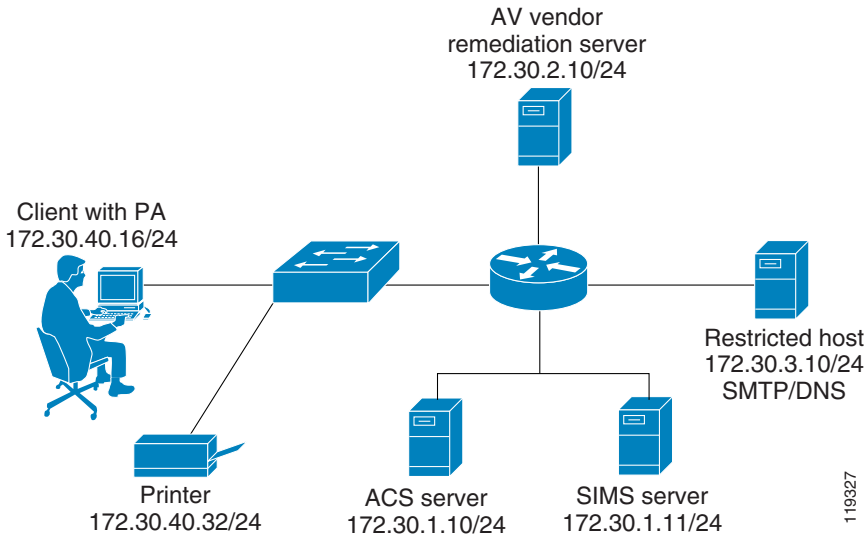
Implementing Network Admission Control

This chapter describes how to implement Network Admission Control (NAC) and includes the following sections:

Network Topology

Figure 2-1 shows the network that is used for the deployment example in this chapter.

Figure 2-1 Network Topology for Test Setup



Configuration Overview

The installation of NAC components can be completed in any order because there are no installation dependencies between the various components. However, perform the configuration of the NAD last, because traffic through the router interface performing NAC is blocked until the CTA and Cisco Secure ACS installations and configuration have been completed. NAC consists of the following components:

- Cisco Secure ACS
- Cisco Trust Agent (CTA)
- Network Access Device (NAD), which is a Cisco IOS router that separates protected and unprotected networks
- Anti-virus vendor software, along with any remediation server software if that has been supplied by the AV vendor

Installing and Configuring the Cisco Secure ACS Server

The following sections detail the installation (where required) and configuration of the individual components that comprise the NAC feature, and include the following topics:

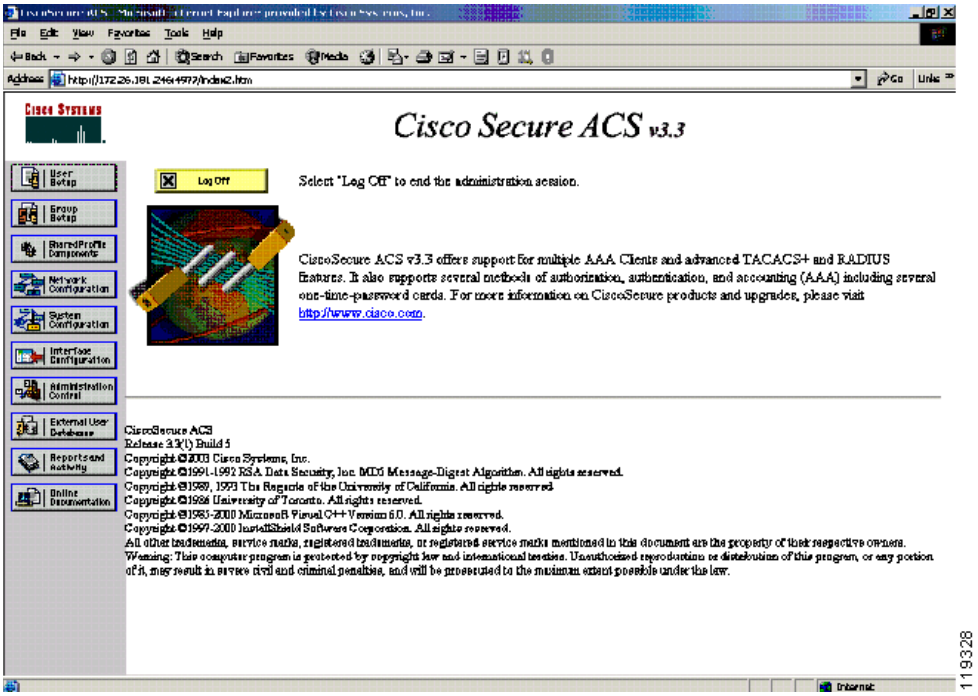
Installing Cisco Secure ACS

To install Cisco Secure ACS version 3.3 software on a machine running a supported operating system, run the setup.exe program provided with the Cisco Secure ACS installation software. When you install Cisco Secure ACS, the Setup program uninstalls any previous version of Cisco Secure ACS before it installs the new version. If you have a previous version, you are given the option to save and reuse your existing configuration.

The following sections describe how to set up Cisco Secure ACS for NAC. User authentication and authorization using TACACS+ or RADIUS and configuration of Cisco Identity-Based Networking Services (IBNS) or 802.1X is not covered and may be found in the Cisco Secure ACS user guide located at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm

You configure Cisco Secure ACS using a web interface. The Welcome window is shown in Figure 2-2.

Figure 2-2 Cisco Secure ACS Welcome Window



Use the buttons on the Cisco Secure ACS main menu, located on the left frame of this window, to select a specific configuration task. This guide describes only the specific configuration that is required for implementing NAC.

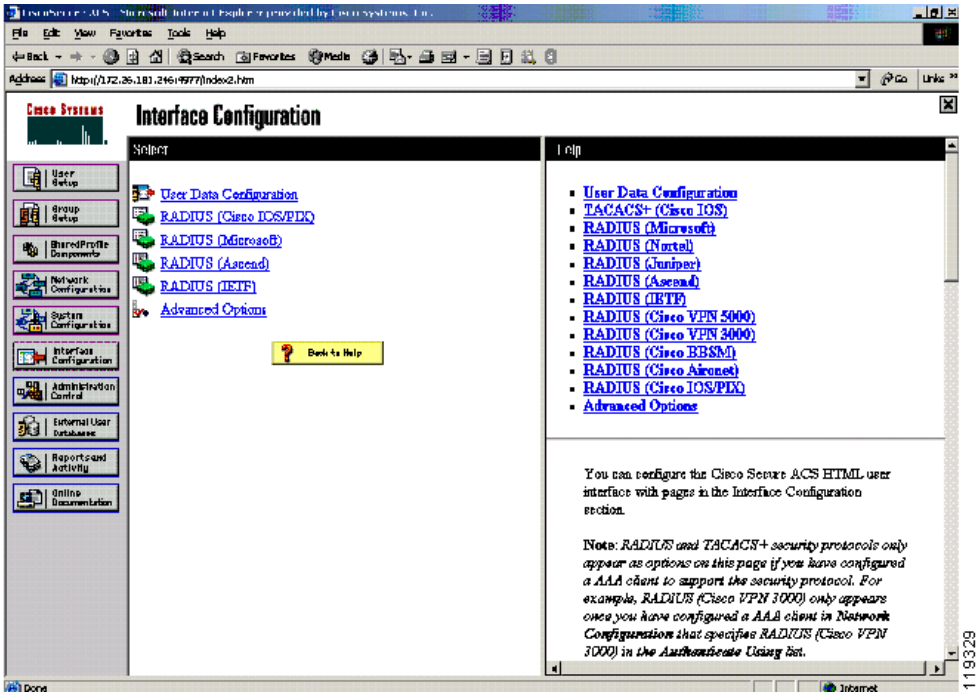
Configuring the Administrator Interface to Cisco Secure ACS

The Cisco Secure ACS administrator windows are missing some necessary options by default. This is done to un-clutter the administrator windows from options that are not normally used. For the NAC solution to work, some of these configuration windows need to be enabled. These windows are used by Cisco Secure ACS to send enforcement actions to the NAD. To enable the appearance of the enforcement action windows in the Cisco Secure ACS administrator interface, perform the following steps:

Step 1 Click **Interface Configuration** on the Cisco Secure ACS main menu.

The system displays the window shown in Figure 2-3.

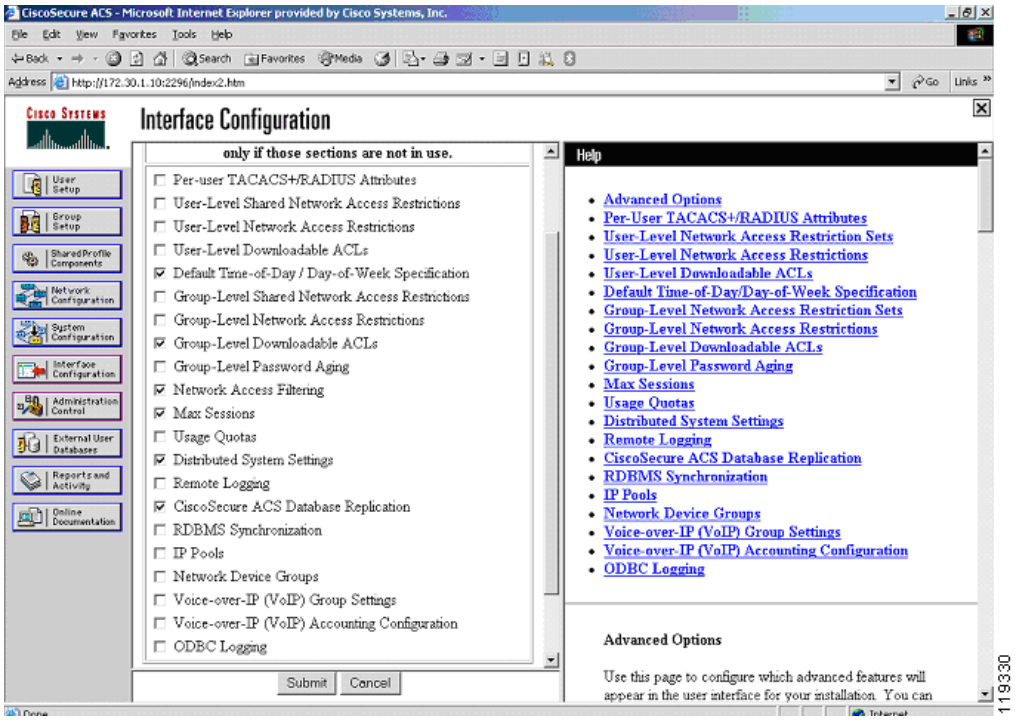
Figure 2-3 Interface Configuration Main Menu



Step 2 Click **Advanced Options** in the middle frame in this window.

The system displays the window shown in Figure 2-4.

Figure 2-4 Interface Configuration Advanced Options



Step 3 Enable the following options in this window:

- Group-Level Downloadable ACLs—This enables the appearance of the downloadable ACLs option in the Shared Profile Components and Group Setup windows. These are used to cause Cisco Secure ACS to send network access policies to the NAD to be applied on a client undergoing NAC.
- Network Access Filtering—This option enables the appearance of the network access filtering option under the Shared Profile Components window. This allows a network to have differing enforcement policies downloaded for application to a client in a particular state depending on where in the network the client is located. For instance, if multiple remediation servers are present in a network, it is best to send a client in a quarantined state to the closest remediation server for its software update.

Step 4 After checking these check boxes, click **Submit**.

This adds the downloadable ACLs configuration option and the network access filters configuration option to the Shared Profile Components window. These options are necessary for the configuration of the enforcement actions taken by the NAD.

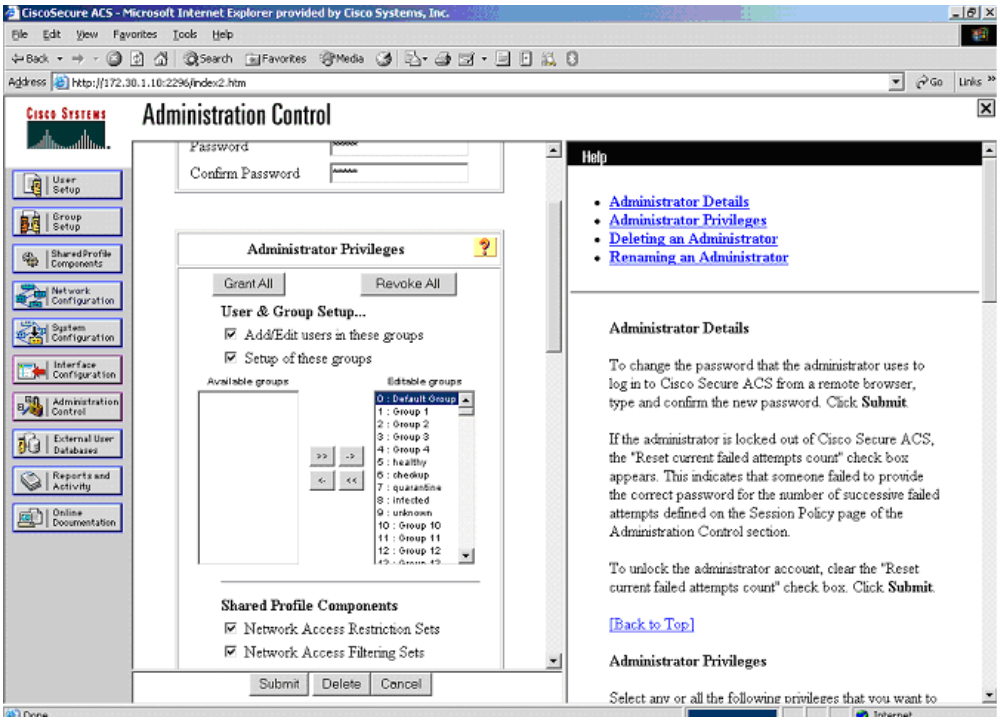
Allowing Administrator Access Via HTTP

To enable remote Cisco Secure ACS configuration through the web interface, you must configure at least one administrator username and password. To do this, perform the following steps:

Step 1 Click **Administration Control** on the Cisco Secure ACS main menu.

The system displays the window shown in Figure 2-5.

Figure 2-5 Administrator Privileges



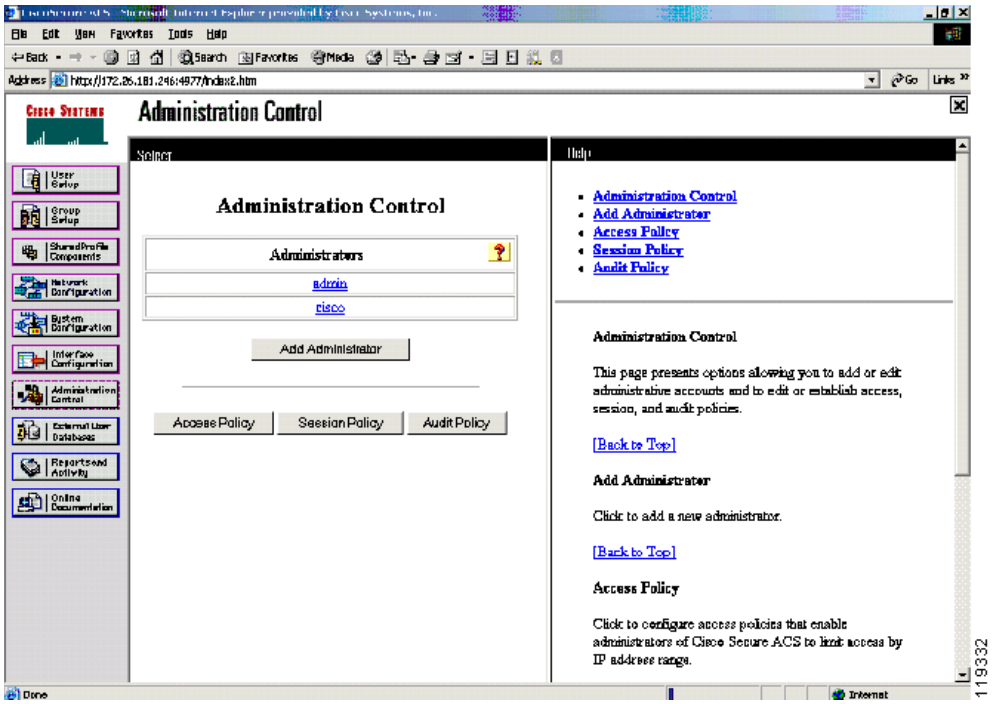
Step 2 Click **Add Administrator**. Fill in the username and password fields, and then configure the individual administration group privileges as needed.

Step 3 Click **Grant All** to give all configuration rights to the administrator being configured.

If desired, the privileges for an individual administrator can be limited to individual groups and components. This can have the effect of placing separate administrators over different parts of the network and network policies.

The system displays the window shown in Figure 2-6.

Figure 2-6 Administration Control



Step 4 Click **Submit** to complete the process.

Installing the Cisco Secure ACS Server Certificate

Protected EAP and the NAC feature require the use of certificates on Cisco Secure ACS and on the clients running CTA. The certificate installation process must be completed and Cisco Secure ACS restarted before beginning the PEAP configuration.

Cisco Secure ACS uses the certificate store that is built into the Windows operating system. The server certificate may be installed in several ways. If the public and private key pair to be used for the server certificate are generated on an external server, the certificate is installed by copying the files to the Cisco Secure ACS server and completing a series of forms. This example uses a certificate and a private key from a certificate authority named “Stress”. These consist of three files: a CA certificate file named “ca.cer”, a server certificate named “server.cer” to be used with the Cisco Secure ACS, and a private key file to be used with the Cisco Secure ACS named “private.pvk”. Your file names may vary.

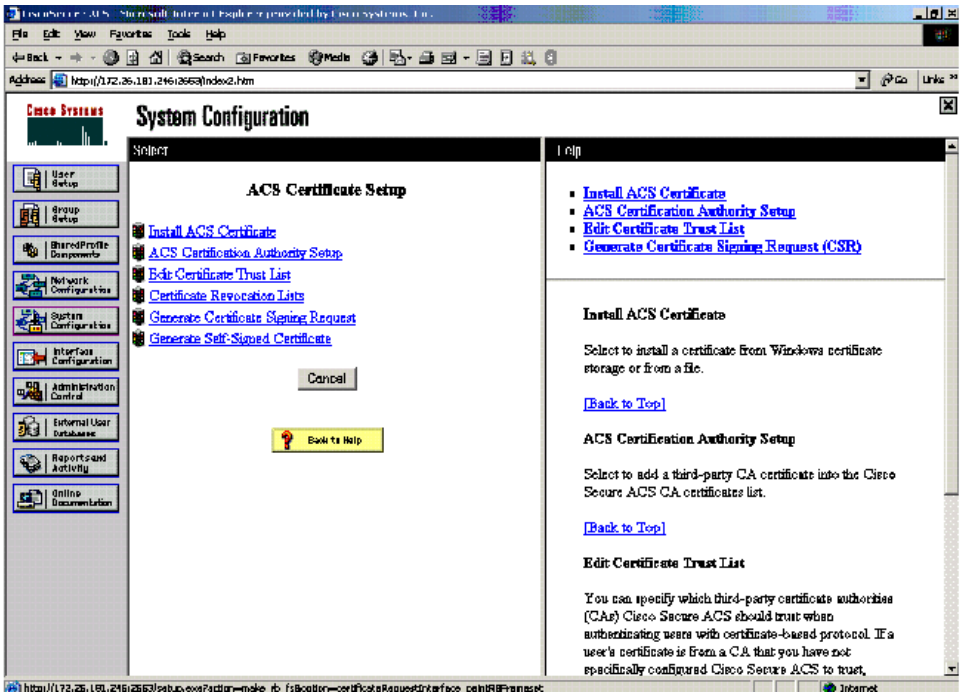
To install a public/private key pair that are generated on an external server, perform the following steps:

Step 1 Copy the public/private key pair files to a directory accessible to the Cisco Secure ACS server.

Step 2 On the System Configuration menu, click **Cisco Secure ACS Certificate Setup**.

The system displays the window shown in Figure 2-7.

Figure 2-7 ACS Certificate Setup



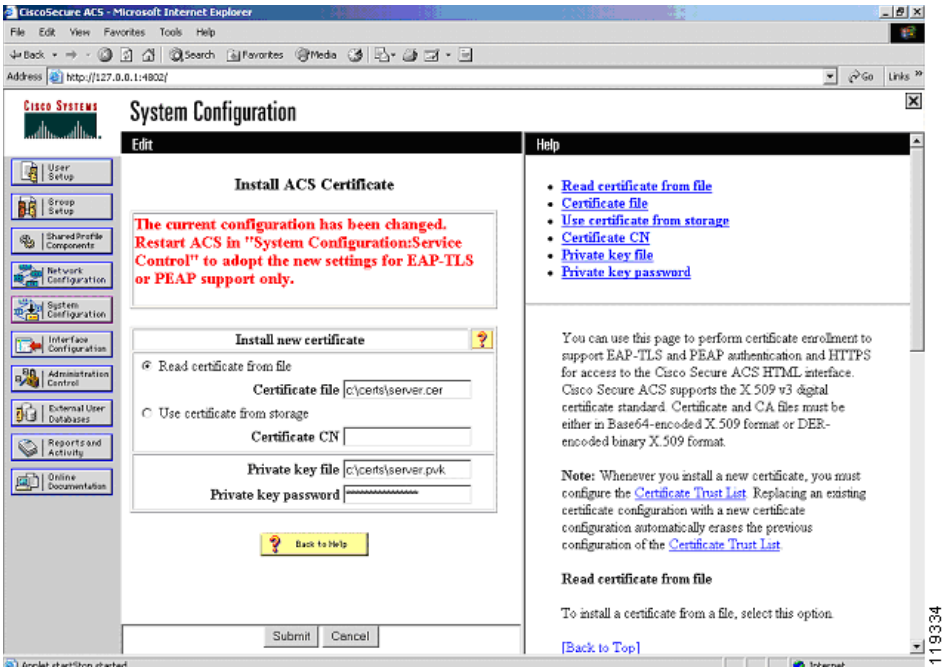
You perform all certificate management operations from this window.

If a set of externally generated private keys and certificates is to be installed, those files need to have been already copied to an accessible folder on the machine running Cisco Secure ACS.

Step 3 Click **Install Cisco Secure ACS Certificate**.

The system displays the window shown in Figure 2-8.

Figure 2-8 Install ACS Certificate

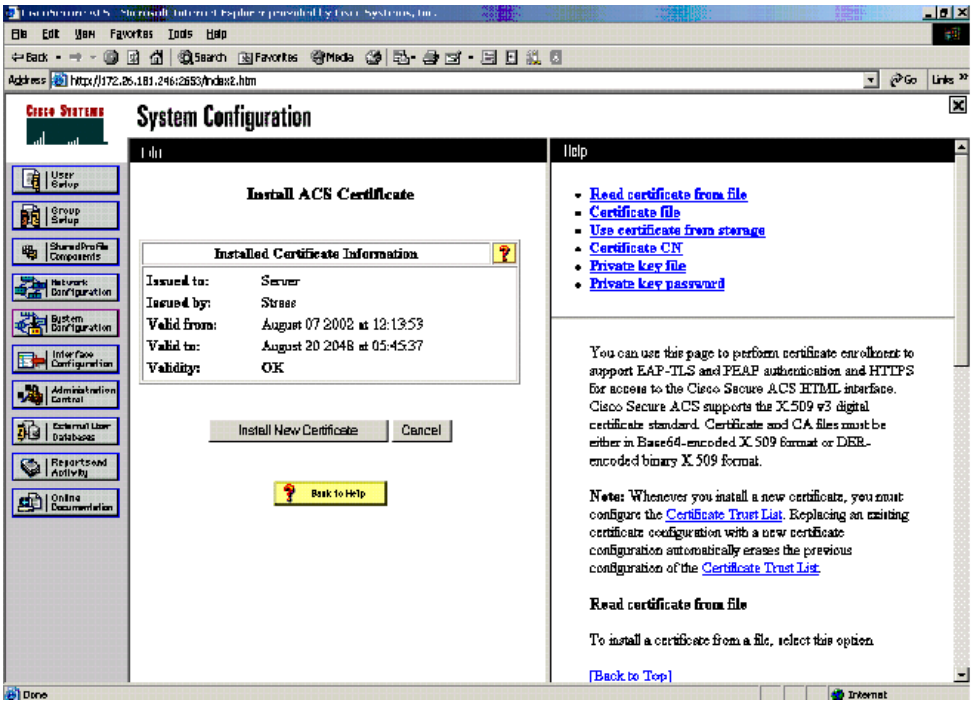


Step 4 Enter the file locations for the certificate file and the private key file and a password for the private key file if required.

Step 5 Click **Submit**.

The system displays the window shown in Figure 2-9.

Figure 2-9 Installed Certificate Information



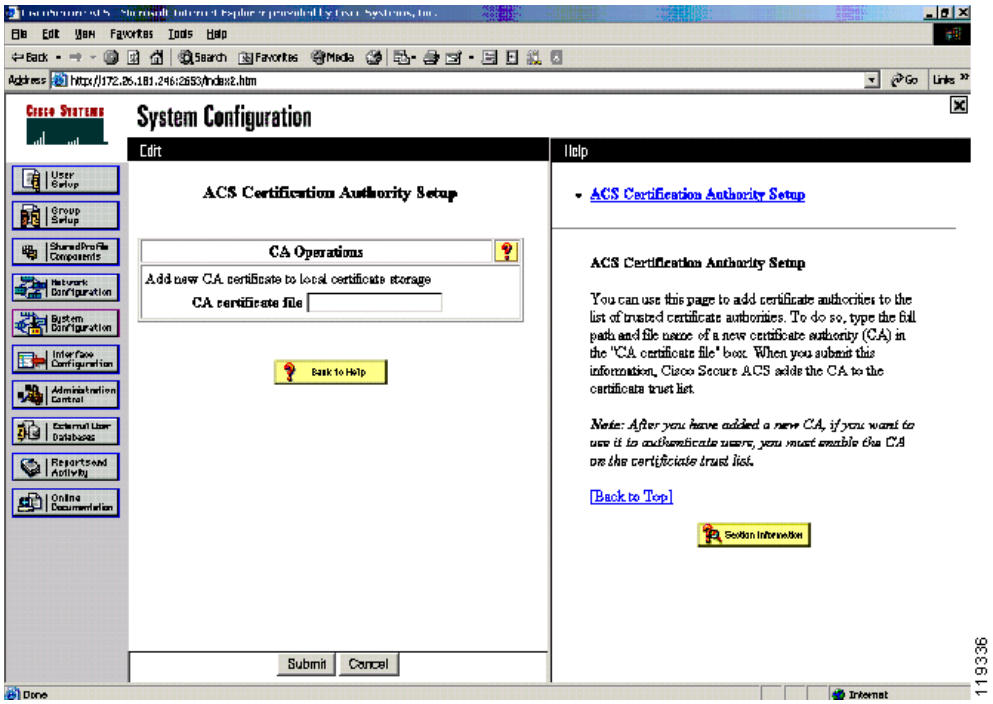
Step 6 To install the CA certificate, click **System Configuration** on the Cisco Secure ACS main menu.

Step 7 In the window that appears, click **Cisco Secure ACS Certificate Setup**.

Step 8 Click **Cisco Secure ACS Certificate Authority Setup**.

The system displays the window shown in Figure 2-10.

Figure 2-10 ACS Certification Authority Setup



Step 9 Enter the drive and directory where the CA certificate file was saved.

Step 10 Click **Submit**.

The certificate trust list must have the root certificate added.

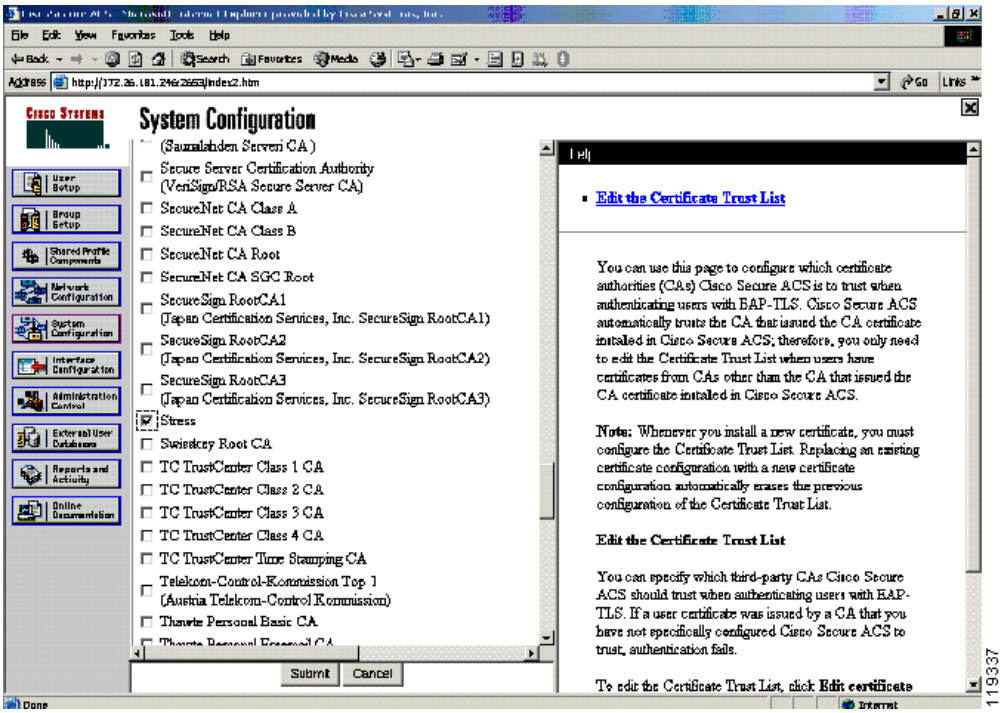
Step 11 To add the stress CA certificate to the trusted list, click **System Configuration** on the Cisco Secure ACS main menu.

Step 12 Click **Cisco Secure ACS Certificate Setup**

Step 13 Click **Edit Certificate Trust List**.

The system displays the window shown in Figure 2-11.

Figure 2-11 Edit the Certificate Trust List



Step 14 Ensure that the check box for the CA to be used is checked.

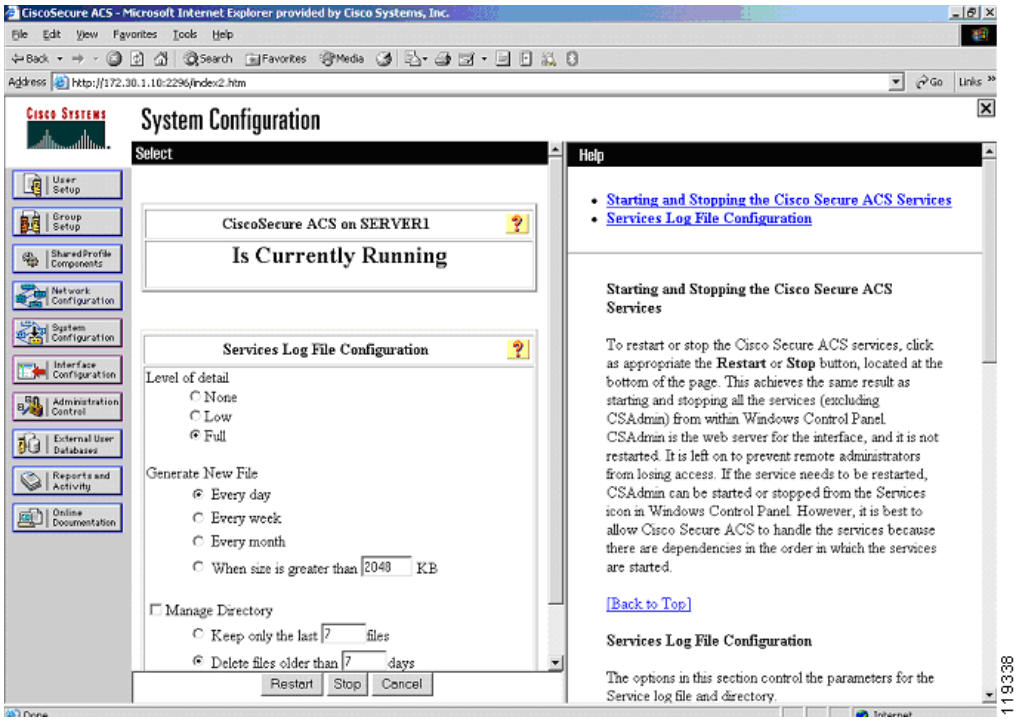
Step 15 Restart Cisco Secure ACS.

Step 16 Click **System Configuration** on the Cisco Secure ACS main menu.

Step 17 Click **Service Control.**

The system displays the window shown in Figure 2-12.

Figure 2-12 Services Log File Configuration



Step 18 Click **Restart**.

Wait until the browser refreshes. Cisco Secure ACS has been successfully restarted.

Generating Signing Request, Enrolling and Installing Certificate

To use a private CA for enabling PEAP between the CTA client and the Cisco Secure ACS server, the Cisco Secure ACS server needs to generate a signing request and have the resulting key enrolled in the CA. You then install the private CA certificate on the Cisco Secure ACS server using the procedure described in Installing the Cisco Secure ACS Server Certificate, page 2-7. Then configure Cisco Secure ACS to trust the private CA and install the CA certificate on all the client machines participating in NAC.

To use a certificate from a private CA, perform the following steps:

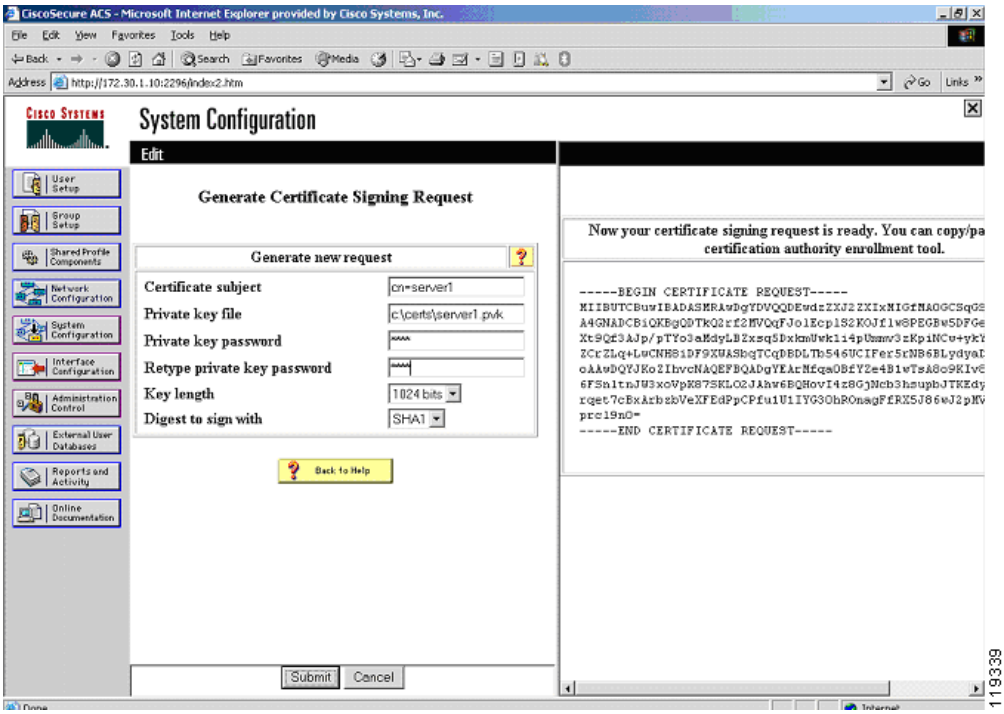
Step 1 In the Cisco Secure ACS Certificate Setup window, click **Generate Certificate Signing Request**.

Step 2 Fill in the blanks with the appropriate information according to your own installation.

Step 3 Click **Submit.**

The system displays the window shown in Figure 2-13.

Figure 2-13 Generate Certificate Signing Request



The private key is stored in the subdirectory and file that you entered.

The right frame in this window is the actual signing request ready for pasting into the CA certificate request. This signing request should then be transferred to the CA and the steps for enrollment completed. Please see the documentation provided with your CA for specific details on the enrollment process.

Using a Self-Signed Certificate

Cisco Secure ACS version 3.3 also allows the generation of a self-signed certificate. A self-signed certificate is useful when no CA or other trust authority is required. The self-signed certificate from the Cisco Secure ACS server is required for installing CTA on each client.

To use a self-signed certificate, perform the following steps:

Step 1 Click **Generate Self-Signed Certificate** in the Cisco Secure ACS Certificate Setup window.

Step 2 Fill in the blanks with the appropriate information according to your own installation.

Step 3 Ensure that you enable **Install generated certificate**.

Step 4 After completing the certificate setup process, restart Cisco Secure ACS.

After generating and installing the self-signed certificate, include the certificate file as part of the install process for each client installing CTA.

Configuring Logging

Logging configuration is crucial for monitoring, reporting, and troubleshooting a NAC implementation. In addition to the local logging being configured here, the fields that you select are sent by the Security Information Management Solution (SIMS) agent that resides on Cisco Secure ACS to the SIMS management tool.

To set up logging, perform the following steps:

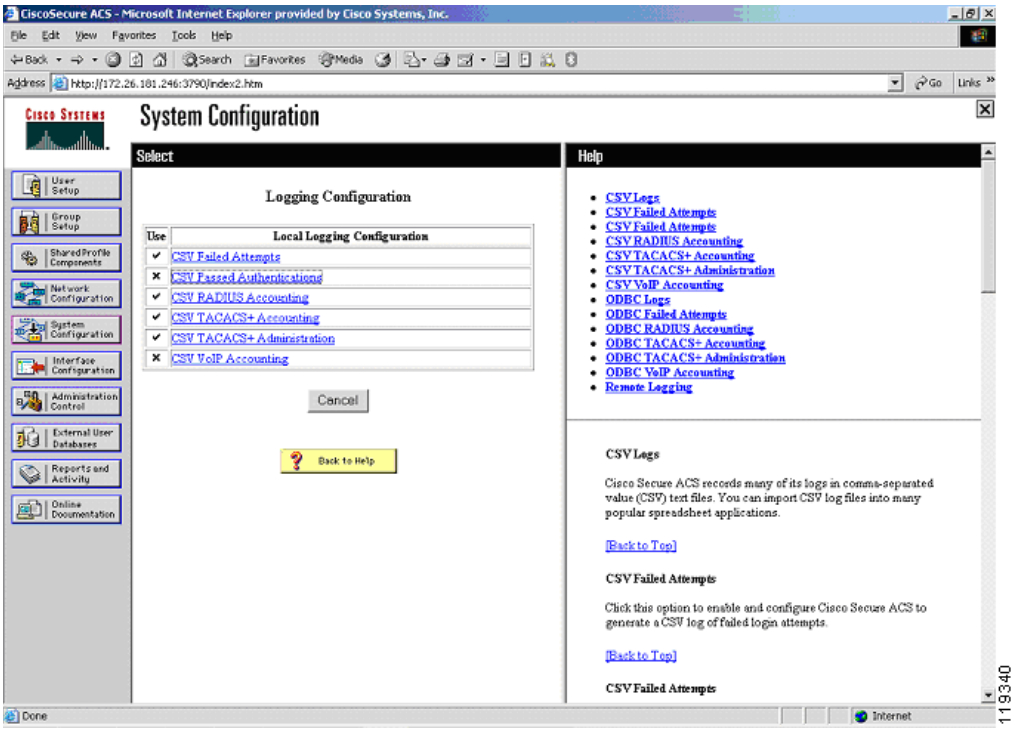
Step 1 Click **System Configuration** on the Cisco Secure ACS main menu.

Click **logging**.

Click **CSV Passed Authentications**.

The system displays the window shown in Figure 2-14.

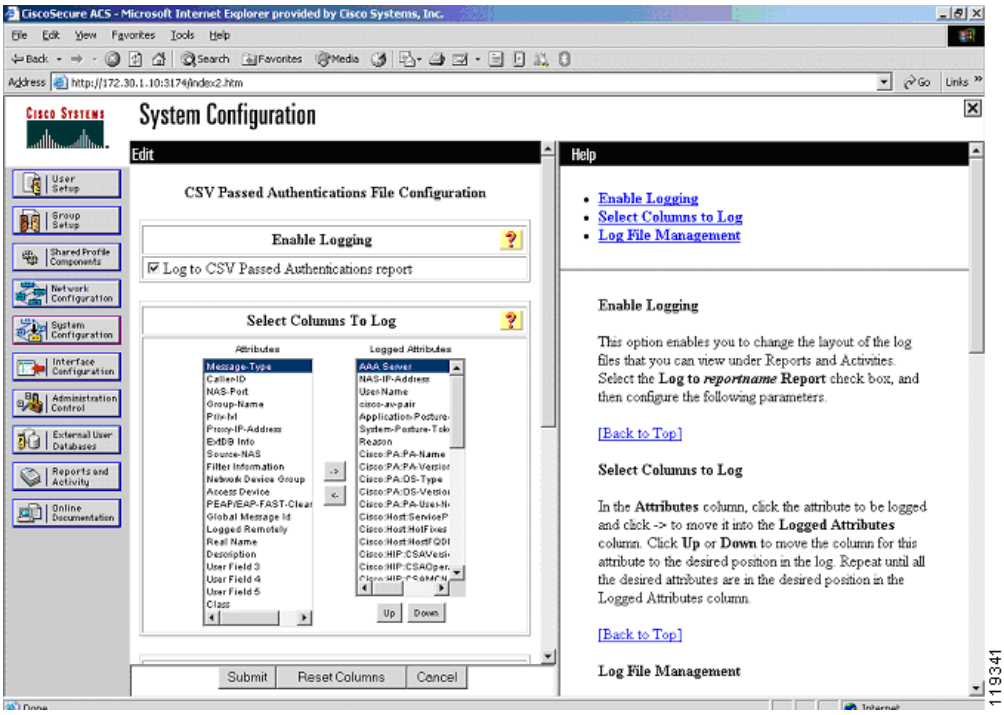
Figure 2-14 Logging Configuration



Step 2 Click **Log to CSV Passed Authentications**.

The system displays the window shown in Figure 2-15.

Figure 2-15 Enable Logging



Step 3 Enable the **Log to CSV Passed Authentications report**.

Step 4 In the Select Columns To Log list, select the attributes (fields) that you wish to include in the log file.

Useful fields to include in the logs include Reason, Application Posture Token, and System Posture Token. These should be moved towards the top of the list of installed attributes for easy access.

You must include the AAA Server field for SIMS to correctly parse the log output from Cisco Secure ACS.

The NAS-IP-Address and User Name fields also provide valuable information during troubleshooting.

The SIMS agent that resides on Cisco Secure ACS sends these fields to the SIMS server, with the SIMS server providing correlation and alerting functions.

You can include other fields as you like.

During initial setup, include the attribute values from the credentials. This makes writing the rules much easier. You can remove the attribute fields after initial configuration and troubleshooting. However, if they are removed, these fields do not appear in SIMS logs.

All client instances successfully completing the posture validation process are logged in the passed authentications log even if the client has posture validated into a state other than healthy. The failed authentication attempts log contains entries for clients failing to complete the posture validation process.

Step 5 Scroll down the window and change the file management settings if desired.

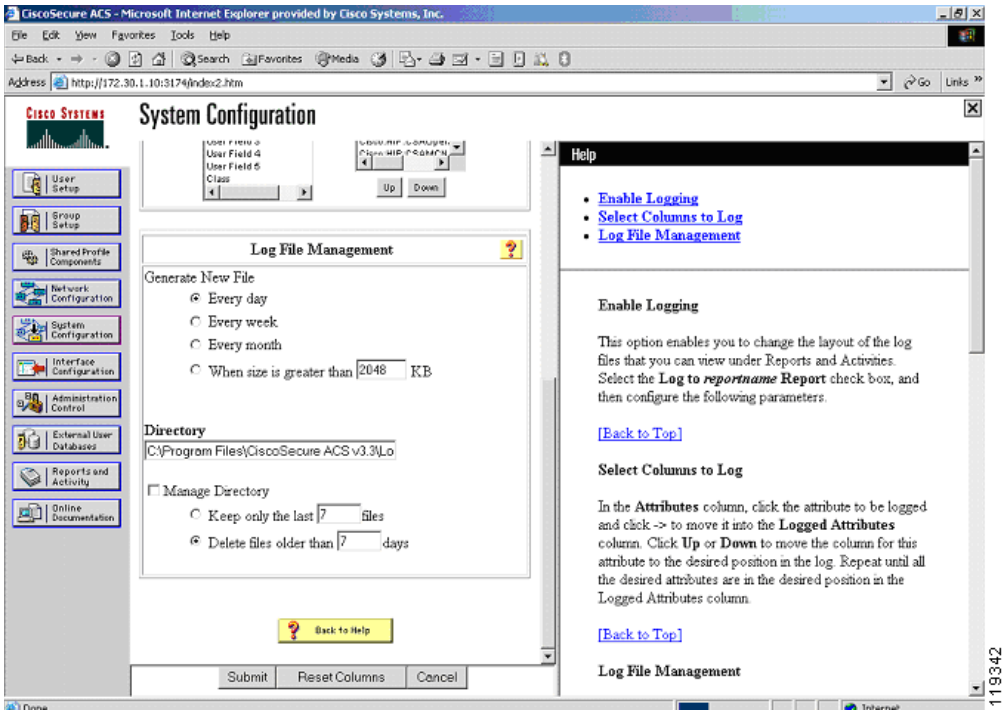
Step 6 Click **Submit**.

Step 7 Click **System Configuration** again on the Cisco Secure ACS main menu.

Step 8 Click **Service Control**.

The system displays the window shown in Figure 2-16.

Figure 2-16 Log File Management



Step 9 Change the service log file configuration to **Level of Detail = Full**

Step 10 Increase the file size from 2048 Kb as necessary.

Step 11 Click **Restart** to apply the new configuration.

Configuring a NAD in Cisco Secure ACS

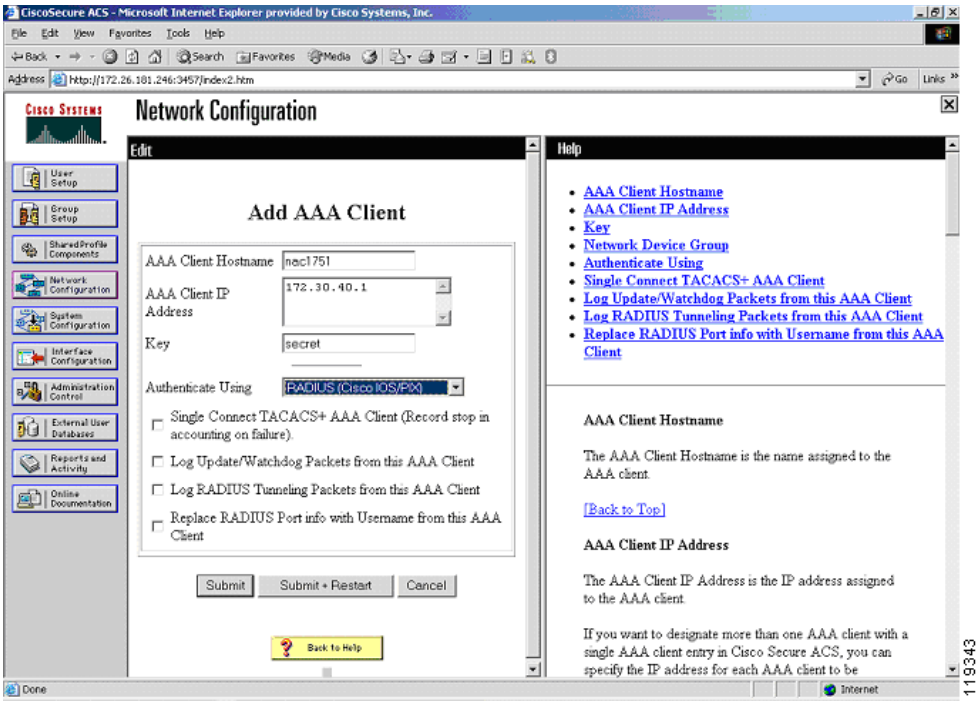
In Cisco Secure ACS terminology, a NAD is a AAA client.

To add a AAA client (NAD), perform the following steps:

Step 1 Click **Network Configuration** on the Cisco Secure ACS main menu.

Step 2 The system displays the window shown in Figure 2-17.

Figure 2-17 Add AAA Client



Step 3 Click **add entry** under the AAA clients table.

Step 4 Add the name of the NAD, the IP address from which the RADIUS packets will be sourced on that device, and the RADIUS key that was (or will be) used in the devices configuration. In the Authenticate Using window, select RADIUS (Cisco IOS/PIX).

Step 5 Click **Submit**.

If there are multiple NADs, complete Step 2 through Step 4 for each NAD.

Step 6 After configuring the last NAD, restart AAA services.

To restart, click **Submit + Restart** or click **System Configuration** from the Secure ACS main menu, then click **Service Control**, and finally click **Restart** at the bottom of the window.

Configuring Network Access Filters

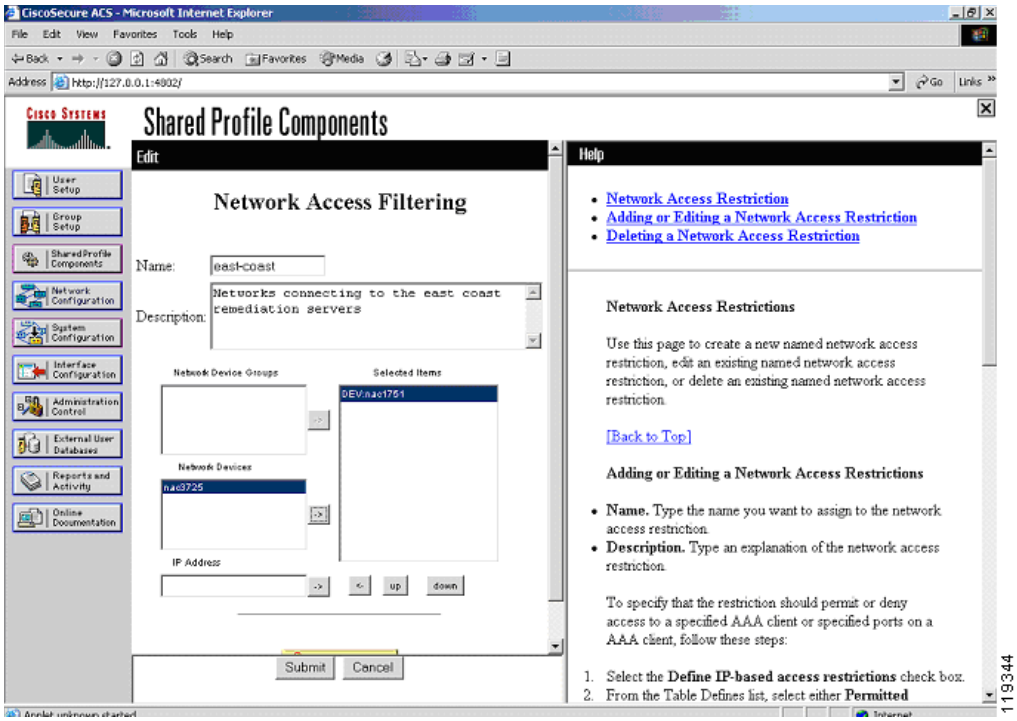
You can vary a downloadable ACL based on the NAD to which it is being downloaded. You might do this when remediation servers have been placed throughout the network and you want clients to connect to the closest remediation server. To do this, use Network Access Filtering (NAF). This feature allows you to control access easily by NAD and ensure that the client connects to the closest remediation server.

To configure a NAF, complete the following steps:

Step 1 In the Shared Profile Components window, click **Network Access Filters**.

The system displays the window shown in Figure 2-18.

Figure 2-18 Network Access Filtering



Step 2 Enter an appropriate name and description for the purpose of this instance of NAF.

An appropriate name might be east-coast or something similar that defines the portion of the network to which this NAF applies.

Step 3 Add the NADs, or if you are using network device groups in your configuration, add the appropriate network device groups.

Step 4 Click **Submit** to save your configuration.

The configuration of Downloadable IP ACLs differs slightly when you use NAFs in your configuration.

Configuring Downloadable IP ACLs

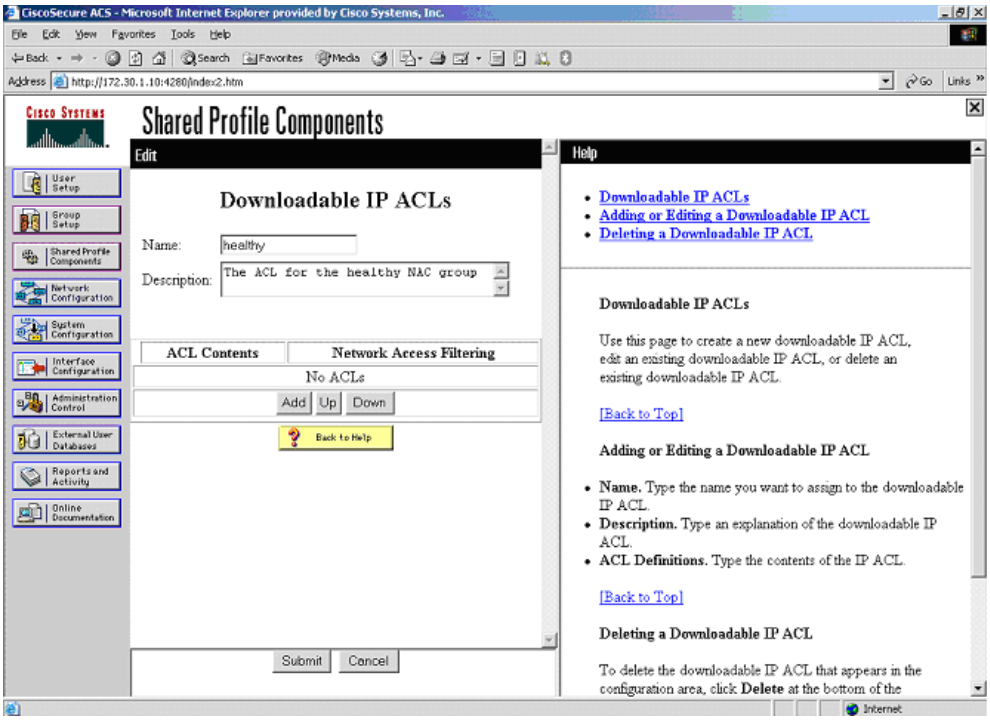
The enforcement action taken by the NAD is configured through Downloadable IP ACLs. Each category into which a client is validated must have a matching downloadable ACL associated with it. The access control entries contained in each ACL depend on your own network configuration and the access policy put in place by the network administrator. To configure downloadable IP ACLs, complete the following steps:

Step 1 Click **Shared Profile Components** on the Secure ACS main menu.

Step 2 Click **Downloadable IP ACLs** from the resulting menu.

The system displays the window shown in Figure 2-19.

Figure 2-19 Downloadable IP ACLs

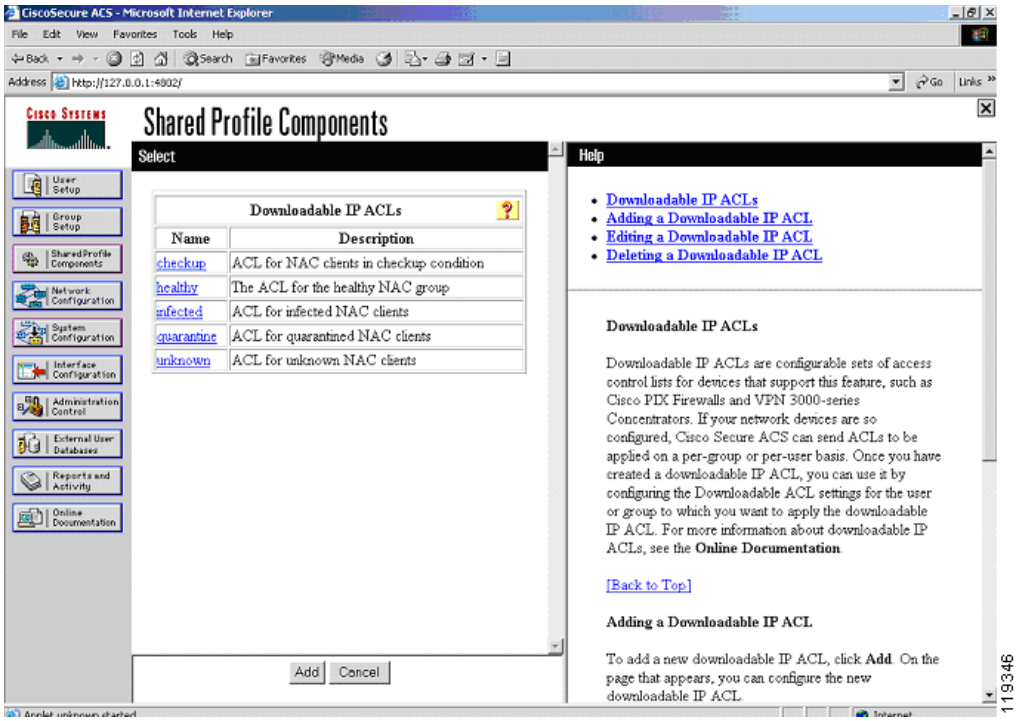


Step 3 Create an ACL for each client condition for which you wish to check: Healthy, Checkup, Quarantine, Infected, and Unknown.

Step 4 Enter a name and a description for an access list for each condition.

The system displays the window shown in Figure 2-20.

Figure 2-20 Defining the Downloadable IP ACL Type



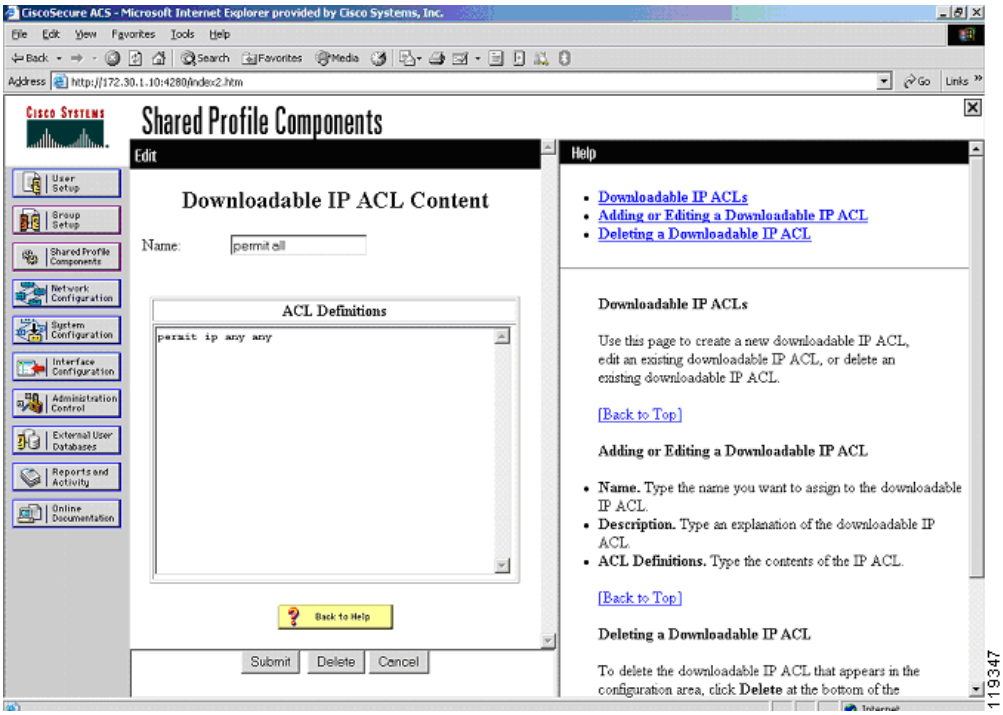
After creating the downloadable ACLs for each condition, define the ACLs that are actually sent to the individual NADs for enforcement action. The ACL elements vary depending on the policy set by the individual network administrator.

Step 5 Click the title of each downloadable ACL and enter a name for each ACL particular condition.

If NAFs are not being used in your network, the name of the ACL can be the same as the name of the condition for which this ACL is associated.

The system displays the window shown in Figure 2-21.

Figure 2-21 Defining an Access Control Entry



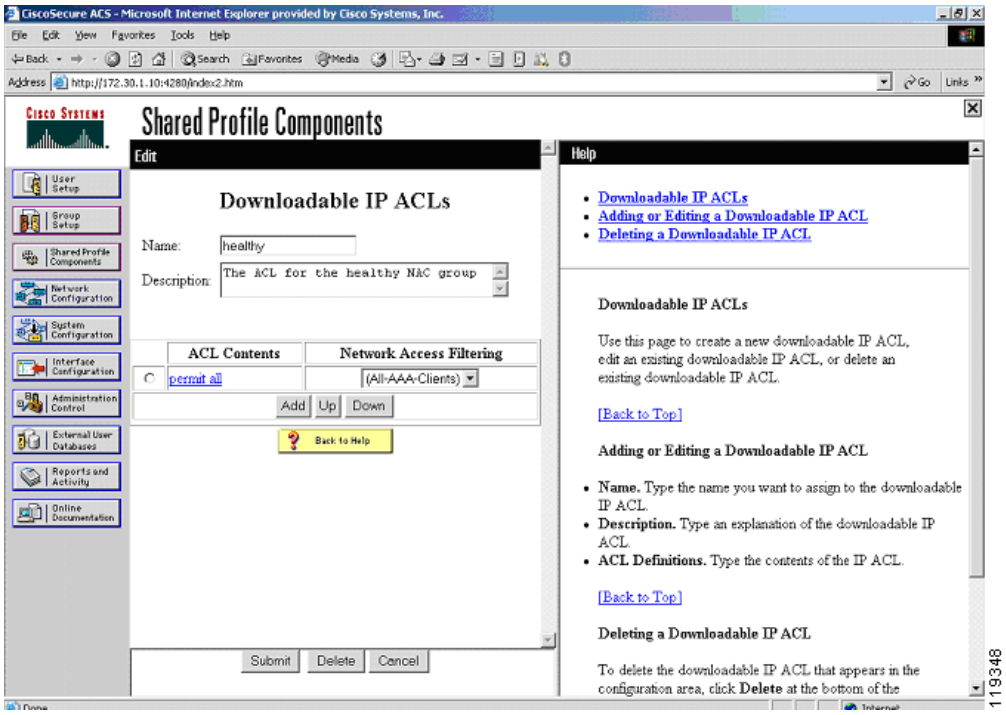
An example of the syntax for the ACL is **permit ip** *any any*. The first "any" in the ACL entry is replaced with the IP address of the host undergoing admission control to which this ACL is being applied. These ACLs are applied "over" the interface ACL. The downloadable IP ACL takes precedence over the interface ACL because the client source IP address is matched first.

Step 6 Click **Submit** after completing the entries in an ACL.

Step 7 Click **Submit** in the resulting window to save the downloadable ACL.

The system displays the window shown in Figure 2-22.

Figure 2-22 Completed ACL



Repeat this process for each ACL. Generally, ACLs should become more restrictive as the token returned in the credential drops in postured condition.

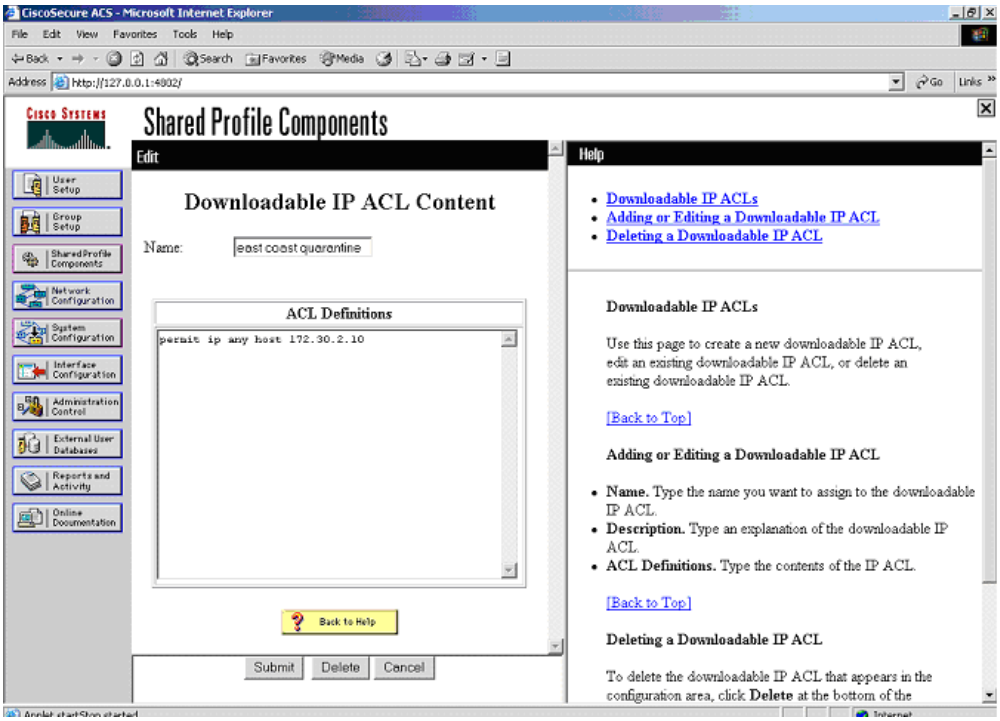
The next example for the quarantine ACL permits access only to the AV remediation server. NAFs are used to cause hosts in one section of the network to contact the closest remediation server.

Step 8 Click **quarantine** previously created from the Downloadable IP ACLs window.

Step 9 Enter a descriptive name for the instance of this ACL; for example, “east coast quarantine”.

The system displays the window shown in Figure 2-23.

Figure 2-23 Adding a Quarantine IP ACL



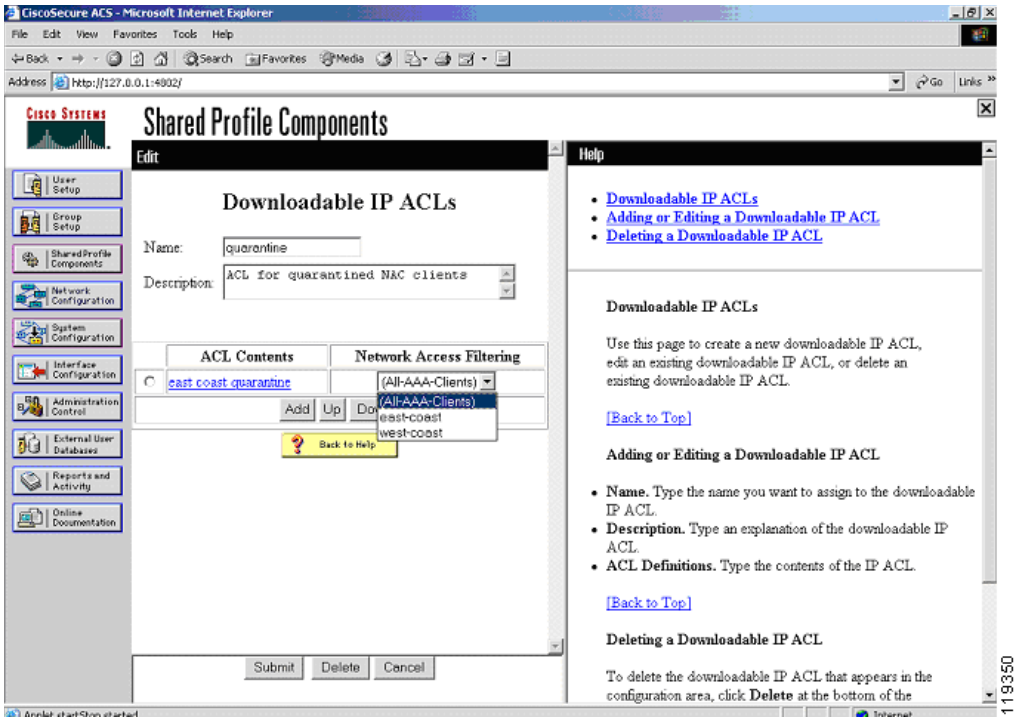
Step 10 Enter the individual lines for the ACL being written.

Step 11 Click **Submit** after completing each window.

Note Do not use the buttons on the Cisco Secure ACS main menu to go to another section, because your entries are not saved unless you click **Submit** after completing each window.

The system displays the window shown in Figure 2-24.

Figure 2-24 Selecting the Filter List



Because the quarantine example uses NAFs, select the set of devices to which this ACL applies.

Step 12 Pick the appropriate filter list from the drop-down list.

Step 13 If NAFs are not being used, select **All-AAA-Clients**.

These ACLs are "inserted" over the top of the interface ALC that is configured and applied to the router interface that participates in the posturing process to block traffic.

Configuring Groups and Vendor Specific Attributes

The group configuration section of Cisco Secure ACS is where actions and attributes are sent to the NAD. This causes any configured enforcement action to be taken by the NAD.

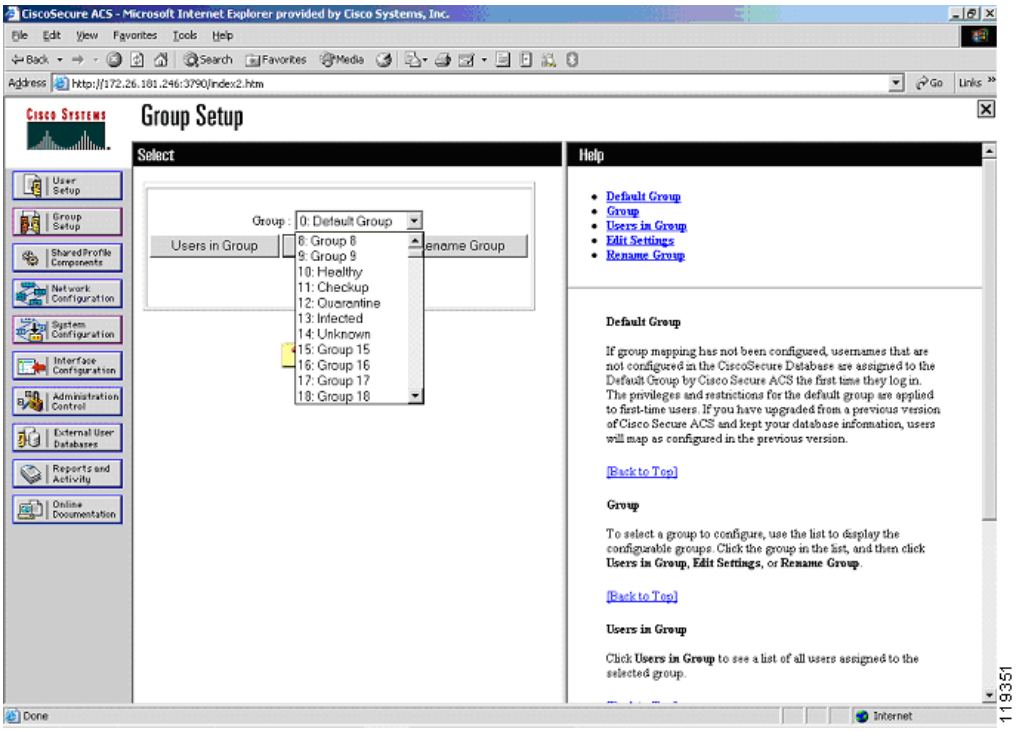
To configure groups and vendor specific attributes, complete the following steps:

Step 1 Click **Group Setup** on the Cisco Secure ACS main menu.

Step 2 Choose the group numbers that correspond to the following conditions: Healthy, Checkup, Quarantine, Infected, and Unknown.

The system displays the window shown in Figure 2-25.

Figure 2-25 Group Setup



The initial group numbers are not important, so any unused groups can be used. For clarity, rename each group for its corresponding condition.

Step 3 For each NAC group, click **Edit Settings**.

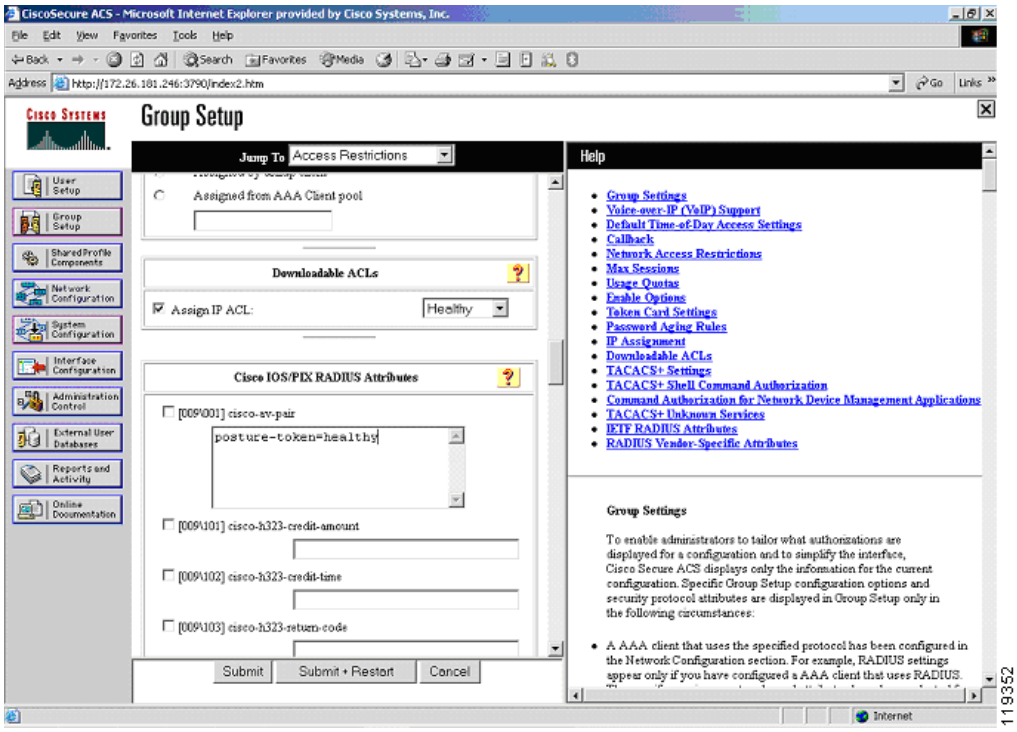
Step 4 Scroll down the edit window to the Downloadable ACLs window.

Step 5 Check the **Assign IP ACL** check box and select the proper access list for the condition to which the group relates.

Step 6 For each group configured, scroll down to the Cisco IOS software/PIX RADIUS Attributes section.

The system displays the window shown in Figure 2-26.

Figure 2-26 Defining an Attribute-Value Pair



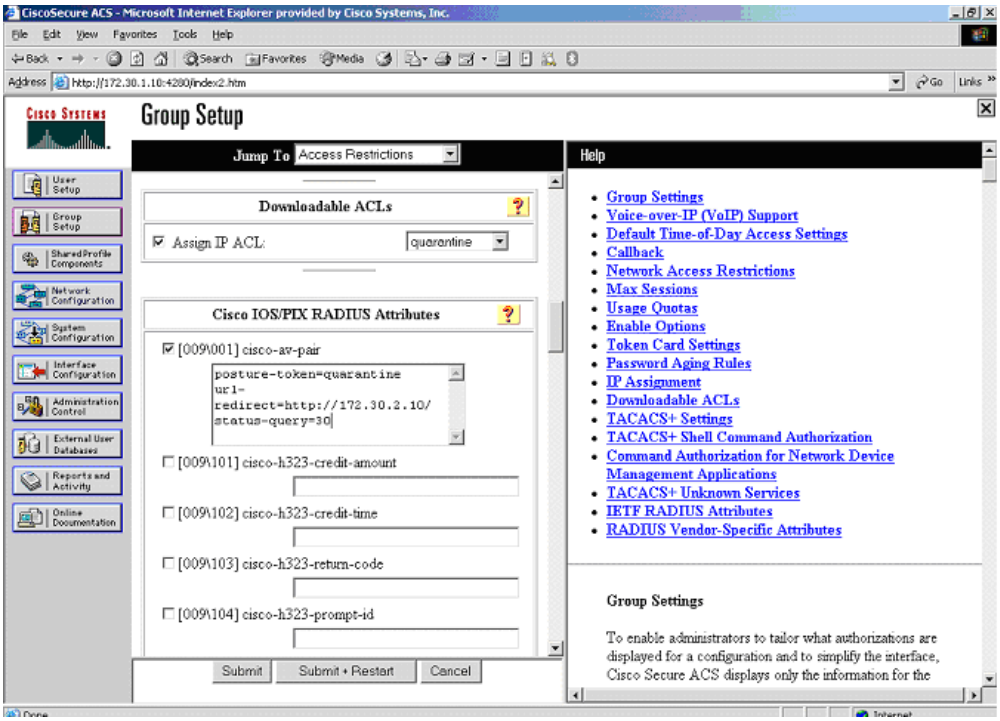
Step 7 In the [009/001] cisco-av-pair window, check the associated check box and enter an appropriate string for the group condition. For example, for the Healthy condition, enter posture-token=*Healthy*. A corresponding posture token must be entered for each group being configured. The Cisco IOS NAD receives this posture token as the only indication of the validated state of the client being posture checked.

The name of the actual AV pair is case-sensitive; for example, the posture token must be all in lower case. The strings for the values are not case-sensitive.

Note The posture-token AV pair is the only way that Cisco Secure ACS notifies the AAA client of the SPT returned by posture validation. Therefore, it is important to type and format the AV name correctly and to identify the correct value for the posture-token attribute. Errors can result in the incorrect SPT being sent. If the AV pair name is mistyped, the AAA client does not receive the SPT.

The system displays the window shown in Figure 2-27.

Figure 2-27 Downloadable ACL and Attribute Configuration for the Quarantine Group



If a client machine is in a quarantined state and its access has been restricted to the AV remediation server, it is helpful to shorten the status query timeout. After the client has been through the upgrade process, a shorter timeout ensures that the client spends a minimal amount of time with restricted access.

Step 8 To change the status query timeout, use the string status-query=*timeout in seconds* where the value is between 30 and 1800 seconds.

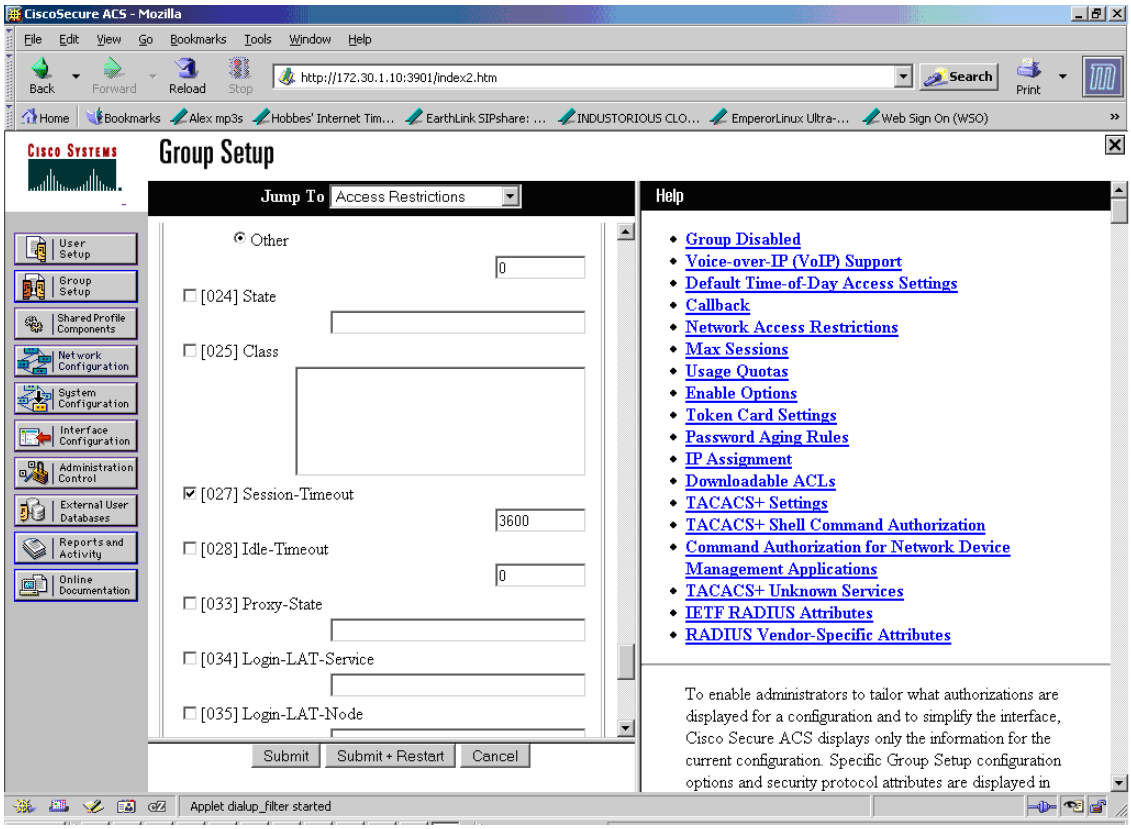
Step 9 To configure URL redirection, use the following string: url-redirect=*http://172.30.2.10/*

This URL redirection is enforced by the NAD.

Note If the interface ACL in the NAD does not contain an access line allowing access to the IP address where the redirection takes place, then a line must be added in the ACL that is paired with the group that has the URL redirection configured.

It may be desirable to change the revalidation timer for a particular group. This accomplished by checking the [027 Session-Timeout] check box in the IETF RADIUS Attribute section. Enter the number of seconds for the revalidation period under the IETF RADIUS Attributes section as shown in Figure 2-28 where the value is between 300 and 86400 seconds.

Figure 2-28 IETF RADIUS Attribute



Step 10 Click **Submit + Restart** after completing the group configuration.

Clientless User Configuration (Non-Responsive Hosts)

A clientless user is one that does not have the CTA installed. Examples include printers, IP phones, or any other IP-connected appliance that does not support CTA. Workstations without supported OS versions are also considered clientless. PCs that have not yet been through the CTA installation process are also clientless.

There are two methods to provide access for clientless users or devices:

- Configuring a username and password combination on Cisco Secure ACS and in the Cisco IOS software NAD—When this method of allowing for clientless devices is used, the NAD constructs an ordinary RADIUS packet on behalf of the clientless device. This packet is sent to the access control server for validation, with the resulting access restrictions applied to all users authenticating with this method.

  This username can be anything, but in the example shown in this section, the username “clientless” is used.

- Configuring the clientless user exception policy with Cisco IOS software commands only—This method can be used only for devices with known IP addresses or MAC addresses. This method does not involve sending a RADIUS packet to Cisco Secure ACS. The configuration of this method is shown in Configuring Clientless User Policy, page 2-51.

In the example shown in this section, the clientless user configuration is used with Cisco IOS software configuration to assign a user ID of "clientless" to the RADIUS packets that are returned by a host with no posture agent loaded.

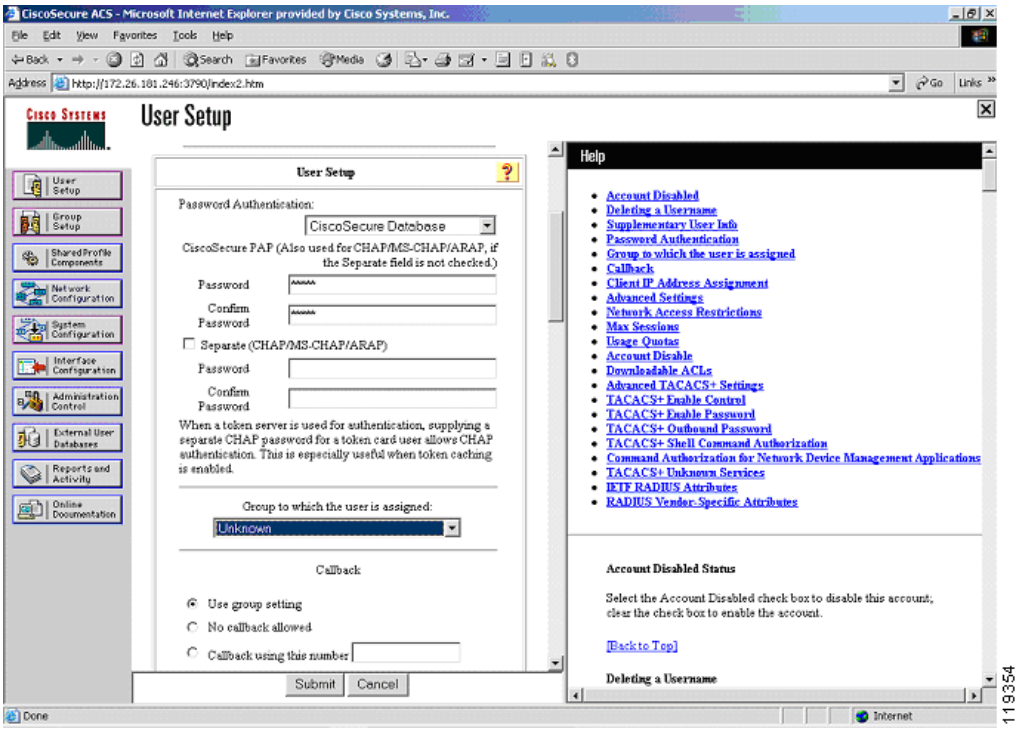
If the user ID clientless is configured on the Cisco IOS software NAD, the user ID clientless must be added to the appropriate group in Cisco Secure ACS. This can be any group with the appropriate restrictions (usually the Unknown group) and downloadable ACL assigned.

To configure access for clientless users, complete the following steps:

Step 1 Click **User Setup** on the Cisco Secure ACS main menu.

The system displays the window shown in Figure 2-29.

Figure 2-29 User Setup



Step 2 Type the username for the clientless user, such as clientless, into the User text field.

This becomes the username configured in the NAD.

Step 3 Click **Add/Edit**.

Step 4 Configure the password to be entered into the Cisco IOS software configuration for the clientless user.

Step 5 Add this user to the group that you have assigned to be the Unknown group.

Setting Up and Enabling Global EAP Authentication

To set up and enable global EAP authentication, complete the following steps:

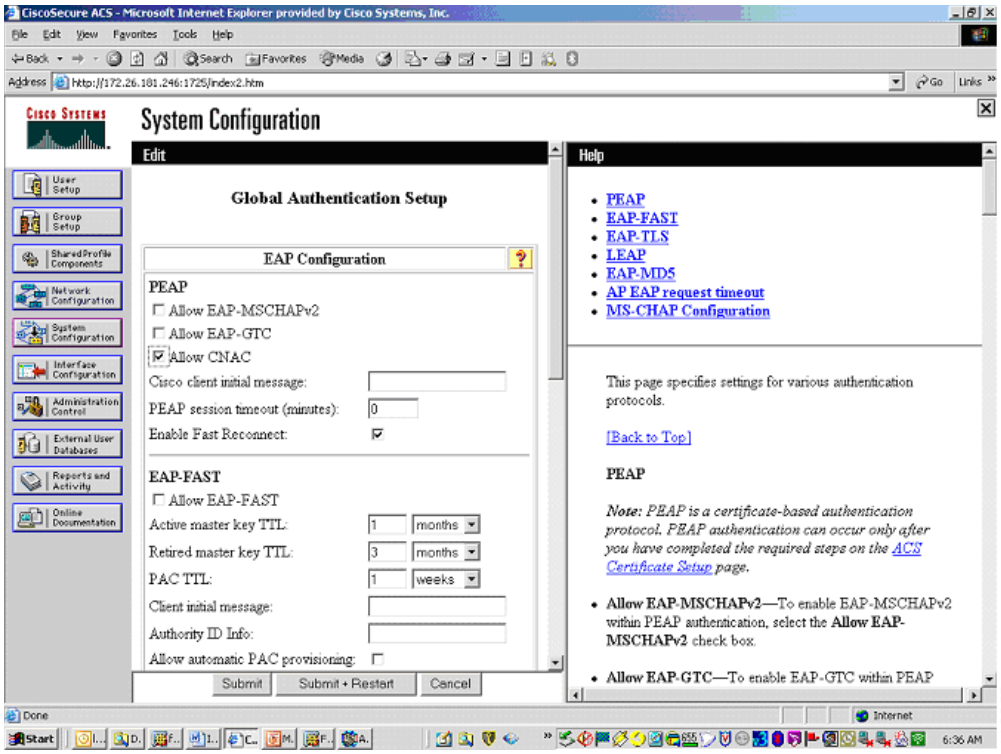
Step 1 Click **System Configuration** on the Cisco Secure ACS main menu.

Step 2 Click **Global Authentication Setup** from the menu presented.

Step 3 Check the **Allow CNAC** check box.

The system displays the window shown in Figure 2-30.

Figure 2-30 Global Authentication Setup



Step 4 Click **Submit + Restart**.

Configuring External User Databases

The external user database configuration is the heart of the NAC configuration process. Here you define the policies to which the clients must adhere for network access. This section describes these configuration steps and provides some background information. It includes the following topics:

- Overview
- Preliminary Configuration
- Configuring Local Policy Verification

Overview

The rules that comprise a posture policy may be stored on Cisco Secure ACS in the form of policies in a NAC external user database, or may be stored where they are checked on an external posture validation server. As part of the query process, CTA forwards its own posture credential to Cisco Secure ACS, as well as any posture credentials it has received from other posture plug-ins. There is normally one credential per posture plug-in, with each credential having one or more attributes. A few posture agents send multiple credentials.

The particular set of credentials forwarded from CTA causes Cisco Secure ACS to select the appropriate NAC external database to use for the posture validation. When the NAC database is initially created, you configure a set of mandatory credentials. Cisco Secure ACS uses these mandatory credentials as the minimum requirement to pick the best matching instance of the NAC external user database to use for credential validation.

If all of the clients in your network have the same set of posture agents loaded, they all forward the same set of credentials to Cisco Secure ACS. In this case, you need only one instance of the NAC external user database. If different clients are returning different sets of credentials because you use more than one AV vendor or some clients have different posture agents loaded, then you may need one instance of the NAC external user database for each set of received client credentials.

Each external user database has a different set of mandatory credentials uniquely identifying the minimum set of received client credentials necessary for that external user database instance to be chosen for the validation session. The received credentials are compared against the list of NAC external user databases in the order in which the external user database names appear in the Cisco Secure ACS configuration. If a NAC external user database with a small number of mandatory credentials (or only a single mandatory credential) appears ahead of a database instance with a larger number of credentials, and the mandatory credential set of the first database matches the received credentials, the first database instance is used for validation of the NAC posture of that particular client. For this reason, the ordering of the databases in the Cisco Secure ACS configuration is important.

The attributes forwarded to Cisco Secure ACS in each credential are evaluated by one or more policies in the NAC external user database. When there are multiple policies present, each policy in the database instance is evaluated. After the attributes in the credentials are checked against the rules in a policy, Cisco Secure ACS assigns an application posture token (APT) for each policy. This APT is returned to the client in a credential specified in the configured action for the policy.

If multiple policies are configured, multiple application posture tokens are sent to the client. Each APT must send a unique credential; if two APTs are returned in the same credential by two different policies, an error occurs. The most restrictive of these APTs becomes the system posture token (SPT). The client is placed in a particular group based on this most restrictive token. Cisco Secure ACS then takes the configured action based on that group. This can include sending an ACL to a NAD for enforcement actions on that host or forcing a URL redirection.

If a particular combination of mandatory credentials are not received from a specific client, Cisco Secure ACS looks for a different NAC external user database with the correct minimum set of mandatory credentials. If a match of the minimum credentials is not found, the posture validation fails, and the client is denied any access except that expressly permitted by the interface ACL configured on the NAD.

You can configure a policy for each mandatory credential in the received packet. Each of these policies includes at least one rule for each posture state that is checked. Each rule is made up of one or more rule elements and each rule element checks the value of a particular attribute in a received credential. A rule returns an APT in a credential if all the rule elements test true. Every rule element in a particular rule must test true for the rule to evaluate true and for the resulting action (returned token and credential) to occur. The first rule that matches in a local policy is the rule that returns the APT configured for that policy.

Preliminary Configuration

To configure the NAC external user database(s), you must complete the following tasks:

1. Determine the number of unique combinations of posture agents present on the clients in your network.

   For example, if a client has a supported anti-virus package and CTA, that is one combination. A client with the same supported anti-virus package and CTA plus CSA is another unique combination.

2. During the configuration of Cisco Secure ACS, create an instance of a NAC database in the External User Database section of Cisco Secure ACS for each unique combination of posture agents.

3. For each database instance, configure a set of mandatory credential types that matches the credentials returned by the posture agents loaded on the client machines. If an exact match is not found, the Cisco Secure ACS picks the best match of mandatory credentials. Under the Unknown User Policy database configuration, order the External User Databases properly so that the proper database is matched first; that is, the least desirable database appears last. For example, if you have configured a database with only the Cisco:PA as the mandatory credential type; this matches all incoming NAC validations. This database should be the last database to be checked.

Configuring Local Policy Verification

When configuring the APTs to be returned by local policies, never configure two policies to return an APT in the same credential, because this results in a failure. If a large number of clients are going to be posture checked, and you expect them to return with a healthy token each time, you should configure and order the rules in the local policies to check for the healthy condition first. This reduces the number of rules Cisco Secure ACS checks and reduces the processing load.

To configure Cisco Secure ACS for using external user databases, complete the following steps:

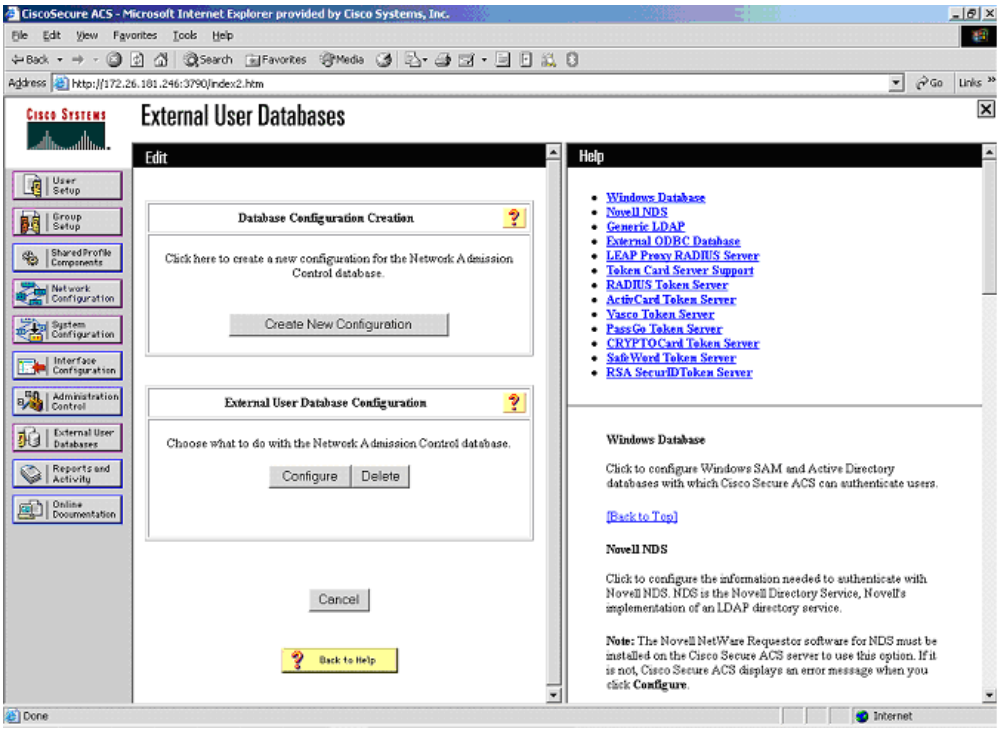
Step 1 To configure Cisco Secure ACS, click **External User Databases** on the Cisco Secure ACS main menu.

Step 2 Click **Database Configuration** from the resulting menu.

Step 3 Click **Network Admission Control**.

The system displays the window shown in Figure 2-31.

Figure 2-31 External User Databases



Step 4 Click **Create New Configuration**.

Step 5 Enter a name for this instance of the NAC database.

If multiple different AV vendor products are present and participating in the admission control process, one instance of the external user database for each AV vendor combination needs to be created.

Step 6 Enter a unique name for the database instance and click **Submit**.

Step 7 If multiple instances of the NAC external user database have been created, as you begin the configuration process make sure that the database name appears in the External Database Configuration window and click **Configure**.

If there is only a single instance of the NAC database, the name of that database is the only option to configure and no drop-down list is present.

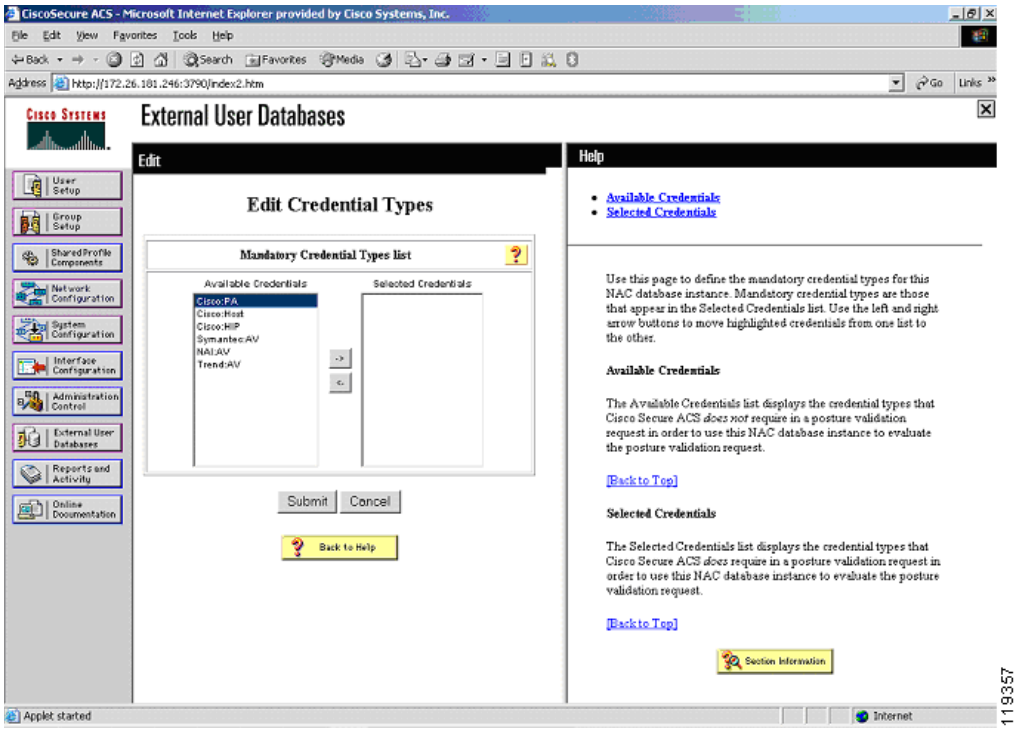
Two windows are displayed; one asking for any mandatory credential types, and the other where you configure the local (or external) policies for the credential validation.

Step 8 Click **Edit List** in the Mandatory Credential Types window.

Step 9 Add the credential types to be returned from your client for this instance of the NAC database by highlighting the desired credential type and clicking the right arrow. If the returned credentials are not an exact match to one of the external user databases, the best match is used. If there are no instances of external user database with matching mandatory credentials returned by a client, that client validation process fails. The mandatory credential set acts as a minimum requirement for the instance of the external user database to be used for validation.

The system displays the window shown in Figure 2-32.

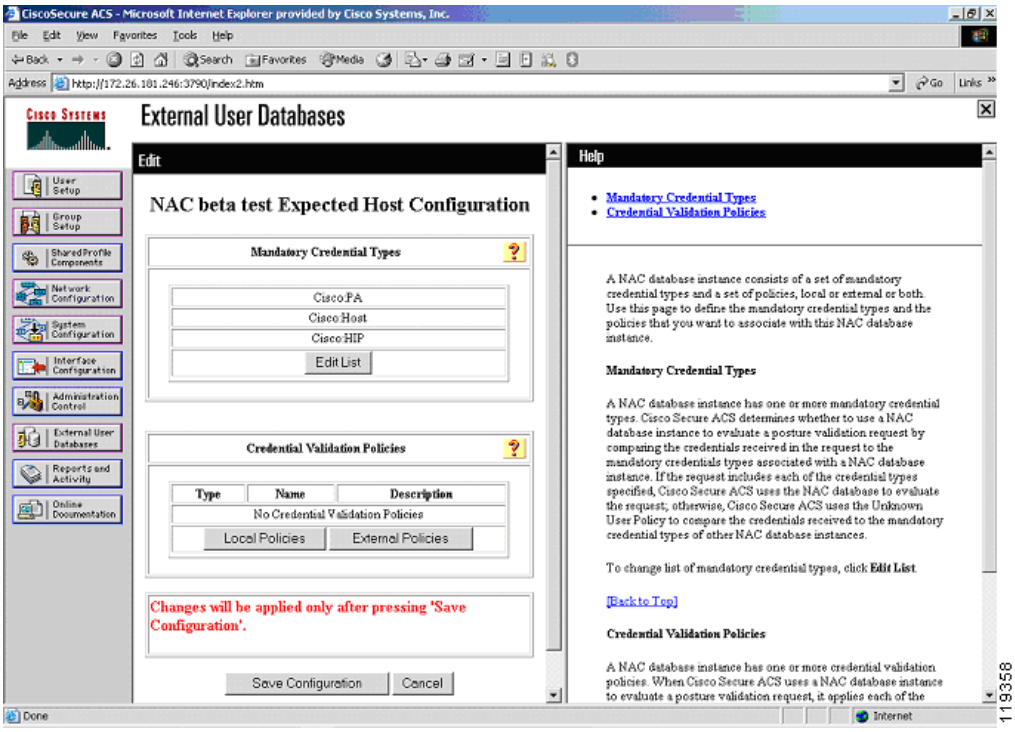
Figure 2-32 Edit Credential Types



Step 10 Click **Submit**.

The system displays the window shown in Figure 2-33.

Figure 2-33 Mandatory Credential Types



In this example, the client to which this instance of NAC database applies is loaded with CTA and with CSA.

Step 11 Click **Local Policies,** and click **New Local Policy** from the Local Policy Selection window.

Step 12 Enter a name and a description for this policy and a description if desired.

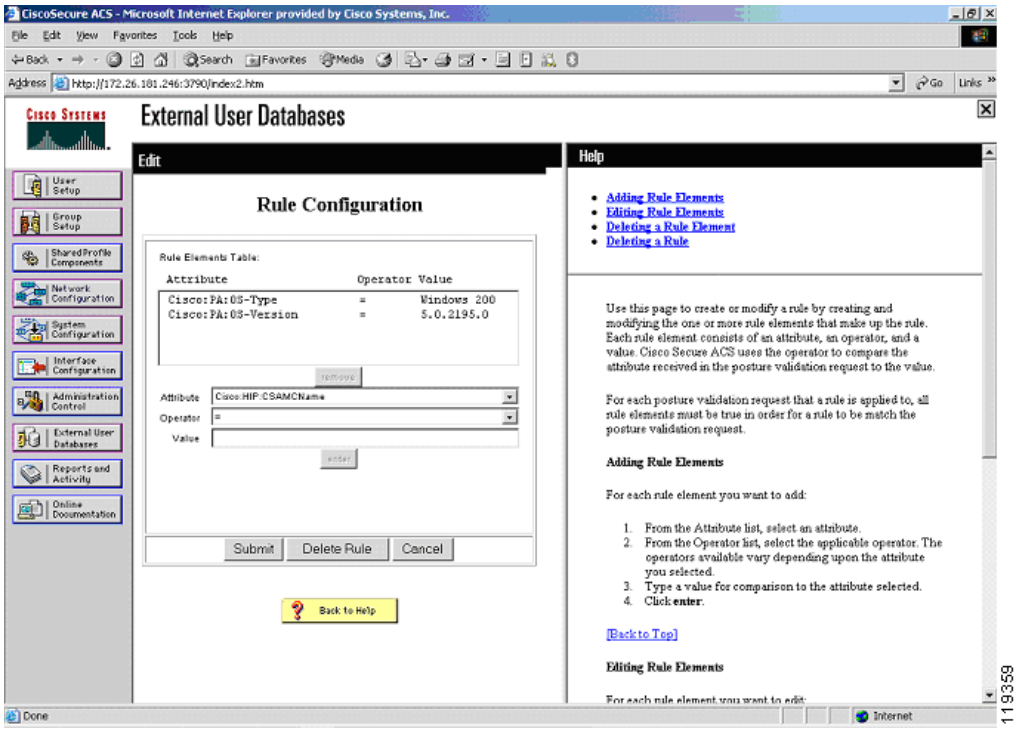
Step 13 Click **New Rule** from the Configurable Rules window.

Step 14 Select the attribute that you wish to validate for this rule element and select the appropriate operator for validation. Each of these becomes a rule element.

Rule element values are case-sensitive. Although it is not mandatory, in most cases only attributes from a single credential type should be checked in a single policy.

The system displays the window shown in Figure 2-34.

Figure 2-34 Rule Configuration

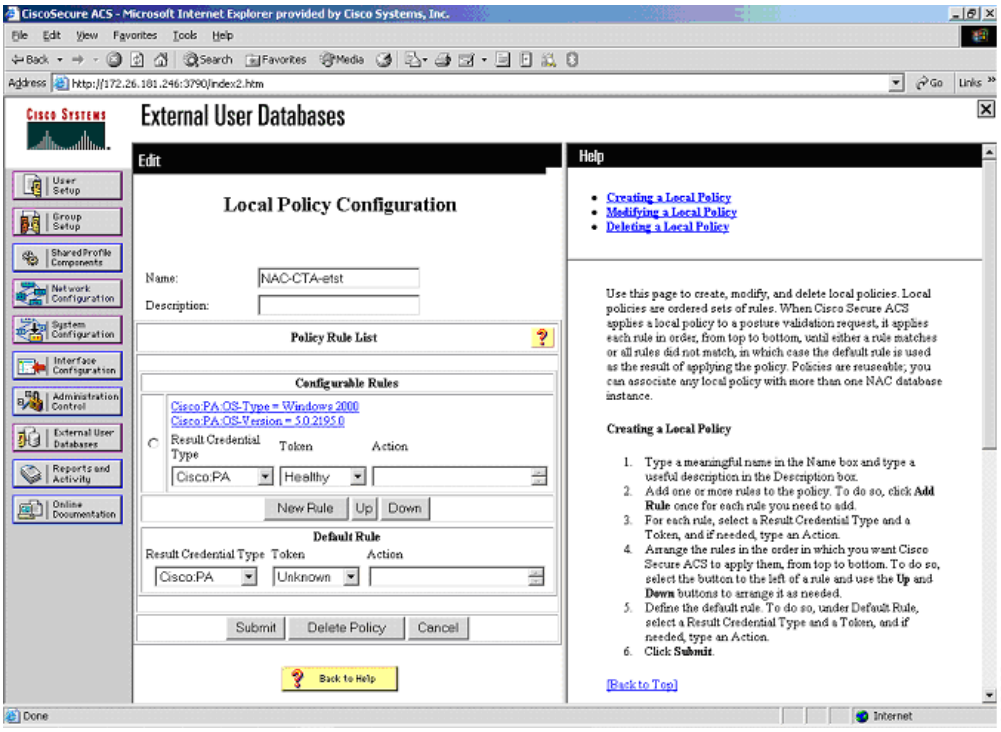


A rule can consist of a single rule element, or you may need to enter multiple rule elements to make up a single rule. After selecting the attribute and the operator and entering the data value, click **Enter** to place the rule in the Rule Elements table.

Step 15 After all of the rule elements have been added, click **Submit** to complete entering the rule.

The system displays the window shown in Figure 2-35.

Figure 2-35 Local Policy Configuration



This completes entering the criteria for a single rule. Directly below the display of the rule elements are several scroll windows and a text window. These define the action Cisco Secure ACS takes on a successful test for this rule. These actions include the return of a token in one of the credentials that contained the tested attributes.

Specific actions may also be entered into the Action window below the configured rule.

Actions are specific to the posture plug-in to which the APT is being returned. See the documentation supplied with the posture plug-in for specific details on these actions.

Step 16 To configure the order in which a rule is checked, highlight the radio button to the left of the rule and click **Up** or **Down**.

The last rule in the policy is the default rule. This rule is matched and the credential result and action returned if no other rules evaluate true for this particular policy. This result token is normally set to a token type such as quarantine or infected.

Step 17 Make configuration changes as needed to the default rule and click **Submit** in this window and click **Submit** again in the next window.

Step 18 To make the changes permanent, click **Save Configuration** in the last window.

Configuring External Policy Verification

Credentials may also be verified by an external posture validation server. A particular instance of the NAC external users database may contain both local and external policies. In these cases, credentials are sent to an external server over a protected connection with the Host Credentials Authorization Protocol

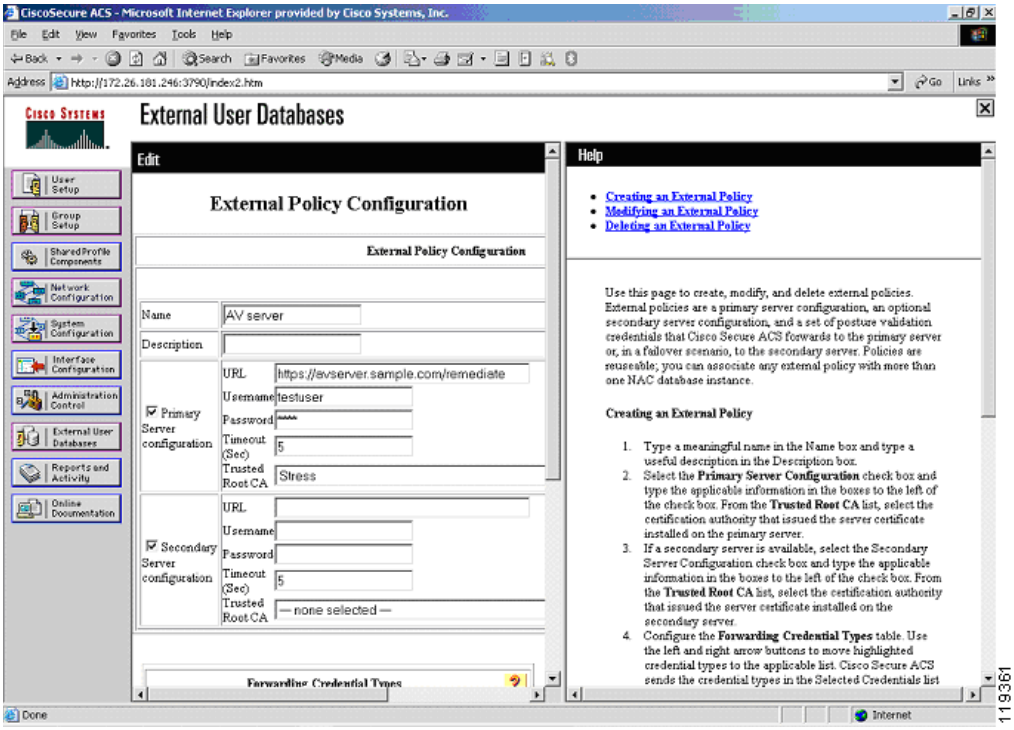
(HCAP). After the credentials and action are checked, the external server returns a token reflecting the current state of the client. The Cisco Secure ACS then puts the client in the corresponding group, with the configured ACLs of the group and Cisco IOS software AV pairs.

To configure Cisco Secure ACS for external policy verification, complete the procedure in Configuring Local Policy Verification, page 2-33 through Step 10. Then complete the following steps:

Step 1 Click **New External Policy**.

The system displays the window shown in Figure 2-36.

Figure 2-36 External Policy Configuration



This is the window in which you enter the access information for the external policy server.

Step 2 Enter a name for the policy and a description if desired.

Step 3 Enter the URL for access (this is available from your AV vendor).

Step 4 If a username and password are required for access, enter them here.

Step 5 Change the connection timeout as required.

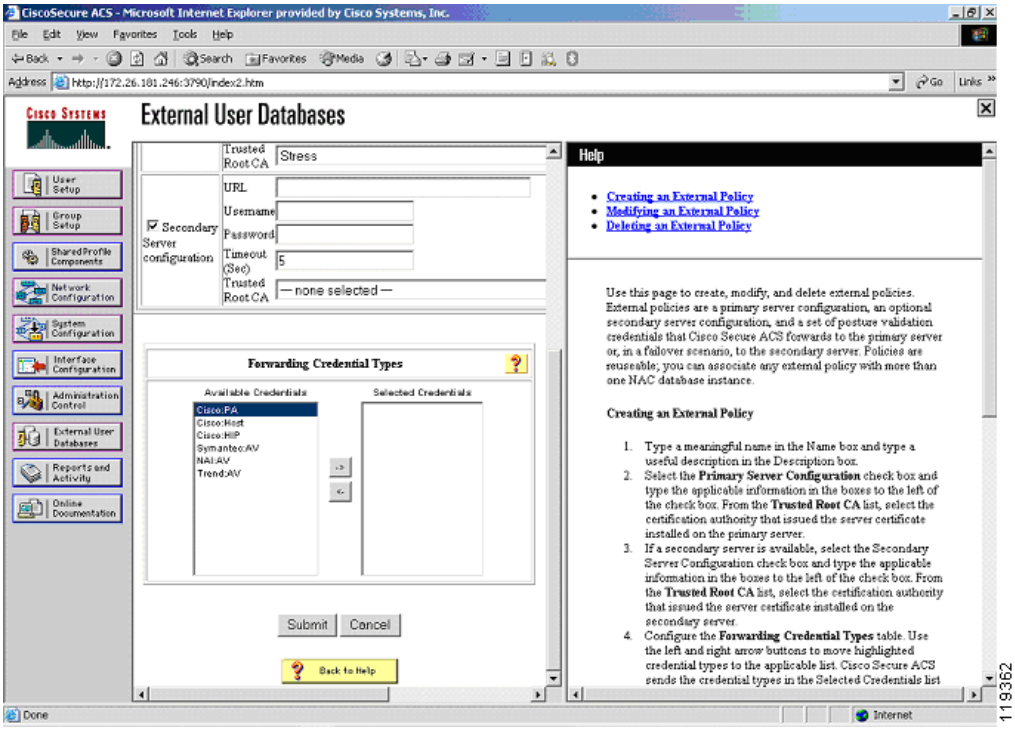
Step 6 Select the trusted root CA for the secure connection (this connection is protected with HTTPS) between the Cisco Secure ACS and the remediation server.

Step 7 Enter information for a secondary remediation server as required.

Step 8 Check the secondary server configuration check box to enable the use of a secondary server.

The system displays the window shown in Figure 2-37.

Figure 2-37 Selecting Forwarding Credential Types



Step 9 Scroll down the window and select the credentials to be passed to the external server.

If a particular credential is to be checked on an external policy server, there is no need to create a policy to check that credential locally.

Ensure that no local policies return an APT in the same credential that is being checked by an external policy server.

Step 10 Click **Submit** to complete the configuration process.

Configuring Token to User Group Mappings

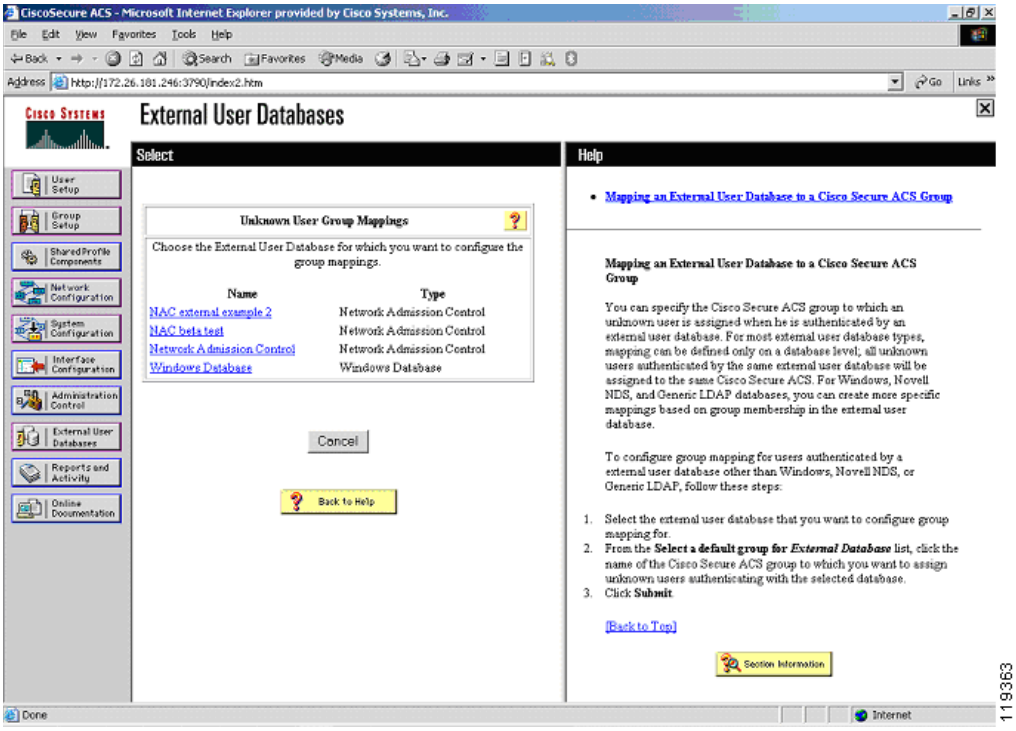
To force a client with CTA into a policy with a particular ACL applied, place the clients with a particular returned token into a specific user group. Multiple sets of user groups may be configured, each with a different downloadable IP ACL, configured URL redirection and so on. This permits different enforcement actions for different instances of the external user databases. To create the token to user group mappings, complete the following steps:

Step 1 Click **External User Databases** on the Cisco Secure ACS main menu.

Step 2 Click **Database Group Mapping**.

The system displays the window shown in Figure 2-38.

Figure 2-38 Unknown User Group Mappings

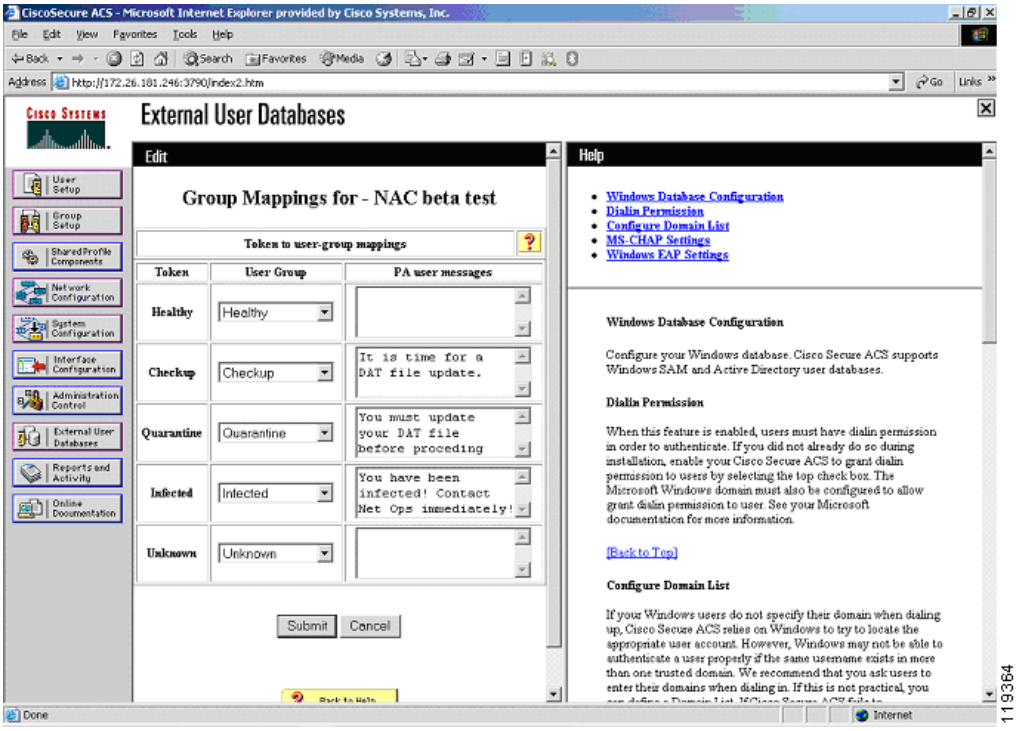


For each instance of a configured database, perform the following steps.

Step 3 Click on the name of the configured database.

The system displays the window shown in Figure 2-39.

Figure 2-39 Token to User Group Mappings



Step 4 For each token, select the appropriate user group in which to place the client that has that token returned.

Step 5 Optionally, enter a message to be displayed on the client in a pop-up window after the initial posturing process has completed.

If a particular token does not have a user group associated with it, clients returning those tokens are given default access.

Step 6 Click **Submit** to save your configuration.

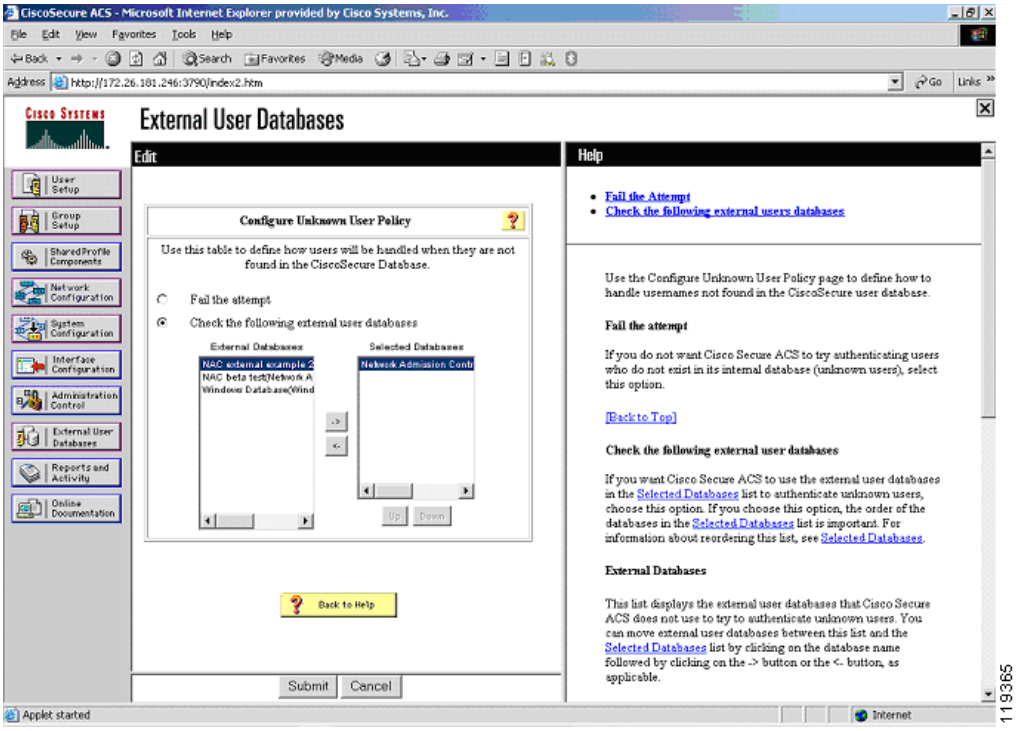
Configuring an Unknown User Policy to Check an External Database

EAP packets received with posture AV pairs are processed with the Unknown user policy. These packets do not contain conventional username password combinations like standard RADIUS authentication packets. To cause these packets to be checked against the policies contained in the external user databases that you have just configured, complete the following steps.

Step 1 From the External User Databases on the Cisco Secure ACS main menu, click **Configure Unknown User Policy**.

The system displays the window shown in Figure 2-40.

Figure 2-40 Configure Unknown User Policy



Step 2 For each external user database you wish to check, add the external user database name to the Selected Databases window with the arrow. Order the databases in the sequence in which you wish to have them compared against the received credential set.

Step 3 Click the Check the following external user databases radio button.

Step 4 Click **Submit**.

Configuring Client Credentials and Type Length Value Data

This section describes the attributes with which the CTA responds to the querying process, and includes the following topics:

- Attributes Overview
- Client Installation Tasks
- Certificate Placement
- Using the ctad.ini File
- Using the ctalogd.ini File
- Installation

Attributes Overview

These attributes set the policy to which clients accessing the network must adhere. Various posture agents reside on a host, each of which responds with a credential containing attributes that reflect the condition of the associated software.

It is the duty of the Cisco Secure ACS or the external policy server to verify the attributes and to match the client to the preconfigured policy. This policy can include an ACL, URL redirection, or other action, which is passed back to the NAD and/or the CTA for enforcement. The attributes available in the returned credentials from different posture plug-ins are summarized in the following tables.

Table 2-1 Cisco Trust Agent

Attribute Type	Attribute Name	Data Type	Data Format	Example
PA	OS-Type	String		Windows 2000 Professional
PA	OS-Version	Version	X.X.X.X	5.0.2195.0
PA	PA-Name	String		Cisco Trust Agent
PA	PA-Version	Version	X.X.X.X	1.0.51.0

Table 2-2 Cisco Security Agent

Attribute Type	Attribute Name	Data Type	Data Format	Example Values
Host	HostFQDN	String		client.cisco.com
Host	ServicePacks	String		Service Pack 4
Host	HotFixes	String		KB87232
HIP	CSAMCName	String		Not supported
HIP	CSAStatus	String		Not supported
HIP	LastSuccessfulPoll	Unsigned integer	X	Not supported
HIP	OperationalState	Unsigned integer	X	Not supported
HIP	CSAVersion	Version	X.X.X.X	4.0.2.611

Table 2-3 Anti-virus Vendor Attributes

Attribute Type	Attribute Name	Data Type	Data Format	Example Values
AV	Dat-Date	Time		2/28/2004 07:00
AV	Dat-Version	Version	X.X.X.X	5.0.4697.0
AV	Protection-Enabled	Unsigned integer	X	0 or 1
AV	Scan-Engine-Version	Version	X.X.X.X	2.9.567.0
AV	Software-ID	Unsigned integer	X	
AV	Software-Name	String		Anti-virus software
AV	Software-Version	Version	X.X.X.X	5.0.2345.0

The specific data values to be tested for and returned from the posture agents can be found in the documentation from the vendor of the posture agent. In addition, there may be other credential types and attribute names returned by your posture agent vendor. Consult the posture agent documentation for details.

Client Installation Tasks

The Cisco Trust Agent is currently compatible with the following Microsoft operating systems:

- Windows 2003 Server
- Windows XP
- Windows 2000
- Windows NT version 4.0 SP4

The way you install CTA depends on the AV vendor participating in the admission control process. Some AV vendor installation processes include CTA installation and others do not. Consult your vendor documentation to determine the method of installation to use. This section describes how to install CTA manually. Complete the CTA installation before installing any application software participating in admission control.

The client needs administrator privileges to complete the installation of CTA. If the user does not have administrator privileges on the client, then Windows installer (MSI) elevated privileges must be enabled on the host. For specific information on the anti-virus software installation, see the documentation supplied with the specific product.

To install CTA on a Windows workstation, run the ctasetup.exe installation file. This setup program is compatible with all supported versions of Windows.

Directory Structure

During installation, ctasetup.exe creates folders in the following directories:

- Two folders in %CommonProgramFiles%\Cisco Systems
  - %CommonProgramFiles%\Cisco Systems\CiscoTrustAgent

    This folder contains the CTA program files.
  - %CommonProgram Files%\Common Files\Cisco Systems\CiscoTrustAgent\Plugins

    This folder contains the posture plug-in files for the Cisco:PA credential ctapp.dll and ctapp.inf.

    Any files required by the posture plug-ins are placed into the Install folder below the previous directory by the posture plug-in installer. These are moved to %CommonProgram Files%\Common Files\Cisco Systems\CiscoTrustAgent\Plugins automatically when CTA registers the posture plug-in.

If logging is enabled, log files are written to the following directory:

%ALLUSERPROFILES%\Application Data\Cisco Systems\CiscoTrustAgent\Logs

Certificate Placement

Using PEAP during the admission control process requires that the CTA trust the PEAP initiator, which is Cisco Secure ACS. This trust is established with an x.509 certificate. You must add the certificate of the CA that issued the Cisco Secure ACS server certificate (or the self-signed certificate from the Cisco Secure ACS) to the \certs folder located in the directory from where the ctasetup.exe file runs before installation.

During installation, the CA certificate is automatically added to the proper store inside the client machine and installed into the CTA. If multiple CA certificates are used, each one should be placed into the \certs subdirectory.

If a certificate needs to be added after the installation has been completed, use the ctacert.exe program, with the following options:

ctacert /add c:\certificate_file_location\ca.cer /store root

Using the ctad.ini File

To change the default behavior of the CTA, you can manually create an initialization file (ctad.ini). Place this file in the directory where the ctasetup.exe file is located before the installation is performed. The installation process automatically copies the ctad.ini file into the proper directory. The format of the ctad.ini file is as follows:

```
=================
ctad.ini template
=================

[UserNotifies]
;
; prevent user from doing anything else when message displayed
SysModal=0/1       {default=1}

;
; these control the messages on the users' desktop
;
EnableNotifies=0/1   {default=1}
MsgTimeout=<seconds> {Default=300, Min=30, Max=0 (infinite)}

;
; These control the behavior for logon desktop. If message comes in on the
; logon desktop and logon desktop messages are disabled, then the message
; will appear on the user's desktop when the user logs in.
;
EnableLogonNotifies=0/1       {default=0}
LogonMsgTimeout=<seconds>     {Default=0 (infinte), Min=30, Max=0}
;

;   This section can be used to adjust the port and behavior of the communication
;   with the NAD. It may be omitted.
[EAPoUDP]
LocalPort=21862
MaxSession=3
SessionIdleTimeout=600
```

Using the ctalogd.ini File

To configure the logging process, manually configure the ctalogd.ini file before installation. This file should be placed in the directory with the ctasetup.exe program before installation. The logging level legend is as follows; 1 = low, 2 = medium, 3 = high, and 15 = everything.

An example ctalogd.ini file is included with the readme file for the ctasetup.exe program. This example file is as follows:

```
====================
ctalogd.ini template
====================
[main]
EnableLog=1

[LogLevel]
PADaemon=3
NetTrans=3
PAPlugin=3
CTAMsg=3
PEAP=3
EAPTLV=3
EAPSQ=3
PPMgr=3
```

This sample file enables the logging daemon and sets the logging level to high for each of the individual CTA subsystems.

Installation

During installation, a log of the installation is placed in the same directory from where ctasetup.exe was launched. This file should be saved for troubleshooting.

After CTA installation is complete, there are two new processes running as Windows services:

- Cisco Trust Agent
- Cisco Trust Agent Logging Services

Both services are configured to automatically start on system boot. See the readme file supplied with CTA for the latest information.

Additional Information

Additional information regarding the Cisco Trust Agent can be found in the administrator guide at the following URL:
http://www.cisco.com/en/US/docs/security/cta/2.1.103.0_supplicant/admin_guide/cta_bundled_with_supplicant.html.

Configuration Tips

This section describes some important configuration tips. It includes the following topics:

Status Query Timeout Values

The status query process ensures that a particular client remains in compliance with the policies configured in the Cisco Secure ACS or the external policy server. You can configure Cisco Secure ACS to set the status query timer for a lower value if a client has been assigned to checkup or a quarantine state. This may be helpful if access restrictions are placed on the client in these posture states. Lowering the status query timeout in these states reduces the amount of time the client spends with restricted access.

Revalidation Timer

The revalidation timer is the time for which the posture check remains valid. It can be set lower if a virus outbreak is detected and an update needs to be pushed to all clients. Revalidation can also be initiated via the Cisco IOS command **eou revalidate all**. This causes all clients to be revalidated.

External User Database Local Policy Rule Ordering

The order in which rules are checked can have a significant impact on the load placed on the Cisco Secure ACS server. For example, if the Cisco Secure ACS server checks first for non-compliant clients and most clients are compliant, the Cisco Secure ACS server must process many more rules than if the rules are ordered so that it checks for a healthy state first.

Installing the Posture Agent and Remediation Server

The specific installation procedures required to install the posture agent and the optional remediation server vary depending on the software in use. Consult the AV vendor documentation for complete details.

The CSA system attributes are validated by the Cisco Secure ACS server at this time. External policy servers are not used. Currently the supported attribute from the CSA is the CSA version.

Configuring the Cisco IOS Software NAD

This section describes how to configure the Cisco IOS software device acting as the NAD. It includes the following topics:

Overview

Because the Cisco IOS software NAD is the enforcement device in NAC, you configure it last, especially if some clients do not have CTA installed. This causes less disruption to network operations. You can remove the Cisco IOS software enforcement commands that turn on NAC if problems occur. The Cisco IOS software NAC functions are built on top of authentication proxy (auth-proxy) code. Some of the commands are familiar if you have configured auth-proxy.

You must complete the following configuration tasks:

1. Configuring AAA server communication
2. Configuring the EOU authentication method
3. Enabling the Cisco IOS software http server
4. Creating an ACL to block interface traffic until the client has successfully completed the admission control process
5. Optionally, building an intercept access list to define the traffic that triggers the admission control process
6. Configuring auth-proxy banner and timers
7. Configuring eou timers and the interface configuration necessary to enable NAC

You can optionally configure a policy for unknown devices with specific IP addresses to bypass the posture checking process. These devices may be subject to specific access limitations on a device-by-device basis if desired. For more information, see the Cisco IOS Software Release 12.3(8)T new features documentation specific to NAC.

To configure a clientless method of handling users with a RADIUS username and password, see Clientless User Configuration (Non-Responsive Hosts), page 2-29.

Configuring AAA EOU Authentication Protocols and Authentication Proxy Authorization Protocols

Enter the following commands to enable AAA services for EOU authentication:

```
aaa new-model
aaa authentication eou default group radius
aaa session-id common
```

RADIUS server groups may be used to send user authentication to different server sets than the posture validation authentication packets.

Configuring AAA Setup, RADIUS Server Host, and Key

Enter the RADIUS host IP address and RADIUS server key information with the following commands in global configuration mode:

```
radius-server host 172.30.1.10 auth-port 1645 acct-port 1646
radius-server key secret
```

Replace the word *secret* with the shared key you entered in the Cisco Secure ACS during the installation and configuration of that server. Also configure the source IP address interface for the RADIUS packets that was configured in Cisco Secure ACS server network configuration.

The source IP address of the transmitted RADIUS packets is configured with the following command:

```
ip radius source-interface FastEthernet0/0
```

This is the IP address from which Cisco Secure ACS receives RADIUS packets.

The following command allows non-standard attributes to be sent to RADIUS:

```
radius-server vsa send authentication
```

Configuring Admission Control EOU

The following command enables the EOU posture validation process. Any packet received on the interface to which this policy is applied triggers the admission control process.

```
ip admission name AVERT eapoudp
```

Optionally, you can exempt traffic from triggering the admission control process by applying an ACL to the NAC policy statement in the configuration. The following example causes traffic with a destination of port 53 (domain) or port 80 (www) to be exempted from the admission control process:

```
ip admission name AVERT eapoudp list 102

access-list 102 deny   udp any host 10.10.30.10 eq domain
access-list 102 deny   tcp any host 10.10.20.10 eq www
access-list 102 permit ip any any
```

These packets need a corresponding entry in the interface ACL to be successfully forwarded without a prior posture validation taking place. No posture validation triggering occurs if only deny statements are present in the intercept ACL.

Configuring an Exception List Configuration for Clientless Hosts

If hosts with a statically-configured IP address and no posture agent installed (non-responsive hosts) are located on the network where posturing is taking place, they may be exempted from the posturing process. The following commands configure a policy that allows a host with a static IP address access defined by an access list:

```
identity profile eapoudp
 device authorize ip-address 172.30.40.32 policy NACless
identity policy NACless
 access-group clientException
 redirect url http://172.30.2.10/update

ip access-list extended clientException
 permit ip any host 172.30.1.10
```

This configuration allows a host with an IP address of 172.30.40.32 to communicate with the host 172.30.1.10 and no other hosts. This configuration is useful for IP-connected printers or IP telephony devices.

In the case of networks where only web clients exist, URL redirection can point those clients to a server where the appropriate software can be obtained.

Note The use of the exception list method of exempting individual hosts from the admission control process requires the use of named access-lists in the Cisco IOS software configuration.

Configuring Clientless User Policy

This section describes a different exception method for hosts without a posture agent installed. The **eou clientless username** command configures the Cisco IOS software NAD to insert a username of *clientless* for clientless end stations in the RADIUS protocol.

```
eou clientless username clientless
eou clientless password password
eou allow clientless
```

The **eou clientless password** command configures the password *cisco123* to be returned.

The **eou allow clientless-host** command enables the return of the previous username/password combination for all hosts the NAD attempts to posture without receiving a valid EOU response.

The Cisco Secure ACS then issues a token according to the group in which a user with the clientless username is placed. This configuration is useful for PCs and workstations that receive their IP addresses through DHCP and do not have the posture agents installed.

Configuring EAP over UDP Timers

The following commands configure the timers for the EOU posturing processes. These timers are shown with their default settings.

```
eou timeout hold-period 60
eou timeout revalidation 1800
eou timeout status-query 300
ip auth-proxy inactivity-timer 10
```

The **eou timeout hold-period** command ignores packets from a host that has just unsuccessfully authenticated for the hold period in seconds. The **eou timeout revalidation** command sets the global revalidation period for all clients. This may be overridden by a RADIUS AV pair from the Cisco Secure ACS. The **eou timeout status-query** command sets the global status query period. This may also be overridden by an AV pair received from the Cisco Secure ACS.

Configuring the Interfaces and Intercept ACL

The interface configuration consists of two commands that must be configured on the interface facing the hosts to be posture validated.

```
interface FastEthernet0/0
 ip address 172.30.40.1 255.255.255.0
 ip access-group 101 in
 ip admission AVERT
access-list 101 permit udp any host 172.30.40.1 eq 21862
```

The **ip access-group 101 in** command places an ACL on the interface in the inbound direction that blocks all traffic entering the interface except for that which is expressly permitted. This ACL, called the interface ACL, is useful for creating pin holes that allow certain kinds of inbound traffic before subjecting that device to the posturing process. For example, an access control element (ACE) permitting UDP packets equal to domain allows for DNS queries to be successfully sent without being postured. The interface ACL at a minimum must permit inbound UDP communication destined to port 21862. The first permit ACE allows this UDP traffic into the NAD. This is necessary for the EOU communications. The **ip admission AVERT** command applies the previously configured NAC policy to the interface.

The traffic specifically permitted by access list 102 is subject to the posturing process.

Configuring the HTTP Server

Enabling the HTTP server is necessary for URL redirection. When URL redirection is configured in the group configuration section, these URL redirections are sent to the Cisco IOS software NAD.

```
ip http server
ip http authentication aaa
no ip http secure-server
```

Enabling EOU Logging

Enable logging from the Cisco IOS software NAD with the following commands:

```
eou logging
logging 172.30.1.20
```

This enables syslog messages at an informational level (syslog level 6) from the posturing process.

Additional Information

Additional information may be found in the *Cisco IOS Configuration Guide and Command Reference for Network Admission Control* found at the following URL:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_nac.html.