Implementing Network Admission Control Phase One Configuration and Deployment

OL-7079-01
Version 1.1

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Implementing Network Admission Control Phase One Configuration and Deployment

Preface

Document Purpose

This document provides guidance for implementing Network Admission Control (NAC), an industry-wide collaboration sponsored by Cisco Systems. It describes deployment considerations and configuration procedures for Cisco IOS software devices acting as Network Access Devices (NADs). It provides installation guidelines for the Cisco Trust Agent (CTA) on Microsoft Windows client machines. It also provides configuration instructions for Cisco Secure ACS, including configuration with anti-virus software products.

Intended Audience

The audience for this document consists of system engineers and network administrators responsible for the implementation of NAC. This document assumes you are familiar with Microsoft Windows operating systems and client machines and with the configuration and operation of Cisco Secure Cisco Secure ACS. It also assumes you know how to configure Cisco IOS devices, and are familiar with certificate authorities and the trust models provided by digital certificates.

Document Organization

Chapter	Description
Chapter 1, "Introducing Network Admission Control."	Provides background information about the Network Admission Control (NAC) and describes how it works.
Chapter 2, "Implementing Network Admission Control."	Describes how to design and Implement NAC.
Chapter 3, "Managing and Troubleshooting NAC."	Describes how to manage and troubleshoot NAC.
Appendix A "Debug Output and CTA Logs."	Provides sample output form debugging and CTA logs.
Appendix B "Reference Information."	Provides a list of acronyms and sources of further information about NAC.

CONTENTS

Introducing Network Admission Control

This chapter provides background information required to implement Network Admission Control (NAC), an industry-wide collaboration sponsored by Cisco Systems. It includes the following sections:

- Overview
- NAC Operational Detail
- Limitations and Guidelines
- Pre-Deployment Considerations
- System Components

Overview

This section describes the benefits of NAC and how it works, and includes the following topics:

- The Benefits of Network Admission Control
- How Network Admission Control Works

The Benefits of Network Admission Control

Virus infection on data networks has become an increasingly serious problem. The resources consumed during just one disinfection process are much greater than the resources necessary to implement an anti-virus feature in the network such as Network Admission Control.

Cisco NAC helps ensure the health of client workstations before they are granted network access. NAC works with anti-virus software to assess the condition, called the posture, of a client before allowing access to the network.

NAC helps ensure that a network client has an up-to-date virus signature set and has not been infected before gaining access to a data network. If the client requires a signature update, the NAC solution directs it to complete the update. If the client has been compromised or if a virus outbreak is occurring on the network, NAC places the client into a quarantined network segment until disinfection is completed.

How Network Admission Control Works

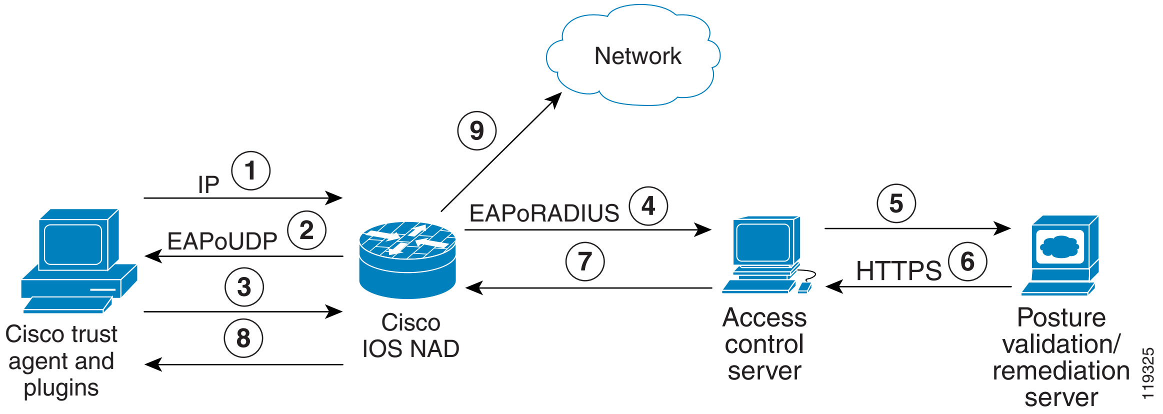
NAC implementation combines a number of existing protocols and Cisco products with some new products and features, including the following:

- Cisco Trust Agent (CTA) and plug-ins
- Cisco IOS Network Access Device (NAD)
- Extensible Authentication Protocol (EAP)
- Cisco Secure Access Control Server (ACS)/Remote Authentication Dial-In User Service (RADIUS)
- Posture validation/remediation server

CTA communicates with other software on the client computer over a published Application Program Interface (API) and answers posture queries from the NAD. CTA also implements the communication (EAP over UDP) necessary to implement NAC. The resident software includes a Posture Plug-In (PP) that interfaces with the CTA. The PP is an agent included with third-party software that reports on the policy and state of this software.

In the current implementation of NAC, the NAD is a Layer 3 Cisco IOS software device that queries client machines seeking network access using EAP over UDP (EOU). The way that the different components of the NAC solution interact is shown in Figure 1-1.

Figure 1-1 NAC Operation



NAC component interaction occurs as follows:

1. Client sends a packet through a NAC-enabled router.
2. NAD begins posture validation using EOU.
3. Client sends posture credentials using EOU to the NAD.
4. NAD sends posture to Cisco ACS using RADIUS.

5. Cisco Secure ACS requests posture validation using the Host Credential Authorization Protocol (HCAP) inside an HTTPS tunnel.
6. Posture validation/remediation server sends validation response of pass, fail, quarantine, and so on.
7. To permit or deny network access, Cisco Secure ACS sends an accept with ACLs/URL redirect.
8. NAD forwards posture response to client.
9. Client is granted or denied access, redirected, or contained.

When the client sends a request for network access (1), the NAD starts the posture validation process (2). The identity it receives from the CTA is passed on to Cisco Secure ACS, which then initiates a protected EAP (PEAP) session with the CTA (the PEAP session is not shown).

CTA then sends its credential with any credentials it gets from PPs on the client machine to the NAD (3), which forwards them using the RADIUS protocol to Cisco Secure ACS (4). These credentials contain attributes that hold information about the current state of the client software.

Cisco Secure ACS checks and validates the credentials by comparing the attributes contained in the credentials against its policy database. Cisco Secure ACS can also be configured to pass these credentials and attributes to an external server for validation (5). This is done using HCAP over an HTTPS tunnel. This may be the preferred option when client software comes with a PP and an external posture validation server for credential evaluation.

Where there is an external posture validation server, the external server checks the credentials and attributes against its internal database and returns an application posture token (APT) to Cisco Secure ACS. Cisco Secure ACS then collects all APTs from any local or external policies. The most restrictive of these APTs becomes the system posture token (SPT).

Cisco Secure ACS then places the client in a group corresponding to its SPT. These groups correspond to the access rights granted by the SPT and may be Healthy, Checkup, Quarantine, Infected, or Unknown. Cisco Secure ACS then sends the appropriate access control list (ACL) for the group to the NAD to be applied against the client (8).

Cisco Secure ACS can optionally include an HTTP redirect in the returned policy sent to the NAD to force a client to visit a particular server for a mandatory update and to determine if remediation has occurred.

A posture agent can be developed to return information contained in its credential by the CTA that can be used in many ways, including assessment for host intrusion detection system (HIDS), host intrusion prevention system (HIPS), personal firewalls, operating system patch levels, and application version control.

NAC Operational Detail

This section provides additional details about the NAC process for those who want to understand the process at a more technical level. This level of understanding is not required to implement NAC, but is helpful for troubleshooting and fine-tuning the process.

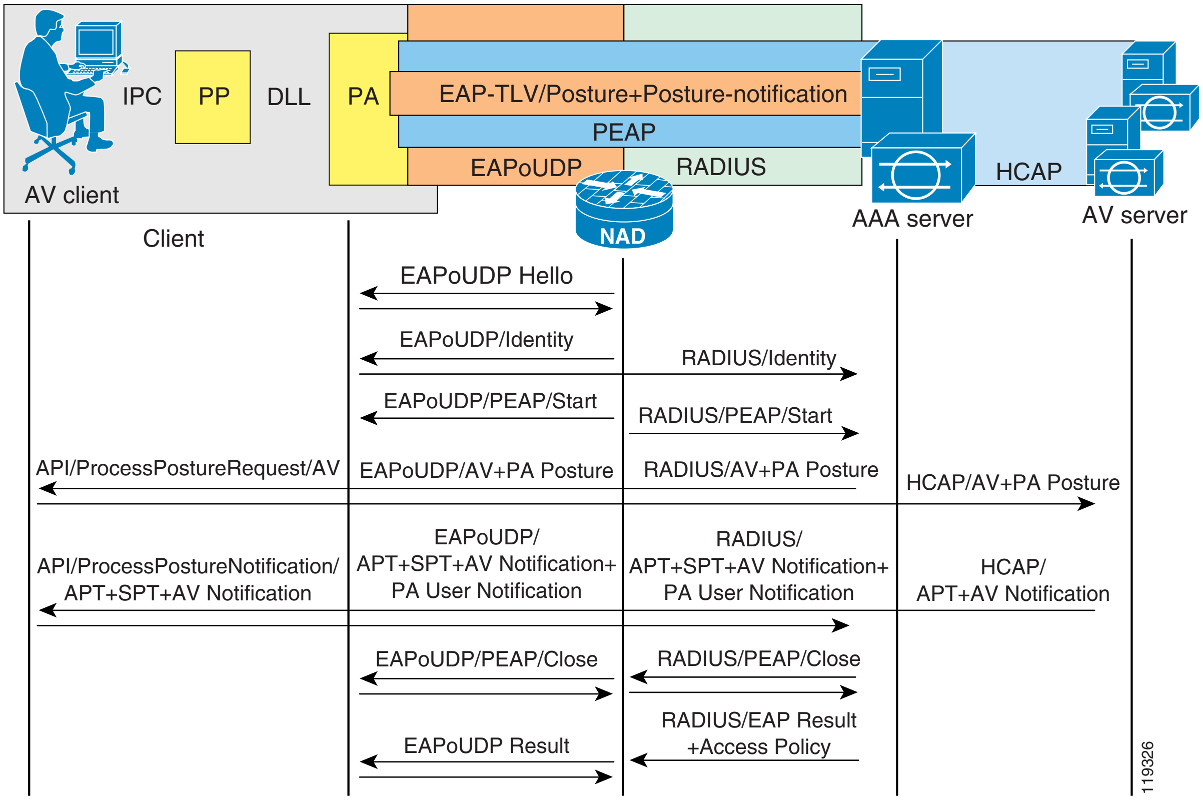
NAC is dependant on a Layer 3 Cisco IOS software device for policy enforcement. The installation of CTA and any compatible client software has no effect until the required commands are configured on the Cisco IOS software enforcement device, called the NAD.

The admission control process is triggered by a Layer 3 packet entering a router interface with admission control configured. After the NAC process is triggered, the router sends an EOU hello message to which the client host answers with an EOU hello. When the NAD and client recognize each other, the NAD asks for the identity of the client. When received, this identify is passed to Cisco Secure ACS in the form of an EAP over RADIUS packet. Cisco Secure ACS then initiates a PEAP session with the client host.

Note that the router acts as a pass-through device at this point; it does not proxy any part of the PEAP session but merely re-encapsulates the PEAP packets from UDP to RADIUS.

After the PEAP session has been established, Cisco Secure ACS queries the client for the credentials from registered software on the client. This causes the CTA on the client to query the PPs that have been registered with CTA for their credentials and attributes. These credentials and attributes are collected and sent to Cisco Secure ACS in the PEAP session. During this initialization phase, the packets received on the router interface are subject to any access list applied on that interface. Some packets may be dropped during this initialization. Figure 1-2 shows the details of this process.

Figure 1-2 Protocol Flows



When Cisco Secure ACS receives the credentials from the CTA, it looks for a NAC external user database configured in ACS with the best match of the same mandatory credentials as those it received from the CTA. The NAC external user databases have one or more policies configured in them. When the Cisco Secure ACS finds a match, it checks the credentials and attributes against any local or external policies in the matched database. These policies specify the values that the attributes in the received credentials must have to meet the admissions policy for the configured network.

Each policy returns an APT in a single credential back to the client, along with any supported actions, which are unique to each posture agent. The most restrictive of the application posture tokens are used as the SPT. The SPT determines the group into which Cisco Secure ACS places the client and the overall posture of that client. The actual enforcement rules are configured in the Cisco Secure ACS group policy. Enforcement rules take the form of downloadable ACLs, URL redirection, and timer adjustments. These enforcement rules are sent to the NAD by ACS at the termination of a successful validation session.

The NAD periodically queries the host to determine whether the posture of the client has changed or whether the host is the same host that has gone through the validation process. The NAD can also enforce a URL redirection to cause a client to automatically go to an attribute-value (AV) server for updates when the client attempts web access. This URL redirection is configurable from Cisco Secure ACS for each posture state.

You can also configure Cisco Secure ACS to shorten the status query value or the re-validation time on the NAD by sending a Cisco IOS AV pair with the specific timer values to be applied for a particular client to help ensure that the client successfully completes the remediation process. As each application is remediated, the application APT returns to a healthy condition, and eventually a healthy SPT is achieved.

If there has been a change, such as a new DHCP address being assigned or a changed DHCP client, (the client holding that address has dropped off line and a new client has been assigned the same address), the status query process fails and the validation process is restarted. If no response is received from the client, the system can download a default enforcement policy to the NAD to limit the network access of the client, depending on the overall network security policy.

Limitations and Guidelines

NAC is a Layer 3 technology, and NAC posture validation and enforcement is currently restricted to Layer 3.

Because communication between Cisco Secure ACS and the CTA uses PEAP, the CTA must trust Cisco Secure ACS. This trust is established using X.509 certificates. If you already have a certification authority (CA), you can generate a certificate signing request from Cisco Secure ACS and send it to your CA for enrollment. The CA (root) certificate must be installed on each client taking part in admission control. CA certificate installation occurs automatically at installation time if the certificate is placed in the \certs directory located below the directory from which the program ctasetup.exe is run. For details, see the section on CTA installation.

Cisco Secure ACS can also generate a self-signed certificate. In this case, the certificate from Cisco Secure ACS is installed on each client taking part in the admissions control process. This also occurs automatically if the certificate is placed in the \certs directory located below the directory from which ctasetup.exe is run.

If you generate an external private key and certificate for use on Cisco Secure ACS, you must install the certificate and private key files on Cisco Secure ACS.

Pre-Deployment Considerations

Successful deployment of NAC requires some planning ahead of the deployment. The primary consideration is the handling of clients as they go through the NAC process. This includes enforcement action for clients without CTA installed yet. Consider using a phased enforcement policy initially to limit the enforcement action taken when a large number of clients do not yet have CTA installed. This significantly limits network disruption.

This section describes other issues to consider and includes the following topics:

- Access Restrictions for Postured Clients
- Non-Responsive Hosts Handling

Access Restrictions for Postured Clients

This section provides an overview of the access restrictions for postured clients and describes the various conditions for which NAC tests. It includes the following topics:

- Category and Token Assignment
- Healthy
- Checkup
- Quarantine
- Infected
- Unknown

Category and Token Assignment

During the admission control process, clients are placed into a particular category and are assigned a token. One token is assigned per policy configured in the Cisco Secure ACS NAC external user databases. The token assigned depends on the values of the attributes contained in the credential originated by the NAC-compliant software on the client. The assigned categories of these returned tokens give each client specific access rights.

Category assignment can also cause pop-up messages to appear on the client screen and redirect a web browser to a specific URL. Cisco Secure ACS can send configured actions to individual software applications taking part in NAC. The particular actions are not discussed in this document because they are specific to the different applications participating in NAC. These actions can include the triggering of a software update or some other type of software-specific action. See specific software documentation for more details about the configurable actions supported by your vendor software.

Healthy

The Healthy category is assigned when the information received from the client posture agent credentials are current with the policy defined in the NAC external user database on Cisco Secure ACS. In this case, the scanning engine and the signature files are considered current for an AV policy or the current policy for a personal firewall are current, and no further action needs to be taken by the user. Normally, no access restriction is placed on a client in this condition.

Checkup

The Checkup category is assigned when the client may have some files, either the AV signature file or the scanning engine or some other third party software that supports NAC, which is not completely current with the network admission policy. Users should upgrade their client software to maintain currency, but no access restrictions are normally placed on the client in this state. This state can trigger normal AV DAT file updates or other non-mandatory file upgrades. A pop-up message can be configured to alert the user of the available upgrade.

Quarantine

When a client is assigned to the Quarantine category, the user must take immediate action to update their anti-virus files. A client might be placed in this condition during a virus outbreak to prevent the spread of the virus or when a particular OS vulnerability has been discovered to force a personal firewall policy upgrade. To enforce this policy, an ACL can be downloaded to the NAD that permits access only to the upgrade server, and a URL redirection can force the client to visit the upgrade server. This effectively blocks any other network access and forces the client to immediately come into compliance with the network access policy.

Infected

The Infected category can be assigned when the client has been actively infected with a virus. It is normally the job of the posture agent installed on the client to check for an infected condition.This condition triggers ACLs to be downloaded that prevent any network access by the infected client until a remediation process is completed. A pop-up message can notify the user of the state of the machine and indicate the required action that must be taken by that user. A URL re-direction is normally configured in this case.

Unknown

The Unknown category can be assigned when there is no CTA on the client or the host did not respond to the EOU queries by the NAD. This can occur with hosts that do not have the admission control software loaded, with hosts that have unsupported operating systems, or with IP devices that do not support NAC. A clientless exception policy can be configured that is applied to any clientless device present on an interface performing NAC by creating a “clientless user” in the IOS NAD configuration. The unknown group contains the access restrictions necessary for these devices. These exception policies can include the specific destination hosts with which the excepted devices are permitted to communicate.

Non-Responsive Hosts Handling

Generally speaking, a non-responsive host is a client without posture agent software loaded. These clients might be IP devices such as IP phones, network-attached printers, or other IP devices. Any PCs or workstations that do not have the CTA or posture agent software loaded are also considered non-responsive hosts. These workstations may be running MacOS, Solaris, or unsupported versions of Windows. This can also occur with a client that does not trust the Cisco Secure ACS that is performing the validation process. Non-responsive hosts may be handled in the following three ways:

- Static policy—This configuration is performed on the NAD device only. These devices can be statically excepted via IP address, MAC address, or by device type (such as a Cisco IP Phone).
- Clientless user—A clientless user name and password is configured on the NAD. The same username and password is configured on the Cisco Secure ACS, and the username is assigned to a particular group with the appropriate access restrictions configured. These access restrictions can include IP access lists and URL redirections. This method of handling non-responsive hosts is identical to the creation of a clientless user for the unknown category mentioned previously.
- Restricted access—This classification takes no action whatsoever. The interface ACL configured on the NAD provides the default access restrictions for all non-responsive hosts on that interface.

Static Policy

One way to handle a non-responsive host is to configure a static policy in Cisco IOS software, which includes the IP address of the host, the MAC address of the host, or the configured NAD host type; and building an ACL that identifies the IP addresses and networks with which an unknown host can communicate. To use a static policy for non-responsive host handling, certain information about the hosts must be known, and this information must remain static.

Clientless User

A second method of handling non-responsive hosts is to define a clientless user. A clientless user is simply a username and password that have been configured in the NAD to be used in a RADIUS authentication packet when no credentials have been received during the posture validation process. A corresponding user is created in Cisco Secure ACS with the appropriate access limitations. For example, the user is placed into the unknown group in Cisco Secure ACS or another group with specific access restrictions enforced by downloadable ACLs. This limits the access of non-responsive clients according to the security policy.

Default Access

A third way to handle non-responsive hosts is to allow them to fail the posture checking process without a static policy configured and without permitting a clientless user. This prevents any access other than what is expressly permitted by the interface ACL configured on the router interface on which the posture validation occurs.

System Components

NAC consists of components from Cisco and various third-party vendors. NAC requires a supported Cisco IOS software platform (a router) between the client undergoing the admissions process and the protected network. NAC also requires Cisco Secure ACS version 3.3 or later as an integral part of the admissions control process. The CTA is a client-side component provided by Cisco that resides on the client and provides an interface to supported third-party software.

This section provides some detailed information about the required system components and includes the following topics:

- Hardware Requirements
- Software Requirements

Hardware Requirements

This section describes the hardware requirements for NAC implementations and includes the following topics:

- Access Control Server Hardware Requirements
- Client Hardware Requirements
- Cisco IOS Software Platform Hardware Requirements

Access Control Server Hardware Requirements

Cisco Secure ACS requires an Intel workstation with the following minimum hardware requirements:

- Pentium III processor running at 550 Mhz or faster
- 256 MB of memory
- 250 MB of free disk space
- Minimum supported graphics resolution is 256 colors at 800 x 600 screen resolution

If a Cisco Secure ACS internal user database is running on the same computer running Cisco Secure ACS, more disk space is recommended.

Client Hardware Requirements

There are negligible additional requirements for the client machines other than the necessary memory and processor speed to run the anti-virus software and Cisco Security Agent. See the anti-virus vendor or CSA documentation for further details about client requirements.

Cisco IOS Software Platform Hardware Requirements

The Cisco hardware platforms that are supported as NADs in a NAC implementation are shown in Table 1-1. This table also summarizes the software images that support NAC, the amount of flash memory required, and the amount of dynamic RAM required for each platform.

Table 1-1 Cisco IOS Software Platform Hardware Requirements

Router Model	Image Name	DRAM Required	Flash Required
Cisco 83x Series Router	c831-k9o3sy6-mz c831-k9o3y6-mz	48 MB 48 MB	12 MB 8 MB
Cisco 1700 Series Router	c1700-adventerprisek9-mz c1700-advipservicesk9-mz c1700-advsecurityk9-mz	128 MB 96 MB 64 MB	32 MB 32 MB 16 MB
Cisco 1841 Integrated Services Router	c1841-advsecurityk9-mz.123-8.T5.bin	128 MB	32 MB
Cisco 2600XM IP Communications Voice/Fax NM	c2600-adventerprisek9-mz c2600-advipservicesk9-mz c2600-advsecurityk9-mz	128 MB 128 MB 96 MB	32 MB 32MB 32 MB
Cisco 2691 Multiservice Platform	c2691-adventerprisek9-mz c2691-advipservicesk9-mz c2691-advsecurityk9-mz	128 MB 128 MB 128 MB	64 MB 64 MB 32 MB
Cisco 2801 Integrated Services Router	c2801-advsecurityk9-mz.123-8.T5.bin c2801-advipservicesk9-mz.123-8.T5.bin c2801-adventerprisek9-mz.123-8.T5.bin	128 MB	64 MB
Cisco 2811, 2821, 2851 Integrated Services Router	c2800nm-advsecurityk9-mz.123-8.T5.bin c2800nm-advipservicesk9-mz.123-8.T5.binc 2800nm-adventerprisek9-mz.123-8.T5.bin	256 MB	64 MB

Table 1-1 Cisco IOS Software Platform Hardware Requirements (continued)

Router Model	Image Name	DRAM Required	Flash Required
Cisco 3640 Multiservice Platform	c3640-jk9o3s-mz	128 MB	32 MB
Cisco 3660-ENT Series Router	c3660-jk9s-mz	128MB	64 MB
Cisco 3725/3745 Multiservice Access Router	c37x5-adventerprisek9-mz c37x5-advipservicesk9-mz c37x5-advsecurityk9-mz	128 MB 128 MB 128 MB	64 MB 64 MB 32 MB
Cisco 3825 Integrated Services Router	c3825-advsecurityk9-mz.123-11.T2.bin	256 MB	64 MB
Cisco 3845 Integrated Services Router	c3845-advsecurityk9-mz.123-11.T2.bin	256 MB	64 MB
Cisco 7200 Series Router	c7200-jk9o3s-mz	128MB	48 MB

Each successfully validated client consumes a fixed amount of about 6 Kb. In addition, each downloadable ACL applied as a dynamic entry uses an additional .8 Kb of memory.

Software Requirements

NAC requires the following software:

- Cisco Secure ACS
- CTA on each client
- PP provided by a supported third-party anti-virus vendor

A posture validation server, which can be obtained from the anti-virus vendor with the appropriate PP, is optional. Table 1-2 summarizes the specific requirements for each of these components.

Table 1-2 Software Requirements

Component	Software Requirement
Access Control Server	• Any of the following: – Windows 2000 Server or Advanced Server with Microsoft Service Pack 3 or 4 – Windows 2003 Server Enterprise Edition • Either of the following: – Internet Explorer version 6.0 SP1 – Netscape 7.0.2 for browser access English language versions only are supported at this time. For further details, see the latest release notes available at the following URL: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/3.3/release/notes/RNwin332.html
Cisco Trust Agent	One of the following: • Microsoft Windows 2000 • Microsoft Windows XP • Microsoft Windows NT version 4.0 with Service Pack 4 or later • One or more posture plug-ins provided by a NAC-supported vendor
Cisco IOS software images	Advanced security images or greater, beginning with version 12.3(8)T. IOS version 12.3(8)T5 is recommended.

Third-Party Supported Software

A variety of third-party Cisco partners provide software that participates in the NAC solution. A list of the supported software and the third-party vendors can be found at the following URL: http://www.cisco.com/en/US/partners/pr46/nac/partners.html.

Implementing Network Admission Control

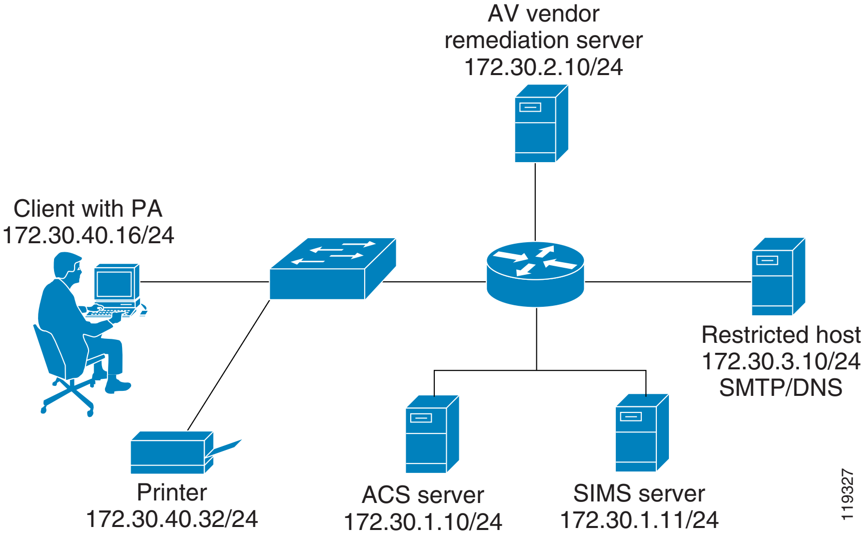
This chapter describes how to implement Network Admission Control (NAC) and includes the following sections:

- Network Topology
- Configuration Overview
- Installing and Configuring the Cisco Secure ACS Server
- Configuring Client Credentials and Type Length Value Data
- Configuration Tips
- Installing the Posture Agent and Remediation Server
- Configuring the Cisco IOS Software NAD

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:

- Configuration Overview
- Installing Cisco Secure ACS
- Configuring the Administrator Interface to Cisco Secure ACS
- Allowing Administrator Access Via HTTP
- Installing the Cisco Secure ACS Server Certificate
- Generating Signing Request, Enrolling and Installing Certificate
- Using a Self-Signed Certificate
- Configuring Logging
- Configuring a NAD in Cisco Secure ACS
- Configuring Network Access Filters
- Configuring Downloadable IP ACLs
- Configuring Groups and Vendor Specific Attributes
- Clientless User Configuration (Non-Responsive Hosts)
- Setting Up and Enabling Global EAP Authentication
- Configuring External User Databases
- Configuring Token to User Group Mappings
- Configuring an Unknown User Policy to Check an External Database

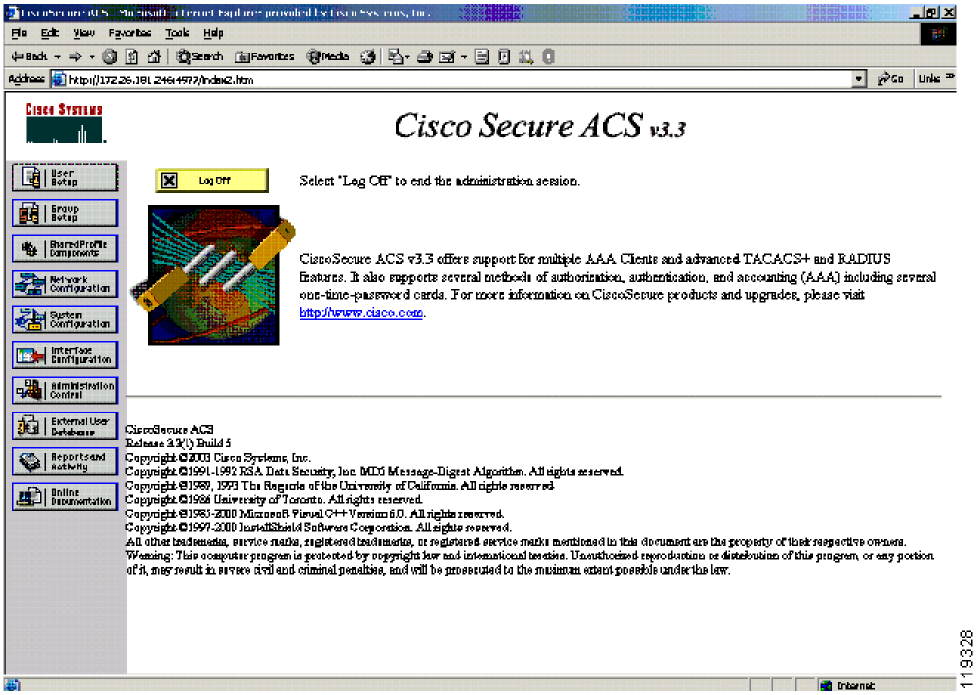
Installing Cisco Secure ACS

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



Cisco Secure ACS v3.3

Select "Log Off" to end the administration session.

CiscoSecure ACS v3.3 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.

CiscoSecure ACS
Release 3.3(1) Build 5
Copyright ©2003 Cisco Systems, Inc.
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved.
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1983-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners.
Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

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.

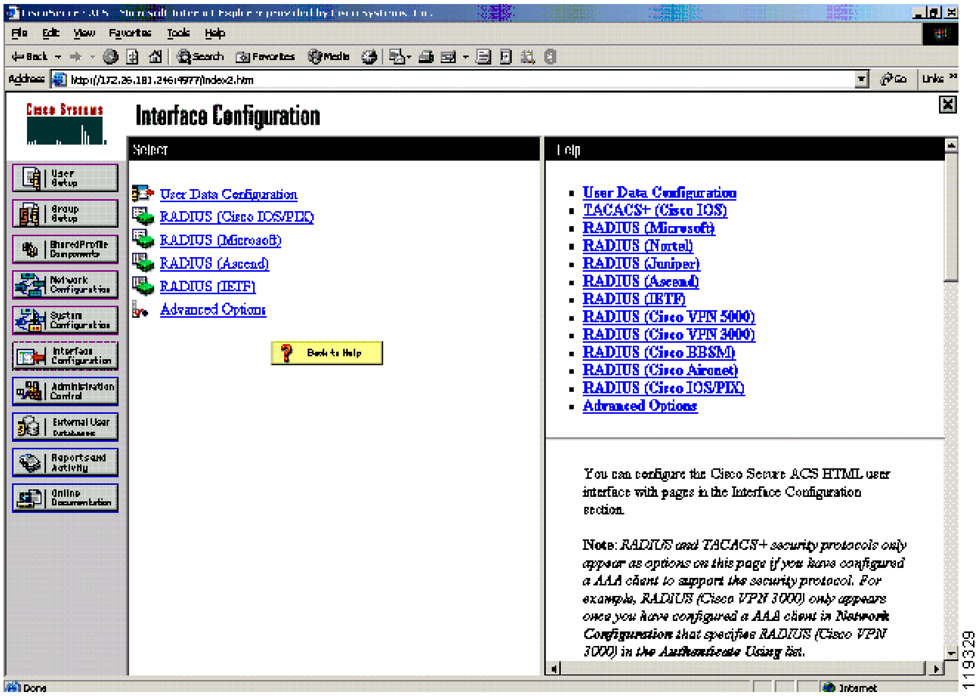
Configuring the Administrator Interface to Cisco Secure ACS

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



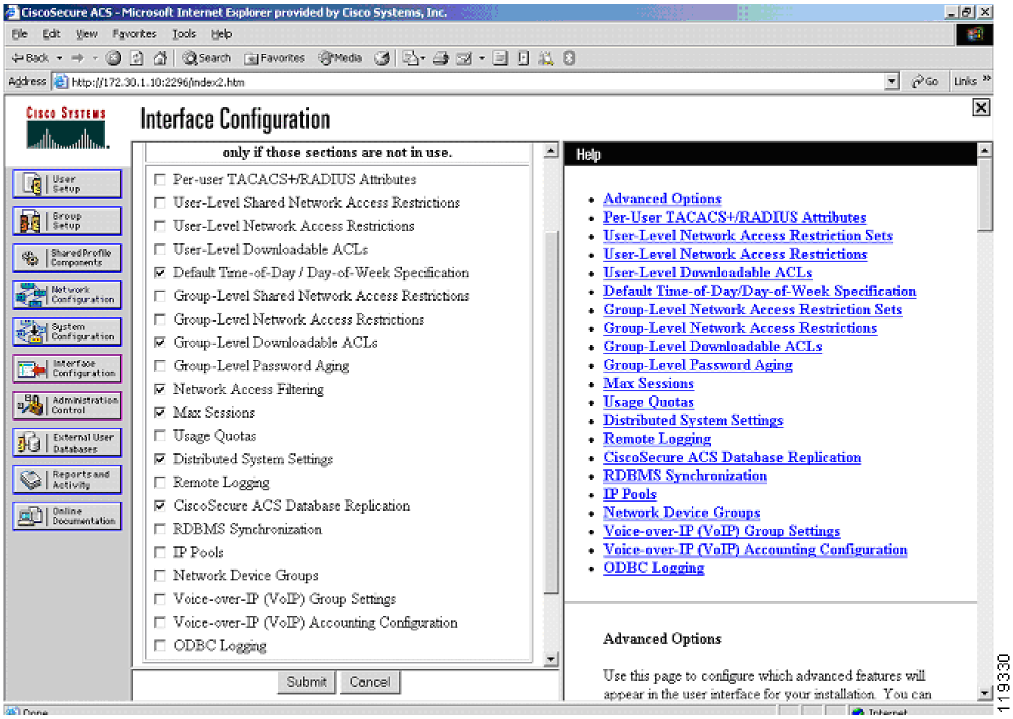
You can configure the Cisco Secure ACS HTML user interface with pages in the Interface Configuration section.

Note: *RADIUS and TACACS+ security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco VPN 3000) only appears once you have configured a AAA client in **Network Configuration** that specifies RADIUS (Cisco VPN 3000) in the **Authenticate Using** list.*

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



Interface Configuration

only if those sections are not in use.

- ☐ Per-user TACACS+/RADIUS Attributes
- ☐ User-Level Shared Network Access Restrictions
- ☐ User-Level Network Access Restrictions
- ☐ User-Level Downloadable ACLs
- ☑ Default Time-of-Day / Day-of-Week Specification
- ☐ Group-Level Shared Network Access Restrictions
- ☐ Group-Level Network Access Restrictions
- ☑ Group-Level Downloadable ACLs
- ☐ Group-Level Password Aging
- ☑ Network Access Filtering
- ☑ Max Sessions
- ☐ Usage Quotas
- ☑ Distributed System Settings
- ☐ Remote Logging
- ☑ CiscoSecure ACS Database Replication
- ☐ RDBMS Synchronization
- ☐ IP Pools
- ☐ Network Device Groups
- ☐ Voice-over-IP (VoIP) Group Settings
- ☐ Voice-over-IP (VoIP) Accounting Configuration
- ☐ ODBC Logging

Help

- Advanced Options
- Per-User TACACS+/RADIUS Attributes
- User-Level Network Access Restriction Sets
- User-Level Network Access Restrictions
- User-Level Downloadable ACLs
- Default Time-of-Day/Day-of-Week Specification
- Group-Level Network Access Restriction Sets
- Group-Level Network Access Restrictions
- Group-Level Downloadable ACLs
- Group-Level Password Aging
- Max Sessions
- Usage Quotas
- Distributed System Settings
- Remote Logging
- CiscoSecure ACS Database Replication
- RDBMS Synchronization
- IP Pools
- Network Device Groups
- Voice-over-IP (VoIP) Group Settings
- Voice-over-IP (VoIP) Accounting Configuration
- ODBC Logging

Advanced Options

Use this page to configure which advanced features will appear in the user interface for your installation. You can

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.

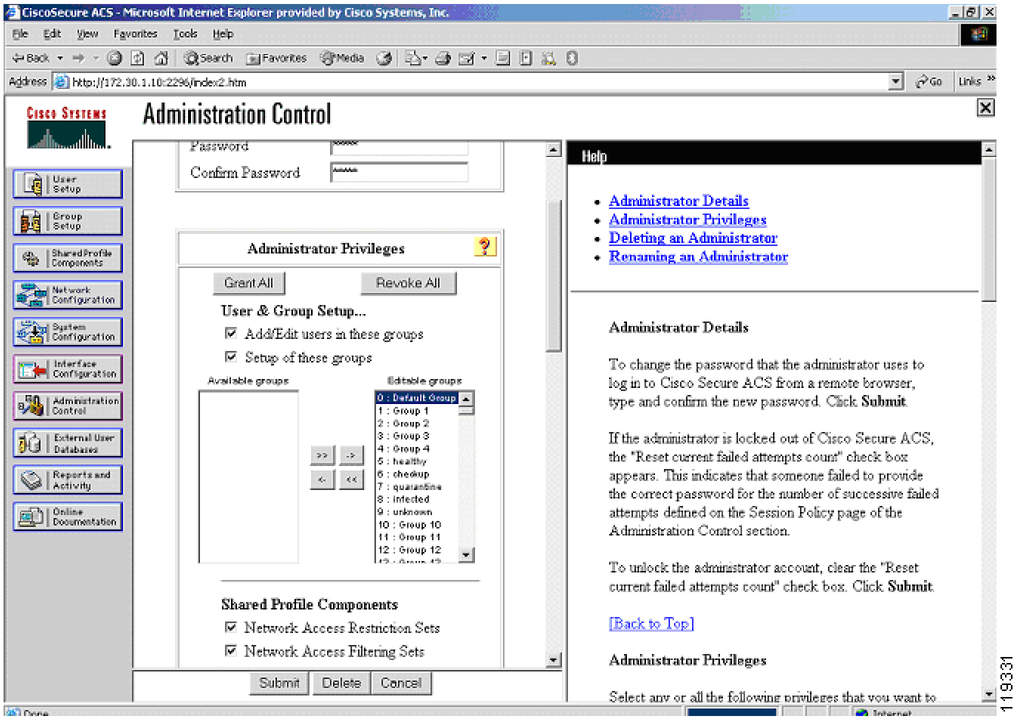
Allowing Administrator Access Via HTTP

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



Password
Confirm Password

Administrator Privileges

User & Group Setup...

☑ Add/Edit users in these groups

☑ Setup of these groups

0 : Default Group
1 : Group 1
2 : Group 2
3 : Group 3
4 : Group 4
5 : healthy
6 : checkup
7 : quarantine
8 : infected
9 : unknown
10 : Group 10
11 : Group 11
12 : Group 12

Shared Profile Components

☑ Network Access Restriction Sets

☑ Network Access Filtering Sets

- Administrator Details
- Administrator Privileges
- Deleting an Administrator
- Renaming an Administrator

Administrator Details

To change the password that the administrator uses to log in to Cisco Secure ACS from a remote browser, type and confirm the new password. Click **Submit**.

If the administrator is locked out of Cisco Secure ACS, the "Reset current failed attempts count" check box appears. This indicates that someone failed to provide the correct password for the number of successive failed attempts defined on the Session Policy page of the Administration Control section.

To unlock the administrator account, clear the "Reset current failed attempts count" check box. Click **Submit**.

[Back to Top]

Administrator Privileges

Select any or all the following privileges that you want to

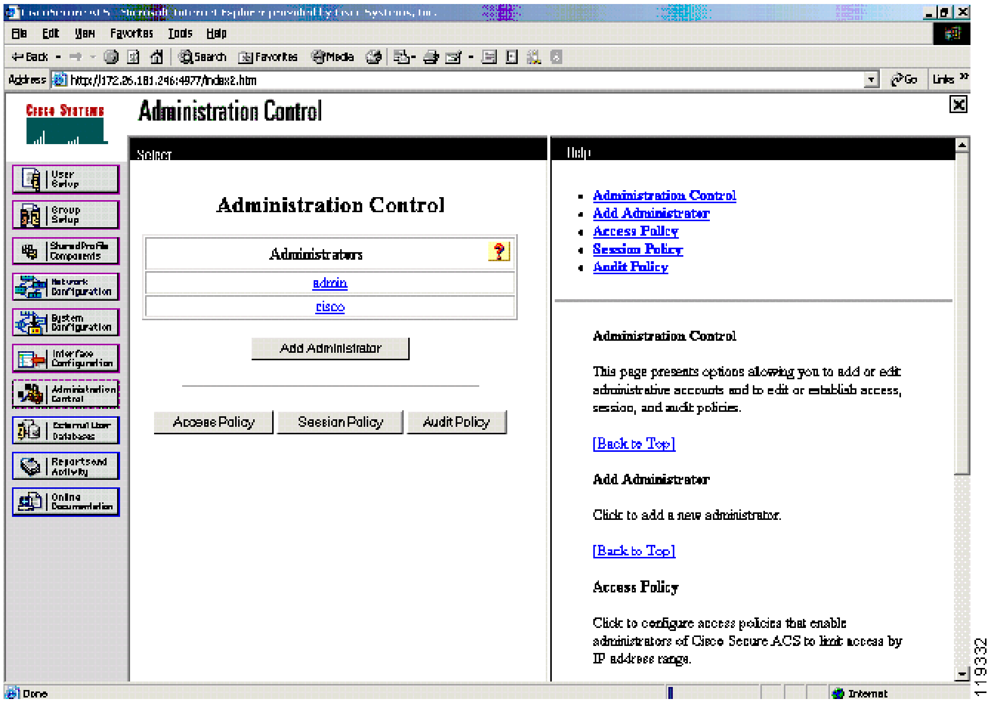
Step 2 Click **Add Administrator**. Fill in the username and password fields, and then configure the individual administration group privileges as needed.

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



Administration Control

Administrators
admin
cisco

- Administration Control
- Add Administrator
- Access Policy
- Session Policy
- Audit Policy

Administration Control

This page presents options allowing you to add or edit administrative accounts and to edit or establish access, session, and audit policies.

[Back to Top]

Add Administrator

Click to add a new administrator.

[Back to Top]

Access Policy

Click to configure access policies that enable administrators of Cisco Secure ACS to limit access by IP address range.

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.

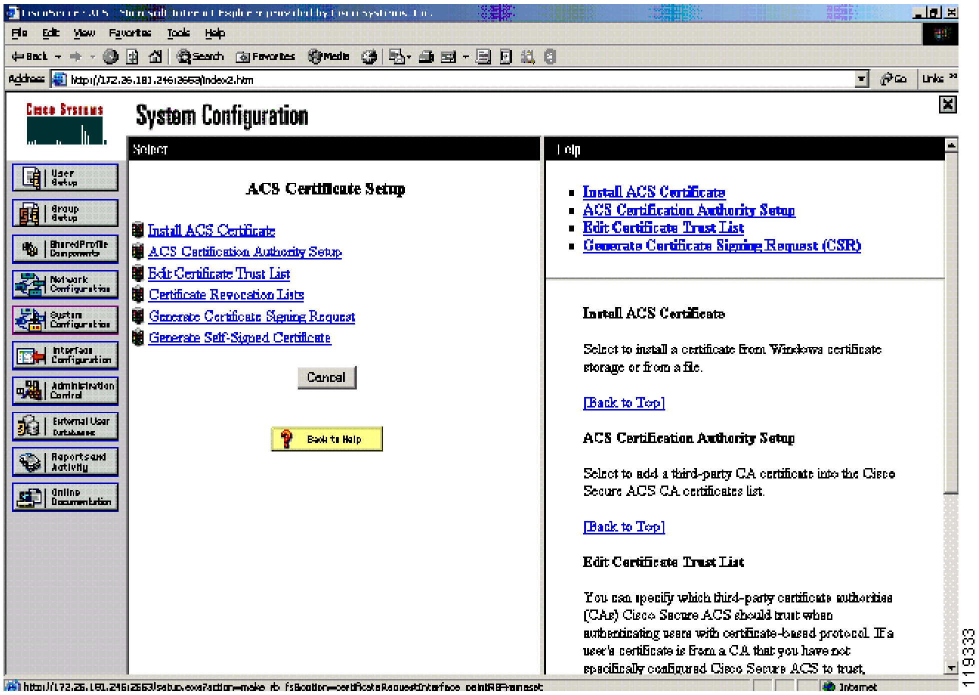
To install a public/private key pair that are generated on an external server, perform the following steps:

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



System Configuration

ACS Certificate Setup

- Install ACS Certificate
- ACS Certification Authority Setup
- Edit Certificate Trust List
- Certificate Revocation Lists
- Generate Certificate Signing Request
- Generate Self-Signed Certificate

- Install ACS Certificate
- ACS Certification Authority Setup
- Edit Certificate Trust List
- Generate Certificate Signing Request (CSR)

Install ACS Certificate

Select to install a certificate from Windows certificate storage or from a file.

[Back to Top]

ACS Certification Authority Setup

Select to add a third-party CA certificate into the Cisco Secure ACS CA certificates list.

[Back to Top]

Edit Certificate Trust List

You can specify which third-party certificate authorities (CAs) Cisco Secure ACS should trust when authenticating users with certificate-based protocol. If a user's certificate is from a CA that you have not specifically configured Cisco Secure ACS to trust,

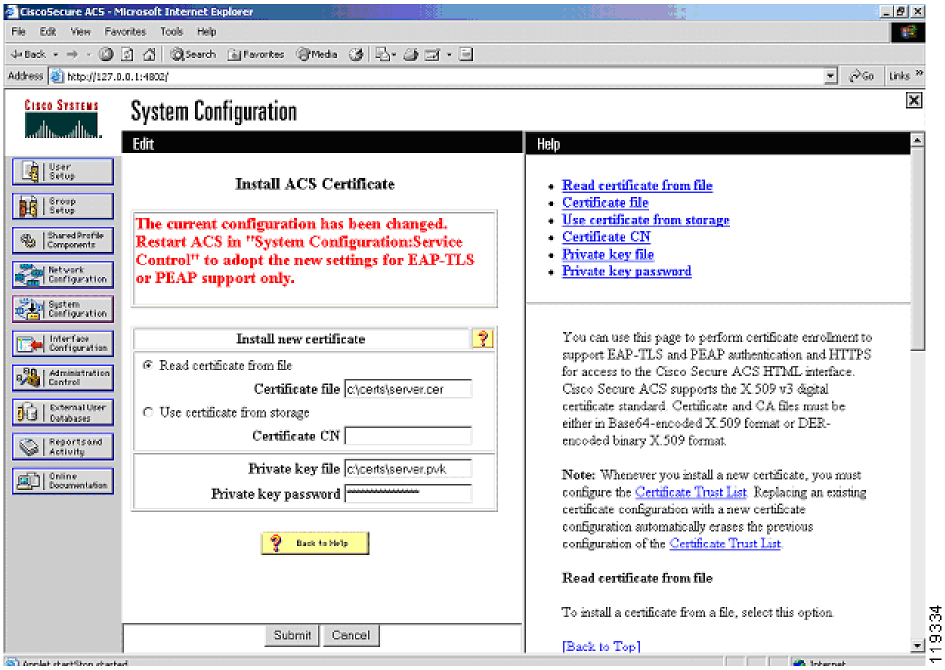
You perform all certificate management operations from this window.

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



Install ACS Certificate

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Install new certificate

● Read certificate from file

Certificate file c:\certs\server.cer

○ Use certificate from storage

Certificate CN

Private key file c:\certs\server.pvk

Private key password ****************

- Read certificate from file
- Certificate file
- Use certificate from storage
- Certificate CN
- Private key file
- Private key password

You can use this page to perform certificate enrollment to support EAP-TLS and PEAP authentication and HTTPS for access to the Cisco Secure ACS HTML interface. Cisco Secure ACS supports the X.509 v3 digital certificate standard. Certificate and CA files must be either in Base64-encoded X.509 format or DER-encoded binary X.509 format.

Note: Whenever you install a new certificate, you must configure the Certificate Trust List. Replacing an existing certificate configuration with a new certificate configuration automatically erases the previous configuration of the Certificate Trust List.

Read certificate from file

To install a certificate from a file, select this option.

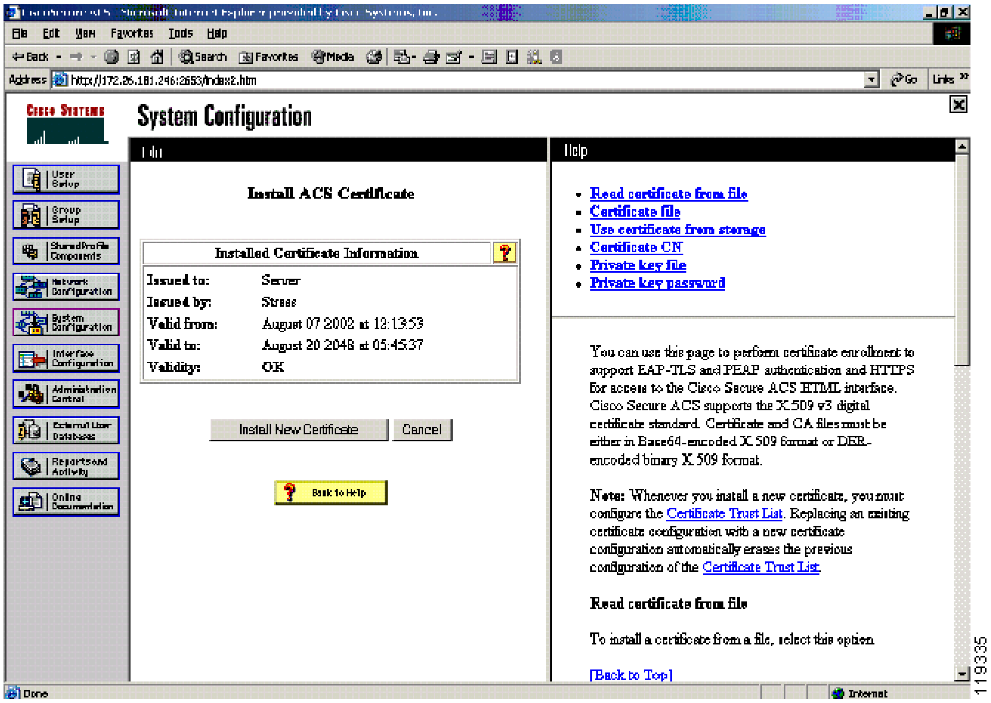
[Back to Top]

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



Install ACS Certificate

Installed Certificate Information

Issued to:	Server
Issued by:	Stress
Valid from:	August 07 2002 at 12:13:53
Valid to:	August 20 2048 at 05:45:37
Validity:	OK

- Read certificate from file
- Certificate file
- Use certificate from storage
- Certificate CN
- Private key file
- Private key password

You can use this page to perform certificate enrollment to support EAP-TLS and PEAP authentication and HTTPS for access to the Cisco Secure ACS HTML interface. Cisco Secure ACS supports the X.509 v3 digital certificate standard. Certificate and CA files must be either in Base64-encoded X.509 format or DER-encoded binary X.509 format.

Note: Whenever you install a new certificate, you must configure the Certificate Trust List. Replacing an existing certificate configuration with a new certificate configuration automatically erases the previous configuration of the Certificate Trust List.

Read certificate from file

To install a certificate from a file, select this option.

[Back to Top]

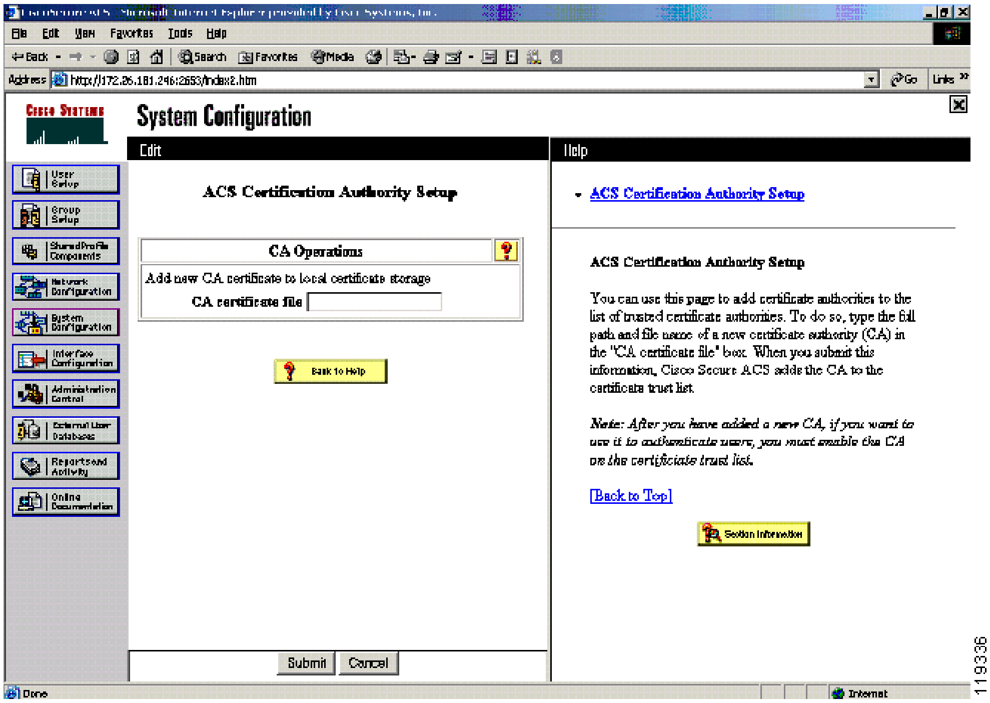
Step 6 To install the CA certificate, click **System Configuration** on the Cisco Secure ACS main menu.

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



System Configuration

ACS Certification Authority Setup

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

ACS Certification Authority Setup

ACS Certification Authority Setup

You can use this page to add certificate authorities to the list of trusted certificate authorities. To do so, type the full path and file name of a new certificate authority (CA) in the "CA certificate file" box. When you submit this information, Cisco Secure ACS adds the CA to the certificate trust list.

Note: After you have added a new CA, if you want to use it to authenticate users, you must enable the CA on the certificate trust list.

[Back to Top]

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.

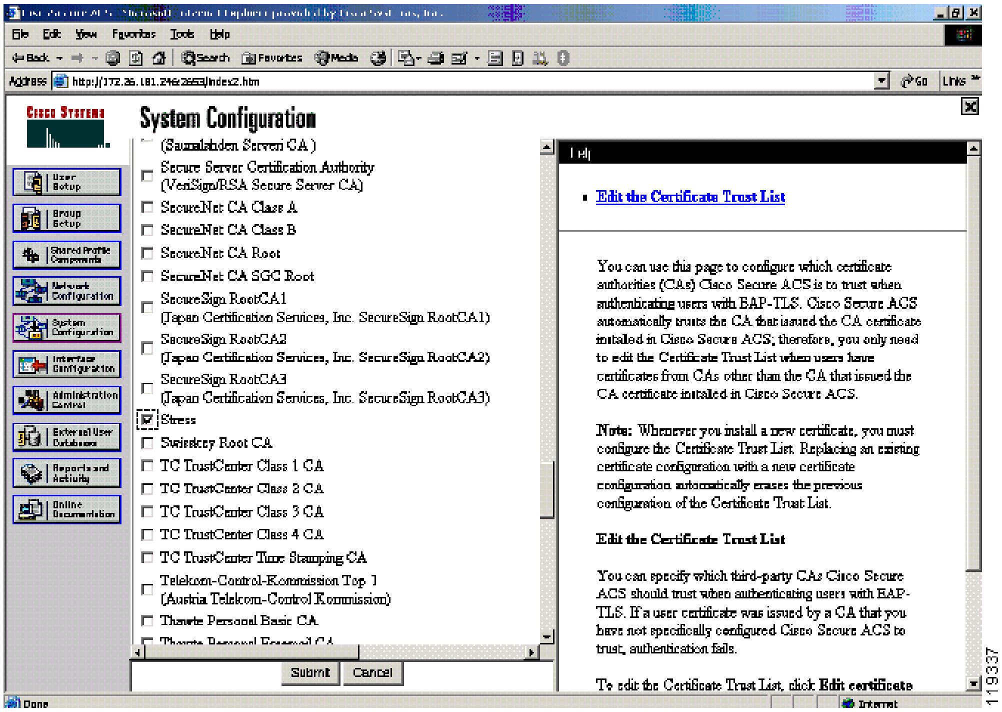
Step 11 To add the stress CA certificate to the trusted list, click **System Configuration** on the Cisco Secure ACS main menu.

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



(Saunalahden Serveri CA)

□ Secure Server Certification Authority (VeriSign/RSA Secure Server CA)

□ SecureNet CA Class A

□ SecureNet CA Class B

□ SecureNet CA Root

□ SecureNet CA SGC Root

□ SecureSign RootCA1 (Japan Certification Services, Inc. SecureSign RootCA1)

□ SecureSign RootCA2 (Japan Certification Services, Inc. SecureSign RootCA2)

□ SecureSign RootCA3 (Japan Certification Services, Inc. SecureSign RootCA3)

☑ Stress

□ Swisskey Root CA

□ TC TrustCenter Class 1 CA

□ TC TrustCenter Class 2 CA

□ TC TrustCenter Class 3 CA

□ TC TrustCenter Class 4 CA

□ TC TrustCenter Time Stamping CA

□ Telekom-Control-Kommission Top 1 (Austria Telekom-Control Kommission)

□ Thawte Personal Basic CA

□ Thawte Personal Freemail CA

- Edit the Certificate Trust List

You can use this page to configure which certificate authorities (CAs) Cisco Secure ACS is to trust when authenticating users with EAP-TLS. Cisco Secure ACS automatically trusts the CA that issued the CA certificate installed in Cisco Secure ACS; therefore, you only need to edit the Certificate Trust List when users have certificates from CAs other than the CA that issued the CA certificate installed in Cisco Secure ACS.

Note: Whenever you install a new certificate, you must configure the Certificate Trust List. Replacing an existing certificate configuration with a new certificate configuration automatically erases the previous configuration of the Certificate Trust List.

Edit the Certificate Trust List

You can specify which third-party CAs Cisco Secure ACS should trust when authenticating users with EAP-TLS. If a user certificate was issued by a CA that you have not specifically configured Cisco Secure ACS to trust, authentication fails.

To edit the Certificate Trust List, click **Edit certificate**

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

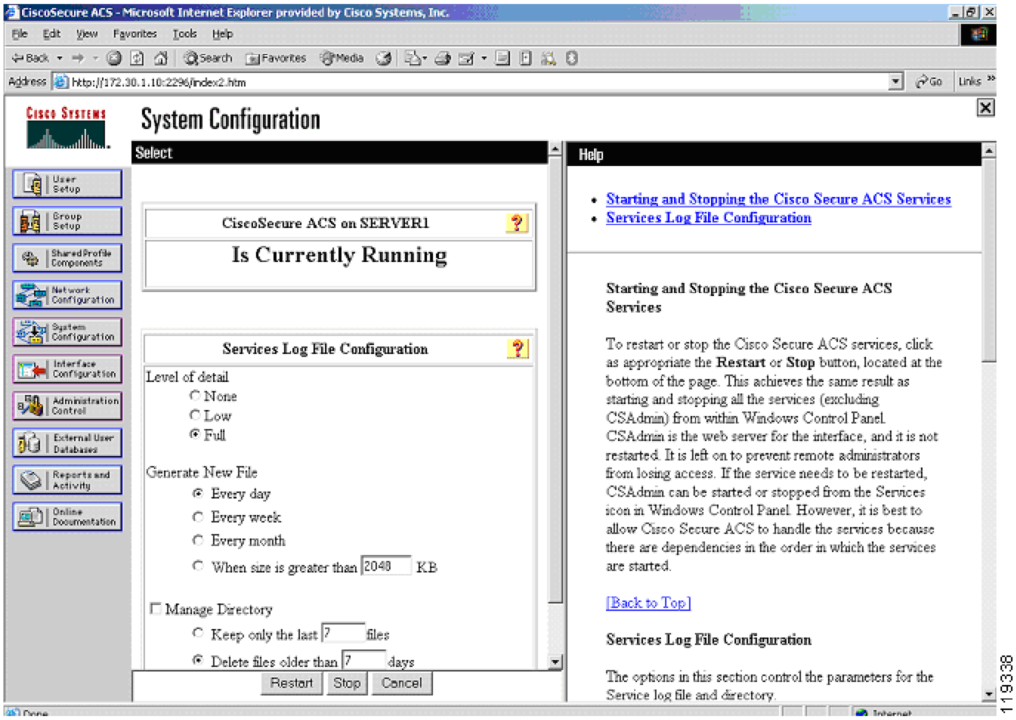
Step 15 Restart Cisco Secure ACS.

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



CiscoSecure ACS on SERVER1

Is Currently Running

Services Log File Configuration

Level of detail
○ None
○ Low
● Full

Generate New File
● Every day
○ Every week
○ Every month
○ When size is greater than 2048 KB

□ Manage Directory
○ Keep only the last 7 files
● Delete files older than 7 days

- Starting and Stopping the Cisco Secure ACS Services
- Services Log File Configuration

Starting and Stopping the Cisco Secure ACS Services

To restart or stop the Cisco Secure ACS services, click as appropriate the **Restart** or **Stop** button, located at the bottom of the page. This achieves the same result as starting and stopping all the services (excluding CSAdmin) from within Windows Control Panel. CSAdmin is the web server for the interface, and it is not restarted. It is left on to prevent remote administrators from losing access. If the service needs to be restarted, CSAdmin can be started or stopped from the Services icon in Windows Control Panel. However, it is best to allow Cisco Secure ACS to handle the services because there are dependencies in the order in which the services are started.

[Back to Top]

Services Log File Configuration

The options in this section control the parameters for the Service log file and directory.

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:

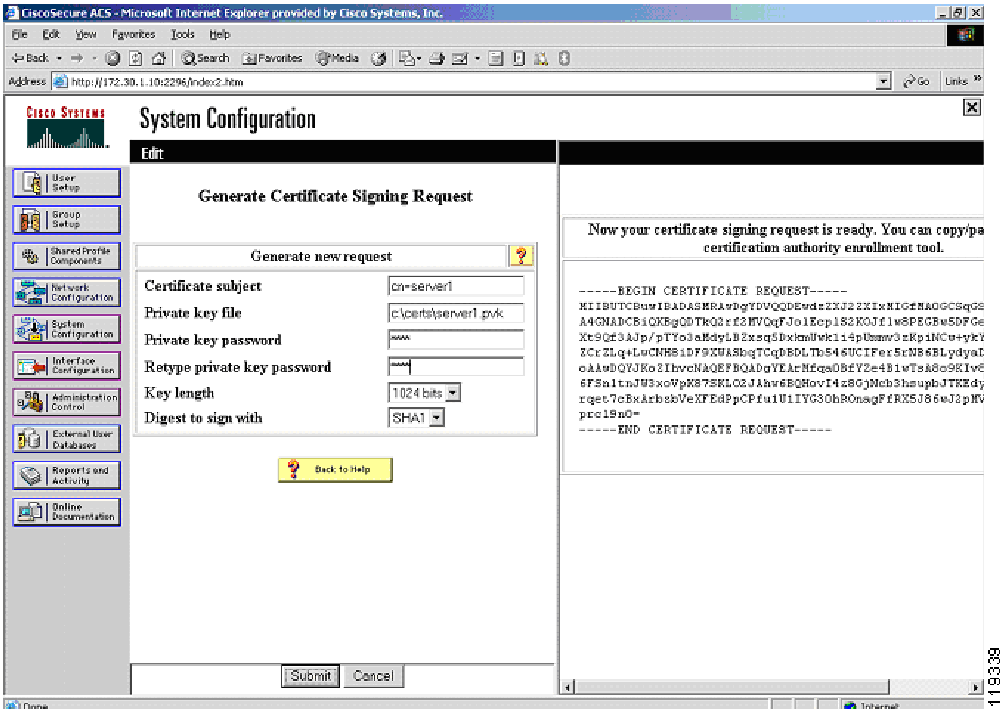
Step 1 In the Cisco Secure ACS Certificate Setup window, click **Generate Certificate Signing Request**.

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



Generate Certificate Signing Request

Generate new request	
Certificate subject	cn=server1
Private key file	c:\certs\server1.pvk
Private key password	****
Retype private key password	****
Key length	1024 bits
Digest to sign with	SHA1

Now your certificate signing request is ready. You can copy/pa
certification authority enrollment tool.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBUTCBuwIBADASMRAwDgYDVQQDEwdzZXJ2ZXIxMIGfMA0GCSqGS
A4GNADCBiQKBgQDTkQ2rf2MVQqFJolEcplS2KOJflw8PEGBw5DFGe
Xt9Qf3AJp/pTYo3aMdyLB2xsq5DxkmUwk1i4pUmmv3zKpiNCu+ykY
ZCrZLq+LwCNH8iDF9XWASbqTCqDBDLTb546UCIFer5rNB6BLydyaD
oAAwDQYJKoZIhvcNAQEFBQADgYEArMfqaOBfY2e4B1vTsA8o9KIv6
6FSnltnJW3xoVpK87SKLO2JAhw6BQHovI4z8GjNcb3hsupbJTKEdy
rqet7cBxArbzbVeXFEdPpCPfu1U1IYG3ObROnagFfRX5J86wJ2pMV
prc19nO=
-----END CERTIFICATE 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:

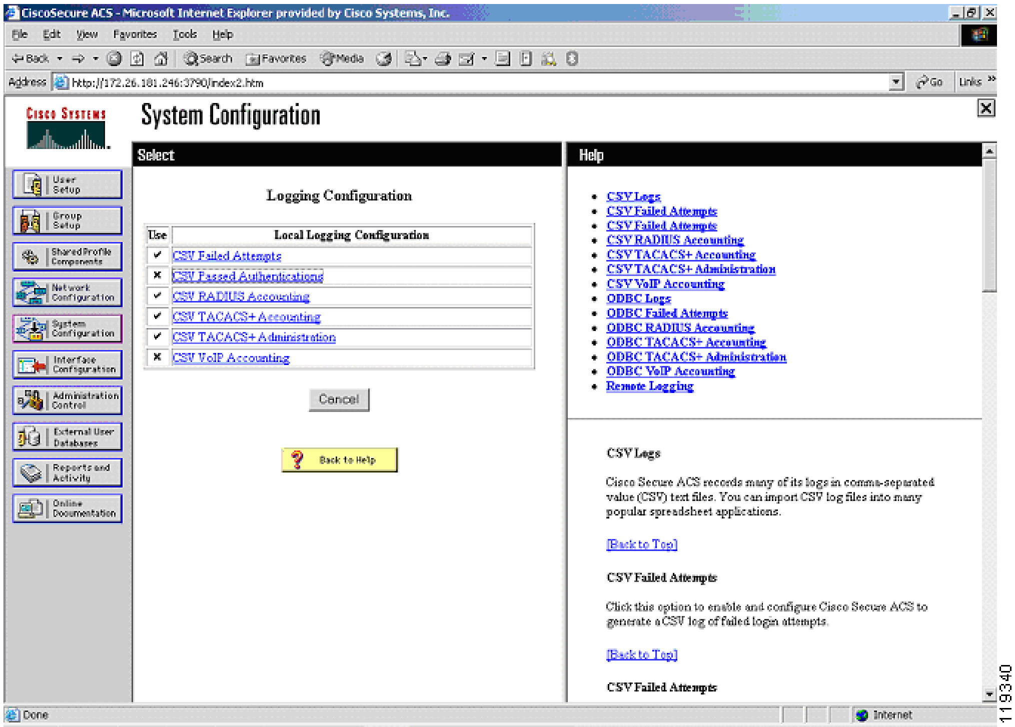
Step 1 Click **System Configuration** on the Cisco Secure ACS main menu.

Click **logging**.

Click **CSV Passed Authentications**.

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

Figure 2-14 Logging Configuration



Logging Configuration

Use	Local Logging Configuration
✓	CSV Failed Attempts
✗	CSV Passed Authentications
✓	CSV RADIUS Accounting
✓	CSV TACACS+ Accounting
✓	CSV TACACS+ Administration
✗	CSV VoIP Accounting

- CSV Logs
- CSV Failed Attempts
- CSV Failed Attempts
- CSV RADIUS Accounting
- CSV TACACS+ Accounting
- CSV TACACS+ Administration
- CSV VoIP Accounting
- ODBC Logs
- ODBC Failed Attempts
- ODBC RADIUS Accounting
- ODBC TACACS+ Accounting
- ODBC TACACS+ Administration
- ODBC VoIP Accounting
- Remote Logging

CSV Logs

Cisco Secure ACS records many of its logs in comma-separated value (CSV) text files. You can import CSV log files into many popular spreadsheet applications.

[Back to Top]

CSV Failed Attempts

Click this option to enable and configure Cisco Secure ACS to generate a CSV log of failed login attempts.

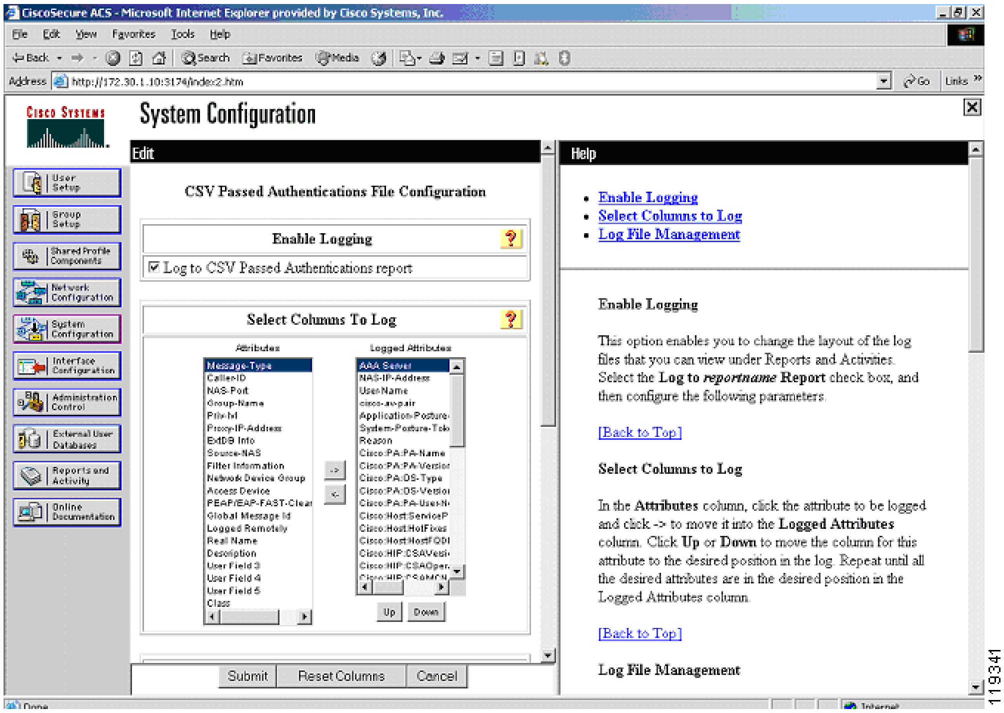
[Back to Top]

CSV Failed Attempts

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

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

Figure 2-15 Enable Logging



CSV Passed Authentications File Configuration

Enable Logging

☑ Log to CSV Passed Authentications report

Select Columns To Log

- Enable Logging
- Select Columns to Log
- Log File Management

Enable Logging

This option enables you to change the layout of the log files that you can view under Reports and Activities. Select the **Log to *reportname* Report** check box, and then configure the following parameters.

[Back to Top]

Select Columns to Log

In the **Attributes** column, click the attribute to be logged and click -> to move it into the **Logged Attributes** column. Click **Up** or **Down** to move the column for this attribute to the desired position in the log. Repeat until all the desired attributes are in the desired position in the Logged Attributes column.

[Back to Top]

Log File Management

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.

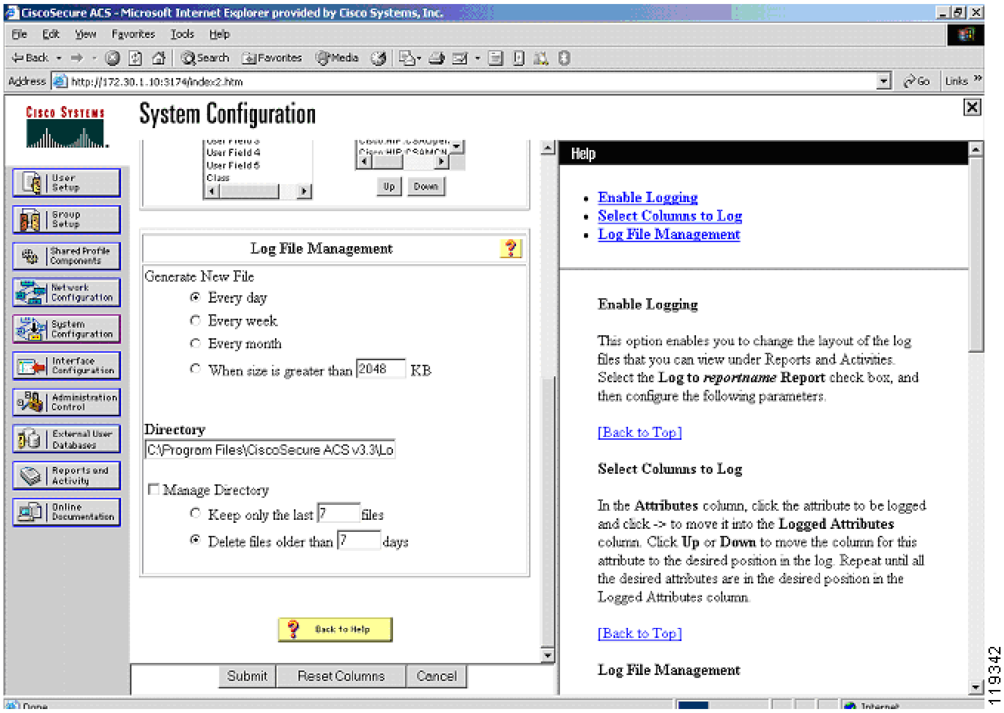
Step 6 Click **Submit**.

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



System Configuration

Log File Management

Generate New File
- ● Every day
- ○ Every week
- ○ Every month
- ○ When size is greater than 2048 KB

Directory
C:\Program Files\CiscoSecure ACS v3.3\Lo

□ Manage Directory
- ○ Keep only the last 7 files
- ● Delete files older than 7 days

Help

- Enable Logging
- Select Columns to Log
- Log File Management

Enable Logging

This option enables you to change the layout of the log files that you can view under Reports and Activities. Select the **Log to *reportname* Report** check box, and then configure the following parameters.

[Back to Top]

Select Columns to Log

In the **Attributes** column, click the attribute to be logged and click -> to move it into the **Logged Attributes** column. Click **Up** or **Down** to move the column for this attribute to the desired position in the log. Repeat until all the desired attributes are in the desired position in the Logged Attributes column.

[Back to Top]

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

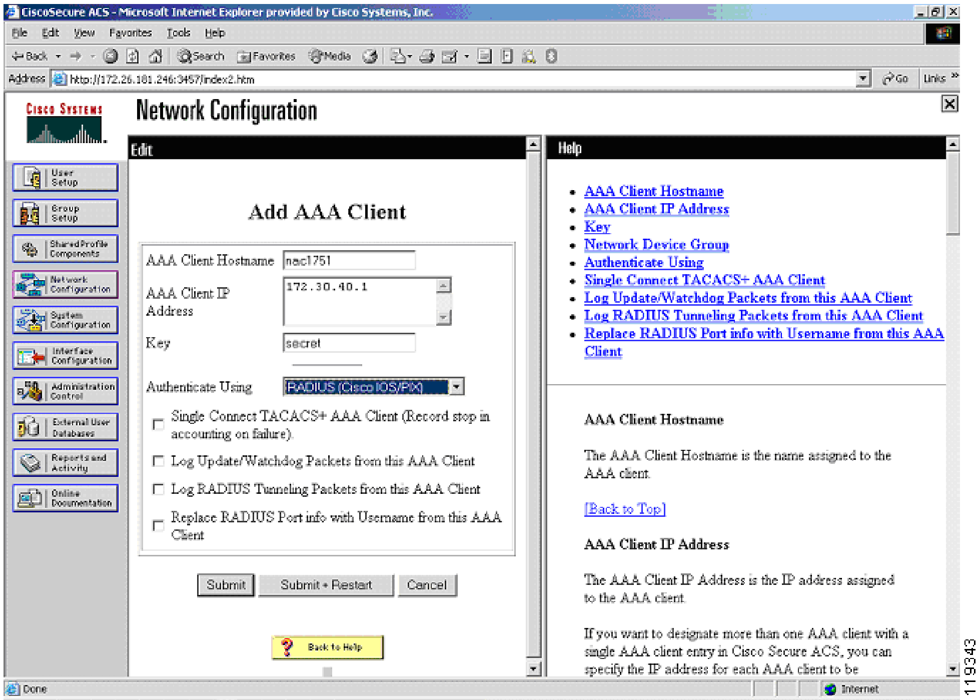
In Cisco Secure ACS terminology, a NAD is a AAA client.

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



Network Configuration

Add AAA Client

AAA Client Hostname: nac1751

AAA Client IP Address: 172.30.40.1

Key: secret

Authenticate Using: RADIUS (Cisco IOS/PIX)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

- AAA Client Hostname
- AAA Client IP Address
- Key
- Network Device Group
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[Back to Top]

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be

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

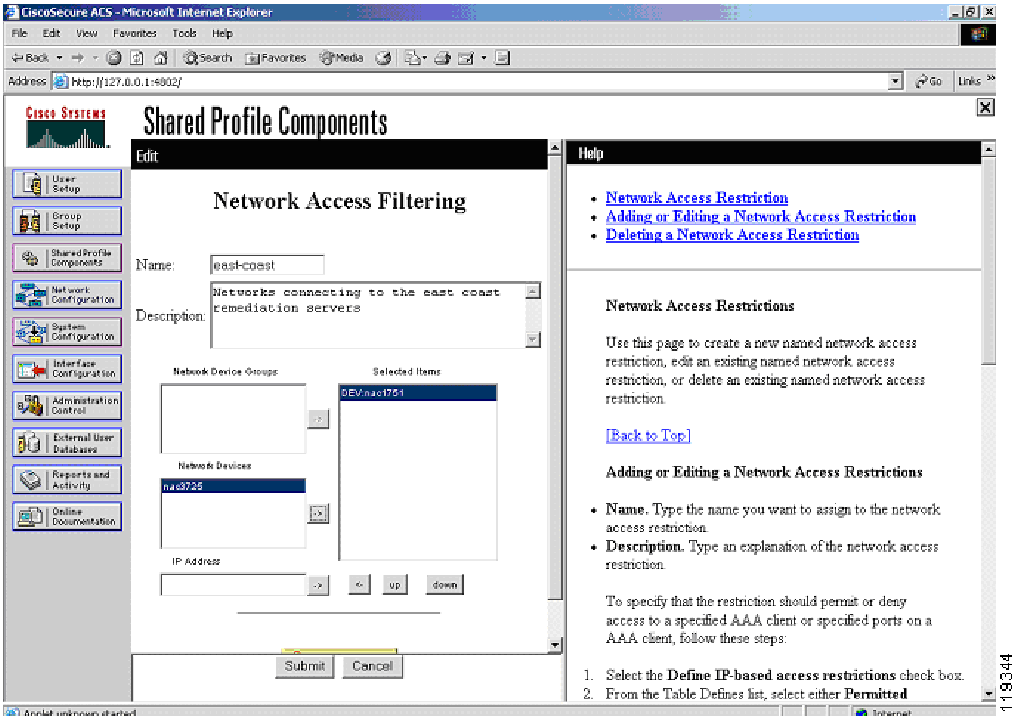
You can vary a downloadable ACL based on the NAD to which it is being downloaded. You might do this when remediation servers have been placed throughout the network and you want clients to connect to the closest remediation server. To do this, use Network Access Filtering (NAF). This feature allows you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



Network Access Filtering

Name: east-coast

Description: Networks connecting to the east coast remediation servers

Selected Items: DEV:nac1751

Network Devices: nac3725

- Network Access Restriction
- Adding or Editing a Network Access Restriction
- Deleting a Network Access Restriction

Network Access Restrictions

Use this page to create a new named network access restriction, edit an existing named network access restriction, or delete an existing named network access restriction.

[Back to Top]

Adding or Editing a Network Access Restrictions

- **Name.** Type the name you want to assign to the network access restriction.
- **Description.** Type an explanation of the network access restriction.

To specify that the restriction should permit or deny access to a specified AAA client or specified ports on a AAA client, follow these steps:

1. Select the **Define IP-based access restrictions** check box.
2. From the Table Defines list, select either **Permitted**

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

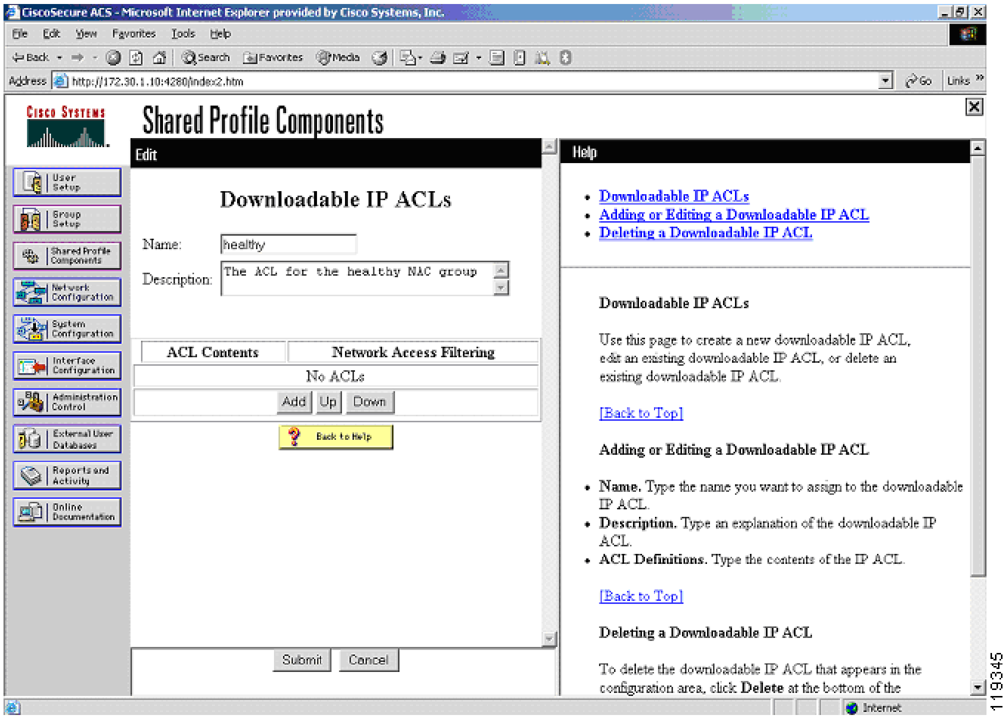
The enforcement action taken by the NAD is configured through Downloadable IP ACLs. Each category into which a client is validated must have a matching downloadable ACL associated with it. The access control entries contained in each ACL depend on your own network configuration and the access policy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



Downloadable IP ACLs

Name: healthy

Description: The ACL for the healthy NAC group

ACL Contents	Network Access Filtering
No ACLs	

- Downloadable IP ACLs
- Adding or Editing a Downloadable IP ACL
- Deleting a Downloadable IP ACL

Downloadable IP ACLs

Use this page to create a new downloadable IP ACL, edit an existing downloadable IP ACL, or delete an existing downloadable IP ACL.

[Back to Top]

Adding or Editing a Downloadable IP ACL

- **Name.** Type the name you want to assign to the downloadable IP ACL.
- **Description.** Type an explanation of the downloadable IP ACL.
- **ACL Definitions.** Type the contents of the IP ACL.

[Back to Top]

Deleting a Downloadable IP ACL

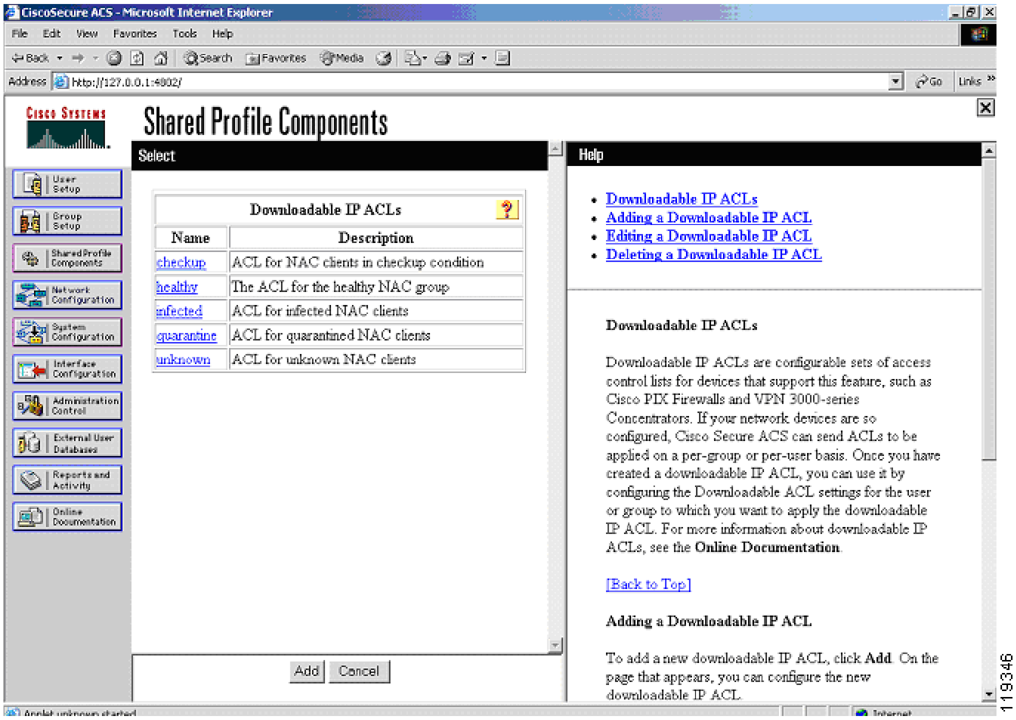
To delete the downloadable IP ACL that appears in the configuration area, click **Delete** at the bottom of the

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



Downloadable IP ACLs

Name	Description
checkup	ACL for NAC clients in checkup condition
healthy	The ACL for the healthy NAC group
infected	ACL for infected NAC clients
quarantine	ACL for quarantined NAC clients
unknown	ACL for unknown NAC clients

- Downloadable IP ACLs
- Adding a Downloadable IP ACL
- Editing a Downloadable IP ACL
- Deleting a Downloadable IP ACL

Downloadable IP ACLs

Downloadable IP ACLs are configurable sets of access control lists for devices that support this feature, such as Cisco PIX Firewalls and VPN 3000-series Concentrators. If your network devices are so configured, Cisco Secure ACS can send ACLs to be applied on a per-group or per-user basis. Once you have created a downloadable IP ACL, you can use it by configuring the Downloadable ACL settings for the user or group to which you want to apply the downloadable IP ACL. For more information about downloadable IP ACLs, see the **Online Documentation**.

[Back to Top]

Adding a Downloadable IP ACL

To add a new downloadable IP ACL, click **Add**. On the page that appears, you can configure the new downloadable IP ACL.

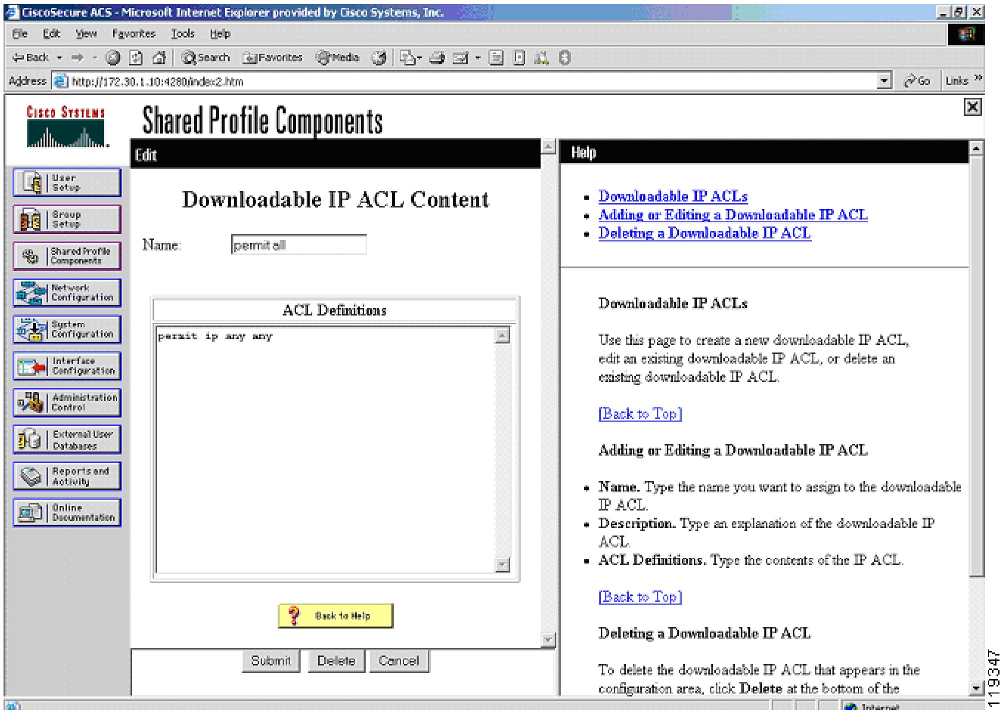
After creating the downloadable ACLs for each condition, define the ACLs that are actually sent to the individual NADs for enforcement action. The ACL elements vary depending on the policy set by the individual network administrator.

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



Shared Profile Components

Downloadable IP ACL Content

Name: permit all

ACL Definitions

```
permit ip any any
```

- Downloadable IP ACLs
- Adding or Editing a Downloadable IP ACL
- Deleting a Downloadable IP ACL

Downloadable IP ACLs

Use this page to create a new downloadable IP ACL, edit an existing downloadable IP ACL, or delete an existing downloadable IP ACL.

[Back to Top]

Adding or Editing a Downloadable IP ACL

- **Name.** Type the name you want to assign to the downloadable IP ACL.
- **Description.** Type an explanation of the downloadable IP ACL.
- **ACL Definitions.** Type the contents of the IP ACL.

[Back to Top]

Deleting a Downloadable IP ACL

To delete the downloadable IP ACL that appears in the configuration area, click **Delete** at the bottom of the

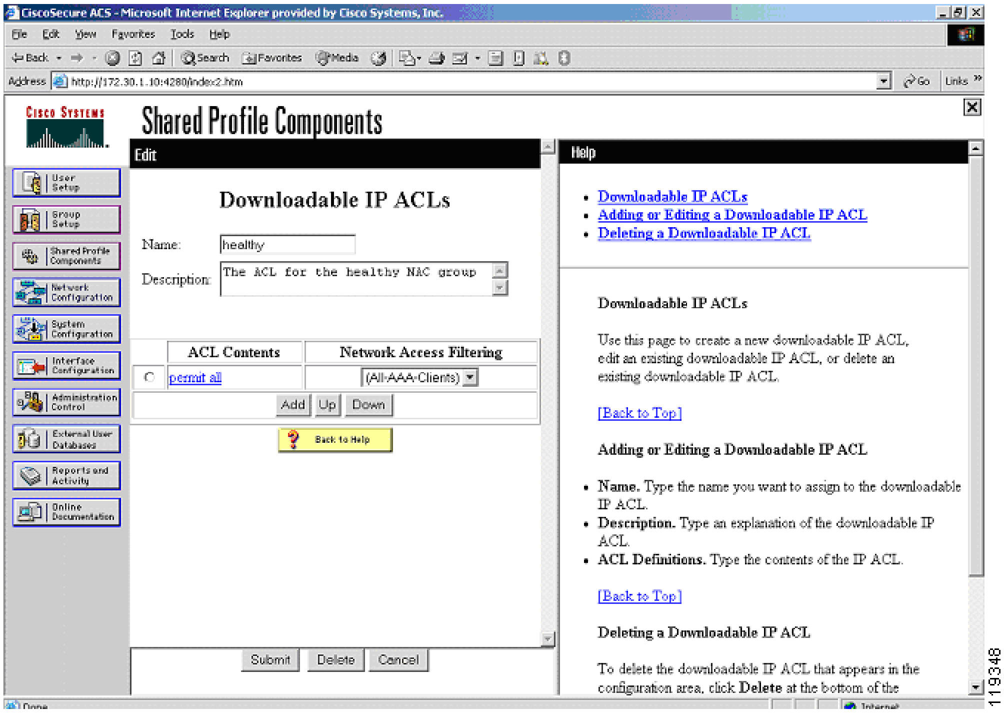
An example of the syntax for the ACL is **permit ip** *any any*. The first "any" in the ACL entry is replaced with the IP address of the host undergoing admission control to which this ACL is being applied. These ACLs are applied "over" the interface ACL. The downloadable IP ACL takes precedence over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


CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address http://172.30.1.10:4280/index2.htm

Shared Profile Components

Edit

Downloadable IP ACLs

Name: healthy

Description: The ACL for the healthy NAC group

	ACL Contents	Network Access Filtering
○	permit all	(All-AAA-Clients)

Help

- Downloadable IP ACLs
- Adding or Editing a Downloadable IP ACL
- Deleting a Downloadable IP ACL

Downloadable IP ACLs

Use this page to create a new downloadable IP ACL, edit an existing downloadable IP ACL, or delete an existing downloadable IP ACL.

[Back to Top]

Adding or Editing a Downloadable IP ACL

- **Name.** Type the name you want to assign to the downloadable IP ACL.
- **Description.** Type an explanation of the downloadable IP ACL.
- **ACL Definitions.** Type the contents of the IP ACL.

[Back to Top]

Deleting a Downloadable IP ACL

To delete the downloadable IP ACL that appears in the configuration area, click **Delete** at the bottom of the

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

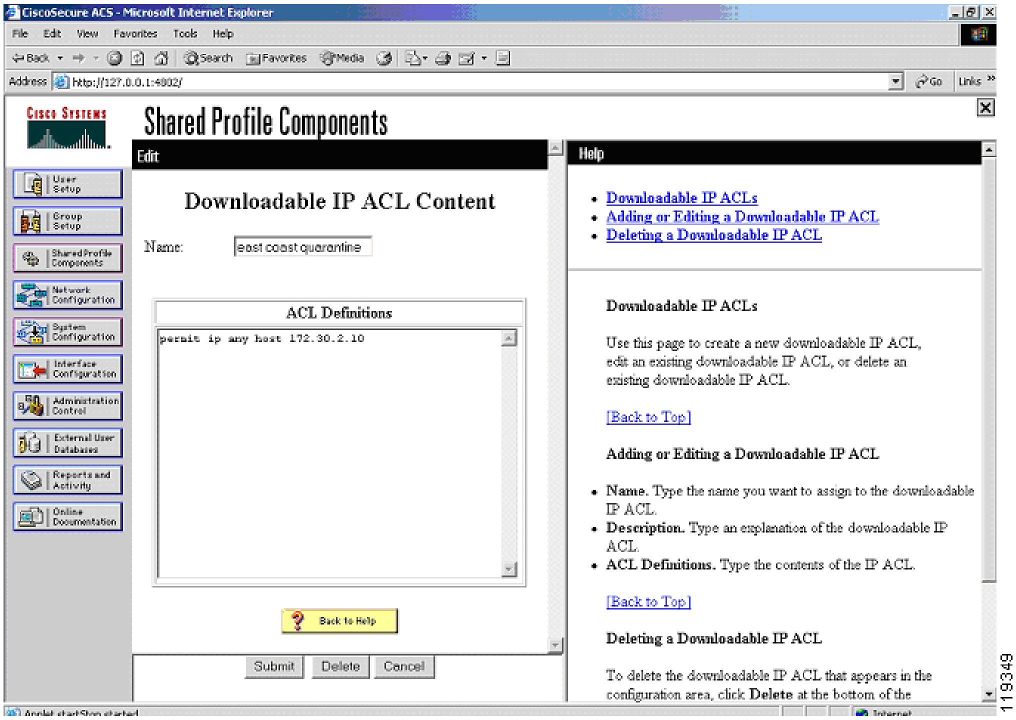
The next example for the quarantine ACL permits access only to the AV remediation server. NAFs are used to cause hosts in one section of the network to contact the closest remediation server.

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



Downloadable IP ACL Content

Name: east coast quarantine

ACL Definitions

```
permit ip any host 172.30.2.10
```

- Downloadable IP ACLs
- Adding or Editing a Downloadable IP ACL
- Deleting a Downloadable IP ACL

Downloadable IP ACLs

Use this page to create a new downloadable IP ACL, edit an existing downloadable IP ACL, or delete an existing downloadable IP ACL.

[Back to Top]

Adding or Editing a Downloadable IP ACL

- **Name.** Type the name you want to assign to the downloadable IP ACL.
- **Description.** Type an explanation of the downloadable IP ACL.
- **ACL Definitions.** Type the contents of the IP ACL.

[Back to Top]

Deleting a Downloadable IP ACL

To delete the downloadable IP ACL that appears in the configuration area, click **Delete** at the bottom of the

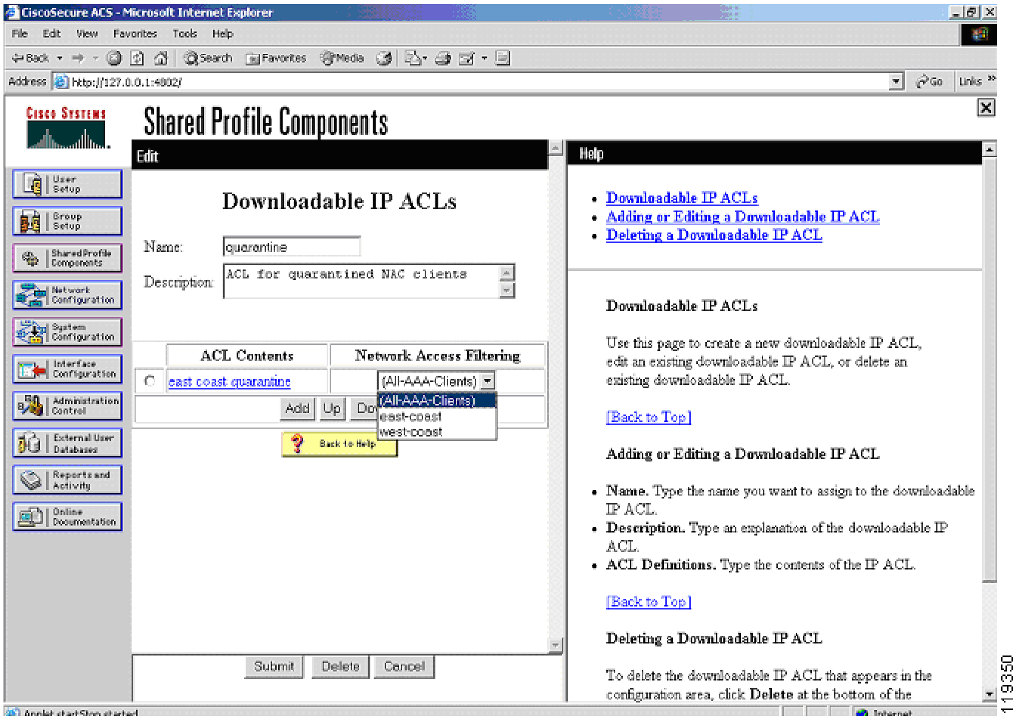
Step 10 Enter the individual lines for the ACL being written.

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



Shared Profile Components

Downloadable IP ACLs

Name: quarantine

Description: ACL for quarantined NAC clients

ACL Contents	Network Access Filtering
○ east coast quarantine	(All-AAA-Clients)

(All-AAA-Clients)
east-coast
west-coast

- Downloadable IP ACLs
- Adding or Editing a Downloadable IP ACL
- Deleting a Downloadable IP ACL

Downloadable IP ACLs

Use this page to create a new downloadable IP ACL, edit an existing downloadable IP ACL, or delete an existing downloadable IP ACL.

[Back to Top]

Adding or Editing a Downloadable IP ACL

- **Name.** Type the name you want to assign to the downloadable IP ACL.
- **Description.** Type an explanation of the downloadable IP ACL.
- **ACL Definitions.** Type the contents of the IP ACL.

[Back to Top]

Deleting a Downloadable IP ACL

To delete the downloadable IP ACL that appears in the configuration area, click **Delete** at the bottom of the

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.

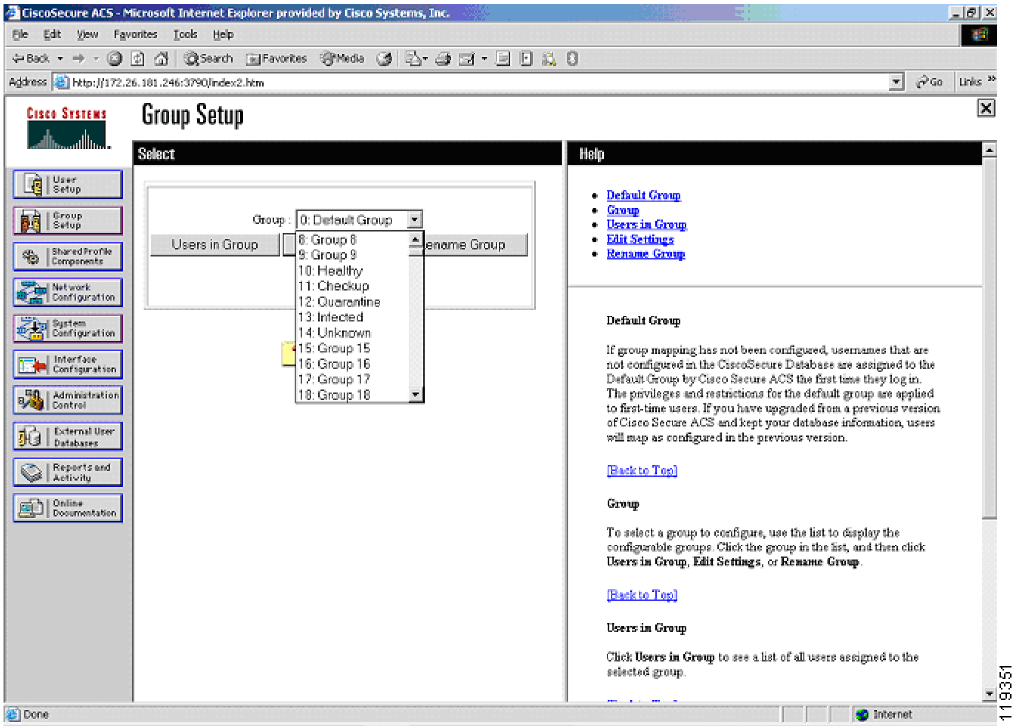
To configure groups and vendor specific attributes, complete the following steps:

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



- Default Group
- Group
- Users in Group
- Edit Settings
- Rename Group

Default Group

If group mapping has not been configured, usernames that are not configured in the CiscoSecure Database are assigned to the Default Group by Cisco Secure ACS the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version.

[Back to Top]

Group

To select a group to configure, use the list to display the configurable groups. Click the group in the list, and then click **Users in Group**, **Edit Settings**, or **Rename Group**.

[Back to Top]

Users in Group

Click **Users in Group** to see a list of all users assigned to the selected group.

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**.

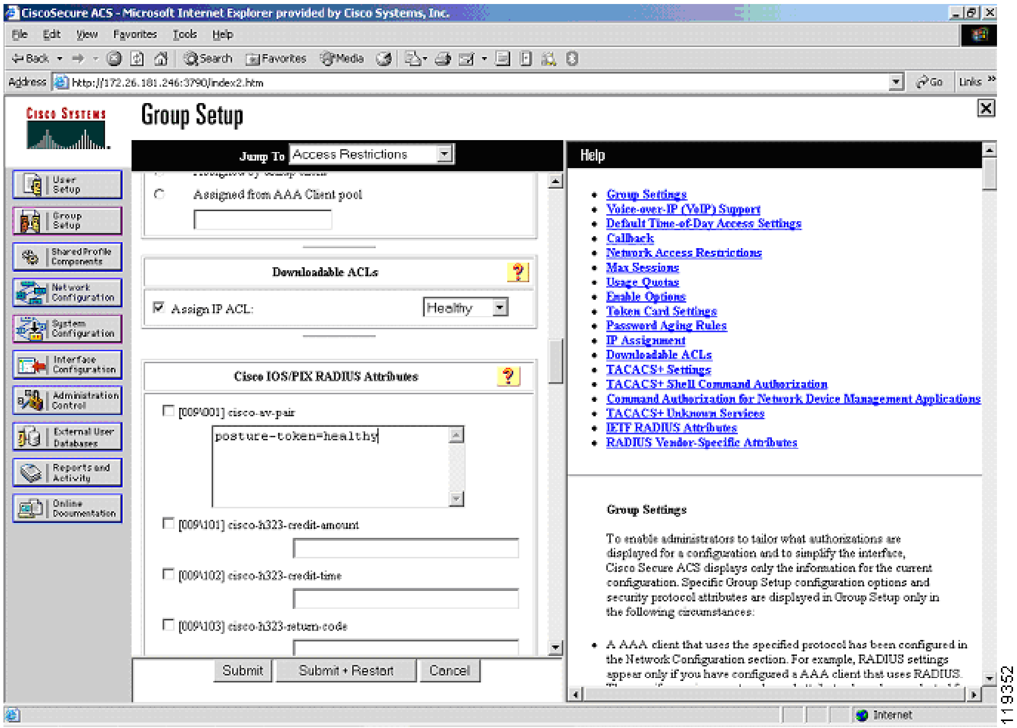
Step 4 Scroll down the edit window to the Downloadable ACLs window.

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



Group Setup

Jump To: Access Restrictions

○ Assigned from AAA Client pool

Downloadable ACLs

☑ Assign IP ACL: Healthy

Cisco IOS/PIX RADIUS Attributes

□ [009\001] cisco-av-pair

posture-token=healthy

□ [009\101] cisco-h323-credit-amount

□ [009\102] cisco-h323-credit-time

□ [009\103] cisco-h323-return-code

Help

- Group Settings
- Voice-over-IP (VoIP) Support
- Default Time-of-Day Access Settings
- Callback
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Enable Options
- Token Card Settings
- Password Aging Rules
- IP Assignment
- Downloadable ACLs
- TACACS+ Settings
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Group Settings

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Cisco Secure ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in Group Setup only in the following circumstances:

- A AAA client that uses the specified protocol has been configured in the Network Configuration section. For example, RADIUS settings appear only if you have configured a AAA client that uses RADIUS.

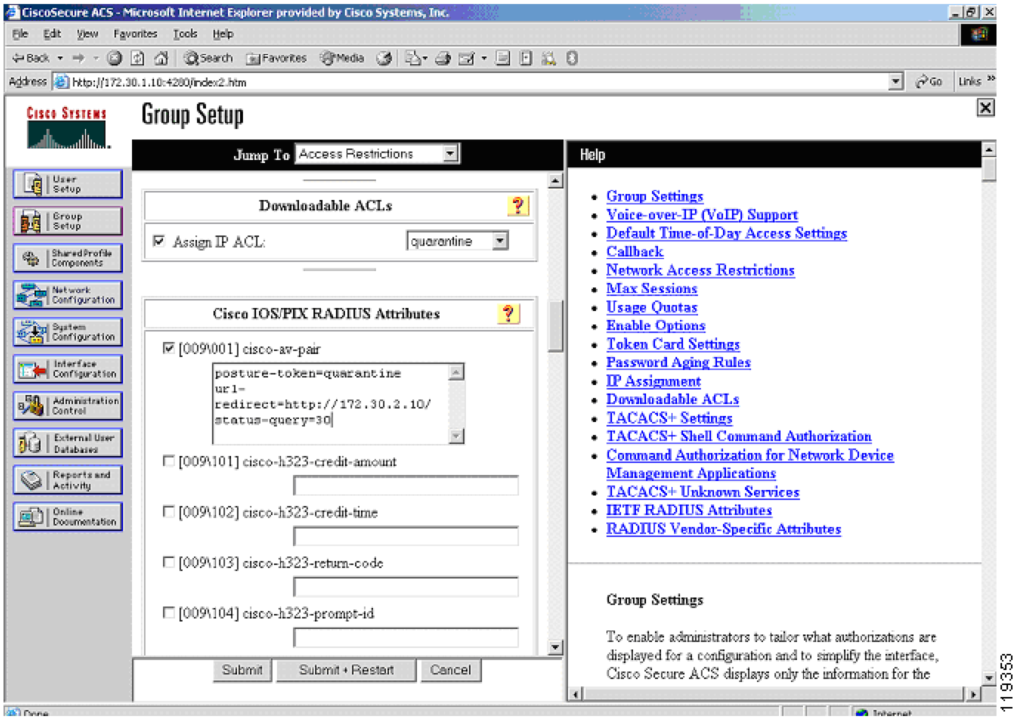
Step 7 In the [009/001] cisco-av-pair window, check the associated check box and enter an appropriate string for the group condition. For example, for the Healthy condition, enter posture-token=*Healthy*. A corresponding posture token must be entered for each group being configured. The Cisco IOS NAD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



Group Setup

Jump To Access Restrictions

Downloadable ACLs

☑ Assign IP ACL: quarantine

Cisco IOS/PIX RADIUS Attributes

☑ [009\001] cisco-av-pair

```
posture-token=quarantine
url-
redirect=http://172.30.2.10/
status-query=30
```

☐ [009\101] cisco-h323-credit-amount

☐ [009\102] cisco-h323-credit-time

☐ [009\103] cisco-h323-return-code

☐ [009\104] cisco-h323-prompt-id

Help

- Group Settings
- Voice-over-IP (VoIP) Support
- Default Time-of-Day Access Settings
- Callback
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Enable Options
- Token Card Settings
- Password Aging Rules
- IP Assignment
- Downloadable ACLs
- TACACS+ Settings
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Group Settings

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Cisco Secure ACS displays only the information for the

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.

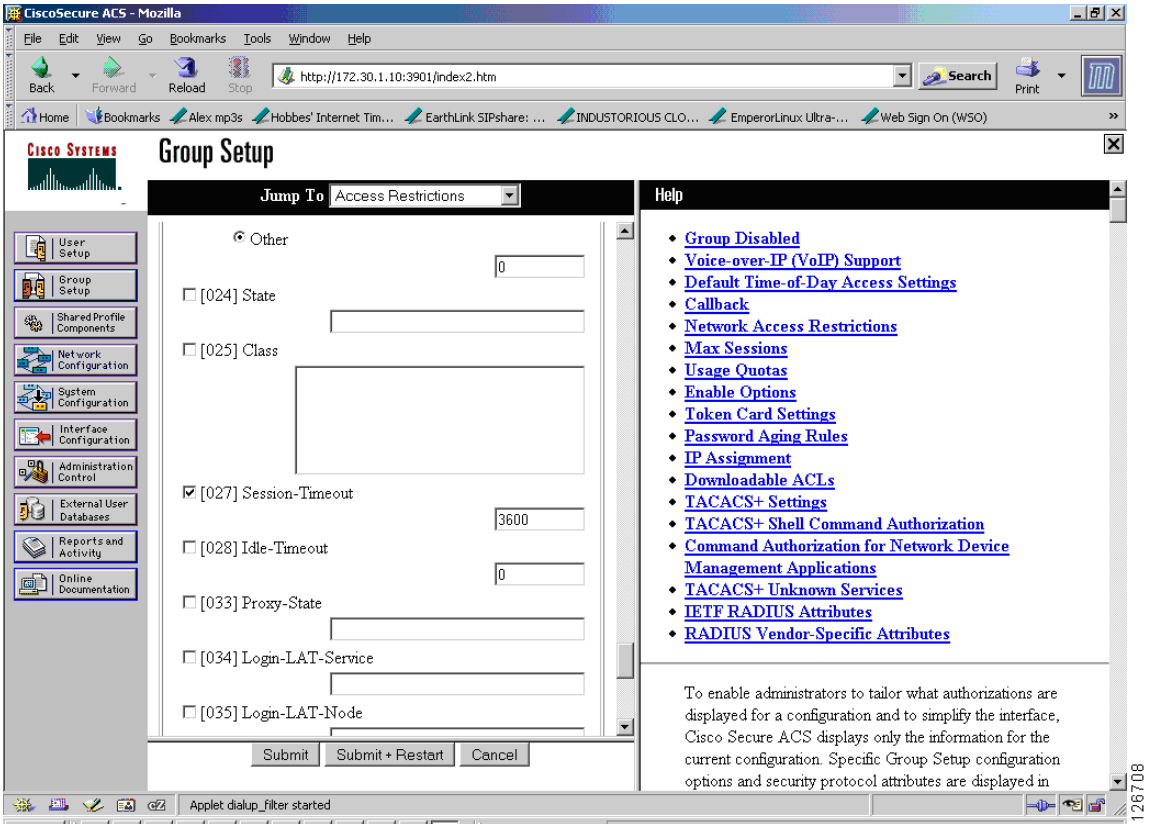
Step 9 To configure URL redirection, use the following string: url-redirect=*http://172.30.2.10/*

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



http://172.30.1.10:3901/index2.htm

Group Setup

Jump To: Access Restrictions

● Other: 0

□ [024] State

□ [025] Class

☑ [027] Session-Timeout: 3600

□ [028] Idle-Timeout: 0

□ [033] Proxy-State

□ [034] Login-LAT-Service

□ [035] Login-LAT-Node

- Group Disabled
- Voice-over-IP (VoIP) Support
- Default Time-of-Day Access Settings
- Callback
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Enable Options
- Token Card Settings
- Password Aging Rules
- IP Assignment
- Downloadable ACLs
- TACACS+ Settings
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Cisco Secure ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in

Applet dialup_filter started

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.

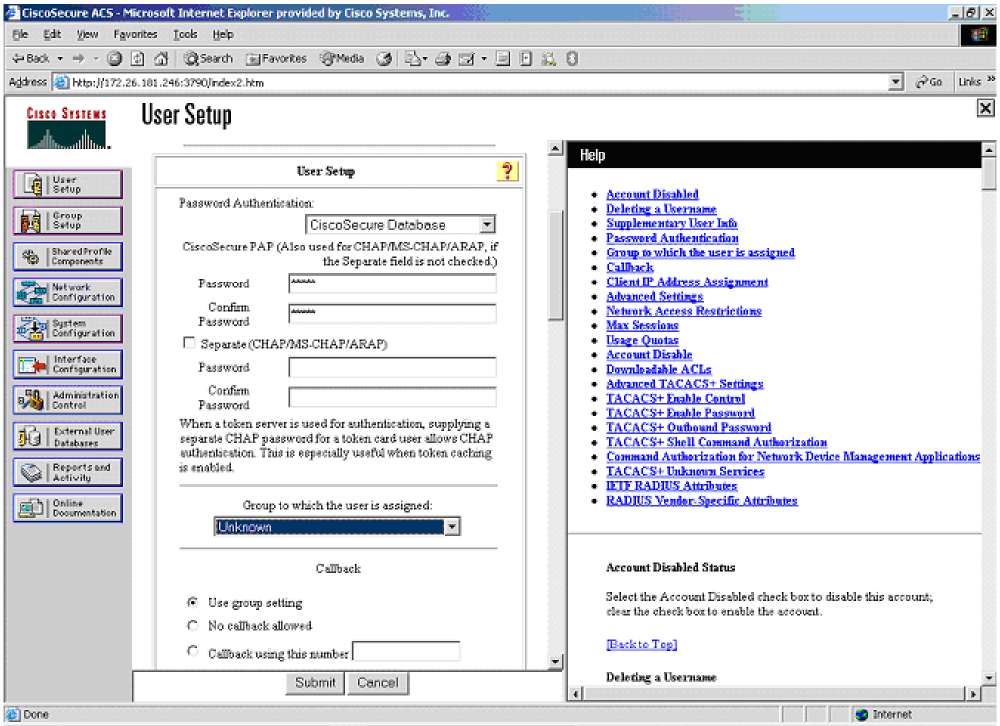
If the user ID clientless is configured on the Cisco IOS software NAD, the user ID clientless must be added to the appropriate group in Cisco Secure ACS. This can be any group with the appropriate restrictions (usually the Unknown group) and downloadable ACL assigned.

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



User Setup

User Setup

Password Authentication:

CiscoSecure Database

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

Password ******

Confirm Password ******

□ Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

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

Group to which the user is assigned:

Unknown

Callback

● Use group setting

○ No callback allowed

○ Callback using this number

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

Deleting a Username

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:

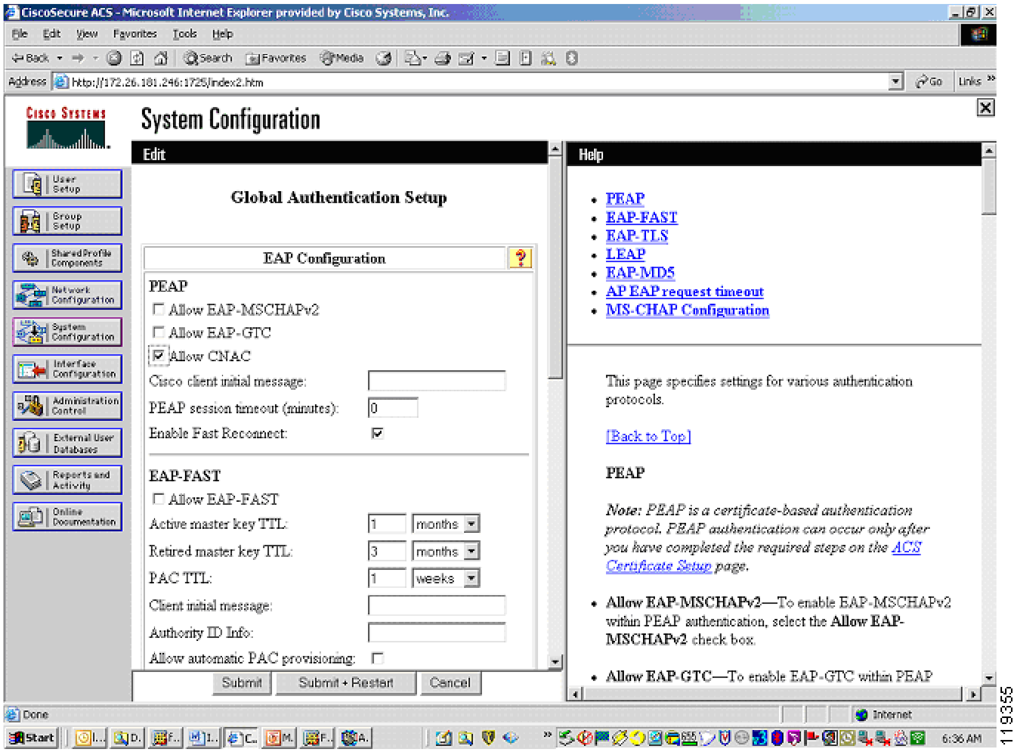
Step 1 Click **System Configuration** on the Cisco Secure ACS main menu.

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



System Configuration

Edit

Global Authentication Setup

EAP Configuration

PEAP

☐ Allow EAP-MSCHAPv2

☐ Allow EAP-GTC

☑ Allow CNAC

Cisco client initial message:

PEAP session timeout (minutes): 0

Enable Fast Reconnect: ☑

EAP-FAST

☐ Allow EAP-FAST

Active master key TTL: 1 months

Retired master key TTL: 3 months

PAC TTL: 1 weeks

Client initial message:

Authority ID Info:

Allow automatic PAC provisioning: ☐

Help

- PEAP
- EAP-FAST
- EAP-TLS
- LEAP
- EAP-MD5
- AP EAP request timeout
- MS-CHAP Configuration

This page specifies settings for various authentication protocols.

[Back to Top]

PEAP

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.

- **Allow EAP-MSCHAPv2**—To enable EAP-MSCHAPv2 within PEAP authentication, select the **Allow EAP-MSCHAPv2** check box.
- **Allow EAP-GTC**—To enable EAP-GTC within PEAP

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:

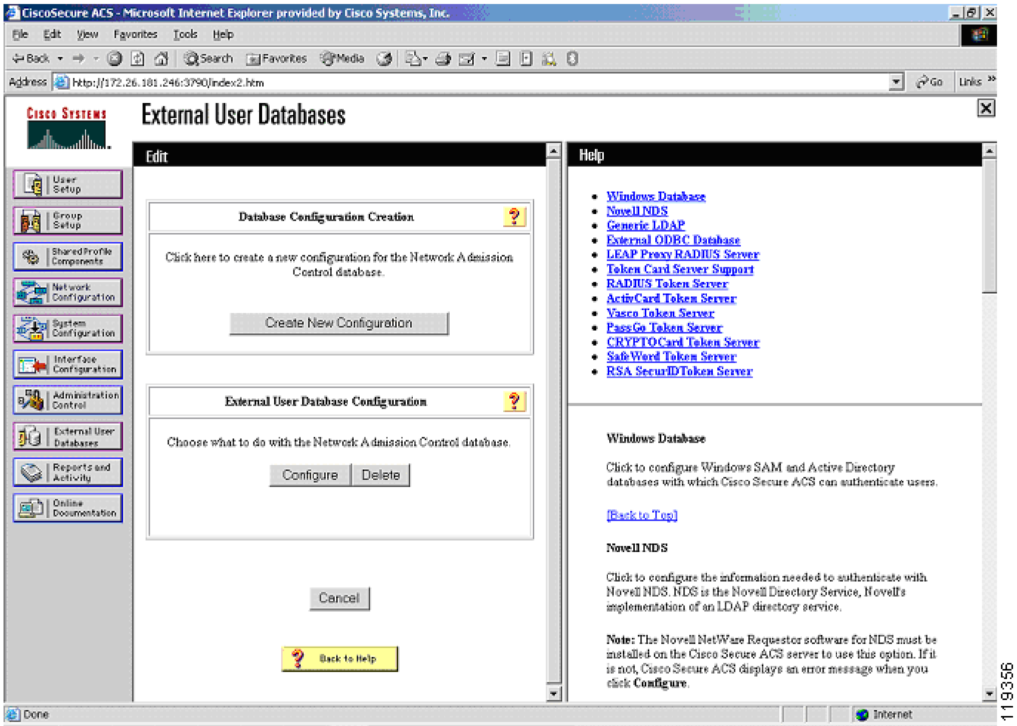
Step 1 To configure Cisco Secure ACS, click **External User Databases** on the Cisco Secure ACS main menu.

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



External User Databases

Database Configuration Creation

Click here to create a new configuration for the Network Admission Control database.

External User Database Configuration

Choose what to do with the Network Admission Control database.

- Windows Database
- Novell NDS
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- Token Card Server Support
- RADIUS Token Server
- ActivCard Token Server
- Vasco Token Server
- PassGo Token Server
- CRYPTOCard Token Server
- SafeWord Token Server
- RSA SecurIDToken Server

Windows Database

Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users.

[Back to Top]

Novell NDS

Click to configure the information needed to authenticate with Novell NDS. NDS is the Novell Directory Service, Novell's implementation of an LDAP directory service.

Note: The Novell NetWare Requestor software for NDS must be installed on the Cisco Secure ACS server to use this option. If it is not, Cisco Secure ACS displays an error message when you click **Configure**.

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.

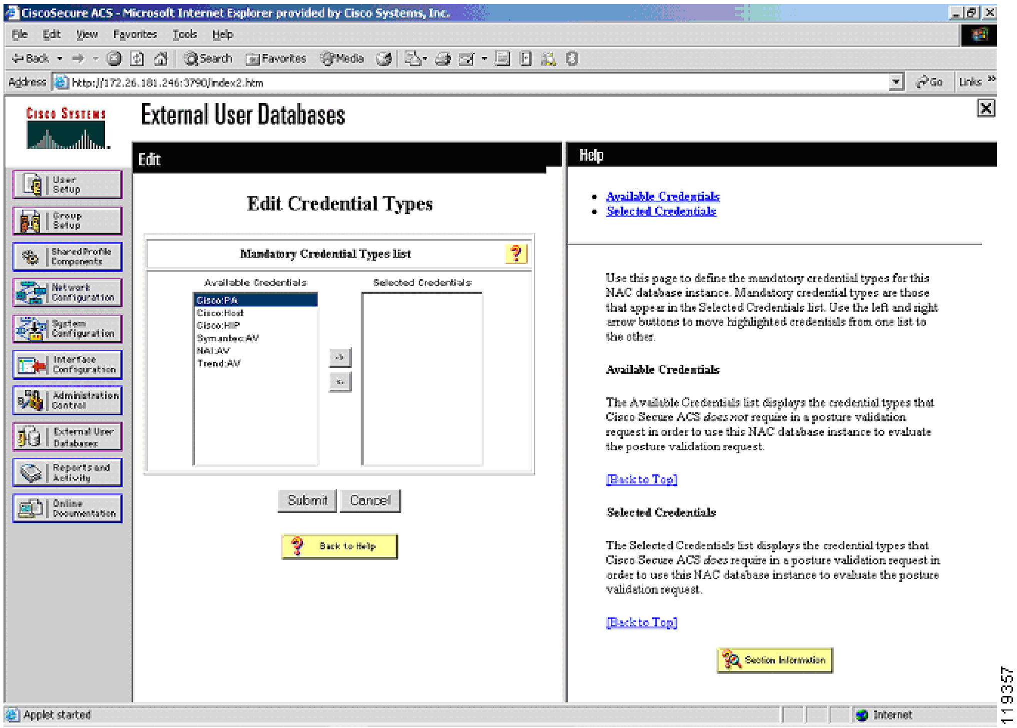
Two windows are displayed; one asking for any mandatory credential types, and the other where you configure the local (or external) policies for the credential validation.

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



Edit Credential Types

Mandatory Credential Types list

Available Credentials	Selected Credentials
Cisco:PA	
Cisco:Host	
Cisco:HIP	
Symantec:AV	
NAI:AV	
Trend:AV	

- Available Credentials
- Selected Credentials

Use this page to define the mandatory credential types for this NAC database instance. Mandatory credential types are those that appear in the Selected Credentials list. Use the left and right arrow buttons to move highlighted credentials from one list to the other.

Available Credentials

The Available Credentials list displays the credential types that Cisco Secure ACS *does not* require in a posture validation request in order to use this NAC database instance to evaluate the posture validation request.

[Back to Top]

Selected Credentials

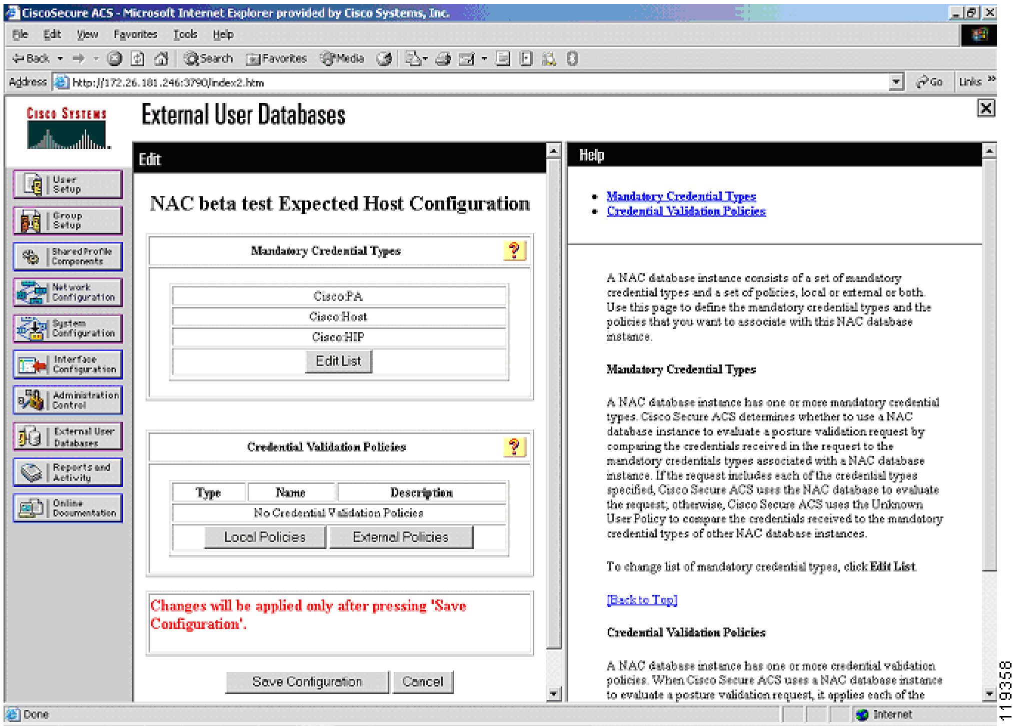
The Selected Credentials list displays the credential types that Cisco Secure ACS *does* require in a posture validation request in order to use this NAC database instance to evaluate the posture validation request.

[Back to Top]

Step 10 Click **Submit**.

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

Figure 2-33 Mandatory Credential Types



External User Databases

NAC beta test Expected Host Configuration

Mandatory Credential Types

Cisco:PA
Cisco:Host
Cisco:HIP

Credential Validation Policies

Type	Name	Description
No Credential Validation Policies		

Changes will be applied only after pressing 'Save Configuration'.

- Mandatory Credential Types
- Credential Validation Policies

A NAC database instance consists of a set of mandatory credential types and a set of policies, local or external or both. Use this page to define the mandatory credential types and the policies that you want to associate with this NAC database instance.

Mandatory Credential Types

A NAC database instance has one or more mandatory credential types. Cisco Secure ACS determines whether to use a NAC database instance to evaluate a posture validation request by comparing the credentials received in the request to the mandatory credentials types associated with a NAC database instance. If the request includes each of the credential types specified, Cisco Secure ACS uses the NAC database to evaluate the request; otherwise, Cisco Secure ACS uses the Unknown User Policy to compare the credentials received to the mandatory credential types of other NAC database instances.

To change list of mandatory credential types, click **Edit List**.

[Back to Top]

Credential Validation Policies

A NAC database instance has one or more credential validation policies. When Cisco Secure ACS uses a NAC database instance to evaluate a posture validation request, it applies each of the

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.

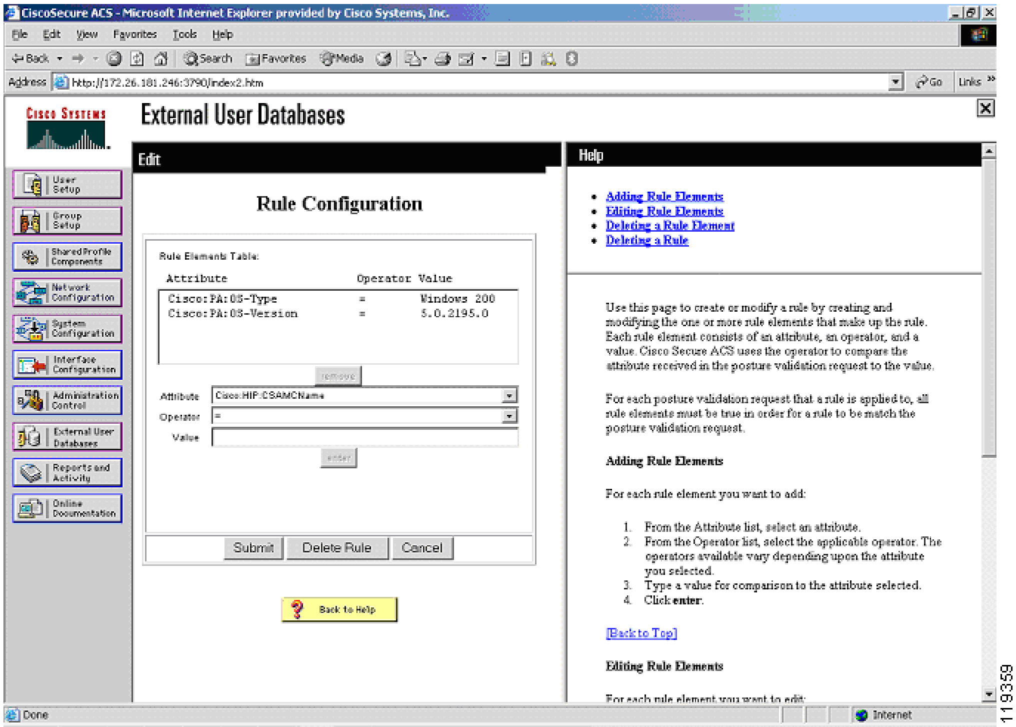
Step 13 Click **New Rule** from the Configurable Rules window.

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



External User Databases

Rule Configuration

Rule Elements Table:

```
Attribute                       Operator Value
Cisco:PA:OS-Type                   =        Windows 200
Cisco:PA:OS-Version                =        5.0.2195.0
```

Attribute: Cisco:HIP:CSAMCName

Operator: =

Value:

- Adding Rule Elements
- Editing Rule Elements
- Deleting a Rule Element
- Deleting a Rule

Use this page to create or modify a rule by creating and modifying the one or more rule elements that make up the rule. Each rule element consists of an attribute, an operator, and a value. Cisco Secure ACS uses the operator to compare the attribute received in the posture validation request to the value.

For each posture validation request that a rule is applied to, all rule elements must be true in order for a rule to be match the posture validation request.

Adding Rule Elements

For each rule element you want to add:

1. From the Attribute list, select an attribute.
2. From the Operator list, select the applicable operator. The operators available vary depending upon the attribute you selected.
3. Type a value for comparison to the attribute selected.
4. Click **enter**.

[Back to Top]

Editing Rule Elements

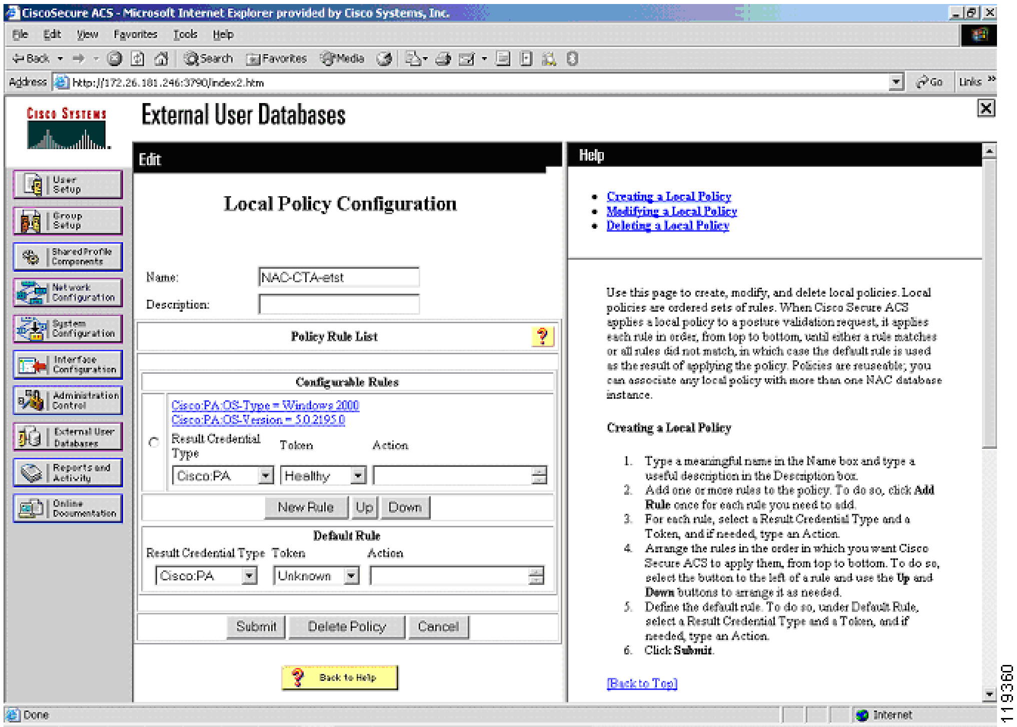
For each rule element you want to edit:

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



External User Databases

Local Policy Configuration

Name: NAC-CTA-etst

Description:

Policy Rule List

Configurable Rules

○ Cisco:PA:OS-Type = Windows 2000
Cisco:PA:OS-Version = 5.0.2195.0

Result Credential Type	Token	Action
Cisco:PA	Healthy	

New Rule | Up | Down

Default Rule

Result Credential Type	Token	Action
Cisco:PA	Unknown	

Submit | Delete Policy | Cancel

Back to Help

- Creating a Local Policy
- Modifying a Local Policy
- Deleting a Local Policy

Use this page to create, modify, and delete local policies. Local policies are ordered sets of rules. When Cisco Secure ACS applies a local policy to a posture validation request, it applies each rule in order, from top to bottom, until either a rule matches or all rules did not match, in which case the default rule is used as the result of applying the policy. Policies are reuseable; you can associate any local policy with more than one NAC database instance.

Creating a Local Policy

1. Type a meaningful name in the Name box and type a useful description in the Description box.
2. Add one or more rules to the policy. To do so, click **Add Rule** once for each rule you need to add.
3. For each rule, select a Result Credential Type and a Token, and if needed, type an Action.
4. Arrange the rules in the order in which you want Cisco Secure ACS to apply them, from top to bottom. To do so, select the button to the left of a rule and use the **Up** and **Down** buttons to arrange it as needed.
5. Define the default rule. To do so, under Default Rule, select a Result Credential Type and a Token, and if needed, type an Action.
6. Click **Submit**.

[Back to Top]

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

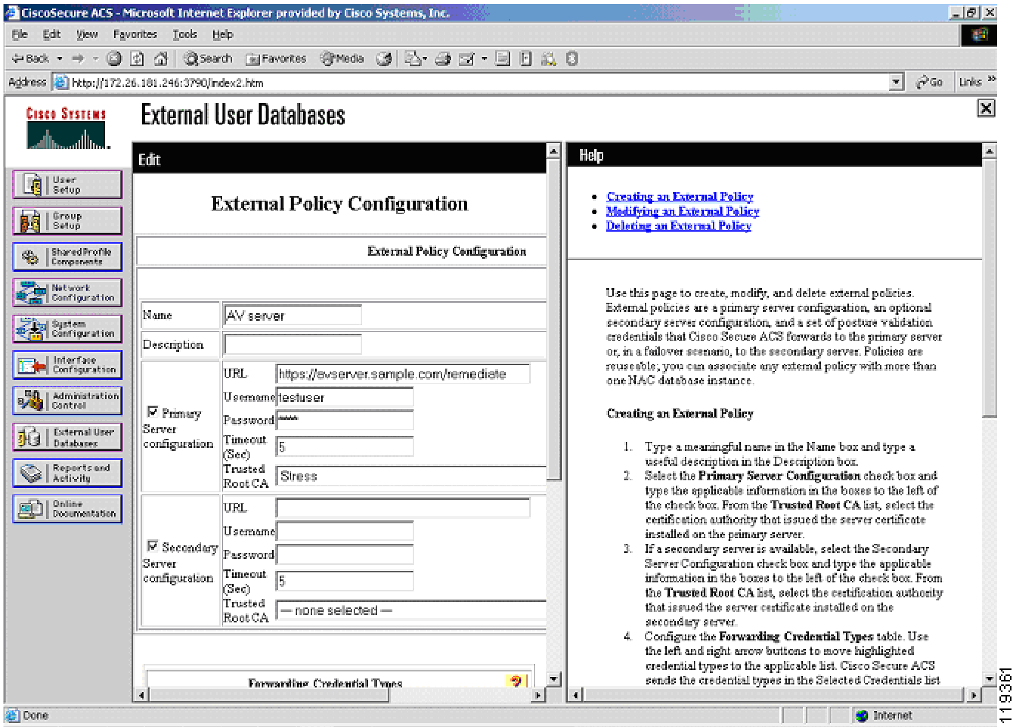
(HCAP). After the credentials and action are checked, the external server returns a token reflecting the current state of the client. The Cisco Secure ACS then puts the client in the corresponding group, with the configured ACLs of the group and Cisco IOS software AV pairs.

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



CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://172.26.181.246:3790/index2.htm
Go Links
Cisco Systems
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Done
Internet
119361

External User Databases

Edit

External Policy Configuration

External Policy Configuration

Name: AV server

Description:

☑ Primary Server configuration
URL: https://evserver.sample.com/remediate
Username: testuser
Password: ****
Timeout (Sec): 5
Trusted Root CA: Stress

☑ Secondary Server configuration
URL:
Username:
Password:
Timeout (Sec): 5
Trusted Root CA: -- none selected --

Forwarding Credential Types

Help

- Creating an External Policy
- Modifying an External Policy
- Deleting an External Policy

Use this page to create, modify, and delete external policies. External policies are a primary server configuration, an optional secondary server configuration, and a set of posture validation credentials that Cisco Secure ACS forwards to the primary server or, in a failover scenario, to the secondary server. Policies are reuseable; you can associate any external policy with more than one NAC database instance.

Creating an External Policy

1. Type a meaningful name in the Name box and type a useful description in the Description box.
2. Select the **Primary Server Configuration** check box and type the applicable information in the boxes to the left of the check box. From the **Trusted Root CA** list, select the certification authority that issued the server certificate installed on the primary server.
3. If a secondary server is available, select the Secondary Server Configuration check box and type the applicable information in the boxes to the left of the check box. From the **Trusted Root CA** list, select the certification authority that issued the server certificate installed on the secondary server.
4. Configure the **Forwarding Credential Types** table. Use the left and right arrow buttons to move highlighted credential types to the applicable list. Cisco Secure ACS sends the credential types in the Selected Credentials list

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.

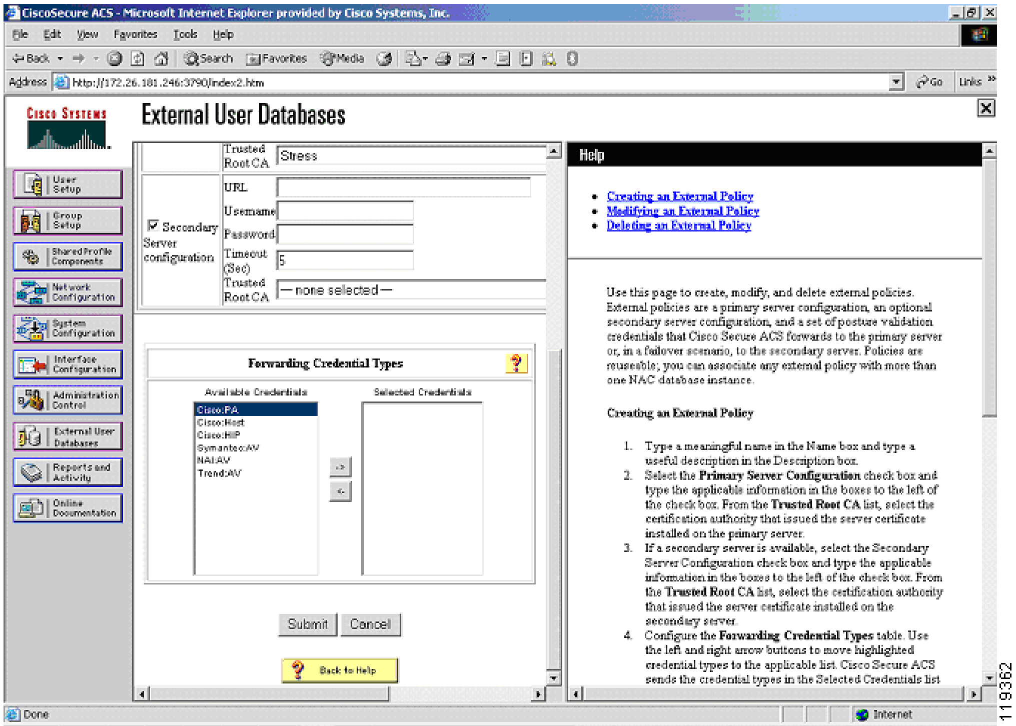
Step 6 Select the trusted root CA for the secure connection (this connection is protected with HTTPS) between the Cisco Secure ACS and the remediation server.

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



External User Databases

	Trusted Root CA	Stress
☑ Secondary Server configuration	URL	
	Username	
	Password	
	Timeout (Sec)	5
	Trusted Root CA	— none selected —

Forwarding Credential Types

Available Credentials	Selected Credentials
Cisco:PA Cisco:Host Cisco:HIP Symantec:AV NAI:AV Trend:AV	

Help

- Creating an External Policy
- Modifying an External Policy
- Deleting an External Policy

Use this page to create, modify, and delete external policies. External policies are a primary server configuration, an optional secondary server configuration, and a set of posture validation credentials that Cisco Secure ACS forwards to the primary server or, in a failover scenario, to the secondary server. Policies are reuseable; you can associate any external policy with more than one NAC database instance.

Creating an External Policy

1. Type a meaningful name in the Name box and type a useful description in the Description box.
2. Select the **Primary Server Configuration** check box and type the applicable information in the boxes to the left of the check box. From the **Trusted Root CA** list, select the certification authority that issued the server certificate installed on the piimary server.
3. If a secondary server is available, select the Secondary Server Configuration check box and type the applicable information in the boxes to the left of the check box. From the **Trusted Root CA** list, select the certification authority that issued the server certificate installed on the secondary server.
4. Configure the **Forwarding Credential Types** table. Use the left and right arrow buttons to move highlighted credential types to the applicable list. Cisco Secure ACS sends the credential types in the Selected Credentials list

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

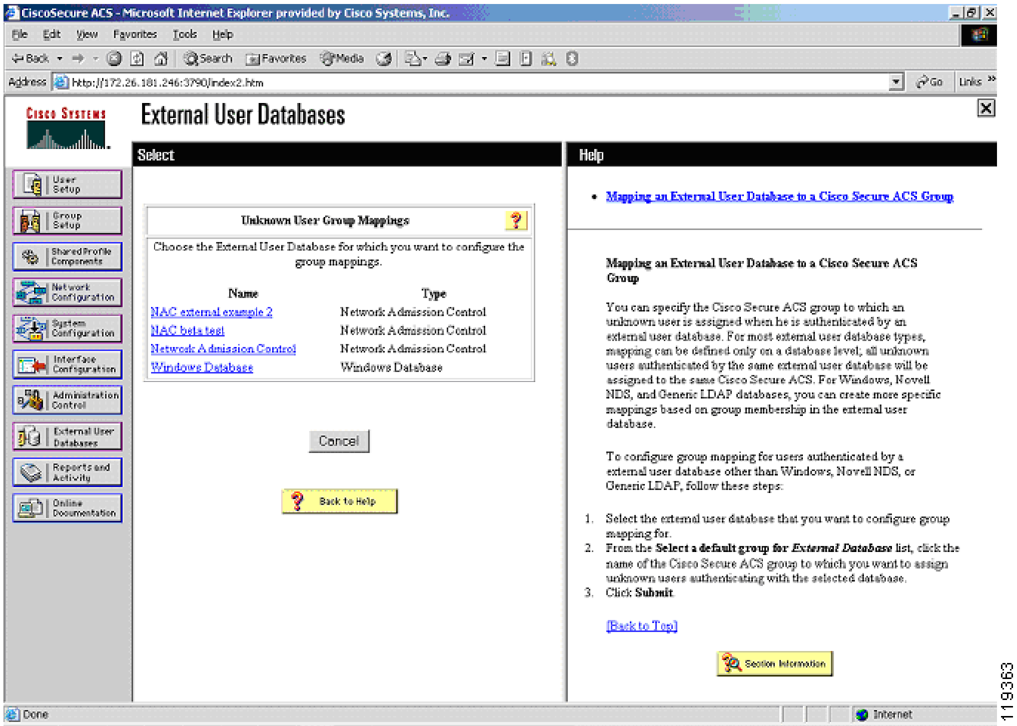
To force a client with CTA into a policy with a particular ACL applied, place the clients with a particular returned token into a specific user group. Multiple sets of user groups may be configured, each with a different downloadable IP ACL, configured URL redirection and so on. This permits different 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



Unknown User Group Mappings

Choose the External User Database for which you want to configure the group mappings.

Name	Type
NAC external example 2	Network Admission Control
NAC beta test	Network Admission Control
Network Admission Control	Network Admission Control
Windows Database	Windows Database

- Mapping an External User Database to a Cisco Secure ACS Group

Mapping an External User Database to a Cisco Secure ACS Group

You can specify the Cisco Secure ACS group to which an unknown user is assigned when he is authenticated by an external user database. For most external user database types, mapping can be defined only on a database level; all unknown users authenticated by the same external user database will be assigned to the same Cisco Secure ACS. For Windows, Novell NDS, and Generic LDAP databases, you can create more specific mappings based on group membership in the external user database.

To configure group mapping for users authenticated by a external user database other than Windows, Novell NDS, or Generic LDAP, follow these steps:

1. Select the external user database that you want to configure group mapping for.
2. From the **Select a default group for *External Database*** list, click the name of the Cisco Secure ACS group to which you want to assign unknown users authenticating with the selected database.
3. Click **Submit**.

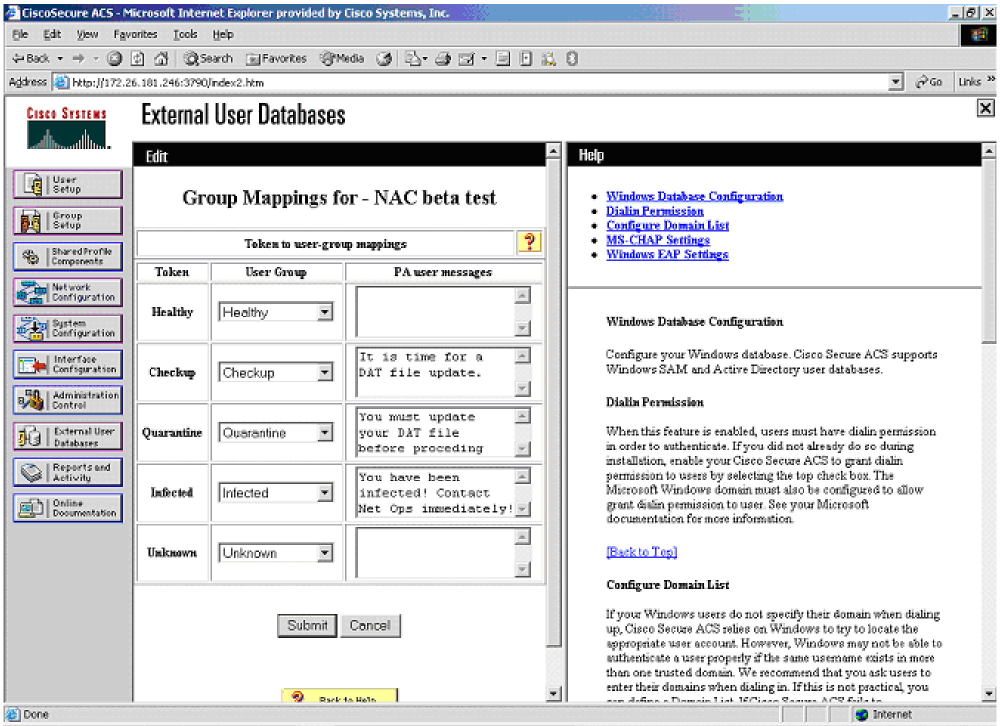
[Back to Top]

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



External User Databases

Group Mappings for - NAC beta test

Token to user-group mappings

Token	User Group	PA user messages
Healthy	Healthy	
Checkup	Checkup	It is time for a DAT file update.
Quarantine	Quarantine	You must update your DAT file before proceding
Infected	Infected	You have been infected! Contact Net Ops immediately!
Unknown	Unknown	

Submit Cancel

- Windows Database Configuration
- Dialin Permission
- Configure Domain List
- MS-CHAP Settings
- Windows EAP Settings

Windows Database Configuration

Configure your Windows database. Cisco Secure ACS supports Windows SAM and Active Directory user databases.

Dialin Permission

When this feature is enabled, users must have dialin permission in order to authenticate. If you did not already do so during installation, enable your Cisco Secure ACS to grant dialin permission to users by selecting the top check box. The Microsoft Windows domain must also be configured to allow grant dialin permission to user. See your Microsoft documentation for more information.

[Back to Top]

Configure Domain List

If your Windows users do not specify their domain when dialing up, Cisco Secure ACS relies on Windows to try to locate the appropriate user account. However, Windows may not be able to authenticate a user properly if the same username exists in more than one trusted domain. We recommend that you ask users to enter their domains when dialing in. If this is not practical, you

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.

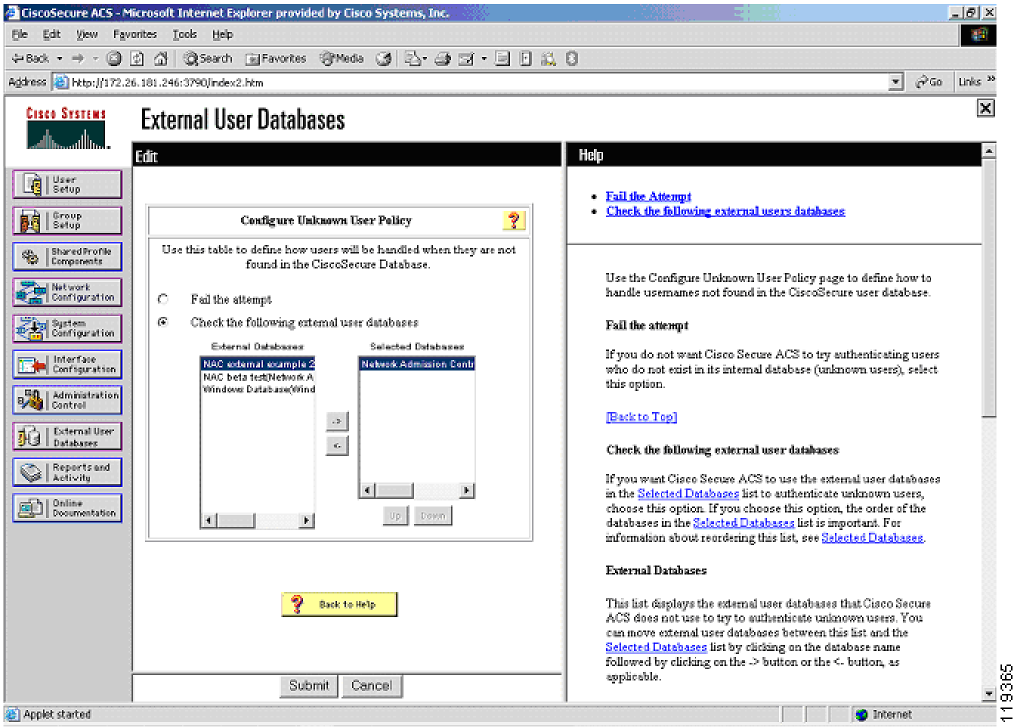
Configuring an Unknown User Policy to Check an External Database

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



External User Databases

Configure Unknown User Policy

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

○ Fail the attempt

● Check the following external user databases

External Databases	Selected Databases
NAC external example 2	Network Admission Contr
NAC beta test(Network A	
Windows Database(Wind	

- Fail the Attempt
- Check the following external users databases

Use the Configure Unknown User Policy page to define how to handle usernames not found in the CiscoSecure user database.

Fail the attempt

If you do not want Cisco Secure ACS to try authenticating users who do not exist in its internal database (unknown users), select this option.

[Back to Top]

Check the following external user databases

If you want Cisco Secure ACS to use the external user databases in the Selected Databases list to authenticate unknown users, choose this option. If you choose this option, the order of the databases in the Selected Databases list is important. For information about reordering this list, see Selected Databases.

External Databases

This list displays the external user databases that Cisco Secure ACS does not use to try to authenticate unknown users. You can move external user databases between this list and the Selected Databases list by clicking on the database name followed by clicking on the -> button or the <- button, as applicable.

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
- Revalidation Timer
- External User Database Local Policy Rule Ordering

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
- Configuring AAA EOU Authentication Protocols and Authentication Proxy Authorization Protocols
- Configuring AAA Setup, RADIUS Server Host, and Key
- Configuring Admission Control EOU
- Configuring an Exception List Configuration for Clientless Hosts
- Configuring Clientless User Policy
- Configuring EAP over UDP Timers
- Configuring the Interfaces and Intercept ACL
- Configuring the HTTP Server
- Enabling EOU Logging

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.

CHAPTER 3

Managing and Troubleshooting NAC

This chapter describes how to manage and troubleshoot NAC and includes the following sections:

- Management and Reporting
- Troubleshooting and Logging

Management and Reporting

The Cisco Security Information Management System (SIMS) is an integral part of a NAC deployment. SIMS is an important tool for monitoring the condition of the network where admission control is implemented. This section describes how to use SIMS for monitoring and reporting NAC activity, and includes the following topics:

- SIMS Hardware Requirements
- Monitoring and Reporting

SIMS Hardware Requirements

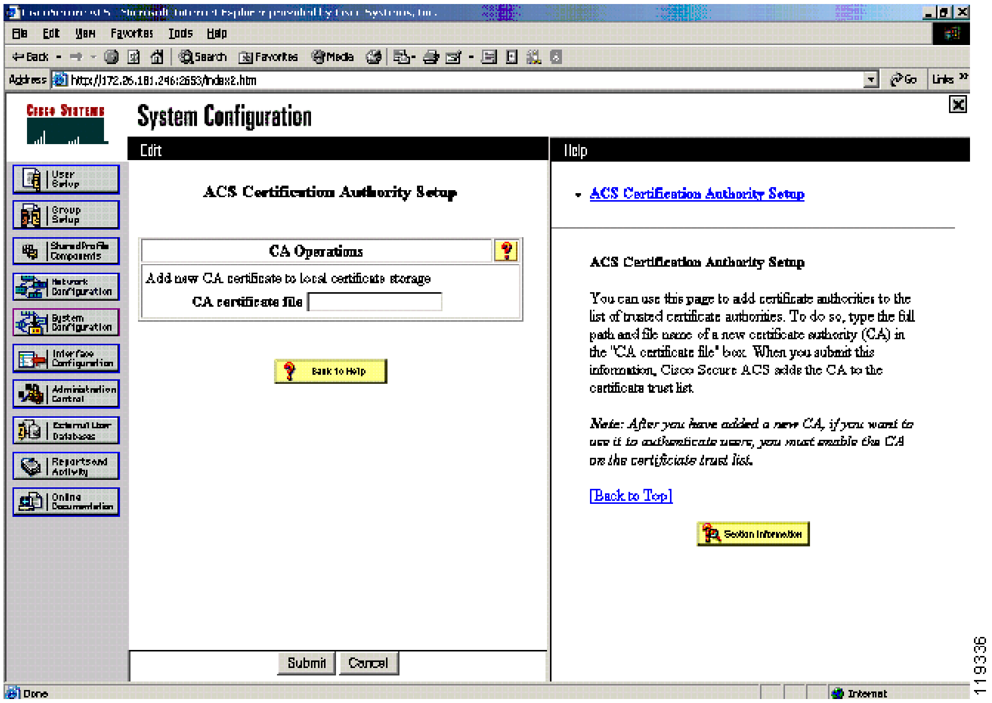
The recommended hardware requirements for a SIMS installation are a dual Xeon processor class machine with 2 GB of memory and 50 GB of disk space.

This machine requirement is for a system that receives 1,000 messages per second. If the load on the server is different, the characteristics of the system may be adjusted accordingly. To obtain installation procedures for the host operation system, RedHat Linux Enterprise v2.1, and the SIMS software, see the documentation provided with SIMS at the following website: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/sims/3_1_1/

Monitoring and Reporting

SIMS provides several features for monitoring and reporting NAC network activity. The NAC dashboard shown in Figure 3-1 provides a consolidated view of the state of the application software being monitored by the NAC system.

Figure 3-1 netForensics SIM Desktop



System Configuration

ACS Certification Authority Setup

CA Operations

Add new CA certificate to local certificate storage

CA certificate file

- ACS Certification Authority Setup

ACS Certification Authority Setup

You can use this page to add certificate authorities to the list of trusted certificate authorities. To do so, type the full path and file name of a new certificate authority (CA) in the "CA certificate file" box. When you submit this information, Cisco Secure ACS adds the CA to the certificate trust list.

Note: After you have added a new CA, if you want to use it to authenticate users, you must enable the CA on the certificate trust list.

[Back to Top]

This window displays the percentage of compliant and non-compliant hosts, and average remediation times. Other available reports list the hosts subject to posture checking and summarize overall network compliance.

For information about using SIMS, see the *netForensics User's Guide* at the following URL: http://www.cisco.com/en/US/docs/security/security_management/sims/3.1_appliance/install/guide/Implement.pdf.

Troubleshooting and Logging

NAC helps ensure that connected client machines are submitted to an access policy that specifies criteria for applications that must be met before the client machine is allowed network access.

By examining the various logs from CTA, the Cisco IOS software NAD, and Cisco Secure ACS, you can obtain a fairly accurate picture of the NAC activity on your network.

The SIMS server correlates the log messages from Cisco IOS software and from Cisco Secure ACS. The Cisco IOS software NAD also provides Cisco IOS software **debug** and **show** commands for monitoring and troubleshooting purposes.

Overview of Operational Checks

When a client in the healthy condition accesses the network, the posturing process takes place transparently. No user notification of the admission control process takes place unless a pop-up message has been configured in the Cisco Secure ACS database mapping section. If network access is not allowed but the client should have been assigned a Healthy condition, make sure that the client CTA services are currently in a started state in the Microsoft Services windows in the control panel, and that the CTA has successfully started a PEAP session with the Cisco Secure ACS. This can be determined by examining the CTA log file.

If PEAP does not start properly, check the certificate installation in both Cisco Secure ACS and CTA. If PEAP starts but an unexpected EAP type is shown in the CTA log file, make sure that the Allow CNAC check box has been checked under the Global Authentication Setup menu in Cisco Secure ACS System Configuration and that the Unknown user policy has been properly configured under the External User Database section of ACS. If a PEAP session is successfully started and the expected results are still not achieved, check the external user database policy configuration and rule sets. The received attribute values may be found in the logging and reporting section of the ACS Administrators screen.

CTA Logging

To start CTA logging, run the **ctalogd enable** command from the command-line interface (CLI) in the directory where CTA is installed. After running this command, ctalogd writes a trace of its current activity into the following directory:

C:\Documents and Settings\All Users\Application Data\Cisco Systems\CiscoTrustAgent\Logs

For sample output from a CTA logging session, see CTA Logging Output, page A-4.

Cisco Secure ACS Logs and Troubleshooting

The passed and failed authentication .csv files log files, which are created by Cisco Secure ACS, are of particular interest to NAC administrators. If properly configured, these logs contain the attribute values that are present in the clients.

Cisco Secure ACS Passed Authentication Log

During the configuration process, Cisco Secure ACS is set up to log passed and failed authentications to comma-separated values (CSV) files. To access these files, use the **Reports and Activity** option from the Secure ACS main menu. During the rule configuration, view these files frequently to verify the attribute values being sent to Cisco Secure ACS in the received credentials.

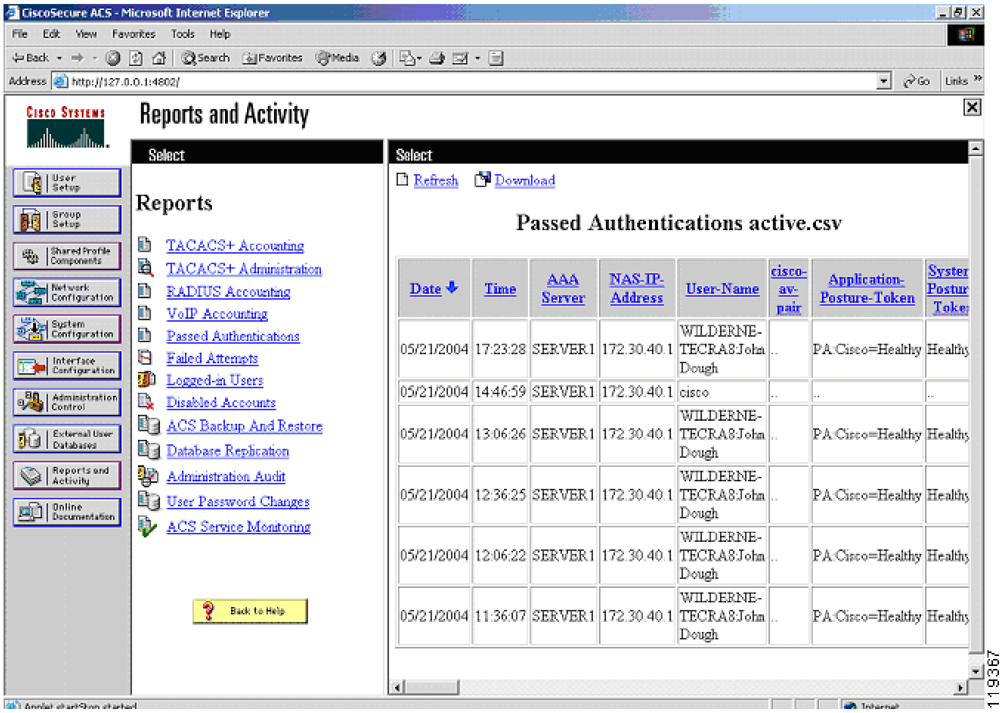
To view the Reports and Activity window, complete the following steps:

Step 1 Click **Reports and Activity** from the Cisco Secure ACS main menu.

Step 2 Click **CSV Passed Authentications** in the window that is displayed.

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

Figure 3-2 Reports and Activity



Reports and Activity

Reports

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Passed Authentications
- Failed Attempts
- Logged-in Users
- Disabled Accounts
- ACS Backup And Restore
- Database Replication
- Administration Audit
- User Password Changes
- ACS Service Monitoring

Passed Authentications active.csv

Date	Time	AAA Server	NAS-IP-Address	User-Name	cisco-av-pair	Application-Posture-Token	Syster Postur Toke:
05/21/2004	17:23:28	SERVER1	172.30.40.1	WILDERNE-TECRA8:John Dough	..	PA:Cisco=Healthy	Healthy
05/21/2004	14:46:59	SERVER1	172.30.40.1	cisco	..	..	..
05/21/2004	13:06:26	SERVER1	172.30.40.1	WILDERNE-TECRA8:John Dough	..	PA:Cisco=Healthy	Healthy
05/21/2004	12:36:25	SERVER1	172.30.40.1	WILDERNE-TECRA8:John Dough	..	PA:Cisco=Healthy	Healthy
05/21/2004	12:06:22	SERVER1	172.30.40.1	WILDERNE-TECRA8:John Dough	..	PA:Cisco=Healthy	Healthy
05/21/2004	11:36:07	SERVER1	172.30.40.1	WILDERNE-TECRA8:John Dough	..	PA:Cisco=Healthy	Healthy

The current admission control session appears in the passed authentications file even if the client was posture checked into an unhealthy state. This is because the posturing process has completed successfully.

Pay special attention to the Reason field in the log file, because this shows the particular instance of the NAC external user database, the policy, and the specific rule in the policy that was matched to produce the SPT.

Cisco Secure ACS Failed Authentication Log

Some useful information may not be written to the failed log file because of the unknown state that a client may be in when the authentication for NAC fails. This information might include the credentials Cisco Secure ACS was expecting to receive as well as the attribute values contained in the credentials.

Some of the reasons a client admission control attempt appears in the failed attempts log include the following:

- The set of NAC external user databases configured may not have a set of mandatory credentials that matches the set of received credentials from that client.
- The NAD may not have been configured properly in Cisco Secure ACS.

Cisco IOS Software Commands

Cisco IOS software contains **show**, **clear**, and **debug** commands useful for verifying and troubleshooting NAC processes.

Cisco IOS Software Log Output

The following shows the console output from a router taking part in the admission control process with the **eou logging** command configured:

```
nac1751#
May 13 13:05:16: %EOU-6-SESSION: IP=172.30.40.16| HOST=DETECTED| Interface=FastEthernet0/0
May 13 13:05:16: %EOU-6-CTA: IP=172.30.40.16| CiscoTrustAgent=DETECTED
May 13 13:05:18: %EOU-6-POLICY: IP=172.30.40.16| TOKEN=healthy
May 13 13:05:18: %EOU-6-POLICY: IP=172.30.40.16| ACLNAME=#Cisco Secure
ACSACL#-IP-healthy-40a00ae9
May 13 13:05:18: %EOU-6-POSTURE: IP=172.30.40.16| HOST=AUTHORIZED|
Interface=FastEthernet0/0
May 13 13:05:18: %EOU-6-AUTHTYPE: IP=172.30.40.16| AuthType=EAP
May 13 13:10:18: %EOU-6-SQ: IP=172.30.40.16| STATUSQUERY|VALIDATED
```

The last line shows a single successful status query. These are informational level messages and are not normally seen by any logging device.

Cisco IOS Software Show Commands

The **show eou all** command displays a list of the currently detected hosts and their posture states if any.

```
nac1751#sh eou all
------------------------------------------------------------------
Address         Interface       AuthType   Posture-Token Age(min)
------------------------------------------------------------------
172.30.40.16    FastEthernet0/0 EAP        healthy         13
```

This command may also be run with an IP address substituted for the **all** keyword to show the state of a single host.

```
show ip auth-proxy cache posture
```

The **show ip access-list** command displays the currently downloaded ACLs at the end of the output.

```
nac1751#sh ip access-lists
Standard IP access list access
    10 deny   192.168.0.1
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
    30 permit 172.30.0.0, wildcard bits 0.0.255.255
    40 permit 172.31.0.0, wildcard bits 0.0.255.255
    50 deny   any
Extended IP access list 101
     permit ip host 172.30.40.16 any (12 matches)
    10 permit ip any host 172.30.40.1 (1227 matches)
Extended IP access list clientException
    10 permit ip any host 172.30.1.10
Extended IP access list sl_def_acl
    10 deny tcp any any eq telnet log
    20 deny tcp any any eq www log
    30 deny tcp any any eq 22 log
    40 permit ip any any log
Extended IP access list xCisco Secure ACSACLx-IP-healthy-40a00ae9
    10 permit ip any any
```

```
nac1751#
```

In this example, the last access list is named xCisco Secure ACSACLx-IP-healthy-40a00ae9. This ACL has a single line, **permit ip any any**.

The first **any** in this ACL has been replaced by the IP address of the posture-checked client and the result has been placed over the top of the ACL (ACL 101 in this case) applied to the interface on the Cisco IOS software device taking part in the admission control process.

Correcting a Blank or Incorrect Posture

If the results of the **show eou all** or **show eou ip address** commands include postures that do not match the actual result of posture validation or display "-------" instead of a posture, the posture-token AV pair may be misconfigured in one or more groups in Cisco Secure ACS, or the group mapping may be misconfigured in the NAC database that processed the posture validation request.

If the posture displayed is "-------," the AAA client (the NAD) is not receiving the posture-token AV pair within a Cisco IOS/PIX RADIUS cisco-av-pair vendor-specific attribute (VSA). If the posture displayed does not correspond to the actual result of posture validation, the AAA client is receiving an incorrect value in the posture-token AV pair.

Check group mappings in the NAC database to verify that the correct user groups are associated with each system posture token (SPT). In the user groups configured for use with NAC, be sure that the Cisco IOS/PIX RADIUS cisco-av-pair VSA is configured correctly.

For example, in a group configured to authorize NAC clients receiving a Healthy SPT, be sure the [009\001] cisco-av-pair check box is checked and that the following string appears in the [009\001] cisco-av-pair text box:

posture-token=Healthy

EOU Commands

The following commands may be used to cause a re-initialization or a revalidation of any or all hosts on a network being subject to admission control:

```
eou initialize all
eou initialize ip x.x.x.x
eou revalidate all
eou revalidate ip x.x.x.x
```

These commands are useful if a virus outbreak is detected and a new signature file is available. Client hosts that had already been successfully validated can be revalidated to immediately get the new signature file.

When a host is initialized, all previous state information about that host is deleted and the admission control process for that host starts with no state. When a host is revalidated, state information about that host is retained so that the host still has its current access during the revalidation process.

Cisco IOS Software Clear Commands

The Cisco IOS software **clear eou** command removes the state information regarding admission control about any or all hosts detected. This command can be used for specific IP addresses or for all the sessions on a specific router.

```
nac1751#clear eou all
nac1751#
```

```
May 13 13:18:47: %EOU-6-SESSION: IP=172.30.40.16| HOST=REMOVED| Interface=FastEthernet0/0
```

Cisco IOS Software Debug Commands

The following debug commands are available for the various admission control components:

```
nac1751#debu eou ?
  all           All EAPoUDP debugging messages turned on
  eap           Debug EAP packets
  errors        Debug Errors
  events        Debug Events
  obj-create    Debug EAPoUDP Session Creation
  obj-destroy   Debug EAPoUDP Session Destroy
  obj-link      Debug EAPoUDP session addition to hash table
  obj-unlink    Debug EAPoUDP session removal from hash table
  packets       Debug EAPoUDP packets
  ratelimit     Debug Ratelimit Events
  sm            Debug EAPoUDP State Machine Events
debug eap
```

For sample debug output, see Admission Control Session Debug Output, page A-1.

APPENDIX A

Debug Output and CTA Logs

This appendix provides sample output form debugging and CTA logs and includes the following sections:

- Admission Control Session Debug Output
- debug eou events Output
- EOU State Machine Debug Output
- CTA Logging Output

Admission Control Session Debug Output

The following shows debug output during a successful admission control session and during the clearing of that session.

```
nac1751#show debug
eou:
  EAPoUDP Session Creation debugging is on
  EAPoUDP Session Destroy debugging is on
  EAPoUDP Session Removal from Hash Table debugging is on
  EAPoUDP Session Addition to Hash Table debugging is on
nac1751#
May 13 13:20:32: eou-obj_create:EOU Init Validation for idb= FastEthernet0/0 src_mac=
0010.a401.efa4 src_ip= 172.30.40.16
May 13 13:20:32: eou-obj_create:172.30.40.16: EAPoUDP Session Created
May 13 13:20:32: eou-obj_link:172.30.40.16: EAPoUDP Session added to Hash table
nac1751#clear eou all
nac1751#
May 13 13:20:56: eou-obj_destroy:(172.30.40.16): Session Timedout
May 13 13:20:56: eou-obj_unlink:172.30.40.16: EAPoUDP Session removed from hash table
May 13 13:20:56: eou-obj_destroy:172.30.40.16: Session Destroyed
nac1751#
```

debug eou events Output

The **debug eou events** command shows the timers being reset during successful communication between a client with CTA and a NAD.

EOU logging has also be enabled in this trace to show when the host is validated. These informational messages begin with EOU-6.

```
nac1751#deb eou events
Events debugging is on
nac1751#
May 13 13:27:35: eou-ev:129.128.203.192: msg = 33(eventEouCreateSession)
May 13 13:27:35: %EOU-6-SESSION: IP=172.30.40.16| HOST=DETECTED| Interface=FastEthernet0/0
May 13 13:27:35: eou-ev:172.30.40.16: msg = 3(eventEouStartHello)
May 13 13:27:35: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:35: eou-ev:eou_send_hello_request: Send Hello Request host= 172.30.40.1
eou_port= 5566 (hex)
May 13 13:27:36: %EOU-6-CTA: IP=172.30.40.16| CiscoTrustAgent=DETECTED
May 13 13:27:36: eou-ev:172.30.40.16: msg = 21(eventEouEapStart)
May 13 13:27:36: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:36: eou-ev:Starting AAA timer 60(172.30.40.16)
May 13 13:27:36: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:37: eou-ev:Starting AAA timer 60(172.30.40.16)
May 13 13:27:37: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:37: eou-ev:Starting AAA timer 60(172.30.40.16)
May 13 13:27:37: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:37: eou-ev:Starting AAA timer 60(172.30.40.16)
May 13 13:27:37: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:37: eou-ev:Starting AAA timer 60(172.30.40.16)
May 13 13:27:37: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:37: eou-ev:Starting AAA timer 60(172.30.40.16)
May 13 13:27:37: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:37: eou-ev:Starting AAA timer 60(172.30.40.16)
May 13 13:27:37: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:37: eou-ev:Starting AAA timer 60(172.30.40.16)
May 13 13:27:37: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:38: eou-ev:Starting AAA timer 60(172.30.40.16)
May 13 13:27:38: %EOU-6-POLICY: IP=172.30.40.16| TOKEN=healthy
May 13 13:27:38: %EOU-6-POLICY: IP=172.30.40.16| ACLNAME=#Cisco Secure
ACSACL#-IP-healthy-40a00ae9
May 13 13:27:38: %EOU-6-POSTURE: IP=172.30.40.16| HOST=AUTHORIZED|
Interface=FastEthernet0/0
May 13 13:27:38: eou-ev:Starting Retransmit timer 3(172.30.40.16)
May 13 13:27:38: %EOU-6-AUTHTYPE: IP=172.30.40.16| AuthType=EAP
May 13 13:27:38: eou-ev:Starting Revalidate timer 1800(172.30.40.16)
May 13 13:27:38: eou-ev:Starting Status Query timer 300(172.30.40.16)
nac1751#
```

EOU State Machine Debug Output

The debug of the EOU state machine shown below is a trace of the different messages that are exchanged between the CTA and NAD during a successful posture validation session.

```
nac1751#deb eou sm
EAPoUDP State Machine Events debugging is on
nac1751#
May 13 13:29:36:     eou_auth 172.30.40.16: during state eou_authenticated, got event
4(eouAbort)
May 13 13:29:36: @@@ eou_auth 172.30.40.16: eou_authenticated -> eou_abort
May 13 13:29:36: %EOU-6-SESSION: IP=172.30.40.16| HOST=REMOVED| Interface=FastEthernet0/0
nac1751#
nac1751#
May 13 13:29:45:     eou_auth 172.30.40.16: initial state eou_initialize has enter
May 13 13:29:45: %EOU-6-SESSION: IP=172.30.40.16| HOST=DETECTED| Interface=FastEthernet0/0
May 13 13:29:45:     eou_auth 172.30.40.16: during state eou_initialize, got event
1(eouCheckProfile)
May 13 13:29:45: @@@ eou_auth 172.30.40.16: eou_initialize -> eou_initialize
May 13 13:29:45:     eou_auth 172.30.40.16: during state eou_initialize, got event
3(eouStartHello)
May 13 13:29:45: @@@ eou_auth 172.30.40.16: eou_initialize -> eou_hello
May 13 13:29:45:     eou_auth 172.30.40.16: during state eou_hello, got event
5(eouHelloResponse)
May 13 13:29:45: @@@ eou_auth 172.30.40.16: eou_hello -> eou_client
May 13 13:29:45: %EOU-6-CTA: IP=172.30.40.16| CiscoTrustAgent=DETECTED
May 13 13:29:45:     eou_auth 172.30.40.16: during state eou_client, got event
12(eouEapStart)
May 13 13:29:45: @@@ eou_auth 172.30.40.16: eou_client -> eou_client
May 13 13:29:45:     eou_auth 172.30.40.16: during state eou_client, got event
14(eouEapResponse)
May 13 13:29:45: @@@ eou_auth 172.30.40.16: eou_client -> eou_server
May 13 13:29:45:     eou_auth 172.30.40.16: during state eou_server, got event
13(eouEapRequest)
May 13 13:29:45: @@@ eou_auth 172.30.40.16: eou_server -> eou_client
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_client, got event
14(eouEapResponse)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_client -> eou_server
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_server, got event
13(eouEapRequest)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_server -> eou_client
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_client, got event
14(eouEapResponse)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_client -> eou_server
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_server, got event
13(eouEapRequest)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_server -> eou_client
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_client, got event
14(eouEapResponse)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_client -> eou_server
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_server, got event
13(eouEapRequest)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_server -> eou_client
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_client, got event
14(eouEapResponse)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_client -> eou_server
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_server, got event
13(eouEapRequest)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_server -> eou_client
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_client, got event
14(eouEapResponse)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_client -> eou_server
May 13 13:29:46:     eou_auth 172.30.40.16: during state eou_server, got event
13(eouEapRequest)
May 13 13:29:46: @@@ eou_auth 172.30.40.16: eou_server -> eou_client
May 13 13:29:47:     eou_auth 172.30.40.16: during state eou_client, got event
14(eouEapResponse)
May 13 13:29:47: @@@ eou_auth 172.30.40.16: eou_client -> eou_server
May 13 13:29:47:     eou_auth 172.30.40.16: during state eou_server, got event
13(eouEapRequest)
May 13 13:29:47: @@@ eou_auth 172.30.40.16: eou_server -> eou_client
May 13 13:29:47:     eou_auth 172.30.40.16: during state eou_client, got event
14(eouEapResponse)
May 13 13:29:47: @@@ eou_auth 172.30.40.16: eou_client -> eou_server
May 13 13:29:47:     eou_auth 172.30.40.16: during state eou_server, got event
13(eouEapRequest)
May 13 13:29:47: @@@ eou_auth 172.30.40.16: eou_server -> eou_client
May 13 13:29:47:     eou_auth 172.30.40.16: during state eou_client, got event
14(eouEapResponse)
May 13 13:29:47: @@@ eou_auth 172.30.40.16: eou_client -> eou_server
May 13 13:29:47: %EOU-6-POLICY: IP=172.30.40.16| TOKEN=healthy
May 13 13:29:47: %EOU-6-POLICY: IP=172.30.40.16| ACLNAME=#Cisco Secure
ACSACL#-IP-healthy-40a00ae9
```

```
May 13 13:29:47: %EOU-6-POSTURE: IP=172.30.40.16| HOST=AUTHORIZED|
Interface=FastEthernet0/0
May 13 13:29:47:     eou_auth 172.30.40.16: during state eou_server, got event
15(eouEapSuccess)
May 13 13:29:47: @@@ eou_auth 172.30.40.16: eou_server -> eou_authenticated
May 13 13:29:47: %EOU-6-AUTHTYPE: IP=172.30.40.16| AuthType=EAP
May 13 13:29:47:     eou_auth 172.30.40.16: during state eou_authenticated, got event
7(eouResultAck)
May 13 13:29:47: @@@ eou_auth 172.30.40.16: eou_authenticated -> eou_authenticated
```

CTA Logging Output

To start CTA logging, run the **ctalogd enable** command from the CLI in the directory where CTA is installed. After executing this command, **ctalogd** writes a trace of its current activity into the following directory:

C:\Documents and Settings\All Users\Application Data\Cisco Systems\CiscoTrustAgent\Logs

The following shows a trace from a successful posture validation session:

```
Cisco Trust Agent Version 1.0.48.0
Copyright © 2003 Cisco Systems, Inc. All Rights Reserved. Trust Agent Type(s):
Windows, WinNT Running on: 5.1.2600

1      17:33:33.27905/21/2004Sev=Info/4PADaemon/0x6300000D
Ctad service stopped

2      17:33:34.48005/21/2004Sev=Info/6NetTrans/0x63100003
EAPoUDP configuration: local address=0.0.0.0, local port=0x5566, support Max 8 sessions,
session idle timeout 3600 seconds

3      17:33:35.51205/21/2004Sev=Info/4PADaemon/0x6300000E
Ctad service started

4      17:33:52.24605/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

5      17:33:52.25605/21/2004Sev=PktDump/13NetTrans/0x63100006
EAPoUDP incoming packet dump:0012000801D116DA0000000080010004A38B9EC1

6      17:33:52.28605/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet
dump:8012001801D116DAA38B9EC18003000CA38B9EC12433048F7E24FE25800100043061E4CE

7      17:33:52.29605/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

8      17:33:52.31605/21/2004Sev=PktDump/13NetTrans/0x63100006
EAPoUDP incoming packet
dump:0013001901D116DB3061E4CE8003000CA38B9EC12433048F7E24FE2580020005010100050 1

9      17:33:52.33605/21/2004Sev=Info/4NetTrans/0x6310000E
EAPoUDP Session 1 created for NAD 172.30.40.1, total session count: 1

10     17:33:52.35605/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet dump:8013000901D116DBA38B9EC1800200050201000501

11     17:33:52.37605/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

12     17:33:52.39605/21/2004Sev=PktDump/13NetTrans/0x63100006
```

```
EAPoUDP incoming packet dump:0013000A01D116DC3061E4CE80020006010400061921

13      17:33:52.43605/21/2004Sev=Info/5PEAP/0x63400009
PEAP module initialization success!

14      17:33:52.45605/21/2004Sev=Info/5PEAP/0x6340000B
PEAP processing begun

15      17:33:52.48605/21/2004Sev=Info/4EAPTLV/0x63500005
Begin EAP-TLV processing

16      17:33:52.86705/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet
dump:8013007401D116DCA38B9EC18002007002040070198100000066160301006101000 05D030140AE9FF00E5
EBE99A7BDA6961FAB7047E35CB1EA474BD741DC4BE55E21EB1BF500003600390038003500160013000A0033003
2002F00070066000500040063006200610015001200090065006400600014001100080006000301 00

17      17:33:52.88705/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

18      17:33:52.89705/21/2004Sev=PktDump/13NetTrans/0x63100006
EAPoUDP incoming packet
dump:001303F801D116DD3061E4CE800203F4010503F419C100000438160301002A02000026030140AE9FF1619
BF4AEB0A422758A3D36C3424810DA1D27E2ABC0C1E239DE47694E000035001603 0103FB0B0003F70003F400020
7308202033082016CA003020102020203E9300D06092A864886F70D0101040500302F311C301A060355040A131
3436973636F2053797374656D732C20496E632E310F300D06035504031306537472657373301E170D303230383
0373132313335335A170D3438303832303035343533375A302F311C301A060355040A1313436973636F2053797
374656D732C20496E632E310F300D060355040313065365727665723081 9F300D06092A864886F70D010101050
003818D0030818902818100DF2ED9651FDDC2EF13E7677710343D3CD68A3964AD0FF123E4249BE114757FE0DDC
123255E8D240878637D415A7C0A91299F1D4CCB4005EA80571A9F27C852D66EFFBEA02D04CC8AE2FBB50DE901C
54E7E00C24D2A897C01914ACE99204D2A44EFB7089A48A614BD8E3CE6B9BC9A4C9C3DBD1396DAF1CD29A2259AA
47F86BC490203010001A32E302C300B0603551D0F0404030203A8301D0603551D250416301406082B060105050
7030106082B0601050507030330 0D06092A864886F70D0101040500038181003AB28DB0F38CC5BB172AD732ED2
4B1E10B8BFA68362378D7B8FD23D476D18C889C78F604A73C14039BEF60D28A78B95FB6012175FCE17EBC10483
E78D5A7A6BA98A4FD012149566642E212B295827555D0FAEE84883735CAF874EAFF918E15CBF7DFEE8B22F3DF1
50339C4C8C8B293C760FD3CE873E443721C7760AD91C680530001E7308201E33082014CA003020102020100300
D06092A864886F70D0101040500302F311C301A060355040A1313436973636F2053797374656D732C20496E632
E310F300D06035504031306537472657373301E170D3032303830373131333830365A170D3438303832303035 3
03935305A302F311C301A060355040A1313436973636F2053797374656D732C20496E632E310F300D060355040
3130653747265737330819F300D06092A864886F70D010101050003818D0030818902818100B9FC383B95B5E14
08A7EC17FC775F509A2D8FD0AB700C18D470D8466030ED3835D5C147978DDA709A14D2A33512B78981EB092058
90DE918593436A30FA64B114334821F64541591F7205CD84DED4A49E5AD53D59E1735E8030D61C956126E6A6B1
219599F6FC5B82404367F14D7C6B2C20622207FC642AC10D145EA60BA6DFF0203010001A30F300D300B0603551
D0F0404030202 04300D06092A864886F70D0101040500038181 00A925307D87296963035BBD1D4C94E561E5CAC
A62B84AF28EEEB9B1C90C2037A243E1F2DC89D584D157B8B697BA68A689E0BDA6C1EC6506F2B86876

19      17:33:52.91705/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet dump:8013000A01D116DDA38B9EC18002000602050006190 1

20      17:33:52.94705/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

21      17:33:52.96705/21/2004Sev=PktDump/13NetTrans/0x63100006
EAPoUDP incoming packet
dump:0013005801D116DE3061E4CE80020054010600541901559798BD604AC37AFC18CA64DB9BAA10172916C59
C2AB66370734BCED3ABD6DE00EF9249E1E982580E30B0E6D11E779A4FA71FD0A47843DA2DB32DFCC86E577873D
CE05DD316030100040E000000

22      17:33:53.02705/21/2004Sev=Info/5PEAP/0x6340000D
Server certificate (/O=Cisco Systems, Inc./CN=Server) has been validated by local CA
certificate (/O=Cisco Systems, Inc./CN=Stress).

23      17:33:53.04705/21/2004Sev=Info/5PEAP/0x6340000E
No rule configured for server certificate DN checking. Pass.
```

```
24      17:33:53.07705/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet
dump:801300D401D116DEA38B9EC1800200D0020600D01981000000C616030100861000008200808E6052D2AE3
311CFB4948DE8EB248DE17F72FEF1C91BDE8890E23CF8016C628A5DF72AA98E76A8D501CD645A2DA99BBBD1367
E2EFC0ED9DE9A1FCA34CEDF5200FA5DEAB49109E836A37BE92FE0E8142E6F28187C3502D6EFE9185D8BE219C17
2BBBECF21C25AB3F297DB2B43DE6B163DE91F090661B9455ABEDEA4F33391CC641403010001011603010030DA
3EB5AAC0586DDAD169105671402F1621DCA81F2BC13104D7ED9BF60D23BFC86C8DDFF2999B7400C273FD6F8396
804

25      17:33:53.09705/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

26      17:33:53.11705/21/2004Sev=PktDump/13NetTrans/0x63100006
EAPoUDP incoming packet
dump:0013004901D116DF3061E4CE80020045010700451981000003B1403010001011603010030 43E9AE8C424
49AF10E9F317BD58E8B5C3A76689CC6400C504ADE949AD213F964B372DDCC75446343DA3AB6015347B009

27      17:33:53.14705/21/2004Sev=Info/4PEAP/0x63400003
PEAP handshake success

28      17:33:53.16705/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet dump:8013000A01D116DFA38B9EC18002000602070006 1901

29      17:33:53.19705/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

30      17:33:53.21705/21/2004Sev=PktDump/13NetTrans/0x63100006
EAPoUDP incoming packet
dump:0013002F01D116E03061E4CE8002002B0108002B19011703010020B70E495379E4E87DF1A1E80AB0CDB04
CE95B6649C330EE19271456F4DA35D1E4

31      17:33:53.23705/21/2004Sev=Debug/7EAPTLV/0x63500003
EAP-TLV starts processing message type: EAP Identity request

32      17:33:53.28805/21/2004Sev=Info/6EAPTLV/0x63500002
EAP Identity:  WILDERNE-TECRA8:John Dough

33      17:33:53.31805/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet
dump:8013004F01D116E0A38B9EC18002004B0208004B19011703010040 14CAF0CB6A5200CA58E6442D8F1F5FA
A9487CE0EFC85D881F4A88BBB26BE7DC133DDD57AA5533268C345BD49D0B00535711668A9BB53C0B563244BAC7
F08CD31

34      17:33:53.33805/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

35      17:33:53.36805/21/2004Sev=PktDump/13NetTrans/0x63100006
EAPoUDP incoming packet
dump:0013002F01D116E13061E4CE8002002B0109002B19011703010020F0A620F661F729277733A265E4A427E
AD3D94DF60EA748692FABEE073CFA3946

36      17:33:53.38805/21/2004Sev=Warning/3EAPTLV/0xA3500005
Unexpected EAP type (0x6)

37      17:33:53.41805/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet
dump:8013002F01D116E1A38B9EC18002002B0209002B190117030100208E826C300AFE850AA6E8A6B73940F51
12B0B781E4D656BE4AFB6F71895EBC5B1

38      17:33:53.43805/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

39      17:33:53.46805/21/2004Sev=PktDump/13NetTrans/0x63100006
```

```
EAPoUDP incoming packet
dump:0013003F01D116E23061E4CE8002003B010A003B1901170301003052D92411274ABF128119EFA3F1F5053
1DE6C1F96EBB87907F0FE049082B2F0A408DEA986AC49642857ED6E7FB29DC87B

40      17:33:53.48805/21/2004Sev=Debug/7EAPTLV/0x63500003
EAP-TLV starts processing message type: EAP Extension

41      17:33:53.51805/21/2004Sev=PktDump/13EAPTLV/0x63500006
Request message dump: 0007001000000009800100080000000000000008

42      17:33:53.56805/21/2004Sev=Debug/7PPMgr/0x63600003
Cisco Systems PostureAgent Request took 0.001290 seconds to execute

43      17:33:53.57805/21/2004Sev=PktDump/13EAPTLV/0x63500007
Response message dump:
000700590000000980010051000000090001005100030016436973636F205472757374204167656E7400000400
0C0001000000300000000005001B57696E646F77732058502050726F66657373696F6E616C0006000C000500010A
280000

44      17:33:53.60805/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet
dump:8013008F01D116E2A38B9EC18002008B020A008B19011703010080BCF08F6F0639506C6551BE2B6CB0242
74E3303F87F2526DAB117CD8105B558F7C49F226975FC40F0508C8E98B7D45EAF0F87700A59636B8BB67569D80
878C7780B384A5D1A7F13A37BC25B3259B76706E68A84C1C239F41A0219E85CDC1CB6A461CB0CE2AD799822E31
F3DE639BB8A420BF0836F8DE1C3FA2C36A810994568B9

45      17:33:53.62805/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

46      17:33:53.65805/21/2004Sev=PktDump/13NetTrans/0x63100006
EAPoUDP incoming packet
dump:0013006F01D116E33061E4CE8002006B010B006B19011703010060D5DD2EBCF633B50C213398C594DF614
1E00041EC83B12EC797F112758E532ED889C573FD09845638F2B74FA0C4A5F44389E9989925FC0F573C9ED51C0
A32B0F279F1FEFEF5F42E819881770D29B4F91AF1ED87CD5CA0955181820CB2F2546BE9

47      17:33:53.67805/21/2004Sev=Debug/7EAPTLV/0x63500003
EAP-TLV starts processing message type: EAP Extension

48      17:33:53.69805/21/2004Sev=PktDump/13EAPTLV/0x63500006
Request message dump:
000700300000000980020028000000090001001000001000800000000000000000000001000020008000000000
00000900010008800300020001

49      17:33:53.73805/21/2004Sev=Info/4PAPlugin/0x63200001
Application Posture Result = Healthy

50      17:33:53.75805/21/2004Sev=Info/4PAPlugin/0x63200002
System Posture Result = Healthy

51      17:33:53.78805/21/2004Sev=Debug/7PPMgr/0x63600004
Cisco Systems PostureAgent Notify took 0.043657 seconds to execute

52      17:33:53.80805/21/2004Sev=PktDump/13EAPTLV/0x63500007
Response message dump: 800300020001

53      17:33:53.83805/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet
dump:8013002F01D116E3A38B9EC18002002B020B002B19011703010020690E8B30BD74E609515CC340D96B73D
95F3EDED48CCF8211C3B08E32425D8665

54      17:33:53.87805/21/2004Sev=Debug/7NetTrans/0x63100005
Received a packet from address 172.30.40.1, port 0x5566

55      17:33:53.88805/21/2004Sev=PktDump/13NetTrans/0x63100006
```

```
EAPoUDP incoming packet dump:0014000801D116E43061E4CE80020004030B0004

56      17:33:53.91805/21/2004Sev=Info/4PEAP/0x63400008
PEAP received a message of: EAP Success

57      17:33:53.93805/21/2004Sev=Info/5EAPTLV/0x63500004
Done with EAP-TLV processing

58      17:33:53.96905/21/2004Sev=Info/5PEAP/0x6340000C
PEAP processing finished

59      17:33:53.98905/21/2004Sev=Info/5PEAP/0x6340000A
PEAP module deinitialized

60      17:33:54.01905/21/2004Sev=PktDump/13NetTrans/0x63100007
EAPoUDP outgoing packet dump:8014000001D116E4A38B9EC1
```

APPENDIX B

Reference Information

This appendix provides a list of acronyms and definitions of terms used in Network Admission Control (NAC). It provides sources of further information about NAC and includes the following sections:

- Acronyms
- Definitions
- Related Documentation

Acronyms

Table B-1 Acronyms

Acronyms	Definition
AAA	Authentication, Authorization, and Accounting
ACE	Access Control Element
ACL	Access Control List
Cisco Secure ACS	Access Control Server
APT	Application Posture Token
AV	Anti Virus
AVP	Attribute Value Pair
CA	Certificate Authority
CTA	Cisco Trust Agent
EAP	Extensible Authentication Protocol
FW	Firewall
HCAP	Host Credential Authorization Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IDS	Intrusion Detection Systems
NAC	Network Admission Control
NAD	Network Access Device
PA	Posture Agent
PB	Posture Broker

Table B-1 Acronyms (continued)

Acronyms	Definition
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Access Dial In User Service
SPT	System Posture Token
TACS+	Terminal Access Controller Access Control System Plus
TLS	Transport Layer Security
TLV	Type Length Value
UDP	User Datagram Protocol
VPN	Virtual Private Network

Definitions

Table B-2 Definitions

Term	Definition
AAA Server	Evaluates credentials from peer and determines network access policy for enforcement by Authenticator. May use back-end servers for credential evaluation, such as vendor-specific posture servers such as the NAI AV Server. Also supports access policies for "clientless hosts".
Access Accept	AAA Server returns Access Accept to Authenticator to indicate that the peer has had its credentials evaluated successfully and (optionally) that a new access policy is to be enforced as a result. Successful evaluation means that the Authenticator must keep state that the Peer has had its credentials checked so that the Peer is not checked again until it is time to re-validate the Peer.
Access Reject	AAA Server returns Access Reject to indicate that the credentials have not been evaluated successfully, and no (new) access is to be provided to the peer. Unsuccessful evaluation means that the Authenticator does not maintain state about the peer; that is, the peer credentials need to be checked again after some configurable hold period. The default access policy continues to apply to rejected peers.
Accounting	The process of collecting quantitative data about sessions for the purposes of troubleshooting, capacity planning, or auditing.
Association	A single instance of the L3 access control protocol (Apocope) between peer and authenticator. Represented by state of conversation, IP address of other party, active timers, keys used in status query.

Table B-2 Definitions (continued)

Term	Definition
Authentication	In the case of identity, the use of credentials to establish that a principal is who he or she claims to be. In the case of posture, the use of credentials to establish that the posture of the end-system is what the principal says it is.
Authenticator	Logical entity in the gateway that initiates the exchange of EAP credentials, relays EAP credential requests and responses between peer and AAA server, and enforces network access policy on a particular port or interface based on the results from the AAA server. Same functionality as authenticator in EAP or 802.1X, but does not include any AAA server functionality. In addition to acting as an EAP "pass-through" for EAP methods that require a AAA server, the authenticator implements EAP methods that do not require AAA server functionality, in particular, the EAP status query method.
Authorization	The act of determining what part of the network a principal is permitted to access based on identity or posture or both.
Cisco Trust Agent	Cisco software that implements peer functionality
Clientless host	A TCP/IP host that does not have the posture agent installed
Credential	A piece of information presented by a principal in support of a claim of identity or posture. Includes identity and posture information itself. Examples include username, password, and AV signature file version.
Default Access Policy	Access policy applied to a peer when the policy has not been updated as a result of an Access Accept
End-system	A TCP/IP host; for example, desktop, server, IP phone, printer
Gateway	L3 network device that has authenticator functionality. May be one or more hops from peer
Identity	A unique name associated with a principal.
IP Intercept ACL	A special type of access control list (ACL) that indicates which packets on an interface trigger validation of the peer (source IP address of the packet)
Network Access Device	First hop network device (as measured from peer) that has authenticator functionality
Network Access Filtering	A method of changing the downloadable access list depending on which network access device is receiving the download.
Network Device	L2 or L3 networking equipment such as switches, routers, wireless access points, and VPN concentrators
Peer	Logical entity in end-system that responds to requests for credentials from authenticator for the purposes of gaining access to restricted network. Referred to as supplicant in 802.1x. Same as peer in EAP.
Posture	The state of a device; for example, set of applications loaded on desktop; AV scan engine version and signature file version; FW version and rules file

Table B-2 Definitions (continued)

Term	Definition
Posture Agent	The software implementing the posturing process on a client machine. This includes, but is not limited to, the Cisco Trust Agent.
Posture Client	Cisco or third-party software that resides on the peer and responds to requests from posture agent for posture credentials.
Posture Server	Cisco or third-party back-end server that responds to requests from AAA server to validate vendor-specific posture credentials from posture client.
Principal	Something with an identity; for example, a user or a device.
Provisioning	Configuration of network devices and servers needed to deliver services for a principal.
User	A human being using a device.

Related Documentation

This section provides URLs to websites where you can obtain additional information about NAC. It includes the following topics:

- Configuring Network Admission Control
- CTA Documentation

Configuring Network Admission Control

- Implementing Authentication Proxy—
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094eb0.shtml
- Configuring Authentication Proxy—
http://www.cisco.com/en/US/docs/ios/12_1/security/configuration/guide/scdauthp.html
- Cisco Secure ACS 3.3—
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/

CTA Documentation

- CiscoWorks SIMS—
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/sims/3_1_1/
- Cisco Security Agent—
http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/40/index.htm