

Complete these steps:

1. Browse to the CA (**http://IP_of_CA_server/certsrv/**) from your ACS server.
2. Select **Check on a Pending Certificate**.
3. Click **Next**.
4. Select the certificate.
5. Click **Next**.
6. Click **Install**.

Install the CA Certificate on the ACS Server

Note: These steps are not necessary if ACS and the CA are installed on the same server.

Complete these steps:

1. From your ACS server, browse to the CA (**http://IP_of_CA_server/certsrv/**).
2. Select **Retrieve the CA certificate or certificate revocation list**.
3. Click **Next**.
4. Select **Base 64 encoded**.
5. Click **Download CA certificate**.
6. Click **Open**.
7. Click **Install certificate**.
8. Click **Next**.
9. Select **Place all certificates in the following store**.
10. Click **Browse**.
11. Check the **Show physical stores** box.
12. Expand the **Trusted root certification authorities** list.
13. Select Local Computer.
14. Click **OK**.
15. Click **Next**.
16. Click **Finish**.

A message box appears.

17. Click **OK**.

Note: If your client certificates were created through a CA different from your server certificate, you must repeat these steps for the root CA and any intermediate CAs involved in client certificate creation.

Set up ACS to Use the Server Certificate

Complete these steps:

1. Click **System Configuration** on the ACS server.
2. Select **ACS Certificate Setup**.
3. Select **Install ACS certificate**.
4. Select **Use certificate from storage**.
5. Type in the CN name (the same name that you typed in Step 8 of the Create a Server Certificate section).
6. Click **Submit**.
7. Click **system configuration** on the ACS server.
8. Select **ACS Certificate Setup**.
9. Select **Edit Certificate Trust List**.
10. Check the **CA** box.
11. Click **Submit**.

Create a Certificate Signing Request

Complete these steps:

1. Go to **System Configuration** > **ACS Certificate Setup** > **Generate Certificate Signing Request**.
2. Type a name in the Certificate subject field in the `cn=name` format.
3. Type a name for the private key file.

   Note: This field caches the path to the private key. Therefore, if you click **Submit** a second time after the CSR is created, the private key is overwritten, and will not match the original CSR. This can result in the `private key does not match` error when you attempt to install the server certificate.
4. Type the private key password.
5. Confirm the password.
6. Choose a key length of 1024.

   Note: ACS can generate key sizes greater than 1024. However, a key larger than 1024 does not work with EAP. Authentication can appear to pass in ACS, but the client just hangs at the authentication attempt.
7. Click **Submit**.
8. Copy the CSR output on the right−hand side to submit to the CA.

Use Your CSR to Create a Server Certificate

Complete these steps:

1. Browse to the CA (**http://IP_of_CA_server/certsrv/**) from your FTP server.
2. Select the **Request a certificate** option.
3. Click **Next**.
4. Select **Advanced request**.
5. Click **Next**.

6. Select **Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**.
7. Paste the output from Step 8 of the Create a Certificate Signing Request section into the Base64 Encoded Certificate Request field.
8. Click **Submit**.
9. Click **Download CA certificate**.
10. Click **Save**, type a name for the certificate, and save it to your FTP directory.

Install the Certificate on a Windows Appliance

Download CA Certificate to your FTP Server

Complete these steps:

1. Browse to the CA (**http://IP_of_CA_server/certsrv/**) from your FTP server.
2. Select **Retrieve the CA certificate or certificate revocation list**.
3. Click **Next**.
4. Select **Base 64 encoded**.
5. Click **Download CA certificate**.
6. Click **Save**, type a name for the certificate, and save it to your FTP directory.

Install CA Certificate on your Appliance

Complete these steps.

1. Go to **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.
2. Click **Download CA certificate file**.
3. Type the IP address or hostname of the FTP server in the FTP Server field.
4. Type a valid username that Cisco Secure ACS can use to access the FTP server in the Login field.
5. Type the correct password for the username in the Password field.
6. Type the relative path from the FTP server root directory to the directory that contains the CA certificate file in the Remote FTP Directory field.
7. Type the name of the CA certificate file in the Remote FTP File Name field.
8. Click **Submit**.
9. Verify the filename in the field.
10. Click **Submit**.
11. Restart the ACS services in **System Configuration > Service Control**.

    Note: If you skip the steps in the Download CA Certificate to your FTP Server and Install CA Certificate on your Appliance sections one of these two situations can arise:

    - You cannot enable EAP−TLS, and an error message appears to state that the server certificate is not installed even though the certificate is installed.
    - Alternatively, the `EAP type not configured` failure occurs in failed attemtps even though the EAP type is configured.

    Note: Also note that, if you used an intermediate CA to create your server certificate, you need to repeat these steps for every CA in the chain between the root CA and the server certificate (including the root CA certificate). Additionally, if you created your client certificates through a CA different from your server certificate, you must repeat these steps for the root CA and any intermediate CAs involved in client certificate creation.

Install Server Certificate on your Appliance

Complete these steps:

1. Go to **System Configuration > ACS Certificate Setup**.
2. Click **Install ACS Certificate**.
3. Select the Read certificate from file option.
4. Click the **Download certificate file** link.
5. Type the IP address or hostname of the FTP server in the FTP Server field.
6. Type a valid username that Cisco Secure ACS can use to access the FTP server in the Login field.
7. Type the correct password in the Password field.
8. Type the relative path from the FTP server root directory to the directory that contains the server certificate file in the Remote FTP Directory field.
9. Type the name of the server certificate file in the Remote FTP File Name field.
10. Click **Submit**.
11. Type the path and password for the private key. Refer to Steps 3 and 4 of the Create a Certificate Signing Request section.
12. Click **Submit**.

Other Tasks

Configure Global Authentication Settings

Complete these steps:

1. Click **System Configuration** on the ACS server.
2. Click **Global Authentication Setup**.
3. Check **Allow EAP−TLS**.
4. Select one or more certificate verification options. If you select all methods, ACS tries each method in sequence until a successful verification occurs or until the last method fails.
5. Click **Submit**.
6. Restart the PC.

Set Up the AP on the ACS

Complete these steps to set up the AP on the ACS:

1. Click **Network Configuration** on the ACS server.
2. Click **Add Entry** in order to add an AAA client.
3. Specify these values in the boxes:

    - ♦ AAA Client IP Address IP_of_your_AP
    - ♦ Key Make up a key (make sure the key matches the AP shared secret key)
    - ♦ Authenticate Using RADIUS (Cisco Aironet)
4. Click **Submit**.
5. Restart the PC.

Note: Do not change any of the defaults on the AAA client setup.

Configure the AP

Note: The network−EAP is necessary if you want to install the ACU.

If you use broadcast key rotation, you do not need to set a key as the key must already be set. If the key is not set, go to **Setup > Radio Advance** and set a value for the broadcast key rotation. You probably do not need to set this any lower then 5 minutes (300 secs). After you set the value, click **OK**, and return to the radio data encryption page.

VxWorks

Complete these steps:

1. Open the AP.
2. Choose **Setup > Security > Authentication Server**.
3. Enter the ACS IP address.
4. Enter the shared secret. This value must match the ACS key.
5. Check the **EAP Authentication** box.
6. Click **OK**.
7. Choose **Setup > Security > Radio Data Encryption**.
8. Check the **Open** box.
9. If you do not use broadcast key rotation, select **WEP key 1** and **128**.
10. Change the Use of Data Encryption by Stations to **Full Encryption** (if you cannot change this, click **Apply** first).
11. Click **OK**.

IOS AP Web Interface

Complete these steps:

1. Choose **Security > Server Manager**.
2. Choose RADIUS from the Current Server List.
3. Type the ACS IP address.
4. Type the shared secret. This value must match the key in ACS.
5. Check the **EAP Authentication** box.
6. From the EAP Authentication list, choose the RADIUS server's IP address.
7. Click **OK** on the warning dialog box.
8. Click **Apply**.

SSID Manager (WEP Encryption Only)

Complete these steps for WEP encryption only:

1. Choose the SSID from the Current SSID List, or specify a new SSID in the SSID field.
2. Check the **Open Authentication** box.
3. Choose **with EAP** from the list.
4. Check the **Network EAP** box.
5. Click **Apply**.

Encryption Manager (WEP Encryption Only)

Complete these steps for WEP encryption only:

1. Choose **Security > Encryption Manager**.
2. Click the **WEP Encryption** radio button.
3. Choose Mandatory from the list.
4. Click the **Encryption Key 1** radio button.
5. Specify the key.
6. Choose **128** from the Key Size list.
7. Click **Apply**.

Note: The configuration differs if you use WPA. See WPA Key Management supplement at the end of this document for details.

Download and Install the Root CA Certificate for the Client

This step is *required* for *each* client for EAP−TLS to work on that client. Complete these steps:

1. Browse to the CA (**http://IP_of_CA_server/certsrv/**) from the client PC.
2. Select **Retrieve a CA certificate**.
3. Click **Next**.
4. Select **Base 64 encoded**.
5. Click **Download CA certificate**.
6. Click **Open**.
7. Click **Install Certificate**.
8. Click **Next**.
9. Select **Place all certificates in the following store**.
10. Click **Browse**.
11. Check the **Show physical stores** box.
12. Expand **Trusted root certification authorities**, and select **Local Computer**.
13. Click **OK**.
14. Click **Next**.
15. Click **Finish**.
16. Click **OK** on the message box with `The import was successful` message.

Create Client Certificate

Enterprise CA

Complete these steps:

1. Browse to the CA (**http://IP_of_CA_server/certsrv/**) from the user account of the client.
2. Select the **Request a certificate** option.
3. Click **Next**.
4. Select **Advanced request**.
5. Click **Next**.
6. Select **Submit a certificate request to this CA using a form**.
7. Click **Next**.
8. Choose **User** in the Certificate Template list.
9. Set these values under Key Options:

- ♦ CSP Microsoft Base Cryptographic Provider v1.0
- ♦ Key Size¡024
- ♦ All other options Retain the default values

10. Click **Submit**.

    A message box appears with the `Your certificate request has been received...` message.

Standalone CA

Complete these steps:

1. Browse to the CA (**http://IP_of_CA_server/certsrv/**) from the user account of the client.
2. Select the **Request a certificate** option.
3. Click **Next**.
4. Select **Advanced request**.
5. Click **Next**.
6. Select **Submit a certificate request to this CA using a form**.
7. Click **Next**.
8. Type the username in the CN field. This value must match username in the authentication database.
9. Select Client Authentication Certificate for Intended Purpose.
10. Set these values under Key Options:

    - ♦ CSP Microsoft Base Cryptographic Provider v1.0
    - ♦ Key Size¡024
    - ♦ All other options Retain the default values

11. Click **Submit**.

    A message box appears with the `Your certificate request has been received...` message.

Approve the Client Certificate from the CA

Complete these steps:

1. Choose **Start** > **Programs** > **Administrative Tools** > **Certificate Authority** to open the CA.
2. Expand the certificate on the left.
3. Click **Pending Requests**.
4. Right−click on the certificate and select all tasks.
5. Select **Issue**.

Install the Client Certificate on the Client PC

Complete these steps:

1. Browse to the CA (**http://IP_of_CA_server/certsrv/**) from the user account of the client.
2. Select **Check on a Pending Certificate**.
3. Click **Next**.
4. Select the certificate.
5. Click **Next**.
6. Click **Install**.

Note: In order to verify the certificate installation, go to Microsoft Internet Explorer, and select **Tools > Internet Options > Content > Certificates**. A certificate with the name of the logged−in user ID or username must be present.

Trust the client certificate on ACS

You need to perform these steps only if the client certificates and the server certificate were created through different CAs.

1. Ensure that the root CA certificate and Intermediate CA certificates were installed as per the steps in the Install the CA Certificate on the ACS Server and Install CA Certificate on your Appliance sections.
2. Go to **System Configuration > ACS Certificate Setup** on the ACS.
3. Click **Edit Certificate Trust List**.
4. Check the box next to the root CA that created the client certificate.
5. Click **Submit**.

Setup the Client for EAP−TLS

Complete these steps:

1. Choose **Start > Control Panel > Network Connections**.
2. Right−click the wireless network, and select **Properties**.
3. Click the **Wireless Network** tab.
4. Ensure that **use windows to configure...** is checked.
5. Click **Configure** if you see the SSID in the list. If not, click **Add**.
6. Put in the SSID.
7. Check the **WEP** and **Key is provided for me automatically** check boxes.
8. Select the **Authentication** tab.

   Note: If you do not see the Authentication tab, the 802.1X service is installed in a disabled state. In order to solve this issue, you must enable the Wireless Configuration service in the list of services. Complete these steps:

   a. Right−click **My Computer**, and select **Manage**.
   b. Click **Services and Applications**.
   c. Click **Services**.
   d. Set the Startup value for the service to **Automatic**.
   e. Start the service.

   Note: If the Authentication tab is present but is unavailable, this indicates that the network adapter driver does not support 802.1x correctly. Refer to Using 802.1x authentication on client computers that are running Windows 2000 .
9. Ensure that **enable network−access control using...** is checked.
10. Select **Smart Card or Other Certificate** for EAP type, and click **Properties**.
11. Select the **Use certificate on this computer** option.
12. Check the **Use simple certificate selection** check box.
13. Check the box for the CA under Trusted root certificate.
14. Click **OK** thrice.

Machine Authentication Supplement

EAP−TLS Machine Authentication *requires* both Active Directory and an Enterprise root CA. In order to acquire a certificate for EAP−TLS machine authentication, the computer must have connectivity to the Enterprise CA either through a wired connection or through the wireless connection with 802.1x security disabled. This is the *only* way to obtain a valid machine certificate (with Machine in the Certificate Template field). When completed, the machine certificate is installed in the **Certificates (Local Computer) > Personal > Certificates** folder when viewed in the Certificates (Local Computer) MMC snap−in. The certificate contains the fully qualified AD machine name in the Subject and SAN fields. A certificate that bears the name of the computer but was not created as described in this section is *not* a true machine certificate (with Machine in the Certificate Template field). Such a certificate is not used for machine authentication but rather the OS sees such a certificate as a normal user certificate.

Setup ACS to Allow Machine Authentication

Complete these steps:

1. Go to **External User Databases > Database Configuration**.
2. Click **Windows Database**.
3. Click **Configure**.
4. Check the **Enable EAP−TLS machine authentication** check box.
5. Click **Submit**.

Configure the domain for certificate auto−enrollment

Complete these steps:

1. Open the Users and Computers MMC snap−in on a domain controller.
2. Right−click the domain entry and select **Properties**.
3. Go to the **Group Policy** tab.
4. select the **Default Domain Policy**.
5. Click **Edit**.
6. Go to **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**.
7. Right−click **Automatic Certificate Request Settings**.
8. Choose **New > Automatic Certificate Request**.
9. Click **Next**.
10. Highlight **Computer**.
11. Click **Next**.
12. Check the enterprise CA.
13. Click **Next**.
14. Click **Finish**.

Setup the Client for Machine Authentication

Join the Domain

If the client joined the domain before you configured auto−enrollment, the certificate must be issued to the machine the next time you reboot the computer after auto−enrollment is configured without the need to re−join the computer to the domain.

Complete these steps to join the domain:

1. Log into Windows with an account that has administrator privileges.
2. Right−click on **My Computer** and choose **Properties**.
3. Select the **Computer Name** tab.
4. Click **Change**.
5. Type the host−name in the Computer name field.
6. Select **Domain**.
7. Type the name of the domain.
8. Click **OK**.

   A login dialog box appears.
9. Log in with credentials of an account that has permission to join the domain.

   The computer joins the domain.
10. Restart the computer.

    The computer is now a member of the domain, and has a certificate for the CA and a machine certificate installed.

Setup EAP−TLS Supplicant for Machine Authentication

Complete these steps:

1. Choose **Start > Control Panel > Network Connections**.
2. Right−click the network connection and select **Properties**.
3. Select the **Authentication** tab.
4. Check **Authenticate as computer**.

WPA Key Management Supplement

This section is applicable to Cisco IOS AP 12.02(13)JA1, ACS 3.2, and XP SP1 with WPA hotfix. According to the documentation in this section, Windows 2000 clients do not natively support WPA key management and you must use the client software of the vendor in order to get this support. Refer to Overview of the WPA wireless security update in Windows XP .

The Cisco ACU does not support WPA key management for host−based EAP (EAP−TLS and PEAP) currently. You must install a third−party client, for example, the Funk Odyssey client or Meetinghouse AEGIS client. Refer to Wireless LAN Adapter Documents for Windows for further information on WPA support for Cisco products. This information is applicable to Windows Mobile 2003 (Pocket PC) clients also.

WPA key management is basically the same, but differs in these two procedures:

1. Configure the AP.
2. Set up the XP Client for EAP−TLS and WPA.

Configure the AP

Complete these steps:

1. Go to **Security > Encryption Manager**.
2. Click the **WEP Cipher** option.
3. Choose **TKIP**.
4. Click **Apply**.

5. Go to **Security > SSID Manager**.
6. Choose the SSID from the Current SSID List. Alternatively, you can specify a new SSID in the SSID field.
7. Check **Open Authentication**.
8. Choose **with EAP** from the list.
9. Check **Network EAP**.
10. Select **Mandatory** from the list under Authenticated Key Management.
11. Click **WPA**.
12. Click **Apply**.

Set up the XP Client for EAP−TLS and WPA

Complete these steps:

1. Choose **Start > Control Panel > Network Connections**.
2. Right−click the wireless network, and select **Properties**.
3. Select the **Wireless Network** tab.
4. Ensure that the **use windows to configure** option is checked.
5. Click **Configure** if you see the SSID in the list. If not, click **Add**.
6. Put in the SSID.
7. Choose **WPA** for Network Authentication.
8. Choose **TKIP** for Data Encryption.
9. Select the **Authentication** tab.
10. Ensure that **enable network−access control using** is checked.
11. Select **Smart Card or Other Certificate** for EAP type.
12. Click **Properties**.
13. Select the **Use certificate on this computer** option.
14. Check the **Use simple certificate selection** check box.
15. Check the box for the CA under Trusted root certificate.
16. Click **OK** thrice.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General

Related Information

- **Cisco Secure ACS for Windows Support Page**
- **Documentation for Cisco Secure ACS for Windows**
- **Cisco Secure ACS for UNIX Support Page**
- **Documentation for Cisco Secure ACS for UNIX**
- **Technical Support & Documentation − Cisco Systems**

Updated: May 15, 2006 Document ID: 64064