

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.

🛃 tasan Secure at 15	Michael Afenant Explorer provided by Essan was crus, Inc.
File Edit View F	izvertes Tools Help 🔢
dedtees de beteu/litz	J II (A) [U]Standh [L]Fevoltes (U) Periods (U) 주는 그가 드러 ~ [[[] 1], [] 7 26 181 246 48728-567 (http://www.com/articles
Cisca Systems	Cisco Secure ACS v3.3
Botap	Select "Log Off" to end the administration sension.
Retvark Retvark Set Ompowers Retvark Seten Configuration	CiscoSecure ACS v3.3 effers support for multiple AAA Cients and advanced TACACS+ and RADIUS Exabres. It also supports several methods of authorization, authorization, and accounting (AAA) including several one-time-parameted cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.
Configuration	n CircoStoure AC3 Robuse 32(1) Build 5 Copyright 63000 Circo Systems, Inc.
Discussent alkon	Copyright 201991-1991 KKA Data Sacuatty, hue MCD Microsop-Digers Algorithm. All ights meared. Copyright 201990, 1993 The Require of the Durin work of Quillage to seared. Copyright 201906 Linewarks of Toronto. All rights reserved. Copyright 201997-2010 hueralizated Software Copyration. All rights reserved. Copyright 201997-2010 hueralizated Software Copyration. All rights reserved. Copyright 201997-2010 hueralizated Software Copyration. All rights reserved. All Units indicated and events in the Copyright of the Software Copyright of the Software Copyright 201997-2010 hueralizated Softw
#	🕴 🕴 🖬 Grizensi:

Figure 2-2 Cisco Secure ACS Welcome Window

implementing NAC. **Configuring the Administrator Interface to Cisco Secure ACS**

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

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

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

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

Figure 2-3 Interface Configuration Main Menu



Step 2 Click **Advanced Options** in the middle frame in this window. The system displays the window shown in Figure 2-4.

CiscoSerure ACS - M	icrosoft Internet Evolution provided by Fiero Systems Tor	
File Edit View Fav	orites Tools Help	
⇔Back • → • 🙆	이 슈 @ Search @ Favorites @ Media 3 8 - 3 3 - 3 - 1 문 요	18
Address 📳 http://172.3	0.1.10:2296/index2.htm	▼ 🖓 Go Units »
4- Book	Image: Construction of the section	O Advanced Options Per-User TACACS+/RADIUS Attributes User-Level Network Access Restriction Sets User-Level Network Access Restrictions User-Level Network Access Restrictions User-Level Network Access Restrictions Oroup-Level Network Access Restrictions Group-Level Password Aging Max Sessions Using Outats Distributed System Settings Remote Logging CiscoSecure ACS Database Replication RDBMS Synchronization P Pools Network Device Groups
Construction	RDBMS Synchronization IP Pools Network Device Groups Voice-over-IP (VoIP) Group Settings Voice-over-IP (VoIP) Accounting Configuration ODBC Logging Submit Cancel	Advanced Options Advanced Options Use this page to configure which advanced features will appear in the user interface for your installation. You can
🚳 Done		Totamat 🔊

Figure 2-4 Interface Configuration Advanced Options

Step 3 Enable the following options in this window:

- Group-Level Downloadable ACLs—This enables the appearance of the downloadable ACLs option in the Shared Profile Components and Group Setup windows. These are used to cause Cisco Secure ACS to send network access policies to the NAD to be applied on a client undergoing NAC.
- Network Access Filtering—This option enables the appearance of the network access filtering option under the Shared Profile Components window. This allows a network to have differing enforcement policies downloaded for application to a client in a particular state depending on where in the network the client is located. For instance, if multiple remediation servers are present in a network, it is best to send a client in a quarantined state to the closest remediation server for its software update.
- Step 4 After checking these check boxes, click Submit.

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

Allowing Administrator Access Via HTTP

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

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

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

CiscoSecure ACS - N	ficrosoft Internet Explorer provided by Cisco Systems, Inc.		@×
Ble Edit View Fav	vorites Iools Help		19
$\Leftrightarrow Back \bullet \bullet \bullet \bigcirc \bigodot$	🚯 🕼 🕅 Search 💿 Favorites 🛞 Media 🎯 🔂 - 🎯 🗹 - 📃	<u>11</u> 0	
Address 🕘 http://172.3	10.1.10:2296/index2.htm		▼ 🖓 Go Links ≫
Cisco Systems	Administration Control		×
User Setup	Confirm Password	Help Administrator Details	<u>*</u>
SharedProfile Components	Administrator Privileges	Administrator Privileges Deleting an Administrator Renaming an Administrat	: <u>0</u>
Configuration System Configuration	User & Group Setup Add/Edit users in these groups Setup of these groups	Administrator Details	the administrator uses to
Administration	Available groups Original Orig	log in to Cisco Secure ACS type and confirm the new pa	from a remote browser, ssword. Click Submit.
Deternal User Debases Reports and Activity Documentation	3: forong 3 3: forong 4 5: foreight 4 5: foreight 4 6: foreight 4 7: quarantine 7: quarantine 9: unknown 10: forough 10 11: foreight 4 11: foreight	If the administrator is locked the "Reset current failed atte: appears. This indicates that is the correct password for the attempts defined on the Sess Administration Control secti	out of Casco Secure ACS, mpts count" check box omenone failed to provide number of successive failed ion Policy page of the on.
	Shared Profile Components	To unlock the administrator current failed attempts count	account, clear the "Reset " check box. Click Submit .
	Network Access Restriction Sets	[Back to Top]	
	✓ Network Access Filtering Sets	Administrator Privileges	ş
	Submit Delete Cancel	Select any or all the followin	g privileges that you want to

Figure 2-5 Administrator Privileges

- **Step 2** Click **Add Administrator**. Fill in the username and password fields, and then configure the individual administration group privileges as needed.
- Step 3 Click Grant All to give all configuration rights to the administrator being configured.

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

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

Fark • 📾	에 해 해Samb Ellevertes Officia (해 타. 클 팩 · 티 티 운	1.61
these 😥 http://172.2	an a	v (∂°Go Lints
Crece Systems	Administration Control	
User Eerlop Serlop Serlop StandOrofile Comparents	Administration Control	Int • Add Administration Control • Add Administrator • Access Folloy • Session Policy • Session Policy
Historic Dan'i puretion Bystem Bystem Dan'i guration Configuration Configuration Contral Control	Add Administrator	Administration Control This page presents options allowing you to add or edit administrative accounts and to edit or establish access, session, and audit policies.
Reparts and April May Cocumentation		[Back to Top] Add Administrator Click to add a new administrator.
		(ESECK to 100) Access Folicy Click to configure access policies that enable administrators of Cisco Secure ACS to limit access by IP address range.

Figure 2-6 Administration Control



Installing the Cisco Secure ACS Server Certificate

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

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

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

- **Step 1** Copy the public/private key pair files to a directory accessible to the Cisco Secure ACS server.
- **Step 2** On the System Configuration menu, click **Cisco Secure ACS Certificate Setup**. The system displays the window shown in Figure 2-7.



Figure 2-7 ACS Certificate Setup

You perform all certificate management operations from this window.

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

Step 3 Click Install Cisco Secure ACS Certificate.

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

CiscoSecure ACS - Microsoft Internet Explorer			_ # ×
File Edit View Favorites Tools Help			12
4-Back + → · ③ ③ ④ ⑤ Search ▲ Parontes ③th	1eda 🥵 🗗 🥔 🗃 - 🖻 👘		
Address ahttp://127.0.0.1:4802/		× .	(∂Go Links »
CISCO SYSTEMS System Configuration			×
additional line Edit		Hala	
User Setup Install ACS	Certificate	Read certificate from file	
Srosp Setup		Certificate file	
The current configuration	has been changed.	Ose certificate from storage Certificate CN	
Control" to adopt the new	v settings for EAP-TLS	 Private key file 	
Configuration or PEAP support only.		Private key password	
System Configuration			
Install new ce	ertificate 🙎	You can use this page to perform certificate enrollment	nt to
Read certificate from file		for access to the Cisco Secure ACS HTML interface	irə t.
Certificate	file c:\certs\server.cer	Cisco Secure ACS supports the X 509 v3 digital	
C Use certificate from storage		certificate standard. Certificate and CA files must be either in Basefi4-encoded X 509 format or DER-	
Certificate	CN	encoded binary X.509 format.	
Private key	file c\certs\server.ovk	Mater MB	
Documentation Private key passy	word	configure the Certificate Trust List, Replacing an exist	ist ting
		certificate configuration with a new certificate	
9	1.11.7	configuration automatically erases the previous	
		congenerator of the <u>certaicate fruit tast</u> .	
		Read certificate from file	
		To install a certificate from a file, select this option.	
Submit	Cancel		
		[Back to Top]	-

Figure 2-8 Install ACS Certificate

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

Step 5 Click Submit.

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



Figure 2-9 Installed Certificate Information

- Step 6 To install the CA certificate, click System Configuration on the Cisco Secure ACS main menu.
- Step 7 In the window that appears, click Cisco Secure ACS Certificate Setup.
- Step 8 Click Cisco Secure ACS Certificate Authority Setup.

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



Figure 2-10 ACS Certification Authority Setup

- Step 9 Enter the drive and directory where the CA certificate file was saved.
- Step 10 Click Submit.

The certificate trust list must have the root certificate added.

- **Step 11** To add the stress CA certificate to the trusted list, click **System Configuration** on the Cisco Secure ACS main menu.
- Step 12 Click Cisco Secure ACS Certificate Setup
- Step 13 Click Edit Certificate Trust List.

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



Figure 2-11 Edit the Certificate Trust List

- **Step 14** Ensure that the check box for the CA to be used is checked.
- **Step 15** Restart Cisco Secure ACS.
- Step 16 Click System Configuration on the Cisco Secure ACS main menu.
- Step 17 Click Service Control.

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



Figure 2-12 Services Log File Configuration

Step 18 Click Restart.

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

Generating Signing Request, Enrolling and Installing Certificate

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

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

- **Step 1** In the Cisco Secure ACS Certificate Setup window, click **Generate Certificate Signing Request**.
- **Step 2** Fill in the blanks with the appropriate information according to your own installation.
- Step 3 Click Submit.

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

CiscoSecure ACS - M	ticrosoft Internet Explorer provided by Cisco Systems, Inc.	
file Edit Yew Fav	ranites Iools Help	10 C
$\Leftarrow Back \ \bullet \ \Rightarrow \ \bullet \ \bigodot$	👔 🕼 Qisearch 🕢 Favorites 🖓 Media 🎯 🖓 - 🌧 🖬 - 📄 🖟 🛝	0
Address 🎒 http://172.3	10.1.10:2296/index2.htm	▼ 🖉 Go Links ≫
CISCO SYSTEMS	System Configuration	×
User Setup	Generate Certificate Signing Request	Now your certificate signing request is ready. You can copy/pa certification authority enrollment tool.
Bured Profile Bured Profile Configuration Configuration Detrets Configuration Detrets Detrets	Generate new request	refunction autooniy enforment tool.
10 Days	1	

Figure 2-13 Generate Certificate Signing Request

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

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

Using a Self-Signed Certificate

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

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

- Step 1 Click Generate Self-Signed Certificate in the Cisco Secure ACS Certificate Setup window.
- **Step 2** Fill in the blanks with the appropriate information according to your own installation.
- **Step 3** Ensure that you enable **Install generated certificate**.
- **Step 4** After completing the certificate setup process, restart Cisco Secure ACS.

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

Configuring Logging

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

To set up logging, perform the following steps:

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

Click logging.

Click CSV Passed Authentications.

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

Figure 2-14 Logging Configuration

Ele Edit View Exceptor Tools Vielo	
He gat yew revolutes loos Hep	12 4 6
→Back + → + 🕼 🖉 🖓 (ØgSearch) 📷 Favorites (@Media ()) 🖓 + 🎒 🔄 + 🧾	1020
Agdress 2 http://172.26.181.246:3790/index2.htm	
Cisco Status Albumutilium	
Logging Configuration	CSVLegs CSVFailed Attempts CSVFailed Attempts
Use Local Logging Configuration Image: Start Street Configuration Image: Start Street Configuration Image: Start Street Configuration Image: Start Stree Configuration Ima	CSV RADIUS Accounting CSV RADIUS Accounting CSV TACACS+ Administration CSV TACACS+ Administration CSV TACACS+ Administration ODBC Logs ODBC Failed Attempts ODBC RADIUS Accounting ODBC CACGS- Administration ODBC TACACS+ Administration ODBC CACGS+ Administration
Image: Sector Sector Image: Sector Sector <td>CSV Logs Cisco Secure ACS records many of its logs in commu-separated value (CSV) test files. You can import CSV log files into many popular spreadsheet applications.</td>	CSV Logs Cisco Secure ACS records many of its logs in commu-separated value (CSV) test files. You can import CSV log files into many popular spreadsheet applications.
	CSVFailed Attempts Click this option to enable and configure Cisco Secure ACS to generate a CSV log of failed login attempts.
	[Bark to Top] CSV Failed Attempts
Done	🤨 Internet

Step 2 Click Log to CSV Passed Authentications.

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



Figure 2-15 Enable Logging

Step 3 Enable the Log to CSV Passed Authentications report.

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

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

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

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

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

You can include other fields as you like.

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

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

- **Step 5** Scroll down the window and change the file management settings if desired.
- Step 6 Click Submit.
- **Step 7** Click **System Configuration** again on the Cisco Secure ACS main menu.

Step 8 Click Service Control.

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

CiscoSecure ACS - M	ticrosoft Internet Explorer provided by Cisco Systems, Inc.	
Ele Edit Yew Fav	rankes Iools Help	18
\Rightarrow Back $\bullet \Rightarrow \bullet \bigcirc$	👔 🕼 🔞 Search 🖓 Favorites 🛞 Media 🎯 🖓 - 🎒 🗹 - 📄 月 🕴	ŭ 8
Address 🧃 http://172.3	10.1.10:3174/index2.htm	▼ (r ² Go Links [™]
CISCO SYSTEMS	System Configuration	×
User Setup Setup Setup	User Freid 5 Class V Down	Hap Enable Logging Select Columns to Log Log File Management
Components Configuration	Generate New File © Every day C Every week	Enable Logging
Configuration	C Every month C When size is greater than 2048 KB	This option enables you to change the layout of the log files that you can view under Reports and Activities. Select the Log to <i>reportname</i> Report check box, and then configure the following parameters.
External User Databases	Directory [C1/Program Files\CiscoSecure ACS v3.3\Lo	[Eack to Top]
Reports and Activity	□ Manage Directory ○ Keep only the last 7 files @ Delete files older than 7 days	Select Columns to Log In the Attributes column, click the attribute to be logged and clock -> 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
	Back to Help	the desired attributes are in the desired position in the Logged Attributes column. [Back to Top] Log File Management
	Submit Preset Columns Cancer	

Figure 2-16 Log File Management

- **Step 9** Change the service log file configuration to Level of Detail = Full
- **Step 10** Increase the file size from 2048 Kb as necessary.
- **Step 11** Click **Restart** to apply the new configuration.

Configuring a NAD in Cisco Secure ACS

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

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

- Step 1 Click Network Configuration on the Cisco Secure ACS main menu.
- **Step 2** The system displays the window shown in Figure 2-17.

CiscoSecure ACS - M	ficrosoft Internet Explorer provided by Cisco Systems, Inc.	_@×
Ele Edit View Fav	rorites Icols Help	1
$\Leftrightarrow Back \bullet \bullet \bullet \textcircled{\begin{subarray}{c} \bullet \\ \bullet \end{subarray}} \bullet \bullet \bullet \bullet \textcircled{\begin{subarray}{c} \bullet \\ \bullet \end{subarray}} \bullet \bullet \bullet \bullet \bullet \textcircled{\begin{subarray}{c} \bullet \\ \bullet \end{subarray}} \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet $	🕼 🕼 🥘 Search 📾 Favorites 🞯 Media 🎯 🛃 🖬 🖼 🖬 🖬	<u>81.</u> 0
Address 🕘 http://172.2	16.181.246:3457/index2.htm	▼ @Go Links **
CISCO SYSTEMS	Network Configuration	
User Setup Setup Shared Profile Configuration Configuration Sparse Optime Configuration	Add AAA Client AAA Client Hostname nec1751 AAA Client IP Address Key Secret	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
Administration Administration External User Databased Activity Oddiset Documentation	Authenticate Using PADIUS (Cisco IOS/PON 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 Submit Submit + Restart Cancel	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.
	😵 Back to Holp	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.

🖨 CiscoSecure ACS - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	10 C
⇔Back • → - 🗿 🗿 🚮 🔞 Search 🕞 Favorites 🔅 Media 🎯 🔂 • 🎯 🖬 • 📃 👘 👘	
Address a http://127.0.0.1:4002/	▼ (∂Go Links **
Shared Profile Components	×
Edit Edit Edit Network Access Filtering Edit Network Access Filtering Edit Network Access Filtering Edit Edit Edit	Network Access Restriction Adding or Editing a Network Access Restriction Deleting a Network Access Restriction
Name User User <thuser< th=""> User User <thu< td=""><td>Network Access Restrictions Use this page to create a new named network access</td></thu<></thuser<>	Network Access Restrictions Use this page to create a new named network access
Interface Interface	restriction, edit an existing named network access
Reports and Activity nat3725	Adding or Editing a Network Access Restrictions
IP Address	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:
Submit Cancel	 Select the Define IP-based access restrictions check box. From the Table Defines list, select either Permitted

Figure 2-18 Network Access Filtering

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

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

- **Step 3** Add the NADs, or if you are using network device groups in your configuration, add the appropriate network device groups.
- **Step 4** Click **Submit** to save your configuration.

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

Configuring Downloadable IP ACLs

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

- Step 1 Click Shared Profile Components on the Secure ACS main menu.
- Step 2 Click Downloadable IP ACLs from the resulting menu.

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



CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.	X
Ele Edit Yew Favorites Iools Help	100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100
$\begin{array}{c} \leftarrow Back \ \bullet \ \to \ \bullet \ \textcircled{O} \ @} \ \end{array}{O} \ \textcircled{O} \ @ \ \textcircled{O} \ @} \ \textcircled{O} \ @ \ \textcircled{O} \ @} \ \textcircled{O} \ @ \ \textcircled{O} \ @} \ @ \ \textcircled{O} \ @} \ @ \ \textcircled{O} \ @} \ @ \ @ \ @} \ @ \ @} \ @ \ @ \ @$	
Agdress 🎒 http://172.30.1.10:4280/index2.htm	▼ 🖓 Go Links ≫
Cisco Statue Shared Profile Components Edit Downloadable IP ACLs Name: healthy Description: The ACL for the healthy NAC group	Downloadable IP ACLs Deleting a Downloadable IP ACL Deleting a Downloadable IP ACL Downloadable IP ACL
ACL Contents Network Access Filtering Interfuse attoin No ACLs Interfuse attoin Add Up Down Interfuse attoin Interfuse attoin	Use this page to create a new downloadable IP ACL, edt 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
Submit Cancel	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.

CiscoSecure ACS - Mic	crosoft Internet	Explorer			8 ×
File Edit View Favor	rites Tools He	Þ			10
🗧 Back 🔹 🔿 🖉 🧕) 🖞 🎯 Searc	h 📷 Favorites 🎯 Media 🎯 🔂 - 🎯 🗊 - 📃			
Address 😰 http://127.0.0	0.1:4802/			▼ ∂ ⁶ 0 I	inks »
Cisco Systems	Sharod P	rafila Componente			×
	Slidieu Fi				
	Select		_	Help	Ê
Setup				Downloadable IP ACLs	
Big Sroup		Downloadable IP ACLs 🤶		Adding a Downloadable IP ACL	
Bog I Serop	Name	Description		Editing a Downloadable IP ACL	
Components	checkup	ACL for NAC clients in checkup condition		Deleting a Downloadable IP ACL	
Network Configuration	healthy	The ACL for the healthy NAC group	-		-1
Han I Sunday	infected	ACL for infected NAC clients		Downloadable IP ACL e	
Configuration	quarantine	ACL for quarantined NAC clients		Downloadable II ROLS	
Configuration	unknown	ACL for unknown NAC clients		Downloadable IP ACLs are configurable sets of access	
50 Ladministration				control lists for devices that support this feature, such as Cisco PIX Firewalls and VPN 3000-series	
8/00 Control				Concentrators. If your network devices are so	
Del External User				configured, Cisco Secure ACS can send ACLs to be	
(Reports and				applied on a per-group of per-user basis. Once you have created a downloadable IP ACL, you can use it by	_
Activity				configuring the Downloadable ACL settings for the user	
Documentation				or group to which you want to apply the downloadable IP A CL. 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	
		Add Cancel		page that appears, you can configure the new	5
				downloadable IP ACL	-

Figure 2-20 Defining the Downloadable IP ACL Type

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

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

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

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

CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.	
Bie Edit View Figworites Iools Help	18
	9
Agdress 👜 http://172.30.1.10:4280/index2.htm	▼ 🖉 Go Links »
Cisco Systems Judiusdhu	Help 🗠
User Downloadable IP ACL Content Stated Profile Name: permit all	Downloadable IP ACLs Adding or Editing a Downloadable IP ACL Deleting a Downloadable IP ACL
ACL Definitions	Downloadable IP ACLs
Configuration Permit ip any any Permit ip any any	Use this page to create a new downloadable IP ACL, edit an existing downloadable IP ACL, or delete an existing downloadable IP ACL.
a Administration Control	[Back to Top]
Datases	Adding or Editing a Downloadable IP ACL
Activity and a second s	 Name. Type the name you want to assign to the downloadable IP ACL.
Decumentation	 Description. Type an explanation of the downloadable IP ACL
	ACL Definitions. Type the contents of the IP ACL.
Back to Melo	[Back to Top]
<u>•</u>	Deleting a Downloadable IP ACL
Submit Delete Cancel	To delete the downloadable IP ACL that appears in the configuration area, click Delete at the bottom of the

Figure 2-21 Defining an Access Control Entry

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

- **Step 6** Click **Submit** after completing the entries in an ACL.
- **Step 7** Click **Submit** in the resulting window to save the downloadable ACL.

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

🚰 CiscoSecure ACS – Microsoft Internet Explorer provided by Cisco Systems, Inc.	
Bie Edit Yew Favorites Looks Help	
	0
Agdress 🕘 http://172.30.1.10:4280/index2.htm	▼ (P ³ Go Links [™]
Clisco Statema Ladinadhadha	Halp 🔺
Downloadable IP ACLs	Downloadable IP ACLs Adding or Editing a Downloadable IP ACL Deleting a Downloadable IP ACL
Description: The ACL for the healthy NAC group Description: ACL Contents Network Access Filtering Permit all Opermit all (Alt-AAA-Clients) Description: Add Up Down Description: Back to Hulp Description: Back to Hulp	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.
Submit Delete Cancel	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

Figure 2-22 Completed ACL

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

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

- Step 8 Click quarantine previously created from the Downloadable IP ACLs window.
- Step 9 Enter a descriptive name for the instance of this ACL; for example, "east coast quarantine".

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



Figure 2-23 Adding a Quarantine IP ACL

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

Step 11 Click Submit after completing each window.



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.

CiscoSecure ACS - Micro	soft Internet Explorer		×
File Edit View Favorites	s Tools Help		
4=Back + + - 🙆 🔄	🕼 🕅 Search 🕞 Favorites 🛞 Media 🎯 🛃 - 🎯 🗹 - 📃 👘		
Address 🙋 http://127.0.0.1:	:4002/	▼ 🖓 Go Links	35
Cisco Systems S	hared Profile Components		<
User Betup Broup Setup Setup Setup Setup Setup Setup Setup Networks Definitional Configuration	Tame: quarantine Description: ACL for quarantined NAC clients X	Hap Downloadable IP ACLs Adding or Editing a Downloadable IP ACL Deleting a Downloadable IP ACL Downloadable IP ACL	
Parter Configuration Configuration Control Contro Con	ACL Contents Network Access Filtering Cast coast quarantine Add Up Do (All-AAA-Clients) Add Up Do (All-AAA-Clients) Back to Holp Back to Holp	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]	
Analyt start Step started	Submit Delete Cancel	Deleting a Downloadable IP ACL To delete the downloadable IP ACL that appears in the configuration area, click Delete at the bottom of the	110350

Figure 2-24 Selecting the Filter List

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

- **Step 12** Pick the appropriate filter list from the drop-down list.
- Step 13 If NAFs are not being used, select All-AAA-Clients.

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

Configuring Groups and Vendor Specific Attributes

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

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

- Step 1 Click Group Setup on the Cisco Secure ACS main menu.
- **Step 2** Choose the group numbers that correspond to the following conditions: Healthy, Checkup, Quarantine, Infected, and Unknown.

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

CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.	_@×
Ble Edit View Favorites Icols Help	10 A
↔Back • → • 🗿 🕼 🕼 🖓 Search 🕞 Favorites 🖓 Media 🎯 🛃 • 🕞 🖬 🛣	1.0
Address 😰 http://172.26.181.246:3790/index2.htm	💌 رُض Unks »
Address (Phyto://172.26.101.246/3790)rdev2.htm Crisco Strategy Crisco St	
	Click Users in Group to see a list of all users assigned to the
ど Done	🚽 🚽 🖉 Internet

Figure 2-25 Group Setup

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

- Step 3 For each NAC group, click Edit Settings.
- **Step 4** Scroll down the edit window to the Downloadable ACLs window.
- **Step 5** Check the **Assign IP ACL** check box and select the proper access list for the condition to which the group relates.
- Step 6 For each group configured, scroll down to the Cisco IOS software/PIX RADIUS Attributes section.The system displays the window shown in Figure 2-26.

LiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.	
e Edit View Favorites Icols Help	(B)
Back • → • ③ 🔄 🖓 @Search 🕞 Favorites @Media 🎯 💁• 🎯 🖬 • 📃	B 🕰 8
dress 📓 http://172.26.181.246:3790/index2.htm	▼ (PGG Links »
Cisco Systems Group Setup	X
Jump To Access Restrictions	Help
Berry C Assigned from AAA Client pool	Group Settings
L Group Setup	Voice-over-IP (VoIP) Support Default Time-of-Day Access Settings Callback
Shared Profile Components Downloadship ACLs	Cannack Network Access Restrictions Max Sessions
Network Configuration	Usage Quotas Enable Options Theory of Conference
System Configuration	Password Aging Rules Password Aging Rules Prosegument
Configuration Cisco IOS/PIX RADIUS Attributes	Downloadable ACLs TACACS+Settings TACACS+Settings
Administration Control	Command Authorization for Network Device Management Applications TACACS+ Unknown Services
Databases posture-token=healthy	IETF RADIUS Attributes RADIUS Vender-Specific Attributes
Reports and Activity	
Douinertation	Group Settings
Ulugitut j elseo-naza-crean-amount	To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface,
[009\102] cisco-h323-credit-time	Cisco Secure ACS displays only the information for the current configuration. Specific Group Setup configuration options and
009/103) cisco-h323-return-code	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
Submit Submit Restart Cancel	appear only if you have configured a AAA client that uses RADIUS.
	👩 Internet

Figure 2-26 Defining an Attribute-Value Pair

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

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

Note

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

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



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

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

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

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

This URL redirection is enforced by the NAD.

Note

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

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

🐺 CiscoSecure ACS - Mozilla		
Eile Edit View Go Bookmarks Tools Window Help		
Back - Porward - Reload Stop	.10:3901/index2.htm	💌 🥖 Search 📑 👻 🔟
🕺 🏠 Home 🛛 😻 Bookmarks 🖌 Alex mp3s 🖌 Hobbes' Internet Tim	🥒 EarthLink SIPshare: 🥠 INDUSTOR	IOUS CLO 🥒 EmperorLinux Ultra 🥠 Web Sign On (WSO) 🛛 🔪
CISCO SYSTEMS Group Setup		×
Jump To Access	Restrictions	Help
Image: Setup Image: Other Image: Setup □ [024] State Image: Setup □ [025] Class Image: Setup □ [025] Class Image: Setup □ [025] Class Image: Setup □ [027] Session-Timeout Image: Setup □ [028] Idle-Timeout Image: Setup □ [028] Idle-Timeout Image: Online □ [033] Proxy-State □ [034] Login-LAT-Service	0	 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+ Shell Command Authorization Command Authorization for Network Device Management Applications TACACS+ Unknown Services IETF RADIUS Attributes
[035] Login-LAT-Node Submit Submit	+ Restart Cancel	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		

Figure 2-28 IETF RADIUS Attribute

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

Clientless User Configuration (Non-Responsive Hosts)

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

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

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

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

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

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

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

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

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

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

CiscoSecure ACS - M	ficrosoft Internet Explorer provided by Cisco Systems, Inc.	
Ele Edit View Fav	orites Icols Help	19 (A)
$ \Leftrightarrow Back \ \bullet \ \Rightarrow \ \bullet \ \bigodot $	😰 🕼 🥘 Search 💼 Favorites 🖓 Media 🎯 🔂 - 🎯 🗹 - 📃 🗄	E 13, 8
Address 📓 http://172.2	t6.181.246:3790/index2.htm	▼ 🖓 Go Links ≫
CISCO SYSTEMS	User Setup	Help
Uter Setup Setup Developments Carrigaration Carrigaration Carrigaration Carrigaration Carrigaration Carrigaration Carrigaration Carrist Carrigaration Carrist Carrigaration Carrist Carrigaration Carrist Carrigaration Carrist Carrigaration Carrist Carrigaration Carrist Carrigaration Carrist Carrist Carrigaration Carrist Carris	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 Confirm Password Confirm Password Confirm Password Confirm Password Confirm Password Oroup to which the user is assigned:	Account Disabled Delefing a Usernane Supplementary User Info Peasowed Authentication Count of the user is assigned Callback Clent IP Address Assignment Advanced Settings Network Access Restrictions Max Sections Usege Quotas Account Disable Downloadable ACLs Advanced TacCaSS Settings Account Disable Downloadable ACLs Advanced TacCaSS Settings TaCACSE Public Paysourd TACACSE Public Paysourd TACACSE Sublic Control TACACSE
	Callback	Account Disabled Status
	Use group setting No callback allowed	clear the check box to enable the account.
	Callback using kie number Submit Cancel	Deleting a Username
E Done		🔮 Internet

Figure 2-29 User Setup

- Step 2 Type the username for the clientless user, such as clientless, into the User text field.This becomes the username configured in the NAD.
- Step 3 Click Add/Edit.
- **Step 4** Configure the password to be entered into the Cisco IOS software configuration for the clientless user.
- **Step 5** Add this user to the group that you have assigned to be the Unknown group.

Setting Up and Enabling Global EAP Authentication

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

- Step 1 Click System Configuration on the Cisco Secure ACS main menu.
- **Step 2** Click **Global Authentication Setup** from the menu presented.
- **Step 3** Check the **Allow CNAC** check box.

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

Figure 2-30 Global Authentication Setup

Cisco Strikts System Configuration Edit Edit Strikts Global Authentication Setup Strikts Global Authentication Setup Strikts EAP Configuration Strikts EAP Configuration Strikts EAP Configuration PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC MS-CHAP Configuration Miscore Configuration PEAP request time Miscore Configuration PEAP Allow EAP-GTC Miscore Configuration Miscore Configuration PEAP request time PEAP session timeout (minutes): 0 Enable Fast Reconnect: PEAP PEAP Sect PEAP	The second
Edit Hop Image: Server Global Authentication Setup Image: Server Global Authentication Setup Image: Server EAP Configuration Image: Server Allow EAP-MSCHAPv2 Image: Server Allow EAP-GTC Image: Server Allow EAP-GTC Image: Server Fallow CMAC Costor Server Costor Chert initial message: Image: Server PEAP session timeout (minutes): Image: Server Enable Fast Reconnect: Image: Server Enable Fast Reconnect: Image: Server PEAP Image: Server PEAP	X
Example of the second secon	A
	<u>eout</u> ation
PG Databased PAD FAST PEAP	ings for various authentication
Activity Contine Active master key TTL: TL: The months TL: TL: The months TL: TL:	ificate-based authentication entication can occur only after he required steps on the <u>ACS</u> s.
Client initial message: Authority ID Info: Allow automatic PAC provisioning: Allow automatic PAC provisioning: Allow EAP-GTC—Tt	Pv2To enable EAP-MSCHAPv2 ation, select the Allow EAP- ox. o 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.

CiscoSecure ACS - M	ficrosoft Internet Explorer provided by Cisco Systems, Inc.	_ @ ×
Ble Edit View Fav	ronites Icols Help	100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100
$\Leftrightarrow Back \star \Rightarrow \star \textcircled{\texttt{O}}$	🔄 🖧 🕲 Search 💼 Favorites 🔅 Media 🎯 💁 🎯 🖬 - 🖃 F 🚉	0
Address 🛃 http://172.2	16.181.246:3790/index2.htm	▼ (P ² Go Links ³⁶
Cisco Systems	External User Databases	Hein 🖉
User Setup Setup Setup Setup Setup Setur Configuration Set Set Set Set Set Set Set Set Set Set	Database Configuration Creation O	Windows Database Novell NDS Generic LDAP External ODBC Database LEAP Proor RADIUS Server Token Card Server Support RADIUS Taken Server ActivCard Token Server PassCo Token Server PassCo Token Server SafeWood Token Server SafeWood Token Server RASA SecurdDToken Server
Control	Choose what to do with the Network Admission Control database. Configure Delete Cancel	Windows Database Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users. [Backto 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 ontion. If it
8) Done	😗 Üsek to Help	is is not. Cased Secure ACS displays an error message when you chick Configure.

Figure 2-31 External User Databases

Step 4 Click Create New Configuration.

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

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

- **Step 6** Enter a unique name for the database instance and click **Submit**.
- Step 7 If multiple instances of the NAC external user database have been created, as you begin the configuration process make sure that the database name appears in the External Database Configuration window and click Configure.

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

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

- **Step 8** Click **Edit List** in the Mandatory Credential Types window.
- Step 9 Add the credential types to be returned from your client for this instance of the NAC database by highlighting the desired credential type and clicking the right arrow. If the returned credentials are not an exact match to one of the external user databases, the best match is used. If there are no instances of external user database with matching mandatory credentials returned by a client, that client validation process fails. The mandatory credential set acts as a minimum requirement for the instance of the external user database to be used for validation.

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

Bit Bit We Back Standa	CiscoSecure ACS - Mic	crosoft Internet Explorer provided by Cisco Systems, Inc.	
 Address in the provide intervalue i	Ele Edit View Favor	rites Icols Help	
Address (***) Problema (****) (****) (****) (*****) (*****) (******) (********	↔ Back • → • 🕥 ₫	🖞 🕼 🎯 Search 📷 Favorites 🧐 Media 🎯 🖄 - 🎯 🖬 - 🖃 🖗	1.0
 External User Databases <l< th=""><th>Address) http://172.26.</th><th>. 181.246:3790/index2.htm</th><th>▼ (PGo Links **</th></l<>	Address) http://172.26.	. 181.246:3790/index2.htm	▼ (PGo Links **
<complex-block><complex-block><complex-block><complex-block><complex-block><complex-block></complex-block></complex-block></complex-block></complex-block></complex-block></complex-block>	Cisco Systems	External User Databases	X Help
Nankatory Credential Types list Aurilable Credentials Aurilable Credentials	User Setup Group Setup	Edit Credential Types	Available Credentials Selected Credentials
	Exercitive Exercitive	Mandatory Credential Types list Available Credentials Selected Credentials Cless Heth Class Heth NalAV TrendrAV Image: Clean transformer of the selected Credentials Submit Concel Submit Concel Image: Class Selected Field	We this page to define the mandatory credential types for this NAC delabage instance. Mandatory credential types are thosy arow buttors to move highlighted credentials from one lat delabage to the mandatory. Available Credentials The Available Credentials in the plane that and right greater that a delabage to the mandatory credential types that for a delabage to the mandatory of the mandator
an appendix started	Applet started		a Internet

Figure 2-32 Edit Credential Types

Step 10 Click Submit.

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

CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.	
Ble Edit View Favorites Icols Help	10
$\Rightarrow Back \ \bullet \ \to \ \bullet \ \textcircled{a} \ \end{array} \end{array} \end{array} \end{array} $)
Agdress 🕘 http://172.26.181.246:3790/index2.htm	▼ PGG Links ≫
Crees System Alternal User Databases	×
Gift Image: Serve point NAC beta test Expected Host Configuration	 Mandatory Credential Types Credential Validation Policies
Interestive Mandatoxy Credential Types Interestion Cisco PA Cisco PA Cisco Host Cisco Hip Cisco Hip Interface Edit List	A NAC database instance consists of a set of mandatory credential types and a set of policies, local or external or both. Use this age to define the mandatory credential types and the policies that you want to associate with this NAC database instance. Mandatory Credential Types
Administration Image: Credential Validation Policies	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 credential 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, atherwise, Cisco Secure ACS uses the Unknown User Policy to compare the credentials received to the mandatory credential types of other NAC database instances.
Changes will be applied only after pressing 'Save Configuration'.	[Backto Top] Credential Validation Policies
Save Configuration Cancel	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

Figure 2-33 Mandatory Credential Types

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

- Step 11 Click Local Policies, and click New Local Policy from the Local Policy Selection window.
- **Step 12** Enter a name and a description for this policy and a description if desired.
- Step 13 Click New Rule from the Configurable Rules window.
- **Step 14** Select the attribute that you wish to validate for this rule element and select the appropriate operator for validation. Each of these becomes a rule element.

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

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

Ele Edt View Favorites Loois Help	1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 -
→Back + → - 🗿 🗗 🖓 Search 📷 Favorites 🧐 Media 🏈 🔄 - 🎯 🖬 + 🔄 🗗	. 0
Agdress 2 http://172.26.181.246:3790/index2.htm	
Cisco Systems External User Databases	×
	Hein
Rule Configuration	Adding Rule Dements Editing Rule Dements Deleting a Rule Dements
SharedProfile Rule Elements Table:	Deleting a Rule
Attribute Operator Value Attribute Operator Value Classer Attribute Operator Value Operator Classer Value Value Operator Value Value Operator Value Value Operator Value Value	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 statibute, an operator, and a value. Cisco Secure ACS uses the operator to compare the attribute received in the posture value/discince 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 Rele Dements For each rule element you want to add:
Submit Delete Rule Cancel	 From the Attribute list, select an attribute. From the Operator list, select the applicable operator. The operators available vary depending upon the attribute you selected. Type a value for comparison to the attribute selected. Click enter.
	[Back to Top]
	Editing Rule Elements
	For each rule element you want to edit:

Figure 2-34 Rule Configuration

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

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

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

CiscoSecure ACS - N	Microsoft Internet Explorer provided by Cisco Systems, Inc.	_ (7) ×
Ble Edit View Fg	vorites I.cols Help	100 C C C C C C C C C C C C C C C C C C
🗧 Back 🔹 🔿 - 🌀	🔹 🖓 🕲 Search 📾 Favorites 🔅 Media 🎯 🖏 - 🎯 🐨 - 🖃 🗎	0
Address 🙋 http://172.:	26.181.246:3790/index2.htm	▼ 🖗 Go Links ≫
Cisco Systems	External User Databases	×
	Edit	Help
User Setup Group Setup	Local Policy Configuration	Creating a Local Policy Medifying a Local Policy Deleting a Local Policy
Shared Profile Components Network Configuration System Configuration	Name: NAC-CTA-etst Description: Policy Rule List ?	Use this page to create, modify, and delete local policies. Local policies are ordered sets of rules. When Cisco Secure ACS upplies 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
Administration Control	Configurable Rules Cisco PA OS Type = Windows 2000 Cisco PA OS Version = 50 21950 C Result Oredential Taken Action	as the result of applying the policy. Policies are seuseable; you can associate any local policy with more than one NAC database instance. Creating a Local Policy
Reports and Activity	Type Cisco.PA V Healthy V 2 New Pule Up Down Default Pule	 Type a meaningful name in the Name box and type a useful description in the Description box. Add one or more rules to the policy. To do so, chick Add Rule once for each rule you need to add. For each rule, select a Result Credential Type and a Token, and if meeded, type an Action.
	Result Credential Type Token Action Cisco:PA V Unknown V -	 Arrange the notes in the order in which you want Ciece Secure ACS to apply them, from top to bottom. To do so, select the bottom to the left of a rule and use the Up and Deem buttoms to arrange it as needed. Define the default rule. To do so, under Default Rule, select a Result Credontial Type and a Token, and if needed, type and Action.
	💡 Back to Help	6. Click Submit [Back to Top]
Done		🔮 Internet

Figure 2-35 Local Policy Configuration

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

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

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

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

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

- Step 17 Make configuration changes as needed to the default rule and click Submit in this window and click Submit again in the next window.
- **Step 18** To make the changes permanent, click **Save Configuration** in the last window.

Configuring External Policy Verification

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

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

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

Step 1 Click New External Policy.

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

Figure 2-36 External Policy Configuration

CiscoSecure ACS - N	Microsoft Interne	et Explorer provided by Cisco Systems, Inc.			_8 ×
Ble Edit View Fa	varites <u>T</u> aols (jelp			1
$\Leftrightarrow Back \ \bullet \ \Rightarrow \ \bullet \ \bigodot$	2 👌 Q See	rch 🖬 Favorites 🎯 Media 🎯 🔂 - 🎯 🗹 - 🗐 F 🕯	10		
Address 🔕 http://172.	26.181.246:3790/ir	ndex2.htm			▼ 🖓 Go Links ≫
CISCO SYSTEMS	External	User Databases			X
User Setup Setup Setup StaredProfile	Edit	External Policy Configuration External Policy Configuration	- Fielp • Crea • Medi • Deler	ting an External Policy fying an External Policy ting an External Policy	
Network Configuration System Configuration	Name Description	AV server	Use t Exten secor crede	his page to create, modify, and delete external nal policies are a primary server configuration, ndary server configuration, and a set of posture entities that Cisco Secure ACS forwards to the g of Advance servers. It	policies. an optional e validation rimary server solicies es
Interface Configuration Control Detabases Control Detabases Control	♥ Primary Server configuration	URL https://evserver.sample.com/remediate Usemamettestuser Password Geo Trusted Sites Rost CA Sitess	Crea 1.	a tuntor of sections, to the sectionary settern Private Market Section as a sociate any external policy with TAC database instance. fing an External Policy Type a meaningful name in the Name box an useful decouption in the Description box. Select the Primary Server Configuration of	d type a
Desementation	Server Configuration	UPL Usemane Password Timeout 5 GRee Trusted RootCA I-none selected	3.	type its approaches into mains in in no core is the check box. From the Trustel Reef CA is certification authority that issued the server installed on the primary server. If a secondary server is available, select the Server Configuration check box and type the information in the boxes to the self of the ch the Trustef Reef CA ht, a solet the certifica- tion issued the server certificate installed on secondary server. Configure the Forwarding Credential Types	to the test of certificate Secondary applicable eck box. From tion authority the table. Use
(iii) Done	4	Forwarding Credential Tracs	.	credential types to the applicable list. Cisco is sends the credential types in the Selected Co	Internet

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.

CiscoSecure ACS - N	ficrosoft Internet Explorer provided by Cisco Systems, Inc.	_0×
Ble Edit View Fav	orites Icols Help	19 B
🗧 Back 🔹 🔿 🐇 🙆	🗈 🕼 🕲 Search 📾 Favorites 🖓 Media 🎯 🔁 - 🎯 🖬 - 📃 🖪 🞎	0
Address 🙋 http://172.2	:6.181.246:3790/index2.htm	
	External User Databases	×
User Setup Setup Setup Setup Setup Setur S		Helip • • Creating an External Policy • Medifying an External Policy • Deleting an External Policy • Deleting 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 Circo Secure ACS forwards to the primary server or, in a fullower semanic, 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 applicible information in the boxes to the left of the check box. From the Trusted Rest CA kits, select the credification authority that issued the server configuration
	Submit Concel	 If a secondary server: If a secondary server is available, select the Secondary Server Configuration check box and type the applicable information in the boxes to the self of the check box. From the Trusted Rost CA hits, aslest the certification authority that issued the server certificate installed on the secondary server.
	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Consider the reversion Credential types tool: Ose the left and right arrow buttens the move highlighted credential types to the applicable list. Circo Secure ACS sends the credential types in the Selected Credentials list
Done		👩 Internet

Figure 2-37 Selecting Forwarding Credential Types

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

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

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

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

Configuring Token to User Group Mappings

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

- Step 1 Click External User Databases on the Cisco Secure ACS main menu.
- Step 2 Click Database Group Mapping.

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



Figure 2-38 Unknown User Group Mappings

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

Step 3 Click on the name of the configured database.

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

CiscoSecure ACS - M	icrosoft Interr	et Explorer provided by	Cisco Systems, Inc.	Le X
Ble Edit View Favi	orites <u>T</u> ools	Help		1997 - 19
🗢 Back 🔹 🔿 🗸 🙆 [ା ଘା ପ୍ରାର	arch 📄 Favorites 🍘 M	eda 🎯 💁 🗃 🖬 🗉 🖬 🛍	10
Address 🙋 http://172.21	6.181.246:3790/	index2.htm		▼ 🖓 Go Links ≫
Cisco Systems	External	User Databases		×
	Edit			A Help
User Setup Group Setup	Gro	oup Mappings fo	or - NAC beta test	Windows Database Configuration Dialin Permission Configure Domain List
Stared Profile		Token to user-grou	ար ապարթուցը 🔋 🏆	MS-CHAP Settings Windows EAP Settings
Components	Token	User Group	PA user messages	
Network Configuration	Healthy	Healthy 💌	×	Windows Database Configuration
Interface Configuration	Checkup	Checkup 💌	It is time for a A DAT file update.	Configure your Windows database. Cisco Secure ACS supports Windows SAM and Active Directory user databases.
Control	Quarantine	Quarantine 💌	You must update A your DAT file before proceeding	Diath Fermission 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 Gicco Secure ACS to erarch dialn
Content of the second s	Infected	Infected 💌	You have been infected! Contact Net Ops immediately!	permission to users by selecting the top check box. The Microsoft Windows domain must also be configured to allow grant Galim permission to user. See your Microsoft documentation for more information.
	Unknown	Unknown	×	(Basik to Top)
		Submit	Cancel	I 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 she to authenticate a user property if the same username casts in more than one trusted domain. We recommend that you ask users to enter their domains when kiding in a 17 this is not prescribed and users to enter their domains when kiding in a 17 this is not prescribed and users to approximate the domain when kiding in a their sectional you

Figure 2-39 Token to User Group Mappings

- **Step 4** For each token, select the appropriate user group in which to place the client that has that token returned.
- Step 5 Optionally, enter a message to be displayed on the client in a pop-up window after the initial posturing process has completed.

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

Step 6 Click Submit to save your configuration.

Configuring an Unknown User Policy to Check an External Database

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

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

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

CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.	
Ble Edit View Favorites Iools Help	100 million (100 million)
부Back 🗿 🖄 🕼 @ Search 🕞 Favorites 영 Media 🎯 🎝 - 🎯 🖬 - 📃 🗄 🎎	0
lddress 🗃 http://172.26.181.246:3790/index2.htm	
Cisco Systems External User Databases	
User Stop Stop Configure Unknown User Pelicy	Fail the Attempt Check the following external users databases
SubwedProfile Use this table to define how users will be handled when they are not found in the CiscoSecure Database. SubwedProfile C Fail the sitempt C Fail the sitempt C Check the following external user databases Selected Databases Subvergention External Databases </td <td>Use the Configure Unknown User Policy page to define how to handle usernames not found in the CiscoSecure user database. Full 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 <u>Selected Databases</u> list to authenticate unknown users, choose this option. If you choose this option, the order of the databases in the <u>Selected Databases</u> list is any outan. For</td>	Use the Configure Unknown User Policy page to define how to handle usernames not found in the CiscoSecure user database. Full 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 <u>Selected Databases</u> list to authenticate unknown users, choose this option. If you choose this option, the order of the databases in the <u>Selected Databases</u> list is any outan. For
Submit Cancel	External Databases This list displays the external user databases that Cisco Secure ACS does not use to try to suffernite te unknown users. You can move external user database between this list and the <u>Selected Databases</u> list by dirking on the database name followed by clicking on the -> button or the <- button, as applicable.
and and a	Internet

Figure 2-40 Configure Unknown User Policy

- **Step 2** For each external user database you wish to check, add the external user database name to the Selected Databases window with the arrow. Order the databases in the sequence in which you wish to have them compared against the received credential set.
- Step 3 Click the Check the following external user databases radio button.
- Step 4 Click Submit.

Configuring Client Credentials and Type Length Value Data

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

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

Attributes Overview

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

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

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 2-1	Cisco	Trust Agent
-----------	-------	-------------

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
SvsModal=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
ctalogd.ini template
[main]
EnableLog=1
[LogLevel]
PADaemon=3
NetTrans=3
Paplueis 2
```

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_s upplicant.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
- 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.

2-52