



Technical Overview

NAC Framework Configuration Guide

TABLE OF CONTENTS

Table of Contents	2
NAC Configuration Guide.....	5
Introduction.....	5
Target Audience	5
NAC Architecture and Overview	5
NAC Assessment Methods	8
NAC L2 IP	8
NAC L2 802.1x.....	8
NAC Reference Network	9
Cisco Secure Access Control Server Common Configuration.....	10
Vendor Attribute-Value Pairs	10
Task 1: Import Partner AVPs.....	11
Network Configuration	11
Task 2: Network Device Group (Optional).....	11
Task 3: AAA Client Configuration	11
Task 4: AAA Server Configuration.....	12
Interface Configuration	12
Task 5: Configure RADIUS Attributes	12
System Configuration.....	12
Task 6: ACS Certificate Setup	13
Task 7: Global Authentication Setup	13
Task 8: Configuring Attributes for Logging	15
Administration Control	16
Task 9: Add Remote Administrator Access	16
Shared Profile Components.....	16
Task 10: Configure Downloadable IP ACLs	17
Task 11: RADIUS Authorization Components.....	17
Group and User Setup.....	20
Task 12: Group Setup	20
Task 13: User Setup	20
Posture Validation.....	20
Task 14: Internal Posture Validation Setup	21
Network Access Profiles	22
NAC L2 IP Configuration on IOS Switch.....	22
Test Network Connectivity.....	23
Configure the IOS Switch for NAC L2 IP	23
Task 1: Configure Authentication Authorization and Accounting.....	23
Task 2: Configure the RADIUS Server.....	24
Task 3: Enable IP Device Tracking and DHCP Snooping	24
Task 4: Configure an Interface ACL.....	24
Task 5: Configure a Cisco NAC Global Policy.....	25
Task 6: Configure the Cisco NAC Interface	25
Task 7: Set EAPoUDP Timers.....	25
Task 8: Enable EAPoUDP Logging.....	26
Task 9: Enable the HTTP Server on the Switch.....	26
Cisco Trust Agent (CTA) Installation and Configuration	26
Cisco Trust Agent Windows.exe Versions.....	26
Windows.....	26
Task 1: Client Certificate for CTA Install.....	27
Task 2: Install CTA 2.0.....	27
Task 3: (Optional) Manual install of root certificate for CTA	31
Network Access Profile Configuration for NAC L2 IP.....	31
Task 1: Create the NAC L2 IP Profile from the Template.....	32
Task 2: Authentication Configuration.....	32
Task 3: Posture Compliance Configuration	34
Task 4: Authorization	35
Task 5: Test the NAC L2 IP Configuration	36

Task 6: Troubleshooting NAC L2 IP	37
URL Redirection	39
Task 1: Configure URL Redirection on the Switch	39
Automated Browser Launch	39
Task 1: Enter the Desired URL in the Notification String	40
Task 2: View the Automated Browser Launch on the Client	41
NAC Agentless Hosts	41
Task 1: Static NAH Configuration in IOS	42
Task 2: Centralized NAH with ACS	43
Task 3: Dynamic NAH with an Audit Server	45
NAC L2 802.1x	50
NAC L2 802.1x for IOS Switches	51
NAC L2 802.1x Deployment Method Overview	51
NAC L2 802.1x Credential Overview	51
Configure the IOS Switch for NAC L2 802.1x	52
Task 1: VLANs for NAC L2 802.1x	52
Task 2: Configure AAA on NAD for NAC L2 802.1x	54
Task 3: Enable 802.1x on the Switch	55
Task 4: Configure 802.1x on the Interface	55
Network Access Profile Configuration for NAC L2 802.1x	55
Task 1: Create the NAC L2 802.1x Profile from the Template	55
Task 2: Authentication	56
Task 3: Posture Validation	57
Task 4: Authorization	58
CTA Installation	59
Task 1: Client Certificate for CTA Install	59
Task 2: Install CTA 2.0	59
Task 3: (Optional) Manual install of root certificate for CTA	63
CTA Configuration	63
Verify NAC L2 802.1x Functionality	63
Configuring Supplicant Single Sign-On	67
CTA Supplicant Configuration	67
Considerations for Hosts Without Supplicants	70
Guest VLANs for Non-802.1x Hosts	70
Guidelines for 802.1x Authentication with the Guest VLANs on Windows XP Hosts	71
Task 1: Enable Guest VLAN Support on the Interface	71
NAC L2 IP CatOS Switch Configuration	72
Task 1: Configure NAC L2 IP	72
Task 2: Configure NAC L2 802.1x	74
Catalyst 6500 Guest VLAN Configuration Example	74
Configuring MAC-Authentication-Bypass on the 6500	75
Task 1: Catalyst 6500 Configuration	75
Task 2: ACS Configuration for MAC-Auth-Bypass	75
Task 3: Monitoring	78
Microsoft Active Directory Integration	80
Microsoft Active Directory	80
Configuring User and Machine Authentication	81
User and Machine Authentication Overview	81
Task 1: Configure ACS to AD Communication	82
Troubleshooting NAC	83
Cisco Trust Agent and CTA Supplicant Logging	83
NAD Logging, Show Commands, Session Control, and Debug	86
NAD Show Commands	86
IOS NAD Clear Commands	88
NAD Debug Commands	88
CatOS NAD Show Commands	88
Troubleshooting Flow	89
Troubleshooting and Interpreting the Logs and Reports	89
No Attempts Problems	89

Failed Attempts Problems	89
Passed Authentications Problems	91
Appendixes	92
Appendix #1: Reference Documents	92
Appendix #2: NAC Attribute Reference	93
Attribute Namespace	93
Attribute Data Types	93
Attribute Reference	94
Appendix #3: RADIUS Attributes for NAC	96
Appendix #4: ACS Digital Certificate Enrollment with Microsoft Windows 2000 Server Certificate Authority	98
Obtain the Certificate Authority Public Certificate	98
Request a Digital Certificate for ACS	99
Appendix #5: Configuring 802.1x with NAC L2 IP	100
802.1x with NAC L2 IP Overview	100
Task 1: ACS Configuration	100
Task 2: Configure 802.1x with NAC L2 IP on the NAD Interface	101
Appendix #6: Policy-Based ACL configuration	102
Appendix #7: Microsoft Supplicant Configuration	107
Appendix #8: Acronyms and Terms	110

NAC CONFIGURATION GUIDE

Introduction

The purpose of this guide is to provide configuration assistance and guidance for each of the components of the Network Admission Control Framework. This document describes the configuration of Cisco Secure ACS for NAC, the installation guidelines for the Cisco Trust Agent (CTA) on Microsoft Windows platforms, and the configuration procedures for Cisco IOS and CatOS software-based switches acting as network access devices (NADs). For additional considerations and information on the design and deployment of NAC, see the NAC Deployment Guide.

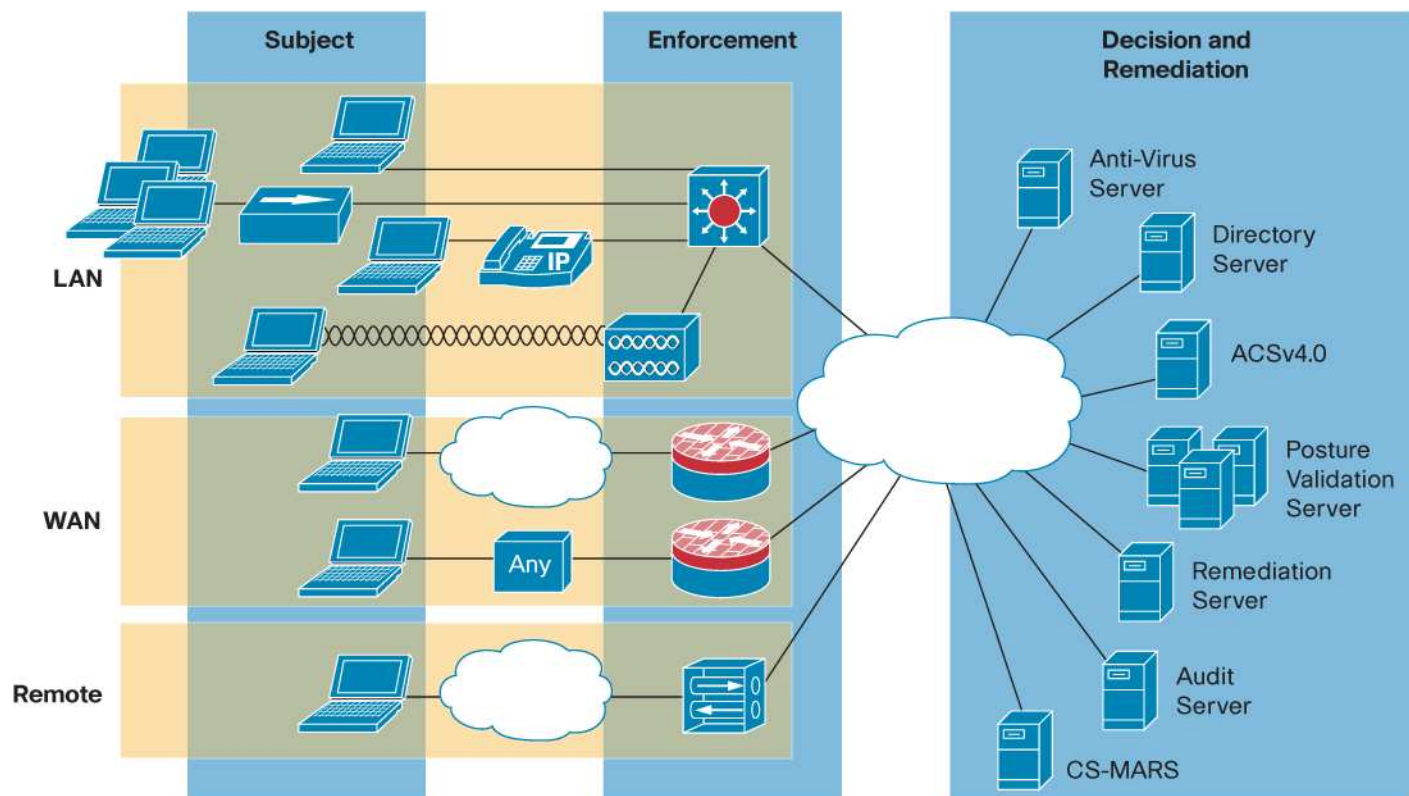
Target Audience

This document is intended for security engineers, network engineers, engineering managers, and network operations staff who need to configure and to deploy Cisco Network Admission Control Framework. This document assumes you are familiar with Microsoft Windows operating systems and client machines and with the configuration and operation of Cisco Secure Cisco Secure ACS. It also assumes you know how to configure Cisco IOS and CatOS devices and are familiar with certificate authorities and the trust models provided by digital certificates.

NAC Architecture and Overview

NAC assesses the state, or posture, of a host to prevent unauthorized or vulnerable endpoints from accessing the network. Enforcement is performed through an authorization policy that is centrally defined on a single ACS server or delegated to multiple NAC posture validation servers. Typical endpoints are desktop computers, laptops, and servers, but can include IP phones, network printers, and other specialized network-attached devices.

Figure 1. NAC Framework Deployment Scenarios



The Cisco NAC posture validation process includes these major architectural components.

Subject:

- **Host**—Machine accessing the network on which NAC is enforced
- **Posture Plugin (PP)**—A Cisco or third-party DLL that resides on a host and provides posture credentials to a posture agent residing on the same device.
- **Posture Agent (PA)**—Host agent software that serves as a broker on the host for aggregating credentials from potentially multiple posture plugins and communicating with the network. The Cisco Trust Agent (CTA) is Cisco's implementation of the posture agent.
- **Remediation Client**—A component of a remediation management solution that operates in conjunction with a remediation server to update specific client software, such as operating system patches.

Enforcement:

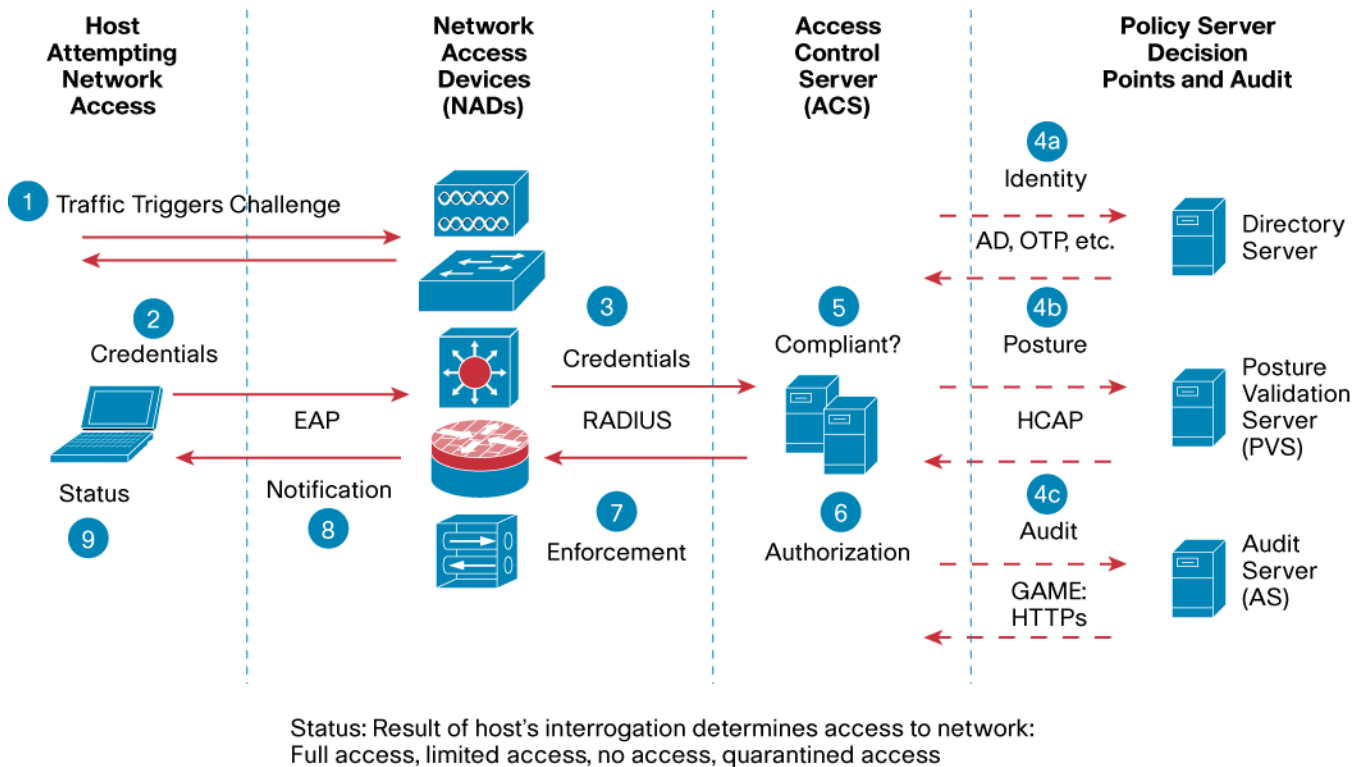
- **Network Access Device (NAD)**— Network devices acting as a NAC enforcement point. These can include Cisco access routers (800-7200), VPN Gateways (VPN3000 series), Catalyst Layer 2 and Layer 3 switches, and wireless access points.

Decision and Remediation:

- **AAA Server (authentication, authorization and accounting Server)**—The central policy server that aggregates one or more authentications, authorizations or both into a single-system authorization decision and maps this decision to a network access profile for enforcement by the NAD. Cisco Secure Access Control Server (ACS) is Cisco's AAA server product that supports NAC
- **Directory Server**—A centralized directory server for performing user or machine authentication or both. Possible directory services include Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory (AD), Novell Directory Services (NDS), and one-time token password servers (OTP).
- **Posture Validation Server (PVS)**—A posture validation server from one or more third parties acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials from one or more posture plugins against a set of policy rules. Examples include antivirus servers or security application servers.
- **Remediation Server**—A management solution used to bring non compliant hosts into compliance. This could be a specialized patch management application or as simple as a web site for distributing software. Audit Server: A server or software that performs vulnerability assessment (VA) technologies against a host to determine the level of compliance or risk of the host prior to network admission.

Figure 2 displays the primary components of the NAC architecture. The communication flows used during the challenge, authorization, and compliance enforcement are also shown.

Figure 2. NAC Architecture Overview



Refer to the numbers in Figure 2 above for each step described in the NAC authorization process.

- Step 1.** Posture validation occurs when a NAC-enabled network access device detects a host attempting to connect or use its network resources.
- Step 2.** Upon detection of a new endpoint, the NAD sets up a communication path between the AAA server (ACS) and the posture agent. After the communication path has been established, the AAA server requests the endpoint for posture credentials from one or more posture plugins.
- Step 3.** The host responds to the request with its posture credentials from available posture plugins from NAC-compatible software components on the host.
- Step 4.** The AAA server either validates the posture information locally, or it can in turn delegate parts of the decision to external posture validation servers.
- Step 5.** The AAA server aggregates the individual posture results, or posture tokens, from all of the delegate servers to determine the overall compliance of the host, or system posture token.
- Step 6.** The identity authentication and system posture token are then mapped to a network authorization in the network access profile, which consists of RADIUS attributes for timers, VLAN assignments, or downloadable access control lists (ACLs).
- Step 7.** These RADIUS attributes are sent to the NAD for enforcement on the host.
- Step 8.** The CTA on the host is then sent its posture status for notifying the respective plugins of their individual application posture as well as the entire system posture.
- Step 9.** A message can be optionally sent to the end-user using the CTA's notification dialog so they know the host's current state on the network.

NAC ASSESSMENT METHODS

In NAC Framework, three types of assessment methods are available to verify host and device policy compliance. These are NAC L2 IP, NAC L3 IP, and NAC L2 802.1X. Both NAC L2 IP and NAC L3 IP use Extensible Authentication Protocol over UDP (EAPoUDP) as a transport mechanism. NAC L2 802.1X uses IEEE 802.1X as a transport mechanism with the addition of a new EAP method called EAP-FAST (Flexible Authentication via Secure Tunneling). The enforcement point for each of these methods is the network access device as shown in Figure 2. This document discusses the configuration of NAC L2 IP and NAC L2 802.1x. For information on configuring NAC L3 IP see the NAC Implementation Guide.

NAC L2 IP

NAC L2 IP is similar to NAC L3 IP in that it uses EAP over UDP (EoU) to transport the posture assessment of a host. However, one primary difference is that NAC L2 IP is implemented at layer 3 on a layer 2 switchport.

There is also no concept of an intercept ACL for NAC L2 IP. With NAC L2 IP, the posture assessment of a host is triggered on the NAD when it receives one of the following from the host:

- DHCP requests
- ARP requests

When the NAD initially receives either a DHCP or ARP request from a host the NAD sends an EoU request to the host to initiate the posture validation process. If the process is triggered based on an incoming DHCP request from the client, it will occur at a somewhat earlier point than the ARP-based trigger.

NAC L2 802.1x

NAC L2 802.1x leverages 802.1x to provide identity information for user and host authentication with the addition the EAP-FAST protocol to also transport posture information for the host. NAC L2 802.1x triggers the assessment of a host via 802.1x on a layer 2 switchport.

NAC L2 802.1x requires a supplicant that supports EAP-FAST for the EAP method to carry identity and posture information in the TLS tunnel. The CTA embedded supplicant supports EAP-FAST and supports EAP-GTC, EAP-MSCHAPv2, and EAP-TLS for client side authentication.

The tables below provide comparison information for each of these methods.

Table 1. NAC Assessment Method Comparison

Assessment Method	Pros	Cons
Unified Layer 2 Identity and Posture	<ul style="list-style-type: none">• Unified identity and posture with NAC L2 802.1x• L2 enforcement• IBNS-compatible	<ul style="list-style-type: none">• Not supported with NAC L2 IP and NAC L3 IP• Retail supplicant license for wireless support• No audit support (Future)
IEEE Legacy 802.1x and Posture	<ul style="list-style-type: none">• IBNS-compatible• Posture• Audit support	<ul style="list-style-type: none">• Disjointed Authorization (posture after VLAN assignment)• Multiple clients or management complexity
IEEE Legacy 802.1x	IBNS-compatible	<ul style="list-style-type: none">• No posture• No audit support
Posture Only (Layer 3)	<ul style="list-style-type: none">• NAC L2 IP and NAC-L3-IP• NAH Audit support (L3-IP in Future)	No identity

Assessment Method	Pros	Cons
	<ul style="list-style-type: none"> • Supplicant optional 	

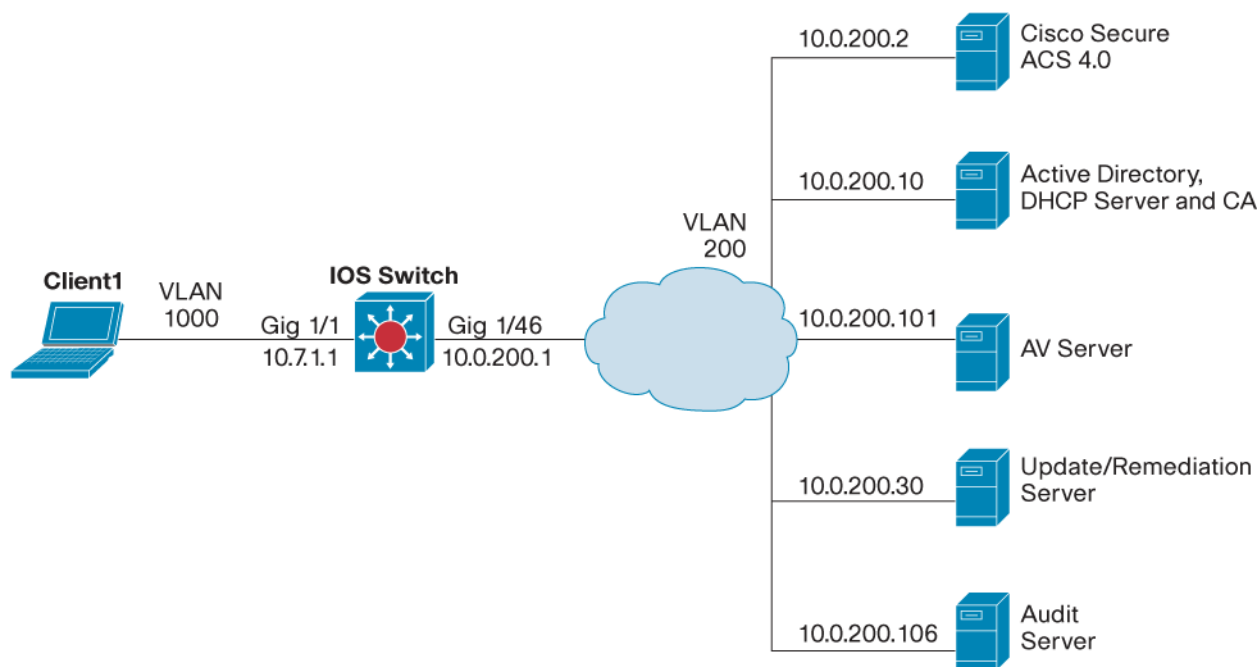
Table 2. NAC Assessment Method Enforcement Features and Trade-Offs.

Feature	NAC L2 802.1x	NAC L2 IP	NAC L3 IP
Trigger Mechanism	Data Link Up	DHCP or ARP	Forwarded Packet
Machine Identity	√	¬	
User Identity	√		
Posture	√	√	√
VLAN Assignment	√		
URL-Redirection		√	√
Downloadable ACLs	6500-only (Policy-Based ACLs)	√	√
Posture Status Queries		√	√
802.1x Posture Change	√		

NAC Reference Network

The following network diagram is used as a reference point for the upcoming IOS switch configuration related sections. The host, Client1, is connected to the IOS switch through Gigabit Ethernet 1/1. This host serves as client for both the NAC L2 IP and NAC L2 802.1x sections of the guide for IOS switches. For the purposes of this document, all servers, including Cisco Secure ACS, Microsoft AD, Antivirus, Remediation, and Audit, reside on VLAN 200.

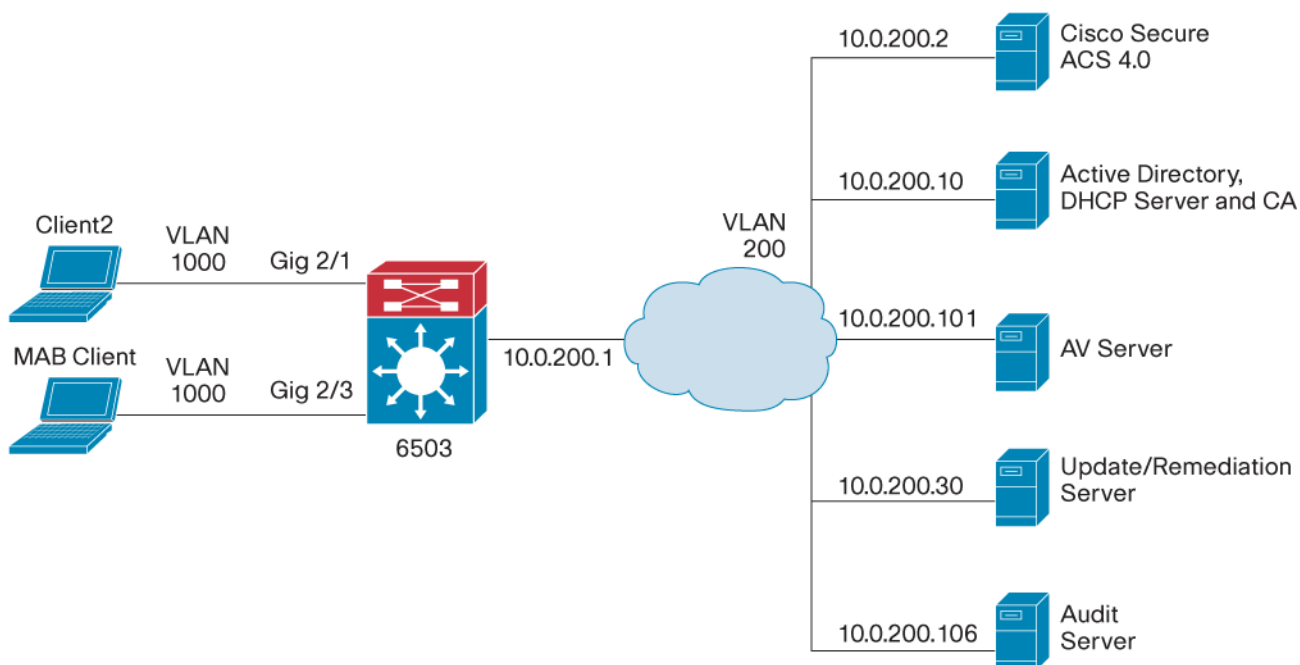
Figure 3. Reference Network for IOS Switch Configuration Section.



The reference network shown in Figure 4 is used in the CatOS switch-related configuration sections.

Client2 is connected to the CatOS switch via port 2/1. This host will serve as client for both the NAC L2 IP and NAC L2 802.1x sections of the guide for CatOS switches. The third host, MABClient, is connected to the CatOS switch via port 2/3. This client is only used for the MAC Authentication Bypass section of the document. For the purposes of this document all servers including Cisco Secure ACS, Microsoft AD, Antivirus, Remediation, and Audit, reside on VLAN 200.

Figure 4. Reference Network for CatOS Switch Configuration Section



In NAC framework, all policy related information is configured in Cisco ACS. The following section will cover the base ACS configuration for NAC. Additional specific policy information will be discussed in each assessment method configuration section.

CISCO SECURE ACCESS CONTROL SERVER COMMON CONFIGURATION

The following assumes that Cisco Secure Access Control Server (ACS) has been preinstalled and that no NAC configuration has been performed. This section walks you through the basic configuration of ACS 4.0 for all NAC deployment scenarios.

Note: ACS v4.0 or later software is required for NAC L2 IP and NAC L2 802.1X deployments. This deployment guide assumes the use of the ACS v4.0 Software for Windows and does not cover steps specific to the ACS Solution Engine.

Vendor Attribute-Value Pairs

NAC introduces the ability to authorize network hosts not only based upon user and machine identity or both but also upon a host's posture compliance. The posture compliance process compares the credentials from the host with those defined in a profile policy. The credentials being requested are created from attribute-value pairs (AVPs) defined by Cisco and other vendors who are NAC partners. Because the range of NAC attributes extends across many vendors and applications, ACS does not include any non-Cisco attributes by default. Therefore, you must import a NAC attribute definition file (ADF) from each vendor application that you want to validate in your NAC compliance policies.

Task 1: Import Partner AVPs

To import a NAC attribute definition file, follow these steps below. It is assumed that you have already obtained the ADF from the desired Cisco partner and have copied it to the ACS server. Additional information is in the Cisco Secure ACS 4.0 user guide.

Step 1. Locate the ADF (.adf) file that has been copied to the ACS server.

Step 2. Place the ADF files into the same directory as the ACS utility CSUtil.exe (<ACS Install Dir>\bin\) or a directory accessible by CSUtil.exe.

Step 3. On the host running Cisco Secure ACS, open an MS DOS command prompt, and change directories to the directory containing CSUtil.exe.

Step 4. Add the AVPs to ACS using the command: CSUtil.exe -addAVP filename.adf

Step 5. After successfully adding each AVP you must restart the following ACS services:

- CSAdmin
- CSLog
- CSAuth

Note: You can access services through **Start Menu->Programs->Administrative Tools->Services**.

Network Configuration

Task 2: Network Device Group (Optional)

If you want to group your Network Access Devices (NADs) into Network Device Groups (NDGs) for location or service-based filtering, you must first enable the use of Network Device Groups. Perform the following:

Step 1. Select **Interface Configuration** from the main ACS menu

Step 2. Select **Advanced Options**, and then click the box at the bottom of the page to enable **Network Device Groups**. Otherwise, you might leave them unassigned.

Step 3. Select **Network Configuration** from the main ACS menu, select the **Add Entry**, and provide the Network Device Group Name and Key.

Network Device Group Name	Key
Switches	cisco123

Task 3: AAA Client Configuration

From the **Network Configuration** screen, select the hyperlink under **Network Device Group**. If you did not previously assign a name, you will see *Not Assigned*. This link will take you to the **AAA Client** screen.

Step 1. Configure the AAA Clients by selecting the **Add Entry** button. You can define all NADs as a single AAA client by using IP address wildcards.

Step 2. Click on submit and apply to save the changes.

(Not Assigned) AAA Clients				
AAA Client Hostname	AAA Client IP Address	Key	Network Device Group	Authenticate Using
Any	*.*.*.*	cisco123	(Not Assigned)	RADIUS (Cisco IOS/PIX6.0)

Note: AAA client definitions with wildcards CANNOT overlap with other AAA client definitions, regardless of authentication types.

Task 4: AAA Server Configuration

Note: Your AAA Server is automatically populated during the installation of ACS, using the hostname assigned to the host operating system.

The AAA Server information is populated with the hostname and IP address of the machine that ACS is installed on. For example, notice that the Server Name w2ks and that the IP address 10.0.200.20 are already configured as shown in Step 1 below.

Step 1. Configure the Key as shown below for the AAA server by selecting the AAA Server Name hyperlink [w2ks](#).

(Not Assigned) AAA Servers				
AAA Server Name	AAA Server IP Address	AAA Server Type	Key	Network Device Group
w2ks	10.0.200.20	Cisco Secure ACS	cisco123	(Not Assigned)

Note: You can optionally assign the ACS server to a previously configured Network Device Group.

Interface Configuration

The items configured in the **Interface Configuration** section, such as RADIUS attributes, must be enabled here to be inherited and available in other portions of the ACS configuration.

Task 5: Configure RADIUS Attributes

Select the Interface configuration button from the main menu, select **RADIUS (IETF)**, make the noted selections. Select **RADIUS Cisco IOS/PIX6.0** and make the proper selections.

Step 1. Select the required RADIUS attributes. Only the attributes checked below are necessary for NAC. All other attributes should be *unchecked* to save time in later configuration steps.

RADIUS (IETF)	[027] Session-Timeout
	[029] Termination-Action
	[064] Tunnel-Type
	[065] Tunnel-Medium-Type
	[081] Tunnel-Private-Group-ID
RADIUS (Cisco IOS/PIX6.0)	[026/009/001] cisco-av-pair

Note: Attributes 64, 65, and 81 are only necessary for VLAN assignments.

Step 2. Enable these options under the **Interface Configuration menu > Advanced Options**.

Advanced Options:	Group-Level Shared Network Access Restrictions Group-Level Network Access Restrictions Group-Level Downloadable ACLs Network Access Filtering Distributed System Settings Cisco Secure ACS Database Replication Network Device Groups
-------------------	---

Note: Check Group Downloadable ACLs box here, or downloadable ACLs will not work with NAC L2 IP.

System Configuration

To access the ACS Certificate Setup menu, select **System Configuration** from the main menu, and select the **ACS Certificate Setup link**.

Task 6: ACS Certificate Setup

ACS should be configured with a digital certificate for establishing client trust when challenging the client for its credentials.

Note: We highly recommend that you use a production PKI and certificates signed by the production CA or an RA for the most scalable NAC deployments. We have significantly compressed and abbreviated this part of a NAC implementation. You will need to use an existing PKI (internal or outsourced) to securely identify the ACS infrastructure to endpoint devices (for example CTA). For information on obtaining a certificate from a certificate authority see Appendix 4.

Note: If your deployment is going to use NAC L2 802.1x and integrate with Microsoft Active Directory you must consider which authentication mechanism, if any, that your deployment requires for machine and user authentication.

The example below is shown using pregenerated digital certificates. In the example, the files are on the ACS server in `c:\files\certs\`

Step 1. Select the **ACS Certificate Authority Setup** link. Specify the location of the CA certificate, and click **Submit**.

ACS Certificate Authority Setup	
Add new CA certificate to local certificate storage	
Certificate file:	C:\files\certs\ca.nac.cisco.com.cer

Step 2. Restart ACS after adding the new CA certificate. Go to **System Configuration, Service Control**, and select **Restart**.

Step 3. After installing the CA certificate, you should add it to the Certificate Trust List (CTL) as a trusted authority. To do this, select the **Edit Certificate Trust List**, link from the **ACS Certificate Setup** screen, and locate the name of your CA in the list. Check the box next to it, and click **Submit** to save the changes.

Edit the Certificate Trust List (CTL)
ca

Step 4. Changing the CTL will require an ACS restart so you go to **System Configuration > Service Control** and click on the **Restart** button.

Step 5. Select the **Install Certificate** link. Specify the location of the ACS certificate, and click **Submit**.

Install New Certificate	
Read certificate from file	
Certificate file:	C:\files\certs\ACS-1.nac.cisco.com.cer
Private key file:	C:\files\certs\ACS-1.PrivateKey.txt
Private key password:	cisco123

Step 6. After a successful installation of the ACS certificate, you must restart ACS. To do this, select **System Configuration** from the main menu, select **Service Control**, and click on the **Restart**. This completes the ACS certificate installation process.

Task 7: Global Authentication Setup

ACS supports many different protocols for securely transferring credentials from the host to the ACS for authentication and authorization. You must tell ACS which protocols are allowed and what the default settings will be for each protocol.

Note: Unless you have a limited deployment environment or specific security concerns, we highly recommend that you enable *all* protocols globally. You will have an opportunity to limit the actual protocol options later when you create the Network Access Profiles for NAC. But if they are not enabled here, they will not be available in the Network Access Profiles.

Step 1. Select System Configuration from the main menu, and pick Global Authentication Setup.

Step 2. Select these global authentication parameters to make them available in the Network Access Profile authentication configuration.

EAP Configuration	
PEAP	
Allow EAP-MSCHAPv2	
Allow EAP-GTC	
Allow Posture Validation	
Cisco client initial message:	<empty>
PEAP session timeout (minutes):	120
Enable Fast Reconnect:	Yes
EAP-FAST	
EAP-FAST Configuration (see below)	
EAP-TLS	
Allow EAP-TLS	
Select one or more of the following options:	
Certificate SAN comparison	
Certificate CN comparison	
Certificate Binary comparison	
EAP-TLS Session Timeout (minutes):	120
LEAP	
Allow LEAP (For Aironet only)	
EAP-MD5	
Allow EAP-MD5	
AP EAP request timeout (seconds):	20
MS-CHAP Configuration	
Allow MS-CHAP Version 1 Authentication	
Allow MS-CHAP Version 2 Authentication	

Step 3. Click **Submit + Restart** to save these changes.

Step 4. Click **EAP-FAST Configuration** to enter the EAP-FAST screen.

EAP-FAST Settings	
EAP-FAST	
Allow EAP-FAST	
Active master key TTL:	1 month
Retired master key TTL:	3 month
Tunnel PAC TTL:	1 week
Client Initial Message:	<empty>
Authority ID Info:	cisco

EAP-FAST Settings

Allow anonymous in-band PAC provisioning

Allow authenticated in-band PAC provisioning

- Accept client on authenticated provisioning
- Require client certificate for provisioning

Allow Machine Authentication

Machine PAC TTL **1 week**

Allow Stateless Session Resume

Authorization PAC TTL **1 hour**

Allow inner methods

- EAP-GTC
- EAP-MSCHAPv2
- EAP-TLS

Select one or more of the following EAP-TLS comparison methods:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate binary comparison

EAP-TLS session timeout (minutes): **120**

EAP-FAST master server

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

Task 8: Configuring Attributes for Logging

Note: To log any non-Cisco NAC attribute values from the hosts, first you need to import the attribute definitions must first be imported into ACS and then select them for logging.

Step 1. To configure which log files are enabled and which event attributes are recorded within them, select the **System Configuration** option from the main menu, and select **Logging**.

The recommended log files and their logged attributes for NAC are shown. Your actual list of logged attributes will probably be longer, depending upon which NAC vendor attributes are of interest in your deployment.

CSV Failed Attempts Log to CSV Failed Attempts	CSV Passed Authentications Log to CSV Passed Auths	CSV RADIUS Accounting Log to RADIUS Accounting
Logged Attributes	Logged Attributes	Logged Attributes
Message-Type	Message-Type	User-Name
User-Name	User-Name	Group-Name
Caller-ID	Caller-ID	Calling-Station-Id
Authen-Failure-Code	NAS-Port	Acct-Status-Type
NAS-Port	NAS-IP-Address	Acct-Session-Id
NAS-IP-Address	AAA Server	Acct-Session-Time
AAA Server	Filter Information	Acct-Input-Octets

CSV Failed Attempts	CSV Passed Authentications	CSV RADIUS Accounting
Log to CSV Failed Attempts	Log to CSV Passed Auths	Log to RADIUS Accounting
Network Device Group	Network Device Group	Acct-Output-Octets
Access Device	Access Device	Acct-Input-Packets
PEAP/EAP-FAST-Clear-Name	PEAP/EAP-FAST-Clear-Name	Acct-Output-Packets
Logged Remotely	Logged Remotely	Framed-IP-Address
EAP Type	EAP Type	NAS-Port
EAP Type Name	EAP Type Name	NAS-IP-Address
Network Access Profile Name	Network Access Profile Name	Class
Shared RAC	Outbound Class	Termination-Action
Downloadable ACL	Shared RAC	Called-Station-Id
System-Posture-Assessment	Downloadable ACL	Acct-Delay-Time
Application-Posture-Assessment	System-Posture-Assessment	Acct-Authentic
Reason	Application-Posture-Assessment	Acct-Terminate-Cause
cisco-av-pair	Reason	Event-Timestamp
Cisco:PA:PA-Name	Cisco:PA:PA-Name	NAS-Port-Type
Cisco:PA:PA-Version	Cisco:PA:PA-Version	Port-Limit
Cisco:PA:OS-Type	Cisco:PA:OS-Type	NAS-Port-Id
Cisco:PA:OS-Version	Cisco:PA:OS-Version	AAA Server
Cisco:Host:ServicePacks	Cisco:Host:ServicePacks	ExtDB Info
Cisco:Host:Hotfixes	Cisco:Host:Hotfixes	Network Access Profile Name
Cisco:Host:Package	Cisco:Host:Package	cisco-av-pair
		Access Device
		Logged Remotely

Administration Control

Task 9: Add Remote Administrator Access

To remotely administer your ACS through a web browser, you must enable this feature by selecting the **Administration Control** button from the main menu. By adding one or more accounts, you can log in to your ACS with HTTP.

Step 1. Click the **Add Administrator** button, and add this information in the Administration Control section.

Administrator Name:	Administrator
Password:	cisco123
Administrator Privilege:	Grant All

Shared Profile Components

Shared Profile Components are configurations that can be reused across many different Network Access Profiles for filtering within ACS or for network authorizations within RADIUS. You will need to define them before configuring Network Access Profiles.

Note: Network Access Profiles are new to ACS 4.0. You can create and map individual authentication, posture validation, and authorization components, depending on the access method being used or the IP address of the NAD.

Task 10: Configure Downloadable IP ACLs

The first shared component to configure is Downloadable IP access control lists (ACLs). These are used to enforce the network authorization of a host by dynamically downloading layer three and layer four (L3/L4) access control entries (ACEs) to a router or VPN concentrator and prepend them to the default interface ACL.

The following ACLs are examples. Actual ACL definitions for your organization should carefully researched and tested based on applications being used, services such as VoIP, and security policies. Before being implemented.

Step 1. To configure the following ACLs, go to **Shared Profile Components** in the main menu, and select **Downloadable IP ACLs**. Click the **Add** button to create each new posture ACL. You then need to **Add** new ACEs (access control entry) with the respective ACL definition (for example, healthy_acl) for your network. After you have finished entering all of the appropriate ACEs for the specific posture ACL, click **Submit** to save the ACEs for this ACL. Finally, click **Submit** again to save the posture ACL.

Step 2. You are now ready to create the second posture ACL (quarantine_acl) for your particular policy. This example shows the configuration with IP addresses for our reference network architecture.

Name	NAF	ACL Definition
healthy_acl	(All-AAA-Client)	permit ip any any
quarantine_acl	(All-AAA-Client)	remark Allow DHCP permit udp any eq bootpc any eq bootps remark Allow EAPoUDP permit udp any any eq 21862 remark Allow DNS permit udp any any eq 53 remark Allow HTTP to UpdateServer permit tcp any host 10.0.200.30 eq www remark allow client access to qualys permit ip any host 10.0.200.106

Note: If you do not see the Downloadable IP ACL option, you need to enable Downloadable ACLs in the RADIUS Attributes section.

Task 11: RADIUS Authorization Components

RADIUS Authorization Components (RACs) are sets of RADIUS attributes that are applied to Network Access Devices during network authorizations.

Step 1. To configure RACs, go to **Shared Profile Components** in the main menu and select **RADIUS Authorization Components**, click the **Add** button for each new RAC. Each RAC can contain one or more vendor RADIUS attributes, including Cisco IOS/PIX 6.0, IETF, and Ascend.

Note: The Session-Timeout values used for NAC deployments can have a significant impact on ACS performance. We strongly recommend that you adjust it for the scale of your network and ACS transaction capacity.

Step 2. Create the RAC entries, attribute assignments, and values for NAC L2 IP:

Note: The RAC below are divided to handle deployments with NAC L2 IP and NAC L2 802.1x. You might choose to have different RACs for different types of NAC services or even for different locations.

RAC Name	Vendor	Assigned Attributes	Value
L2_IP_Healthy_RAC	Cisco	cisco-av-pair (1)	status-query-timeout=300
	Cisco	cisco-av-pair (1)	sec:pg=Healthy_hosts
	IETF	Termination-Action (29)	RADIUS-Request (1)
	IETF	Session-Timeout (27)	36000
L2_IP_Transition_RAC	IETF	Session-Timeout (27)	60
	IETF	Termination-Action (29)	RADIUS-Request (1)
L2_IP_Quarantine_RAC	Cisco	cisco-av-pair (1)	status-query-timeout=300
	Cisco	cisco-av-pair (1)	url-redirect-acl=quarantine_url_redir_acl
	Cisco	cisco-av-pair (1)	sec:pg=Quarantine_hosts
	IETF	Session-Timeout (27)	36000
	IETF	Termination-Action (29)	RADIUS-Request (1)

Note: For detailed information on RADIUS attributes, see Appendix 2.

Note: The ACL specified by the url-redirect-acl attribute must be configured on the switch. It is case sensitive and must match exactly. (ACL name shown: **quarantine_url_redir_acl**). If it does not match, the ACL will not function on the switch.

Note: Although the Cisco AVP for the url-redirect string can be entered in the RAC, we recommend you enter this URL value in the NAP > posture validation > Specific Rule > System Posture Token Configuration > URL Redirect field.

Step 3. Create these RAC entries, attribute assignments, and values for NAC L2 802.1x:

RAC Name	Vendor	Assigned Attributes	Value
L2_1x_Healthy_RAC	IETF	Session-Timeout (27)	3600
	IETF	Termination-Action (29)	RADIUS-Request (1)
	IETF	Tunnel-Type (64)	[T1] VLAN (13)
	IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)
	IETF	Tunnel-Private-Group-ID (81)	[T1] healthy
L2_1x_Transition_RAC	IETF	Session-Timeout (27)	30
	IETF	Termination-Action (29)	RADIUS-Request (1)
L2_1x_Quarantine_RAC	IETF	Session-Timeout (27)	3600
	IETF	Termination-Action (29)	RADIUS-Request (1)
	IETF	Tunnel-Type (64)	[T1] VLAN (13)
	IETF	Tunnel-Medium-Type (65)	[T1] 802 (6)
	IETF	Tunnel-Private-Group-ID (81)	[T1] quarantine

Table 3 is only for reference and lists all of the attributes that might be sent from ACS in a RADIUS-Accept response for NAC:

Table 3. RADIUS Attributes.

NAC-L2-802.1x	NAC-L2-IP	NAC-L3-IP	#	Attribute Name	Description
√			1	User-Name	Copied from EAP Identity Response in Access Request.
	√	√	8	Framed-IP-Address	IP address of host.
	√	√	26	Vendor-Specific Cisco (9,1) CiscoSecure-Defined-ACL	ACL name. Automatically sent by ACS.
√			26	Vendor-Specific Cisco (9,1) sec:pg	Policy-based ACL assignment. Only applies to Catalyst 6000. sec:pg = <group-name>
	√	√	26	Vendor-Specific Cisco (9,1) url-redirect	Redirection URL. url-redirect=<URL>
	√	√	26	Vendor-Specific Cisco (9,1) url-redirect-acl	Apply the named ACL for the redirect URL; ACL must be defined locally on the NAD. Only works on switches with IOS. url-redirect-acl=<ACL-Name>
√	√	√	26	Vendor-Specific, Cisco (9,1), posture-token	Posture token/state name. Automatically sent by ACS.
	√	√	26	Vendor-Specific Cisco (9,1) status-query-timeout	Sets Status Query timer.
	√	√	26	Vendor-Specific Cisco (9,1) host-session-id	Session identifier used for auditing. Automatically sent by ACS.
	√	√	26	Vendor-Specific Microsoft = 311	Key for Status Query: MS-MPPE-Recv-Key Automatically sent by ACS.
√	√	√	27	Session-Timeout	Sets Revalidation Timer (in seconds).
√	√	√	29	Termination-Action	Action on Session Timeout (0) Default: Terminate session (1) Radius-Request: Re-authenticate.
√			64	Tunnel-Type	13 = VLAN.
√			65	Tunnel-Medium-Type	6 = 802.
√	√	√	79	EAP Message	EAP Request/Response Packet in Access Request and Access Challenge: <ul style="list-style-type: none"> EAP Success in Access Accept. EAP Failure in Access Reject.
?	?	?	80	Message Authenticator	HMAC-MD5 to ensure integrity of packet.
√			81	Tunnel-Private-Group-ID	VLAN name.

Group and User Setup

Task 12: Group Setup

The following provides an example of using local usernames and groups for authentication. This provides a means for testing user authentication before integrating ACS with Microsoft AD. ACS and Microsoft AD integration for user and group authentication are covered further in another section of this document.

Group and User Setup			
Group Number	Group Name	Local ACS Users	Password
1: Group 1	Employees	Administrator	cisco
1: Group 1	Employees	employee1	cisco
2: Group 2	Contractors	contractor1	cisco
3: Group 3	Guest	guest1	cisco
4: Group 4	Utilities	Utilities1	cisco

Step 1. Click **Group Setup** in the main ACS menu.

Step 2. Click **Rename**. You can rename the first three default groups to any name you choose. For the configuration example shown here you can use the names as shown in the table above under Group Setup from the main menu. You can also rename another group to Utilities for use with application-specific devices (ASDs).

Task 13: User Setup

Step 1. Click **User Setup** in the main ACS menu. In the **User** dialog box, enter the first username as shown: **employee1**, and select the **Add/Edit** button.

Step 2. In the **User: employee1 (New User)** screen under **User Setup**, enter **cisco** as the user's password. In the **Group to which the user is assigned** drop-down box assign the user to the **Employees** group. Scroll to the bottom, and click **Submit**.

Step 3. Repeat these steps for creating the remaining users: **contractor1**, **guest1**, **utilities**.

Note: The individual RADIUS attributes are configured and applied in the Network Access Profile section and do not need to be configured for each individual group.

Posture Validation

Posture Validation is a core component of the NAC configuration. In the Posture validation section, rules are created to validate host posture compliance. Tokens are delivered to the NAD granting or denying network access as a result of this compliance. The resulting tokens could be healthy, checkup, transition, quarantine, infected, and unknown.

ACS can perform posture validation in these ways:

- Locally within ACS
- Externally by using the HCAP protocol to one or more posture validation servers (PVS)
- Externally by using the GAME protocol to an audit server for NAC Agentless Host (NAH) support.

Note: You can perform both local and external posture validation at the same time. However, you cannot perform local and external posture validation for the same NAC credential types (vendor/application combinations). Example: Verifying Trend Micro information locally in ACS and externally in the Trend Policy Server.

Posture validation policies are configured in ACS under **Posture Validation** in the main menu. These policies are later selected and applied to network access profiles. The policies are defined separately so that you can mix and match or reuse them to provide differentiated access for multiple network services across many locations.

Task 14: Internal Posture Validation Setup

Posture validation policies consist of rules, and these rules are built from a set of conditions. Each of these conditions can match a received credential from the client and result in a potential policy assessment.

- Step 1.** To create the policy requirements of the reference network locally on the ACS, the set of NAC posture validation policies should be defined, according to the table below. To create these policies, select **Posture Validation** from the main menu and then select **Internal Posture Validation Setup**.
- Step 2.** Select **Add Policy** to create a new policy.
- Step 3.** Enter a name, and optionally a description, for your new Posture Validation Policy, and then click **Submit**.
- Step 4.** You now enter the specific Posture Validation Rules for your new policy. You build a set of Conditions for the given policy that match to a specific posture assessment result. To create this rule, click **Add Rule**.
- Step 5.** Click **Add Condition Set** to move to the screen where you define the conditions that comprise the posture validation rule.
- Step 6.** Using this table as a reference, add the appropriate Attributes, Operators, and Values for the needed condition, and click **Submit**. For example, to set a condition for validating the CTA version on the client, choose the *Cisco:PA:PA-Version* credential from the Attribute menu, change the Operator to \geq and enter “2.0.0.30” into the Value field and click **Enter**. If you need to evaluate multiple credentials together, continue to add those conditions into the rule.
- Note:** To evaluate these conditions together as a single rule, after selecting **Submit**, choose the modal option *Match ‘OR’ inside Condition and ‘AND’ between Condition Sets*, and click **Submit** again.
- Step 7.** Click **Done** to return the original Posture Validation Rules screen.
- Step 8.** After any and all changes have been made in the Rules, click on **Apply and Restart** at the bottom of the page.

Policy Name	#	Condition	Posture Assessment	Notification String
CTA	1	Cisco:PA:PA-Version \geq 2.0.0.30 AND Cisco:PA:Machine-Posture-State \geq 1	Cisco:PA:Healthy	
	2	Default	Cisco:PA:Quarantine	
Windows	1	(Cisco:PA:OS-Type contains Windows XP AND Cisco:Host:ServicePacks contains 2) OR (Cisco:PA:OS-Type contains Windows 2000 AND Cisco:Host:ServicePacks contains 4)	Cisco:Host:Healthy	
	2	Default	Cisco:Host:Quarantine	
CSA	1	Cisco:HIP:CSAOperationalState = 1 AND Cisco:HIP:CSAVersion \geq 4.5.0.0	Cisco:HIP:Healthy	
	2	Default	Cisco:HIP:Quarantine	

Note: When defining the individual rules, you can fill in the notification string on any rule. Filling in the notification string causes CTA to attempt to launch the default web browser on the client device. For instance, you can automatically launch a browser for a quarantine assessment by entering <http://x.x.x.x/quarantine.html> in the posture assessment notification string of a rule.

Network Access Profiles

The configuration for individual Network Access Profiles is shown in the sections for each access method: NAC L2 IP, NAC L2 802.1x, and NAC Agentless Host (NAH) sections.

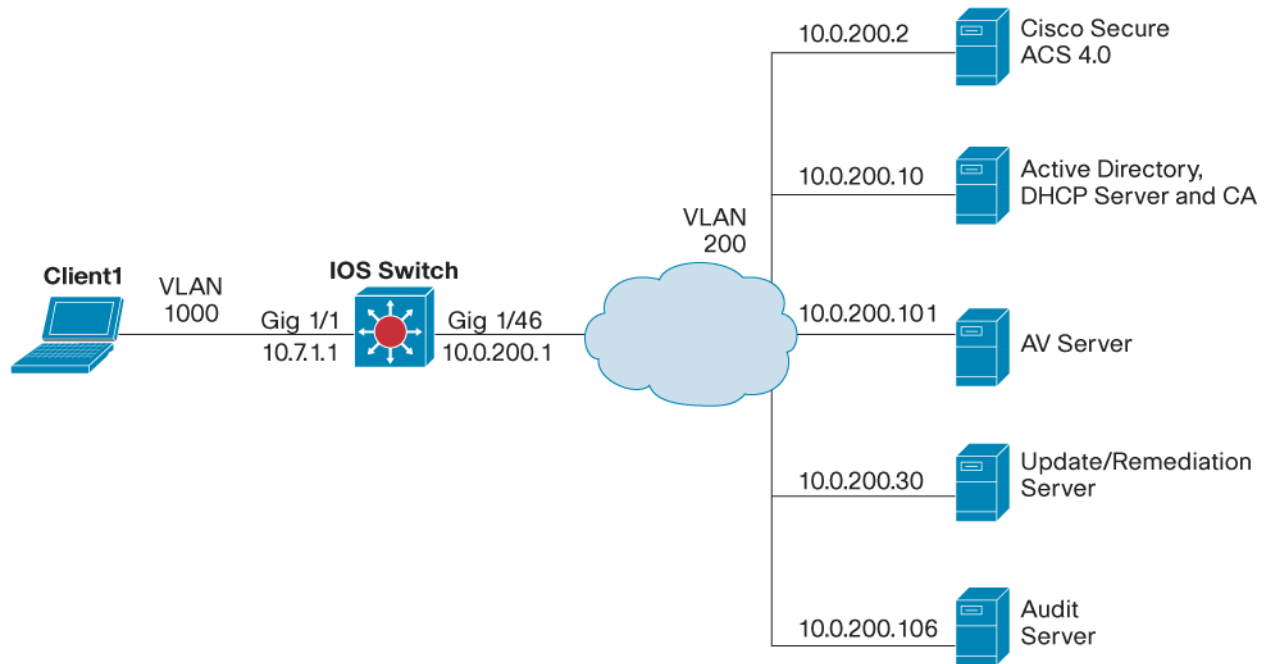
NAC L2 IP CONFIGURATION ON IOS SWITCH

In this section you will configure the various components to enable the base functionality of NAC L2 IP on an IOS switch. This is the basic order of operations for this section:

1. Test network connectivity (between the NAD and ACS server).
2. Configure the IOS switch for NAC L2 IP.
3. Install and configure the Cisco Trust Agent on the client.
4. Configure ACS 4.0 for NAC L2 IP.
5. Test NAC L2 IP functionality.
6. Configure auditing (Qualys, NAD, ACS) support for NAC L2 IP.
7. Test Auditing configuration.
8. Configure NAC L2 IP for agentless host support.
9. Test agentless host support for NAC L2 IP.

Figure 5 serves as a reference point to the NAC L2 IP configuration information discussed in this section.

Figure 5. IOS Switch Reference Diagram.



Test Network Connectivity

Verify that you can ping the ACS server from the switch console and any other necessary servers such as DHCP, DNS, remediation, and AV.

Configure the IOS Switch for NAC L2 IP

Task 1: Configure Authentication Authorization and Accounting

These are the steps required to enable AAA for NAC L2 IP on a Cisco IOS switch for Cisco NAC:

Step 1. Enable AAA on the switch service using the **aaa new-model** global configuration command.

```
IOS-Switch(config)#aaa new-model
```

Step 2. Configure the switch to use RADIUS for EAPoUDP authentication using the **aaa authentication eou default group radius** command.

```
IOS-Switch(config)#aaa authentication eou default group radius
```

Step 3. Configure the switch to run authorization for all network-related service requests using the **aaa authorization network default group radius** command.

```
IOS-Switch(config)#aaa authorization network default group radius
```

Step 4. Enable AAA accounting for EAPoUDP authentication using the **aaa accounting network default start-stop group radius** command.

```
IOS-Switch(config)#aaa accounting network default start-stop group radius
```

Task 2: Configure the RADIUS Server

These are the minimum steps required to configure a RADIUS server on Cisco IOS:

Step 5. Specify the hostname or IP address of the RADIUS server (and optionally the authentication and accounting ports) using the **radius-server host** command. The default RADIUS port number for authentication is 1645. The default RADIUS port number for accounting is 1646.

```
IOS-Switch(config)#radius-server host 10.0.200.20
```


Step 6. Specify the RADIUS server encryption key **using radius-server key**. Note that this key must match the key configured in the Cisco Secure ACS server for this NAD. If they do not match, the NAD and the Cisco Secure ACS will not be able to communicate posture validation information. See the ACS common configuration section: Network Configuration: Task 2: AAA Clients.

```
IOS-Switch(config)#radius-server key cisco123
```

Step 7. Configure the switch to send Framed-IP-Address RADIUS attribute (Attribute[8]) in access-request or accounting-request packets using the **radius-server attribute 8 include-in-access-req** command.

```
IOS-Switch(config)#radius-server attribute 8 include-in-access-req
```

Step 8. Configure the NAD to recognize and use vendor-specific attributes using the **radius-server vsa send authentication** command.

```
IOS-Switch(config)#radius-server vsa send authentication
```

Step 9. Specify the NAD interface for all outgoing RADIUS packets using the **ip radius source-interface** command.

```
IOS-Switch(config)#ip radius source-interface Vlan200
```

Note: Step 9 is optional. However, we recommend if there are multiple paths between the NAD and the Cisco Secure ACS. Assigning a source interface allows the Cisco Secure ACS to know from which NAD the RADIUS messages originated. You must configure this same IP address in the Cisco Secure ACS AAA client record that represents this NAD.

Task 3: Enable IP Device Tracking and DHCP Snooping

When IP device tracking is enabled, and a host is detected, the switch adds an entry to the IP device tracking table that includes this information: IP and MAC address of the host, and the interface on which the switch detected the host. The state of the host is set to ACTIVE when the host is detected.

Step 1. Enable IP device tracking on the switch. You can optionally set the probe count and probe interval.

```
IOS-Switch(config)#ip device tracking
```

Step 2. DHCP Snooping can optionally be used to trigger NAC posture validation.

```
IOS-Switch(config)#ip dhcp snooping
```

Step 3. Enable DHCP snooping on the client VLAN.

```
IOS-Switch(config)#ip dhcp snooping vlan 1000
```

Step 4. Set DHCP snooping to trust the port the DHCP server resides on. In this example this is port Gigabit Ethernet 1/46.

```
IOS-Switch(config-if)#ip dhcp snooping trust
```

Task 4: Configure an Interface ACL

This topic describes the steps required to configure the interface ACL on the NAD.

Create a default ACL for the ingress client traffic. This ACL will be applied to the client ingress switch port in an upcoming section. This is the default security policy on the switch port. Any downloaded ACLs from ACS are prepended with the interface ACL.

Step 1. Configure the interface ACL

```
IOS-Switch(config)#ip access-list extended interface_acl
IOS-Switch(config-ext-nacl)#permit udp any any eq 21862
IOS-Switch(config-ext-nacl)#remark Allow DHCP
IOS-Switch(config-ext-nacl)#permit udp any eq bootpc any eq bootps
IOS-Switch(config-ext-nacl)#remark Allow DNS
IOS-Switch(config-ext-nacl)#permit udp any any eq domain
```

```
IOS-Switch(config-ext-nacl)#remark Allow HTTP access to update server
IOS-Switch(config-ext-nacl)#permit tcp any host 10.0.200.30 eq www
IOS-Switch(config-ext-nacl)#remark Allow ICMP for test purposes
IOS-Switch(config-ext-nacl)#permit icmp any any
IOS-Switch(config-ext-nacl)#remark Implicit Deny
IOS-Switch(config-ext-nacl)#deny ip any any
```

Task 5: Configure a Cisco NAC Global Policy

This topic describes the step required to configure a Cisco NAC global policy on the Cisco IOS switch.

Step 1. Create the IP Admission rule to enable the EAPoUDP posture process

```
IOS-Switch(config)#ip admission name NAC-L2-IP eapoudp
```

Task 6: Configure the Cisco NAC Interface

This topic describes the steps required to configure a Cisco NAC interface on a Cisco IOS switch.

Step 1. Apply the interface ACL you created to ingress traffic on the client switchport.

```
IOS-Switch(config-if)#ip access-group interface_acl in
```

Note: NAC is not configurable on VLANs, only physical switchports.

Step 2. Apply the admission control rule that you created to the client-facing Cisco NAC interface by using the **ip admission** command. Be sure to use the name of the rule you specified in the previous step.

```
IOS-Switch(config-if)#ip admission NAC-L2-IP
```

Note: If the switch interface does not accept the **ip admission name** command, verify that **switchport mode access** is enabled on the interface.

Task 7: Set EAPoUDP Timers

Step 1. Configure the EAPoUDP hold-period timer by using the **eou timeout hold-period** command. The timer specifies the time to wait (in seconds) following a failed credential validation (Accept-Reject) or an EAPoUDP association failure, before a new association can be retried. The default is 180 seconds.

```
IOS-Switch(config)#eou timeout hold-period 180
```

Step 2. Configure the EAPoUDP status query timer using **eou timeout status-query**. After a client credential validation and security posture session is successfully established, the NAD will send a status-query to the client. If the NAD does not receive a successful response from the client, the NAD waits the specified amount of time (in seconds) before sending a new status-query message. This timer is reset each time a successful status-query command and response is received. The default is 300 seconds.

```
IOS-Switch(config)#eou timeout status-query 300
```

Step 3. Configure the EAPoUDP revalidation period timer using **eou timeout revalidation**. Once a credential validation and security posture session is established, the NAD waits the specified amount of time (in seconds) before revalidating the client credentials. This is to verify if any changes in the Cisco NAC client admission policy have occurred. The default is 36000 seconds (10 hours).

```
IOS-Switch(config)#eou timeout revalidation 36000
```

Note: The status query and revalidation timeouts can be configured in Cisco Secure ACS and sent to the NAD for specific posture tokens. In this case, the Cisco Secure ACS timers take precedence over the switch global EAPoUDP timers discussed here.

Task 8: Enable EAPoUDP Logging

This topic explains how to enable EAPoUDP logging on the NAD.

Step 4. Enable EAPoUDP logging by using the **eu logging** command.

```
IOS-Switch(config)#eu logging
```

Task 9: Enable the HTTP Server on the Switch

This topic explains how to enable the HTTP Server on the NAD.

Step 5. Enable the HTTP Server with the **ip http server global** configuration command.

```
IOS-Switch(config)#ip http server
```

Cisco Trust Agent (CTA) Installation and Configuration

CTA is a requirement for performing posture validation of the client. Detailed information on installing, configuring, and administering CTA can be found in the Cisco Trust Agent Administrator Guide 2.0 located at:

http://www.cisco.com/en/US/products/ps5923/prod_maintenance_guides_list.html

The Cisco Trust Agent is installed by using one of the ctasetup.exe files.

Note: The CTA Admin Guide provides detailed information regarding CTA files and installation.

Cisco Trust Agent Windows.exe Versions

CTA for Windows provide several options for deploying and packaging CTA. Administrators can deploy the scripting interface, the supplicant, or both for Windows as noisy or silent installs.

The available packages for Windows are shown:

Windows

CTA.exe Files	Description
ctasetup-win-[version].exe	If you use this package, the install is noisy. This means that the end user will be prompted to accept a license agreement, choose the installation destination folder, and other general installation options. This package only installs the CTA scripting interface. The supplicant is not installed with this package.
ctasetup-supPLICANT-win-[version].exe	If you use this package, the install is interactive. This means that the end user will be prompted to accept a license agreement, choose the install destination folder, and other general installation options. This package can install both the CTA scripting interface and the supplicant. The end user is prompted to select which CTA features they want to install.
CtaAdminEx-win-[version].exe	If you use this package, you are choosing to create a silent installation package for the end user. You extract a file named ctasilent-win-[version].exe from this package. As the administrator, you accept the license agreement for end-users and then deploy the ctasilent-win-[version].exe file as a completely silent installation that does not prompt the end user for any options. The supplicant is not installed with this package.
CtaAdminEx-supPLICANT-win-[version].exe	If you use this package, you are choosing to create a silent installation package for the end user. You extract a file named ctasilent-supPLICANT-win-[version].exe from this package. As the administrator, you accept the license agreement for end-users and then deploy the ctasilent-supPLICANT-win-[version].exe file as a completely silent install that does not prompt the end user for any options. The supplicant is installed with this package.

Note: The supplicant is required for clients to connect to and access a network that is protected by the IEEE 802.1x security protocol. Only after successful client-server authentication does the port access control on the 802.1x-enabled access device (the Ethernet switch) allow the end-user to connect to the network.

Task 1: Client Certificate for CTA Install

CTA must install the certificate that you have installed on ACS to properly authenticate. There are two methods available to add the certificate to CTA on the client. The first method shown, should be done before the CTA installation. You can use the other method (described later) to add the certificate to the root store after CTA is installed.

Step 1. Create a folder called *certs* on the client1, and place it in the same directory as the CTA.exe file.

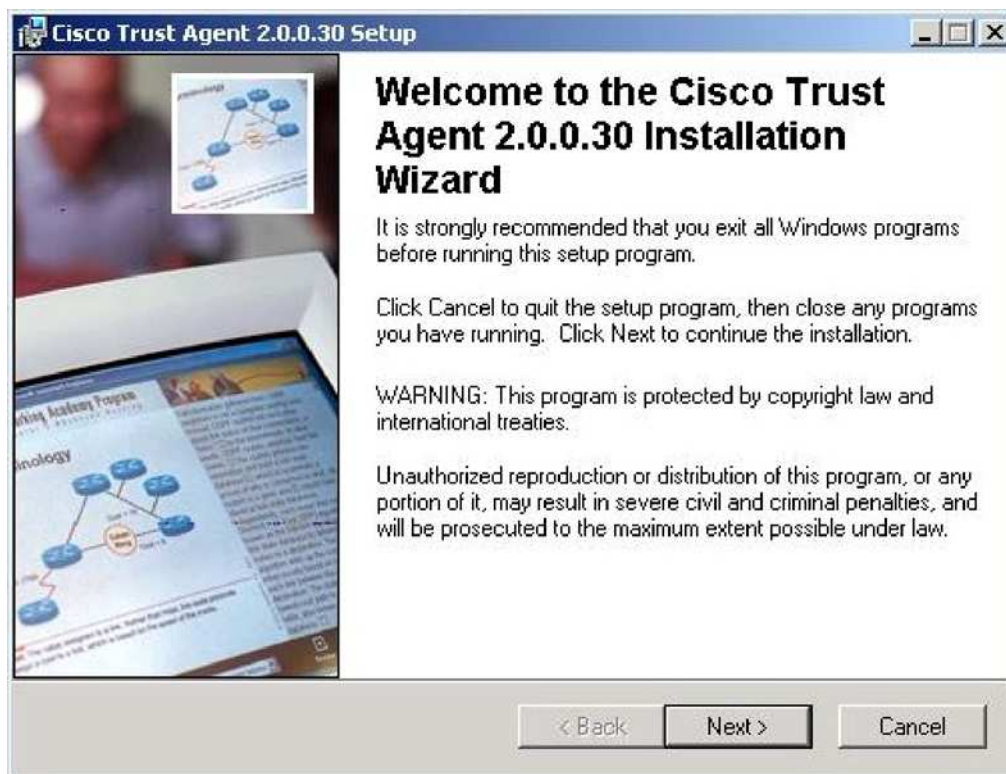
Step 2. The *certs* folder contains the CA certificate that must be used by CTA to authenticate the client to ACS.

Note: CTA will import any public certificate located in the “*certs*” subdirectory. This folder must be located in the same directory as the cta.exe file.

Task 2: Install CTA 2.0

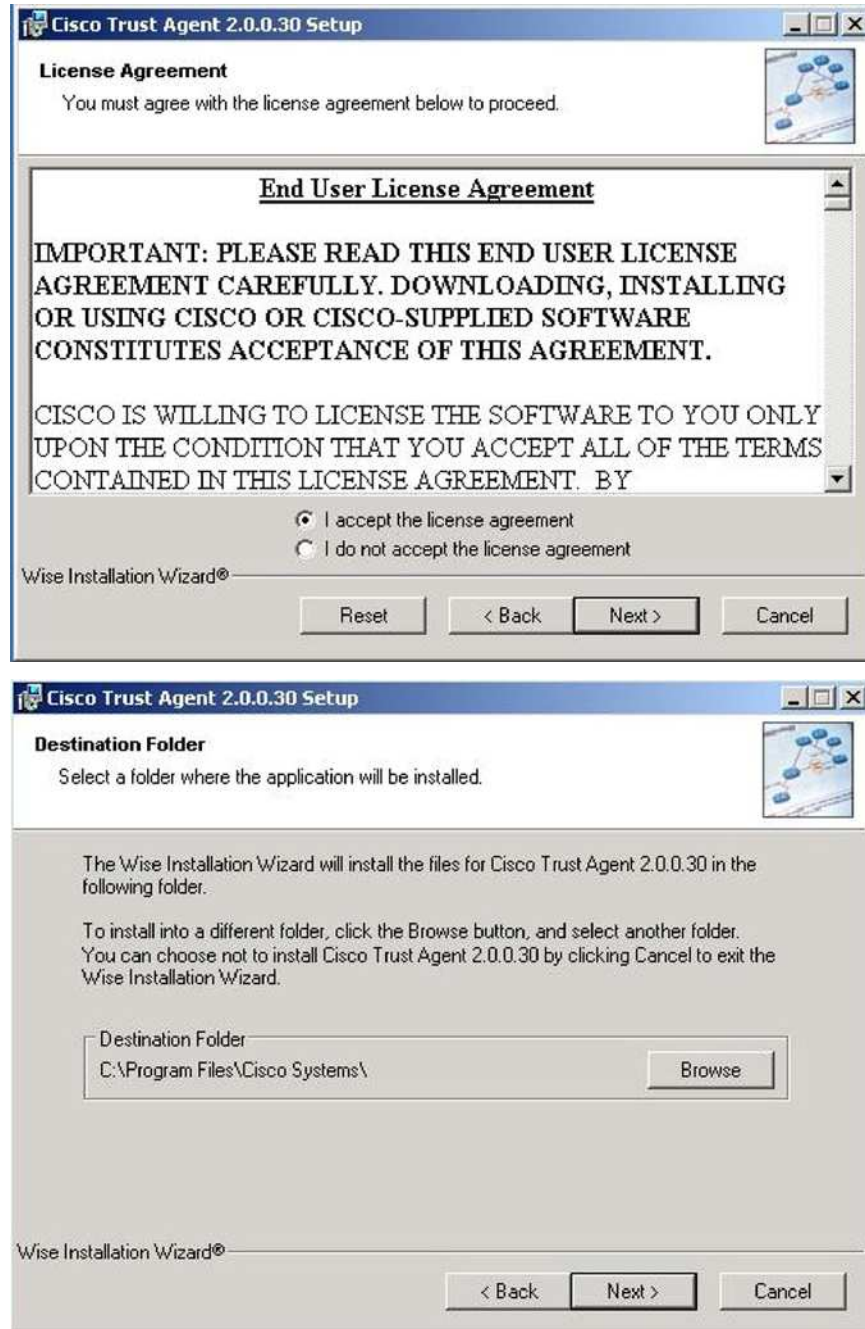
Step 1. Download or copy the CTA setup file to the client. Open the folder containing the CTA.exe file on the client, and double-click the appropriate ctasetup file. (In this example, we use **ctasetup-win-[version].exe**.)

The Cisco Trust Agent **Installation Wizard** appears.



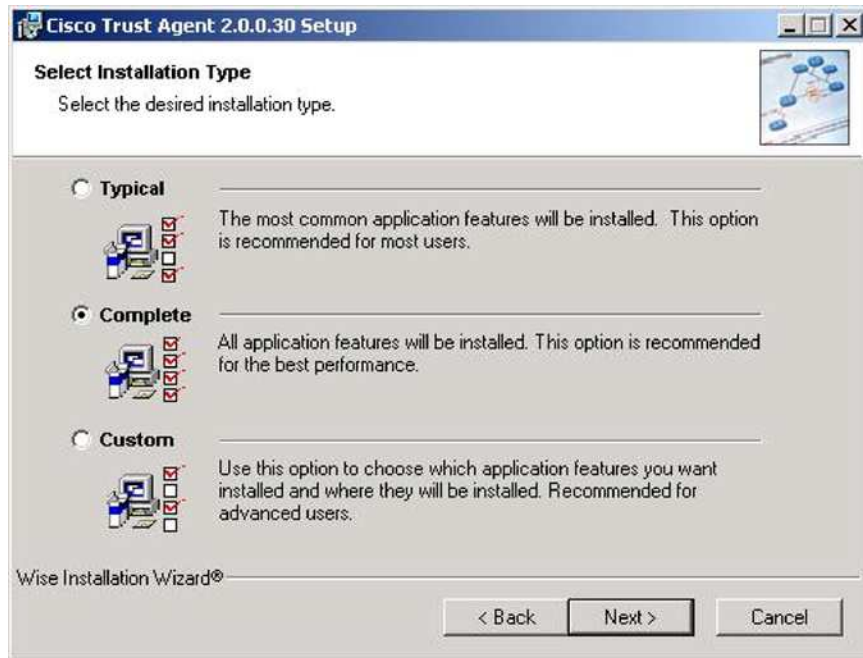
Step 2. Click **Next**.

Step 3. Accept the license agreement by clicking **Next**, and the Destination Folder window appears.



Step 4. Accept the default Destination Folder location, and click **Next**.

Step 5. The Select Installation Type dialog box appears.



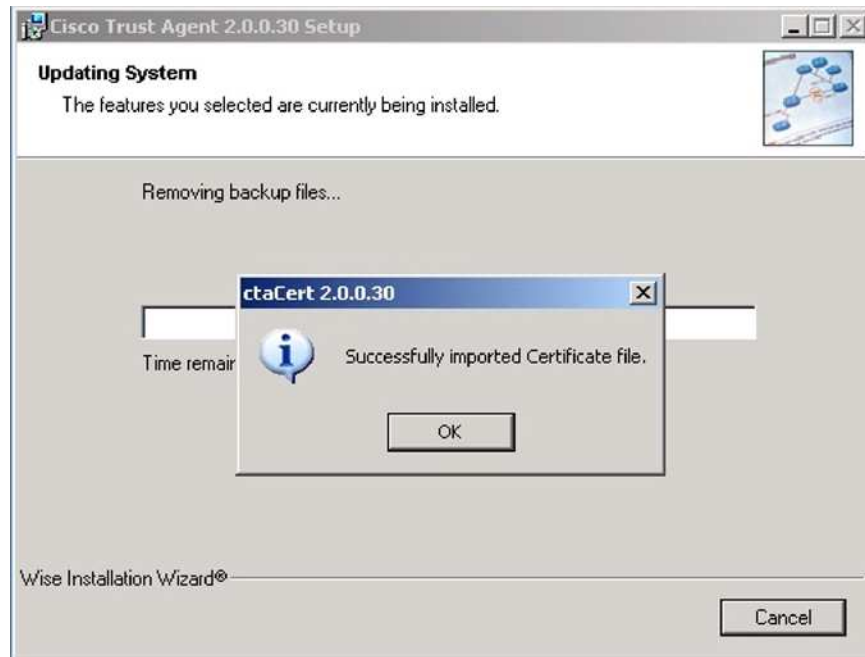
Step 6. Click the **Complete** radio button.

Step 7. Select your features, and then click **Next**.

Step 8. Click **Next**.

Step 9. The application installs into the selected directory.

Step 10. The following message appears when the certificate is successfully imported during the installation. Click **OK**.



Step 11. When the installation is completed, the installer displays the **Installation Completed** window.



Step 12. Click **Finish** to close the installation application.

Task 3: (Optional) Manual install of root certificate for CTA

If you did not copy the *certs* folder into the CTA folder in [Task 1: Step 1](#), you need to install the root certificate before using Cisco Trust Agent.

You can manually install the certificate by using the following steps

Step 13. Copy the certificate to the network client.

Step 14. Open a command prompt on the network client.

Step 15. Change directories to where the Cisco Trust Agent is installed. By default, the location is
C:\Program Files\Cisco Systems\CiscoTrustAgent\.

Step 16. Enter `ctaCert.exe /add "cert_path_&cert_name" /store "Root"`, where `cert_path_&cert_name` is the full path and file name to the certificate.

The certificate is added to the trusted certificate store on the network client.

Network Access Profile Configuration for NAC L2 IP

In this section, you will be instructed on how to configure a Network Access Profile (authentication, posture validation, and authorization) to support NAC L2 IP. In ACS 4.0, there are two methods of configuring Network Access Profiles.

- Add an empty profile, and configure all the necessary information.
- Using the Template Profiles, customize the Network Access Profile desired with the base information included in the template.

There are seven Network Access Profile templates predefined in ACS 4.0:

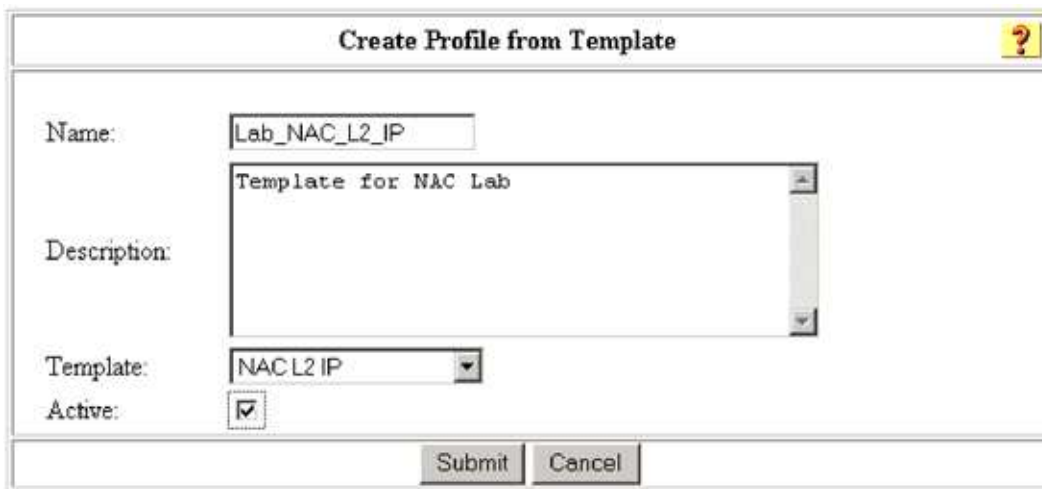
- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x
- Microsoft IEEE 802.1x
- Wireless (NAC L2 802.1x)
- Authentication Bypass (802.1x fallback)
- Agentless Host

In this section of the configuration guide we use the NAC L2 IP Network Access Profile template to create a base profile and then make the necessary changes to customize this template.

Task 1: Create the NAC L2 IP Profile from the Template.

Step 1. Go to **Network Access Profiles** main menu and select **Add Template Profile**

Step 2. Create a template for NAC L2 IP by selecting it from the Template drop down box. Name the template with something similar to the one shown below. Check **Active** to enable the profile.



Step 3. Click **Submit**.

Task 2: Authentication Configuration

Step 1. Select the **Authentication** link for the new Network Access Profile you have just created:

	Lab NAC L2 IP	Authentication Posture Validation Authorization	Template for NAC Lab	YES
--	-------------------------------	--	----------------------	-----

Step 2. Notice that **Allow Posture Validation** is already selected as part of the base template

PEAP

- ☐ Allow EAP-GTC
- ☐ Allow EAP-MSCHAPv2
- ☒ Allow Posture Validation

Step 3. Click **Submit**.

Task 3: Posture Compliance Configuration

The posture validation configuration below is for reference.

Step 1. Select the **Posture Validation** link from the Network Access Profile screen for the profile that you created.

Step 2. Select the **Add Rule** button on the Posture Validation Rules screen.

Step 3. Add the following information for the new posture validation rule.

Name: Lab_NAC_L2_IP			
Required Condition Types	Cisco:PA Cisco:Host		
Posture Validation Policies	CTA Windows		
Assessment Result Configuration	Result	Message	URL Redirect
	Healthy	NAC-L2-IP: Healthy	
	Checkup	NAC-L2-IP: Checkup	
	Transition	NAC-L2-IP: Transition	
	Quarantine	NAC-L2-IP: You have been Quarantined. Please click on the link below and follow the procedures to update your system: http://update.nac.cisco.com/quarantine.htm	http://update.nac.cisco.com/quarantine.htm !
	Infected	NAC-L2-IP: Infected	http://update.nac.cisco.com/quarantine.htm !
	Unknown	NAC-L2-IP: Unknown	http://update.nac.cisco.com/quarantine.htm !
Audit Selection			
Audit Server	None		

Step 4. Click **Submit**.

Step 5. Move the Lab_NAC_L2_IP rule to the top of the list by selecting the radio buttons on the left and using the **Up/Down** buttons.

Posture Validation for Lab_NAC_L2_IP		
Rule Name	Condition	Action
	Required Credential Types	Associate With
• Lab_NAC_L2_IP	Cisco:PA Cisco:Host	Windows, CTA (Internal)
• NAC-SAMPLE-POSTURE-RULE	Cisco:PA	NAC-SAMPLE-CTA-POLICY, (Internal)

Add Rule
Up
Down

The Up/Down buttons submit and save the sort order to the database

Determine Posture Validation for NAH:

No Audit Server was selected

Select

Done

Step 6. Click **Done**.

Step 7. Click **Apply and Restart** on the Network Access Profiles screen.

Task 4: Authorization

Step 1. Select the **Authorization** link from the template.

Step 2. Enable authorization.

User Group	Assessment Result	Deny Access	Shared RAC	Downloadable ACL
Any	Healthy	No	L2_IP_Healthy_RAC	healthy_ACL
Any	Checkup	No	L2_IP_Healthy_RAC	healthy_ACL
Any	Transition	No	L2_IP_Quarantine_RAC	quarantine_ACL
Any	Quarantine	No	L2_IP_Quarantine_RAC	quarantine_ACL
Any	Infected	No	L2_IP_Quarantine_RAC	quarantine_ACL
Any	Unknown	No	L2_IP_Quarantine_RAC	quarantine_ACL
If a condition is not defined or there is no matched condition:		No	L2_IP_Quarantine_RAC	quarantine_ACL
Include RADIUS attributes from user's group:				No
Include RADIUS attributes from user record:				No

Step 3. Click **Submit**.

Task 5: Test the NAC L2 IP Configuration

This section helps you to verify that NAC L2 IP is configured properly, that you are being passed the correct posture token from ACS, and the correct downloadable ACLs from ACS are being applied on the NAD.

Note: You do not apply URL redirection in this task. This is done later as a separate task.

To be considered healthy and to be placed in the healthy role, the client must correctly pass back the required credential information to the NAD and then to ACS. The posture validation requirements for each credential created in the previous Network Access Profile section must be met for the client to be passed an application posture token of *healthy*. The credentials include: **Cisco Trust Agent**, the agent version is **>=2.0.0.30**, and the OS-Type contains **Windows XP**.

Note: It is important to remember that the client will only pass to ACS the credentials ACS is specifically requesting.

Step 1. First, re-enable the switchport to which the client (GigabitEthernet 1/1) is connected by entering the **no shut** command.

Step 2. On the NAD, you will see the following output on the console:

```
04:01:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigEthernet1/1, changed state to up
1d19h: %EOU-6-SESSION: IP=10.7.1.2| HOST=DETECTED| Interface=GigabitEthernet1/1
1d19h: %EOU-6-SESSION: IP=10.7.1.3| HOST=DETECTED| Interface=GigabitEthernet1/1
1d19h: %EOU-6-CTA: IP=10.7.1.3| CiscoTrustAgent=DETECTED
1d19h: %EOU-6-POLICY: IP=10.7.1.3| HOSTNAME=
1d19h: %EOU-6-POSTURE: IP=10.7.1.3| HOST=AUTHORIZED| Interface=GigabitEthernet1/1
1d19h: %EOU-6-AUTHTYPE: IP=10.7.1.3| AuthType=EAP
1d19h: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=NOT DETECTED
1d19h: %EOU-6-POLICY: IP=10.7.1.3| HOSTNAME=
1d19h: %EOU-6-POSTURE: IP=10.7.1.3| HOST=AUTHORIZED| Interface=GigabitEthernet1/1
1d19h: %EOU-6-AUTHTYPE: IP=10.7.1.3| AuthType=EAP
1d19h: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=NOT DETECTED
```

Step 3. Notice that from the output the Cisco Trust Agent was detected, the token assigned to the client is *Healthy*, and the downloadable *Healthy_ACL* created in ACS has been applied to the NAD.

Step 4. Enter the **show eou all** command to verify the client's current status.

```
NAC4948#show eou all
```

```
-----
Address          Interface          AuthType    Posture-Token Age(min)
-----
10.7.1.2         GigEthernet1/1     EAP         Healthy       12
```

Step 5. Verify that the *Healthy_ACL* had been downloaded and applied to the switchport.

```
NAC4948#show ip access-lists
Extended IP access interface_acl
 10 permit udp any any eq 21862
 20 permit udp any host 10.0.200.10 eq domain
 30 permit udp any eq bootpc any eq bootps
 40 permit icmp any any
```

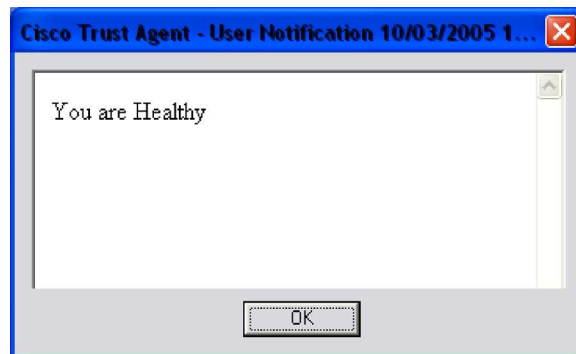
```
Extended IP access list xACSACLx-IP-Healthy_ACL-433866ab
```

```
10 permit ip any any
```

Step 6. Make sure that the downloadable ACL has been applied to the switchport. You should see the client IP address replace the source *any* in the Healthy ACL.

```
NAC4948#show ip access-list interface GigE 1/1
IP Admission access control entires (Inbound)
permit ip host 10.7.1.2 any
```

Step 7. On the client, you will see the CTA pop-up a message:



Step 8. On ACS, verify the client information in the appropriate report. For example, it appears that we have correctly established communications between the client and ACS, the most appropriate report to check is **passed authentications**.

Task 6: Troubleshooting NAC L2 IP

This information provides an important summary view and will help you in troubleshooting efforts. Suppose the client is not given a token of *Healthy* and is given a *Quarantine* token instead. What are some of the ways to troubleshoot this?

Step 1. Force the client into a Quarantine role. Perform this by configuring a posture validation rule in ACS that you know the client will fail. Change the minimum version of the trust agent being requested for a healthy posture status. Because we are running CTA version 2.0.0.30 the client should fail this rule.

Policy Name	#	Condition	Posture Assessment	Notification String
CTA	1	Cisco:PA:PA-Name contains Cisco Trust Agent Cisco:PA:PA-Version >= 3.0.0.0	Cisco:PA:Healthy	
	2	Default	Cisco:PA:Quarantine	

Step 2. Enter the **clear eou all** command to restart the validation process.

```
NAC4948#clear eou all
04:53:29: %EOU-6-SESSION: IP=10.7.1.2| HOST=REMOVED| Interface=GigEthernet1/1
04:53:34: %EOU-6-SESSION: IP=10.7.1.2| HOST=DETECTED| Interface=GigEthernet1/1
04:53:34: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=DETECTED
04:53:34: %EOU-6-POLICY: IP=10.7.1.2| ACLNAME=#ACSACL#-IP-Quarantine-43408f9d
04:53:34: %EOU-6-POLICY: IP=10.7.1.2| TOKEN=Quarantine
04:53:34: %EOU-6-POLICY: IP=10.7.1.2| HOSTNAME=DMA-WXP01:dma
04:53:34: %EOU-6-POSTURE: IP=10.7.1.2| HOST=AUTHORIZED| Interface=GigEthernet1/1
04:53:34: %EOU-6-AUTHTYPE: IP=10.7.1.2| AuthType=EAP
```

Step 3. Notice the client has now been assigned the quarantine token and the quarantine ACL has been downloaded to the NAD.

```
NAC4948#show eou all
```

```
-----  
Address           Interface           AuthType    Posture-Token  Age(min)  
-----  
10.7.1.2          GigEthernet1/1      EAP         Quarantine     2
```

```
NAC4948#show access-lists
```

```
Extended IP access list interface_acl
```

```
10 permit udp any any eq 21862  
20 permit udp any host 10.0.200.10 eq domain  
30 permit udp any eq bootpc any eq bootps  
40 permit icmp any any
```

```
Extended IP access list quarantine_url_redir_acl
```

```
10 deny tcp any host 10.0.200.30 eq www  
30 permit tcp any any eq www
```

```
Extended IP access list xACSACLx-IP-Quarantine-43408f9d
```

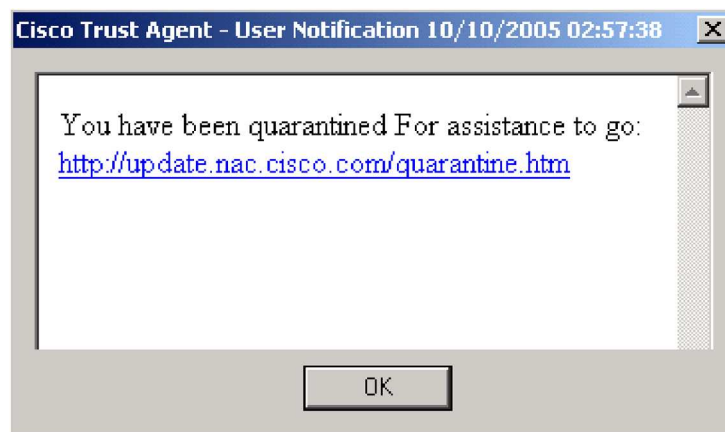
```
10 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps  
20 permit udp any any eq 21862  
30 permit udp any any eq domain  
40 permit ip any 10.0.200.0 0.0.0.255
```

```
NAC4948#show access-lists dynamic interface GigE 1/1
```

```
IP Admission access control entires (Inbound)
```

```
permit udp host 10.7.1.2 eq bootpc host 255.255.255.255 eq bootps  
permit udp host 10.7.1.2 any eq 21862  
permit ip host 10.7.1.2 10.0.200.0 0.0.0.255
```

Step 4. On the client, CTA should provide a pop-up message similar to the following:



Step 5. See the ACS reports to gather information on why the client was quarantined.

URL Redirection

This section discusses using URL redirection to provide hosts with remediation access to needed updates or software to become compliant with security policies.

In the base ACS configuration section, the URL ACL information was defined in the Quarantine RADIUS Authorization Component configuration.

Reference: [Task 11 RADIUS Authorization Components \(RACs\)](#) (url-redirect-acl=quarantine_url_redir_acl). The URL for the update server was defined in the Posture Validation section of the Network Access Profile configuration: [Task 3: Posture Compliance Configuration](#).

Task 1: Configure URL Redirection on the Switch

The URL redirect ACL needs to be configured on the switch. Remember that the name of the ACL defined in ACS must match the name of the ACL configured on the switch.

Step 1. Configure the URL redirect ACL on the switch.

```
IOS-Switch(config)#ip access-list extended quarantine_url_redir_acl
deny tcp any host 10.0.200.30 eq www
permit tcp any any eq www
```

Step 2. Force the client into a quarantine role to test URL redirection.

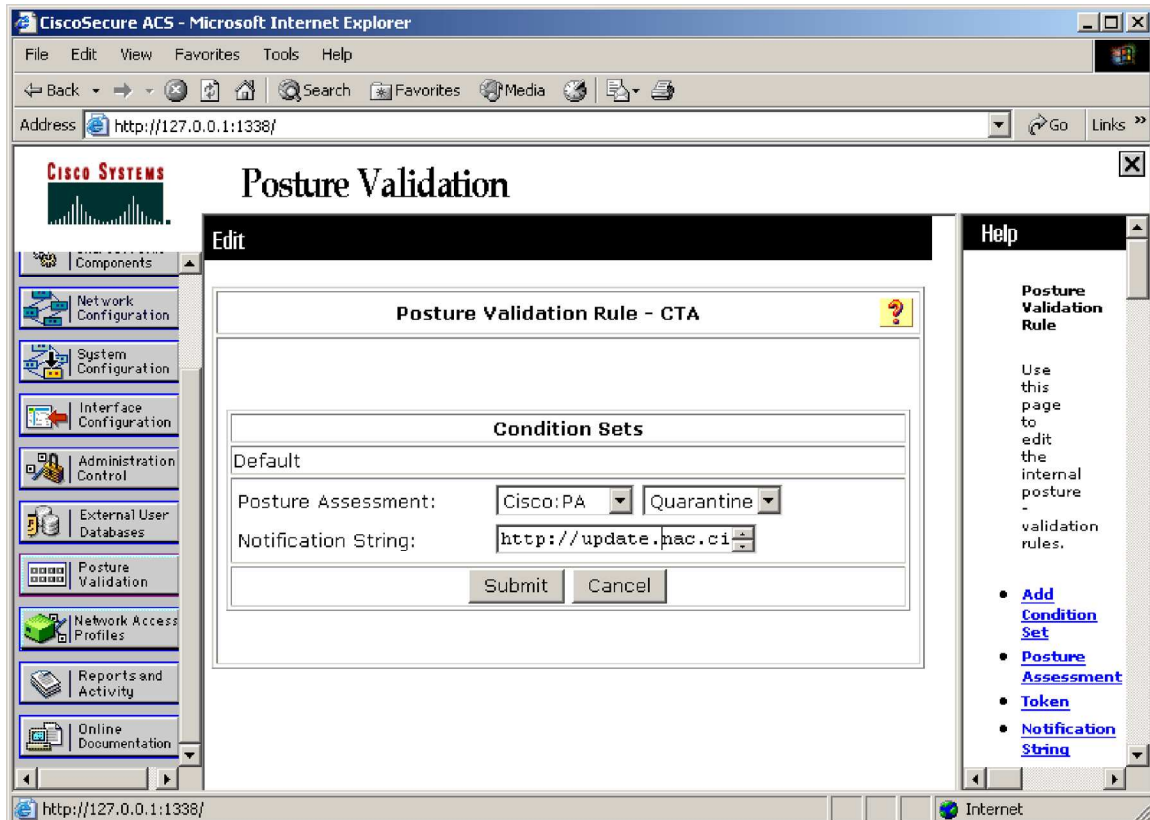
Note: The URL redirection ACL specifies that any traffic destined to the update server will not be redirected and that traffic to any other destination will be redirected.

Automated Browser Launch

CTA 2.0 has the capability to automatically open the default web browser to a on a client machine when CTA receives a URL that has been predefined in ACS. You can set the URL when defining individual posture validation rules in the notification string field. Filling in the notification string causes CTA to attempt to launch the default web browser to the URL on the client device. For example, you can automatically launch a browser for a quarantine assessment by entering <http://x.x.x.x/quarantine.html> in the posture assessment notification string of the quarantine rule.

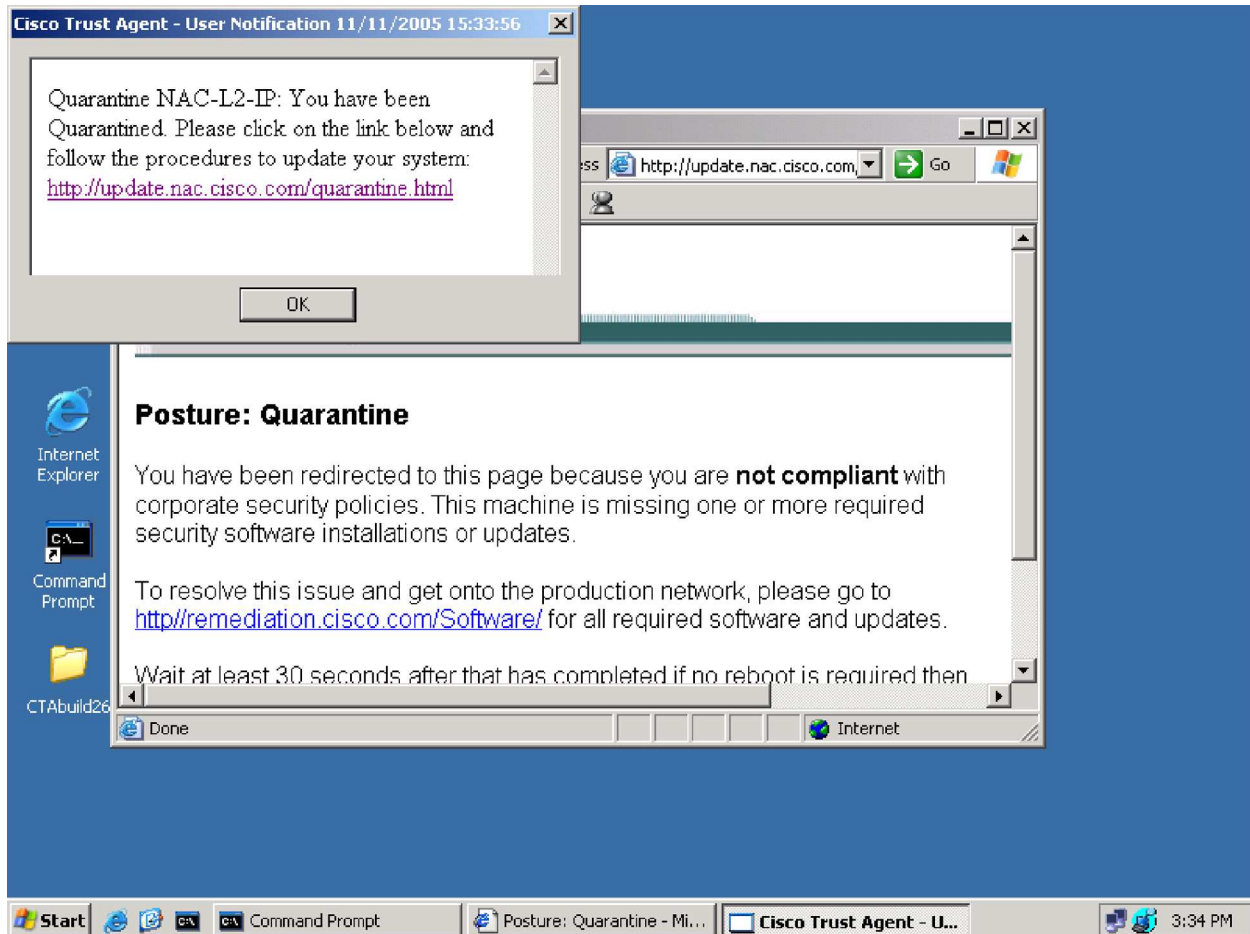
Task 1: Enter the Desired URL in the Notification String

Step 1. In the notification string, enter the URL you want the browser to open on the client. To get to the notification string page, first, Click on **Posture Validation** from the ACS menu, click the **Internal Posture Validation Setup** link, and select the posture validation rule you would like to use. In this example we are using the CTA posture validation rule's default quarantine setting. As an example, when the client does not have CTA version 3.0.0.0 or greater installed, the client will fail validation and be placed in a quarantine role. When this occurs, CTA will receive the notification string for the remediation URL <http://update.nac.cisco.com/quarantine.html> and will forward the client to this site.



Task 2: View the Automated Browser Launch on the Client

Step 2. Connect the client to the switch port. Because the client is not running CTA version 3.0.0.0, it will be placed in a quarantine role. You will see the client's default browser open and attempt to connect to the URL specified in the notification string.



NAC Agentless Hosts

There are several methods in NAC to allow hosts network access that are incapable of performing authentication due to the lack of a posture agent such as printers, scanners, and hosts with unsupported operating systems.

The methods available include:

- Static Exceptions defined on the switch
 - MAC
 - IP
- ACS
 - NAP Advanced Filtering
 - Network Access Restrictions (NARs)
- Audit Server

Task 1: Static NAH Configuration in IOS

You can configure static exceptions in IOS to allow hosts access based on an IP or a MAC address.

The following steps will walk you through configuring a static exception.

Step 3. Create an authorization statement under the identity profile configuration to allow a client based on the IP address.

```
#exception based method, DEVICE-TYPE (CDP IP PHONE), MAC or IP
identity profile eapoudp
! static NAC bypass by IP address
device authorize ip-address 10.7.1.x policy NAH_Profile
! static NAC bypass by MAC address
device authorize mac-address 000c2986cfbf policy NAH_Profile
```

Step 4. Create an authorization statement under the identity profile configuration to allow a client based on the MAC address. For this example, we are using 000c.2999.fa96, which represents the client's MAC addresses.

Note: This is an example MAC address only

```
! statically permit this MAC to bypass NAC instead of ACS
device authorize mac-address 000c.2999.fa96
```

Step 5. You can also configure a profile that allows URL redirection to agentless hosts. Create an identity profile for agentless hosts and the redirect URL to allow access to the update server.

```
! Statically permit access to NAHs
ip access-list extended NAH_ACL
permit ip any any

identity policy NAH_Profile
access-group NAH_ACL
! Optional URL redirection
redirect url http://update.nac.cisco.com/quarantine.htm\_match
quarantine_url_redir_acl
```

Step 6. Clear the EoU table to re-authenticate the statically authorized client.

```
clear eou all
```

Step 7. After your client is statically authorized by the NAD, view the EoU table to see how the static authorization is different from the ACS authorization.

```
IOS-Switch(config)#show eou all
```

```
-----
Address          Interface          AuthType  Posture-Token  Age(min)
-----
10.7.1.2         GigEthernet1/1     STATIC    -----      12
```

Step 8. This was an example of creating static exceptions on the NAD. The next section shows how to create centralized static exceptions in ACS. For the ACS exception to function you must disable this static NAH authorization on the NAD that you created above by entering **no device authorize ip-address** and **no device authorize mac-address** commands.

Task 2: Centralized NAH with ACS

For this section, in order to simulate a NAC agentless host (NAH) ACS exception, we will stop the agent EoU process rather than uninstalling CTA on the client, which you might want to use later. We will then configure ACS for an exception.

Note: This method is used for centralized MAC-based exceptions when not using Audit/GAME.

Note: Remove any configuration on the NAD from Task 1 above before starting this task.

Step 1. On the Client#1, right-click the desktop icon for the computer, and select **Manage**.

Step 2. From the **Computer Management** window, select **Services and Applications**, and then **Services**. Find the service named **Cisco Trust Agent EOU Daemon**, right-click on the entry, and select **stop**.

Step 3. On the client note the MAC address of the interface. You can view this information by entering **ipconfig /all** in a command window.

Step 4. Change the ACS administration console, select **Network Access Profiles**, and click **Add Template Profile**. Use the values shown (substitute the correct MAC address.):



Create Profile from Template

Name: NAC-EOU

Description: This is the profile for EoU MAC exceptions.

Template: Agentless Host

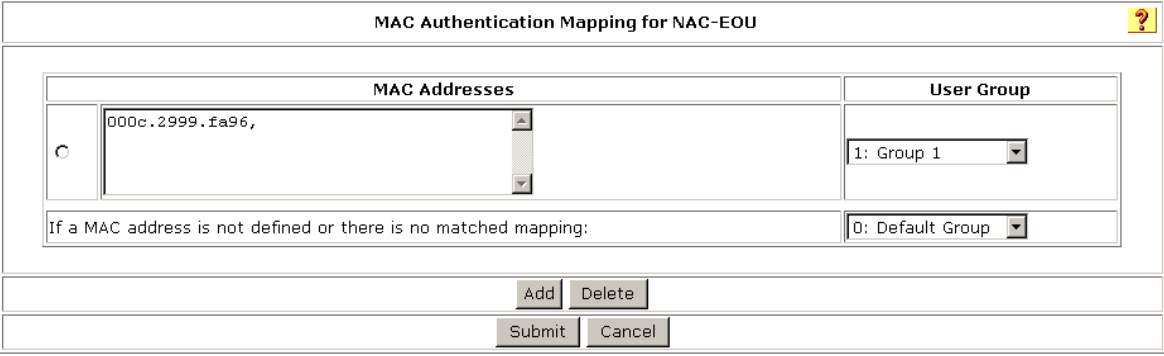
Active: ☒

Submit Cancel

Step 5. Click the **Authentication** link in the Network Access Profile NAC-EOU. On the list of **Authentication Profiles**, select **Allow MAC-Authentication-Bypass**, and click **Submit**.

Step 6. Once again, click the **Authentication** link in the Network Access Profile NAC-EOU, and select **MAC Authentication Bypass Configuration** link.

Step 7. Configure the MAC exception for your client as show here; take care to enter **xxxx.xxxx.xxxx** and not **XX-XX-XX-XX-XX-XX** as formatted in Windows. Note that **Group 1** is used for *authorized* agentless hosts, and that the **Default Group** is used for *unauthorized* devices.

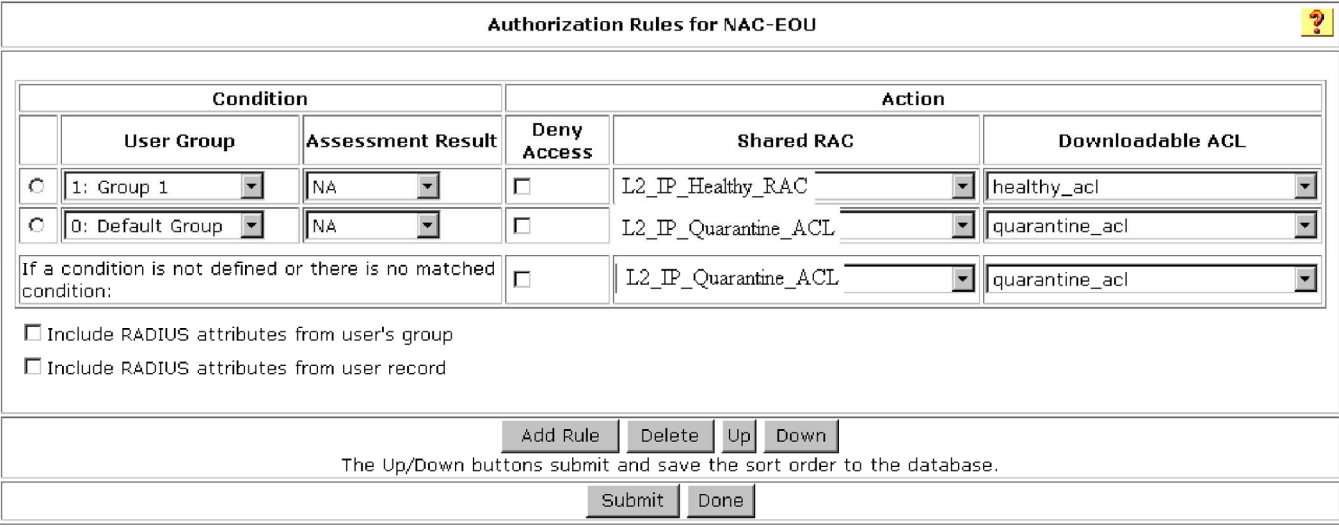


The screenshot shows the 'MAC Authentication Mapping for NAC-EOU' window. It contains a table with two columns: 'MAC Addresses' and 'User Group'. The first row has a radio button, a text field containing '000c.2999.fa96,', and a dropdown menu set to '1: Group 1'. Below the table is a row for 'If a MAC address is not defined or there is no matched mapping:' with a dropdown set to '0: Default Group'. At the bottom are buttons for 'Add', 'Delete', 'Submit', and 'Cancel'.

MAC Addresses		User Group
<input type="radio"/>	000c.2999.fa96,	1: Group 1
If a MAC address is not defined or there is no matched mapping:		0: Default Group

Buttons: Add, Delete, Submit, Cancel

Step 8. Click on the **Authorization** link in the NAC-EOU Network Access Profile, and configure the policy as described here.



The screenshot shows the 'Authorization Rules for NAC-EOU' window. It features a table with columns for 'Condition' (User Group, Assessment Result) and 'Action' (Deny Access, Shared RAC, Downloadable ACL). There are three rows, each with a radio button. The first row is for '1: Group 1' with 'NA' assessment, 'L2_IP_Healthy_RAC' shared RAC, and 'healthy_acl' downloadable ACL. The second row is for '0: Default Group' with 'NA' assessment, 'L2_IP_Quarantine_ACL' shared RAC, and 'quarantine_acl' downloadable ACL. The third row is for 'If a condition is not defined or there is no matched condition:' with 'L2_IP_Quarantine_ACL' shared RAC and 'quarantine_acl' downloadable ACL. Below the table are checkboxes for 'Include RADIUS attributes from user's group' and 'Include RADIUS attributes from user record'. At the bottom are buttons for 'Add Rule', 'Delete', 'Up', 'Down', 'Submit', and 'Done'. A note states: 'The Up/Down buttons submit and save the sort order to the database.'

Condition		Action		
User Group	Assessment Result	Deny Access	Shared RAC	Downloadable ACL
<input type="radio"/> 1: Group 1	NA	<input type="checkbox"/>	L2_IP_Healthy_RAC	healthy_acl
<input type="radio"/> 0: Default Group	NA	<input type="checkbox"/>	L2_IP_Quarantine_ACL	quarantine_acl
If a condition is not defined or there is no matched condition:		<input type="checkbox"/>	L2_IP_Quarantine_ACL	quarantine_acl

Buttons: Add Rule, Delete, Up, Down, Submit, Done

The Up/Down buttons submit and save the sort order to the database.

Step 9. Select **Apply and Restart** to enable your EoU Agentless access profile.

Step 10. On the NAD, enable EoU clientless:

```
IOS-Switch(config)#eou allow clientless
```

Step 11. If you wish, enable the **debug eou all** command to see debugging information for the process occur in these steps.

Step 12. To speed up the clientless handling process, enter the commands **clear eou all** and **clear ip device tracking all**.

Step 13. On Client #1, renew the interface address by entering **ipconfig/renew** from the command prompt. This triggers the clientless device handling.

Step 14. Finally, on the NAD, run a **show eou all** command to see the results of the clientless handling. See the sample output of the table and the applied access control lists.

```

Telnet 128.107.210.5
Pod18-4948#show eou all
-----
Address          Interface          AuthType  Posture-Token Age(min)
-----
10.7.1.2         GigabitEthernet1/1 CLIENTLESS ----- 0
10.7.1.3         GigabitEthernet1/1 CLIENTLESS ----- 0

Pod18-4948#
Pod18-4948#
Pod18-4948#show access-1
Extended IP access list interface_acl
 10 permit udp any any eq 21862
 20 permit udp any eq bootpc any eq bootps (34 matches)
 30 permit udp any any eq domain (85 matches)
 40 permit icmp any any (264 matches)
 50 permit tcp any host 10.0.200.30 eq www
 60 deny ip any any (835 matches)
Extended IP access list xACSACLx-IP-healthy_acl-434cbd2b
 10 permit ip any any
Extended IP access list xACSACLx-IP-quarantine_acl-434e0738
 10 permit udp any eq bootpc any eq bootps
 20 permit udp any any eq 21862
 30 permit udp any any eq domain
 40 permit tcp any host 10.0.200.1 eq www
Pod18-4948#

```

Step 15. View the Passed Authentications Active log file under Reports and Activities.

	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared RAC	Downloadable ACL
5	00:45:28	Authen OK	000d.880f.ffd4	Default Group	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	L2_IP_Healthy_RAC	healthy_acl
5	00:45:28	Authen OK	000c.2999.fa96	Group 1	000c.2999.fa96	000c.2999.fa96	10.0.200.1	NAC-EOU	L2_IP_Quarantine_RAC	quarantine_acl

Task 3: Dynamic NAH with an Audit Server

In this task we discuss how to configure ACS to use and external audit server.

Note: In the prior configuration the MAC Authentication Bypass Configuration option was used for exceptions. It should be noted that exceptions can also be provided for non-responsive hosts that the Administrator does not wish to audit.

Note: To test the information in this task, be sure to remove any configuration on the NAD from Task 2.

Step 1. You must import the appropriate attribute definition for the audit server into ACS through CSUtil as outlined in the example provided earlier:

```

[attr#0]
vendor-id=

```

vendor-name=
application-id=
application-name=
attribute-id=attribute-name=
attribute-profile=
attribute-type=

Step 2. After the attributes are imported, you can configure the audit server as an external posture validation server. From the ACS startup screen, select the **Posture Validation** tab. Select **External Posture Validation Audit Setup**. Click **Add Server**. If under **Audit Server Vendor:** you do not see your audit server vendor listed, make certain you completed Step 1 successfully.

Step 3. Fill out the template as outlined here, taking care to use the *valid* MAC address:

External Posture Validation Audit Server Setup	
Name:	NAC-Test
Description:	Audit NRHs
Which Hosts Are Audited	
Do not audit these hosts:	Host IP Addresses and Ranges (IP/MASK) (comma separated values): Host MAC Addresses (comma separated values): 000c.2999.fa96
Select a token for the hosts that will not be audited:	Healthy
Use These Audit Servers	
Audit Server Vendor:	Qualys
<input checked="" type="checkbox"/> Primary Server Configuration	URL: http://10.0.200.106/audit.cgi Username: Cisco NAC Password: ***** Timeout (sec): 5 Trusted Root CA: ca Validate Certificate Common Name: <input checked="" type="checkbox"/>

As an example, we are showing an audit exception, using Client#1 (000c.2999.fa96) by MAC address. IP address exceptions are also supported in this manner for audit.

Known or authorized hosts (000c.2999.fa96) are given a Healthy token.

Unauthorized hosts will be Audited by the server.

Continue the configuration as demonstrated here:

Audit Flow Settings	
Use this token while Audit Server does not yet have a posture validation result:	Transition
Polling Intervals and Session-Timeout:	Use timeouts sent by Audit Server for Polling Intervals and Session-Timeout
	Polling Interval (seconds):
Maximum amount of times the Audit Server should be polled:	3
Policy string to be sent to the Audit Server:	default

Typically, the Transition state is used for the intermediate state between the time a NRH is discovered and the result from the audit vendor has been received. It is *required* that the Transition RAC, or any intermediate token and associated RAC, provide access between the audit vendor and the host. Otherwise, the scan never runs to completion, and the audit fails.

In this guide, we use the Transition token and let the audit server determine the rate at which ACS should query it for scanning results.

Step 4. Modify the existing NAC-EOU by selecting **Network Access Profile**, selecting **Posture Validation**, and then **Select Audit**. You should now see the audit server configuration entered in the previous step. Make this active.

Select Audit Server						
Select	Name	Description	Server Details			
<input checked="" type="radio"/>	NAC-Test	Audit NRHs	Server	URL	Exemption Token	InProgress Token
			Primary	http://10.0.200.106/audit	Healthy	Transition
			Secondary			
<input type="radio"/>	Do Not Use Audit Server					

Fail Open Configuration	
<input checked="" type="checkbox"/> Do Not reject when Audit failed	Use this token when unable to retrieve posture data: Healthy
	Timeout (sec): 10

Also note that we have selected **Do Not reject when Audit failed**. The purpose of this command is to *fail open* in case the audit server(s) are unreachable. In this case we've selected the healthy posture and a time out of 10 seconds. Any NRHs that are discovered that are not successfully scanned within 10 seconds will automatically receive a Healthy token.

Step 5. The final main step in configuration of Audit is to define the token applied to the host, depending on the result returned by the vendor. Enter the values shown.

Condition			Action		
	User Group	Assessment Result	Deny Access	Shared RAC	Downloadable ACL
<input type="radio"/>	NA	Healthy	<input type="checkbox"/>	L2_IP_Healthy_RAC	healthy_acl
<input type="radio"/>	NA	Transition	<input type="checkbox"/>	L2_IP_Transition_RAC	quarantine_acl
<input type="radio"/>	NA	Quarantine	<input type="checkbox"/>	L2_IP_Quarantine_RAC	quarantine_acl
If a condition is not defined or there is no matched condition:			<input type="checkbox"/>	L2_IP_Quarantine_RAC	quarantine_acl
<input type="checkbox"/> Include RADIUS attributes from user's group <input type="checkbox"/> Include RADIUS attributes from user record					
<input type="button" value="Add Rule"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>					
The Up/Down buttons submit and save the sort order to the database.					
<input type="button" value="Submit"/> <input type="button" value="Done"/>					

Step 6. To speed up the audit triggering process, make these additions to your NAD configuration:

```
IOS-Switch(config)#eou max-retry 2
IOS-Switch(config)#eou timeout retransmit 5 [Verify]
```

As with the prior NAH example, you will find that **clear ip device tracking all** results in the fastest NRH handling trigger by the switch.

Make certain that **eou allow clientless** is still enabled and that the CTA EOU Daemon has not started.

Sample reports and eou output are provided for reference.

```
Pod18-4948#clear ip device tracking all
Pod18-4948#show eou
18:21:39: %EOU-6-SESSION: IP=10.7.1.2| HOST=DETECTED| Interface=GigabitEthernet1/1
18:21:39: %EOU-6-SESSION: IP=10.7.1.3| HOST=DETECTED| Interface=GigabitEthernet1/1
18:21:39: %EOU-6-SESSION: IP=10.7.1.2| HOST=REMOVED| Interface=GigabitEthernet1/1
18:21:39: %EOU-6-SESSION: IP=10.7.1.3| HOST=REMOVED| Interface=GigabitEthernet1/1
18:21:44: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=NOT DETECTED
18:21:44: %EOU-6-CTA: IP=10.7.1.3| CiscoTrustAgent=NOT DETECTED
18:21:44: %EOU-6-POLICY: IP=10.7.1.3| ACLNAME=#ACSACL#-IP-healthy_acl-434cbd2b
18:21:44: %EOU-6-POLICY: IP=10.7.1.3| TOKEN=Healthy
18:21:44: %EOU-6-POLICY: IP=10.7.1.3| HOSTNAME=Unknown User
18:21:44: %EOU-6-POSTURE: IP=10.7.1.3| HOST=AUTHORIZED| Interface=GigabitEthernet1/1
18:21:44: %EOU-6-AUTHTYPE: IP=10.7.1.3| AuthType=CLIENTLESS
18:21:44: %EOU-6-POLICY: IP=10.7.1.2| ACLNAME=#ACSACL#-IP-quarantine_acl-434e2aa9
18:21:44: %EOU-6-POLICY: IP=10.7.1.2| TOKEN=Transition
18:21:44: %EOU-6-POLICY: IP=10.7.1.2| HOSTNAME=Unknown User
18:21:44: %EOU-6-POSTURE: IP=10.7.1.2| HOST=AUTHORIZED| Interface=GigabitEthernet1/1
18:21:44: %EOU-6-AUTHTYPE: IP=10.7.1.2| AuthType=CLIENTLESS
-----
Address          Interface          AuthType    Posture-Token  Age(min)
-----
10.7.1.2         GigabitEthernet1/1  CLIENTLESS  Transition      0
10.7.1.3         GigabitEthernet1/1  CLIENTLESS  Healthy         0
Pod18-4948#
18:21:59: %EOU-6-POLICY: IP=10.7.1.2| ACLNAME=#ACSACL#-IP-quarantine_acl-434e2aa9
18:21:59: %EOU-6-POLICY: IP=10.7.1.2| TOKEN=Transition
18:21:59: %EOU-6-POLICY: IP=10.7.1.2| HOSTNAME=Unknown User
18:21:59: %EOU-6-POSTURE: IP=10.7.1.2| HOST=AUTHORIZED| Interface=GigabitEthernet1/1
18:21:59: %EOU-6-AUTHTYPE: IP=10.7.1.2| AuthType=CLIENTLESS
Pod18-4948#
18:22:04: %EOU-6-CTA: IP=10.7.1.2| CiscoTrustAgent=NOT DETECTED
18:22:04: %EOU-6-POLICY: IP=10.7.1.2| ACLNAME=#ACSACL#-IP-healthy_acl-434cbd2b
18:22:04: %EOU-6-POLICY: IP=10.7.1.2| TOKEN=Healthy
18:22:04: %EOU-6-POLICY: IP=10.7.1.2| HOSTNAME=Unknown User
```

Step 7. Note the **show eou all** output:

- Client#1 was immediately granted an exception (hence the Healthy state).
- A second example client is shown (10.7.1.2) as being in transition pending the scanning result. Later it is also assigned a healthy state (see below).

Address	Interface	AuthType	Posture-Token	Age(min)
10.7.1.2	GigabitEthernet1/1	CLIENTLESS	Healthy	0
10.7.1.3	GigabitEthernet1/1	CLIENTLESS	Healthy	0

Step 8. View the ACS Passed Authentications log to see the state changes:

Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared RAC	Downloadable ACL	System-Posture-Assessment
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Healthy_RAC	healthy_acl	Healthy
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Transition_RAC	quarantine_acl	Transition
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Transition_RAC	quarantine_acl	Transition
Authen OK	000c.2999.fa96	..	000c.2999.fa96	000c.2999.fa96	10.0.200.1	NAC-EOU	Healthy_RAC	healthy_acl	Healthy
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Healthy_RAC	healthy_acl	Healthy
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Transition_RAC	quarantine_acl	Transition
Authen OK	000d.880f.ffd4	..	000d.880f.ffd4	000d.880f.ffd4	10.0.200.1	NAC-EOU	Transition_RAC	quarantine_acl	Transition
Authen OK	000c.2999.fa96	..	000c.2999.fa96	000c.2999.fa96	10.0.200.1	NAC-EOU	Healthy_RAC	healthy_acl	Healthy

In this case, the second example client has a MAC address of 000d.880f.ffd4.

NAC L2 802.1X

The following sections will cover NAC L2 802.1x configuration for switches running IOS and for switches running CatOS.

NAC L2 802.1x for IOS Switches

In this section, you configure the various components to enable the base functionality of NAC L2 802.1x. These steps are performed.

- Step 1.** Configure the IOS switch for NAC L2 802.1x
- Step 2.** Configure the ACS for NAC L2 802.1x
- Step 3.** Install CTA (with NAC L2 802.1x Supplicant)
- Step 4.** Test NAC L2 802.1x
- Step 5.** Configure NAC L2 802.1x for agentless host (MAC-Auth-Bypass)
- Step 6.** Test MAC-Auth-Bypass
- Step 7.** Configure NAC L2 802.1x for guest access
- Step 8.** Test NAC L2 802.1x guest access

Note: The CTA version installed in the NAC L2 IP section did not include the NAC L2 802.1x supplicant. Therefore, CTA with the supplicant is installed in this section to support NAC L2 802.1x.

NAC L2 802.1x Deployment Method Overview

Before beginning the configuration section for 802.1x NAC, it is important to understand that there are two ways to deploy 802.1x: NAC L2 802.1x and traditional IEEE 802.1x.

The first method, NAC L2 802.1x, uses a NAC-enabled 802.1x supplicant to perform identity and posture credential validation within an 802.1x access control conversation.

The second method for deployment is to use a non-NAC enabled 802.1x supplicant to do the identity credential validation for port access and then use NAC L2 IP to do a posture credential validation after the endpoint has an IP address and has triggered a NAC L2 IP interrogation.

The primary difference between the two options is the EAP method used to combine identity and posture in the client to server communication. A NAC-enabled 802.1x must use EAP-FAST for the EAP method because it has been modified to carry identity and posture credentials in a TLS tunnel. The CTA supplicant supports EAP-GTC, EAP-MSCHAPv2, and EAP-TLS for client side authentication.

The following sections guide you through the configuration of the first method: NAC L2 802.1x using the NAC-enabled supplicant in CTA 2.0. Additional configuration details are included in the appendix for those readers who wish to configure the second method, 802.1x and NAC L2 IP, as well.

NAC L2 802.1x Credential Overview

To gain a better understanding of NAC L2 802.1x, let's begin by discussing two aspects of the credentials that can be sent from the client to the network. In a Microsoft Windows environment, there are two sets of identity credentials that can be presented to the network.

The first credential involves the concept of machine authentication where the machine is authenticated in advance of the user of the computer. Microsoft introduced the machine authentication facility to allow the client system to authenticate by using the identity and credentials of the computer at boot time so that the client can establish the required secure channel to update and participate in the domain GPO (Group Policy Objects) model.

Machine authentication allows the computer to authenticate itself to the network by using 802.1x, just after a PC loads device drivers at boot time. This allows the computer to subsequently communicate with Windows domain controllers to pull down machine group policies. This was designed to alleviate the problem of domain GPOs not functioning with the introduction of 802.1x.

The second type of credential used for 802.1x is referred to as user authentication. After the GINA (login screen) is presented, a user can log in to the computer or the Windows domain, and the username and password used for login can be used as the identity credentials for 802.1x authentication.

In a NAC L2 802.1x environment, the CTA supplicant uses EAP-FAST to perform machine and user authentication. EAP-FAST uses a Protected Access Credential (PAC) to mutually authenticate the client and RADIUS server. The PAC is a unique shared credential used to mutually authenticate client and server. It is associated with a specific client username and a server authority ID. A PAC removes the need for Public Key Infrastructure (PKI) and digital certificates. EAP-FAST is detailed here:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/techref/eapfast/eapfast.htm>

EAP-FAST comprises three basic phases:

- Phase 0 (optional): The PAC is initially distributed to client.
- Phase 1: Using the PAC, a secure tunnel is established.
- Phase 2: The client is authenticated through the secure tunnel.

In the EAP-FAST specification, there are two ways to provision the PAC, out-of-band-provisioning or in-band-provisioning. With the NAC L2 802.1x CTA supplicant, you can only provision a PAC with in-band-provisioning. The CTA supplicant only provisions a PAC on the client if the ACS server has been configured to allow in-band-provisioning and if the client side authentication is a successful machine authentication using a certificate assigned to the machine (machine certificate) or a successful user authentication. Out-of-band provisioning is not supported with the NAC-L2-802.x CTA supplicant.

For simplicity in this document, only user authentication is configured. Authentication is performed against the local username and password database in ACS.

Configure the IOS Switch for NAC L2 802.1x

Note: If you configured NAC L2 IP in the previous section for testing purposes be sure to clear the NAC L2 IP configuration from the switchport before starting the NAC L2 802.1x configuration.

Step 1. Clear the NAC L2 IP configuration from the switch port. To accomplish this the following needs to be performed:

```
IOS-Switch(config)#int gig 1/1
IOS-Switch(config-if)#no switchport acces vlan 1000
IOS-Switch(config-if)#no ip admission NAC-L2-IP
IOS-Switch(config-if)#no ip access-group interface_acl in
```

Step 2. Add the switchport command back to Gige 1/1

```
IOS-Switch(config-if)#switchport
IOS-Switch(config-if)#switchport mode access
```

You are now ready to start the NAC L2 802.1x configuration.

Task 1: VLANS for NAC L2 802.1x

NAC L2 802.1x uses VLAN assignment for policy enforcement. Therefore you need to configure the appropriate VLANs on the switch. The following VLANs and VLAN interfaces are used as an example on the switch for 802.1x:

VLAN Name	VLAN	4948 Subnets
employees	10	10.7.10.*
contractors	20	10.7.20.*

utilities	30	10.7.30.*
guests	40	10.7.40.*
healthy	50	10.7.50.*
checkup	60	10.7.60.*
transition	70	10.7.70.*
quarantine	80	10.7.80.*
infected	90	10.7.90.*
unknown	100	10.7.100.*
voice	110	10.7.110.*
servers	200	10.0.200.*
nads	255	10.0.255.*

```

interface Vlan10
  description Corporate VLAN
  ip address 10.7.10.1 255.255.255.0
  ip helper-address 10.0.200.10
!
interface Vlan20
  description Contractors VLAN
  ip address 10.7.20.1 255.255.255.0
  ip helper-address 10.0.200.10
!
interface Vlan30
  description Utilities VLAN
  ip address 10.7.30.1 255.255.255.0
  ip helper-address 10.0.200.10
!
interface Vlan40
  description Guests VLAN
  ip address 10.7.40.1 255.255.255.0
  ip helper-address 10.0.200.10
!
interface Vlan50
  description Healthy VLAN
  ip address 10.7.50.1 255.255.255.0
  ip helper-address 10.0.200.10
!
interface Vlan60
  description Checkup VLAN
  ip address 10.7.60.1 255.255.255.0
  ip helper-address 10.0.200.10
!
interface Vlan70

```

```

description Transition VLAN
ip address 10.7.70.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan80
description Quarantine VLAN
ip address 10.7.80.1 255.255.255.0
ip access-group Interface_ACL in
ip helper-address 10.0.200.10
!
interface Vlan90
description Infected VLAN
ip address 10.7.90.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan100
description Unknown VLAN
ip address 10.7.100.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan110
description Voice VLAN
ip address 10.7.110.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan200
description Servers VLAN
ip address 10.0.200.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan255
description Unknown VLAN
ip address 10.0.255.7 255.255.255.0
ip helper-address 10.0.200.10

```

Task 2: Configure AAA on NAD for NAC L2 802.1x

This topic describes the steps required to enable AAA on the NAD for NAC L2 802.1x.

Note: Skip step 1 *if* you already enabled AAA for NAC L2 IP in the previous section.

Task 2 includes the minimum steps required to enable AAA for NAC L2 802.1x on an IOS switch.

Step 1. Enable the switch AAA service by using the **aaa new-model** global configuration command as shown in the figure.

Step 2. Configure the switch to use RADIUS for 802.1x authentication by using the **aaa authentication dot1x default group radius** global configuration command.

```
IOS-Switch(config)#aaa authentication dot1x default group radius
```

Note: Omit step 1 and 3 if you already enabled AAA for NAC L2 IP in the previous section.

Step 3. Configure the switch to run authorization for all network-related service requests by using the **aaa authorization network default group radius** global configuration command.

Step 4. Enable AAA accounting for 802.1x accounting using the **aaa accounting dot1x default start-stop group radius** global configuration command.

```
IOS-Switch(config)#aaa accounting dot1x default start-stop group radius
```

Step 5. Specify the NAD interface for all outgoing RADIUS packets by using the **ip radius source-interface** global configuration command.

Task 3: Enable 802.1x on the Switch

Step 6. Enable 802.1x using the **dot1x system-auth-control** global configuration command.

```
IOS-Switch(config)#dot1x system-auth-control
```

Task 4: Configure 802.1x on the Interface

Step 7. Set the 802.1x port control to auto on Gigabit Ethernet 1/1 using **dot1x port-control auto**.

```
IOS-Switch(config-if)#dot1x port-control auto
```

Step 8. Set the 802.1x reauthentication timer to use the timer set in ACS using the **dot1x timeout reauth-period server** command.

```
IOS-Switch(config-if)#dot1x timeout reauth-period server
```

Step 9. Enable 802.1x reauthentication for the interface using the **dot1x reauthentication** command.

```
IOS-Switch(config-if)#dot1x reauthentication
```

Network Access Profile Configuration for NAC L2 802.1x

In this section, you configure a Network Access Profile (authentication, posture validation, and authorization) to support NAC L2 802.1x. In ACS 4.0, there are two methods of configuring Network Access Profiles.

- Add an empty profile and configure all the necessary information.
- Using the Template Profiles, customize the Network Access Profile desired with the base information included in the template.

There are seven Network Access Profile templates predefined in ACS 4.0:

- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x
- Microsoft IEEE 802.1x
- Wireless (NAC L2 802.1x)
- Authentication Bypass (802.1x fallback)
- Agentless Host

In this section of the document, we use the NAC L2 802.1x Network Access Profile template to create a base profile and then make the necessary changes to customize this template.

Task 1: Create the NAC L2 802.1x Profile from the Template.

- Step 1.** Click **Network Access Profiles** from the main menu, and select **Add Template Profile**
- Step 2.** Create a template for NAC L2 802.1x by selecting it from the Template drop-down menu. Name the template with something similar to the one shown below. Be sure to select **Active** to enable the profile.

Create Profile from Template

Name:

Lab_NAC_L2_802.1X

Description:

Template for NAC Lab

Template:

NAC L2 802.1x

Active:

☒

Submit

Cancel

- Step 3.** Click **Submit**
- Note:** Sample RADIUS Authorization Components are created as part of the ACS 4.0 templates. You can ignore these for the purposes of this configuration guide.

Task 2: Authentication

- Step 1.** On the Network Access Profiles screen, select the Authentication link for the new profile.

<input type="radio"/>	Lab NAC L2 802.1X	Authentication Posture Validation Authorization	Template for NAC Lab	YES
-----------------------	-------------------	--	----------------------	-----

Step 2. Notice that a portion of the EAP-FAST configuration is already selected as part of the base template.

Network Access Profiles

EAP-FAST <input checked="" type="checkbox"/> Allow EAP-FAST <input type="checkbox"/> Allow anonymous in-band PAC provisioning <input checked="" type="checkbox"/> Allow authenticated in-band PAC provisioning <input checked="" type="checkbox"/> Accept client on authenticated provisioning <input type="checkbox"/> Require client certificate for provisioning <input type="checkbox"/> Allow Stateless session resume Authorization PAC TTL <input type="text" value="1"/> <input type="text" value="hours"/> Allowed inner methods <input checked="" type="checkbox"/> EAP-GTC <input checked="" type="checkbox"/> EAP-MSCHAPv2 <input type="checkbox"/> EAP-TLS Posture Validation: <input type="radio"/> None <input checked="" type="radio"/> Required <input type="radio"/> Optional - Client may not supply posture data. Use token <input type="text" value="Unknown"/> <input type="radio"/> Posture only <hr/> EAP-TLS <input type="checkbox"/> Allow EAP-TLS <hr/> EAP-MD5 <input type="checkbox"/> Allow EAP-MD5
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>

Step 3. Click **Submit**

Note: If you enable EAP-GTC and use the CTA supplicant, you are always prompted for user credentials. This occurs even if you have configured the supplicant to use single sign-on. To disable this, simply uncheck the EAP-GTC method.

Task 3: Posture Validation

The posture validation configuration below is for reference.

Step 1. Select the **Posture Validation** link for the profile from the Network Access Profile screen.

Step 2. Add the following posture policies to the template.

Name: L2-Posture																								
Required Condition Types	Cisco:PA Cisco:Host																							
Posture Validation Policies	CTA Windows																							
Assessment Result Configuration	<table><tr><th>Result</th><th>Message</th><th>URL Redirect</th></tr><tr><td>Healthy</td><td>NAC L2 802.1x Healthy</td><td></td></tr><tr><td>Checkup</td><td>Please update your software to prevent being quarantined by the network.</td><td></td></tr><tr><td>Transition</td><td>Computer under audit...</td><td></td></tr><tr><td>Quarantine</td><td>NAC L2 802.1x Quarantined</td><td></td></tr><tr><td>Infected</td><td>Infected</td><td></td></tr><tr><td>Unknown</td><td></td><td></td></tr></table>			Result	Message	URL Redirect	Healthy	NAC L2 802.1x Healthy		Checkup	Please update your software to prevent being quarantined by the network.		Transition	Computer under audit...		Quarantine	NAC L2 802.1x Quarantined		Infected	Infected		Unknown		
Result	Message	URL Redirect																						
Healthy	NAC L2 802.1x Healthy																							
Checkup	Please update your software to prevent being quarantined by the network.																							
Transition	Computer under audit...																							
Quarantine	NAC L2 802.1x Quarantined																							
Infected	Infected																							
Unknown																								
Audit Selection																								
Audit Server	None																							

Step 3. Click **Submit**.

Task 4: Authorization

Step 1. Select the **Authorization** link from the template

Step 2. Enable authorization.

User Group	Assessment Result	Deny Access	Shared RAC	Downloadable ACL
Employees	Healthy	No	L2_1x_Healthy_RAC	
Contractors	Healthy	No	L2_1x_Healthy_RAC	
Any	Healthy	No	L2_1x_Healthy_RAC	
Guests	Any	No	L2_1x_Quarantine_RAC	
Utilities	Any	No	L2_1x_Quarantine_RAC	
If a condition is not defined or there is no matched condition:			L2_1x_Quarantine_RAC	
Include RADIUS attributes from user's group:				No
Include RADIUS attributes from user record:				No

Step 3. Click **Submit**.

CTA Installation

This section covers the installation of CTA and the NAC L2 802.1x supplicant.

Task 1: Client Certificate for CTA Install

To properly authenticate, CTA must install the certificate that you have installed on ACS. There are two methods available to add the certificate to CTA on the client. Use the first shown here should before installing CTA on the client. The other can be used to add the certificate to the root store after CTA is installed. The second method will be shown at the end of this section.

Step 1. Create a folder called *certs* on the client1, and place it in the same directory as the CTA.exe file.

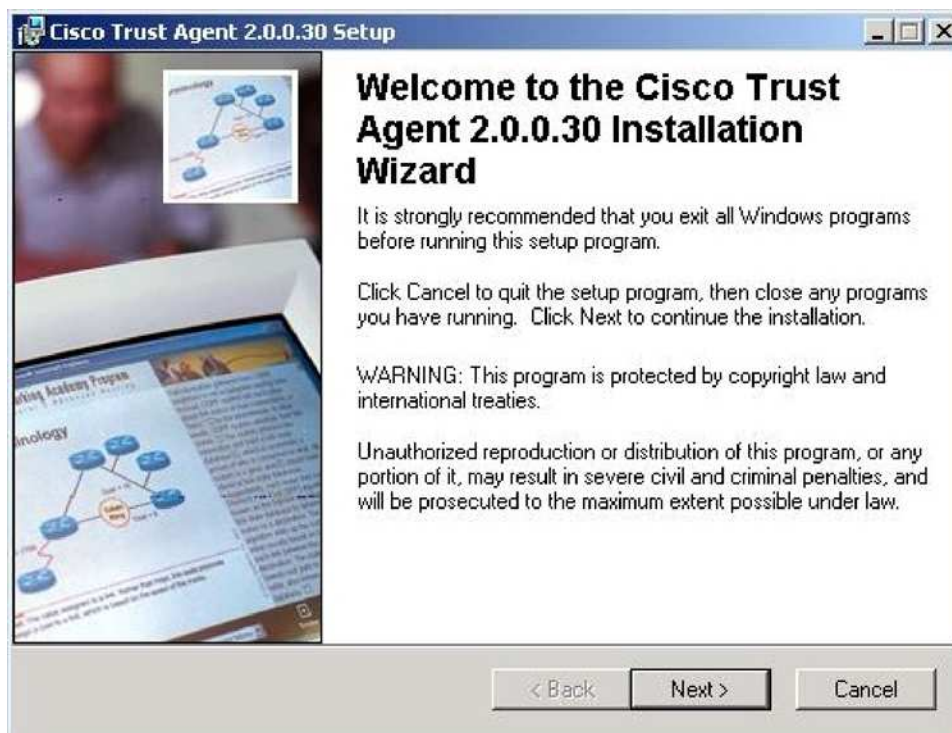
Step 2. The *certs* folder contains the CA certificate that must be used by CTA to authenticate the client to ACS.

Note: CTA will import any public certificate located in the *certs* subdirectory. This folder must be located in the same directory as the *cta.exe* file.

Task 2: Install CTA 2.0

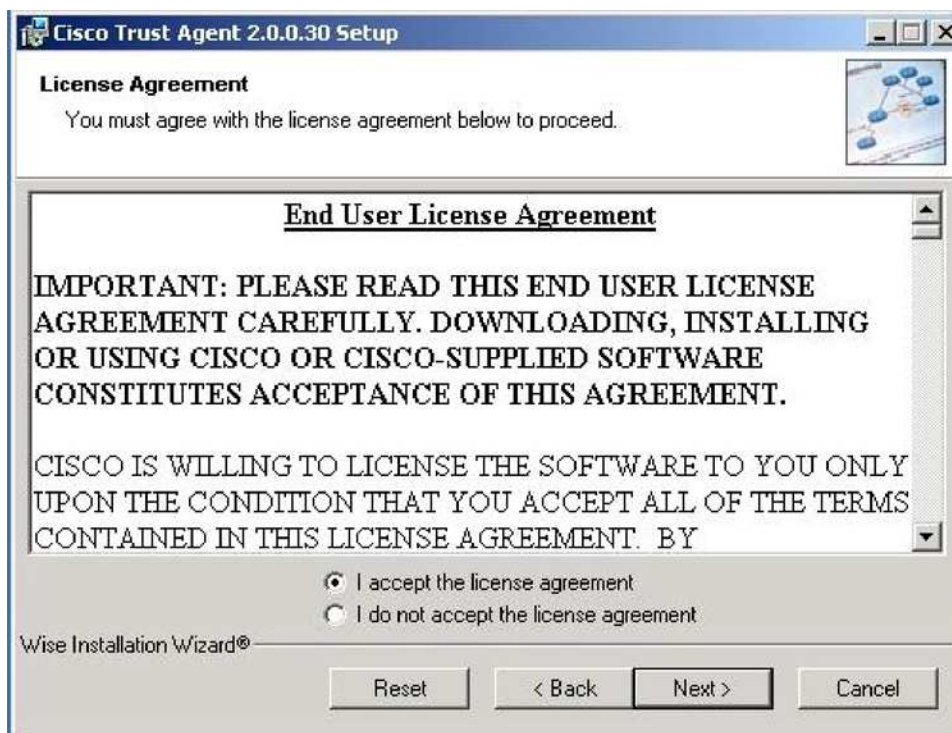
Step 1. Download the CTA-suppliant setup file to the client. Open the folder containing the CTA.exe file located on the client, and double click the appropriate *ctasetup* file. (In this example, we use **ctasetup supplicant-win-[version].exe**).

The Cisco Trust Agent **Installation Wizard** appears.

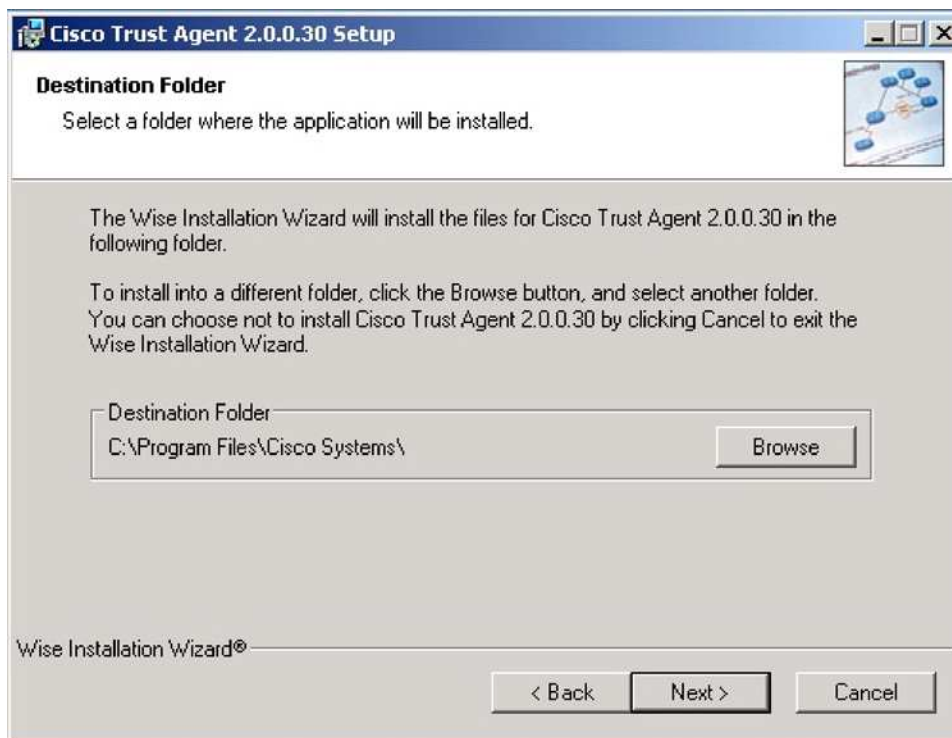


Step 2. Click **Next**.

Step 3. Accept the license agreement by clicking **Next**, the Destination Folder window appears



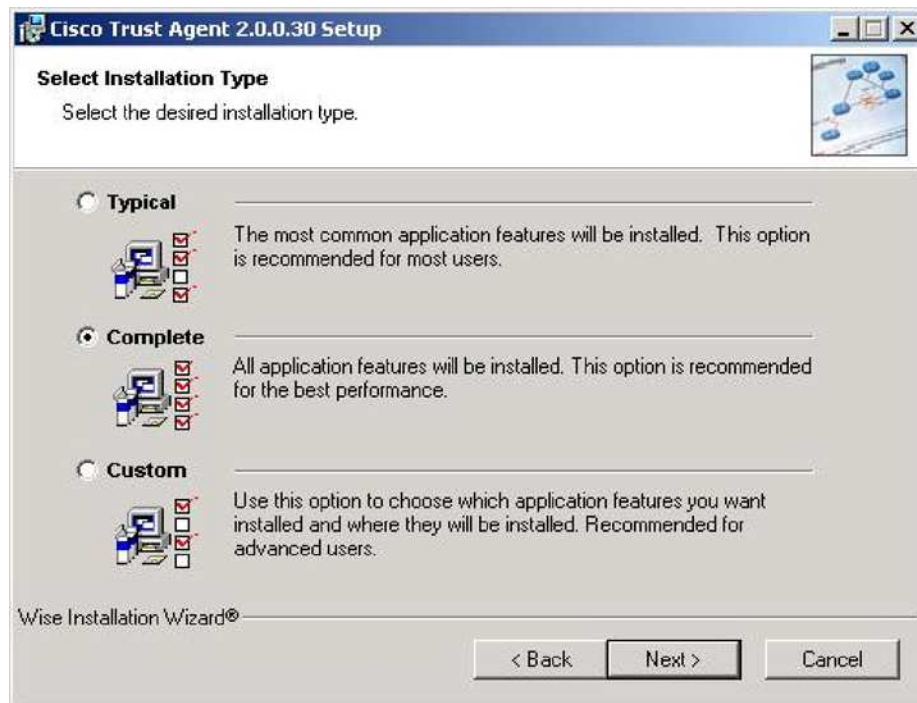
Step 4. Accept the default Destination Folder location and click **Next**



Step 5. The Select Installation Type dialog box appears.

Step 6. Click the **Complete** radio button.

Step 7. Click **Next**.



Step 8. The application installs to the selected directory.

Step 9. The following message appears when the certificate is successfully imported during the installation. Click **OK**.

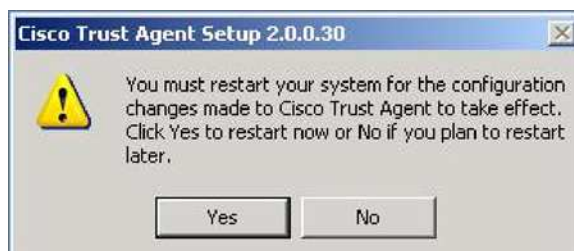


Step 10. When the installation is completed, the wizard displays the **Installation Completed** window.



Step 11. Click **Finish** to close the installation application.

Step 12. You will need to restart your system. You will be prompted to do so when necessary.



Task 3: (Optional) Manual install of root certificate for CTA

If you did not copy the *certs* folder into the CTA folder in [Task 1: Step 1](#), you need to install the root certificate before using Cisco Trust Agent.

You can manually install the certificate by following these steps:

Step 1. Copy the certificate to the network client.

Step 2. Open a command prompt on the network client.

Step 3. Change directories to where Cisco Trust Agent is installed. By default, the location is **C:\Program Files\Cisco Systems\CiscoTrustAgent**

Step 4. Enter `ctaCert.exe /add "cert_path_&cert_name" /store "Root"`, where `cert_path_&cert_name` is the full path and file name to the certificate.

The certificate is added to the trusted certificate store on the network client.

CTA Configuration

There are no configuration changes to be done on the supplicant. The supplicant by default always tries to do machine authentication. ACS issues a RADIUS Access-Reject in response to the first RADIUS Request from the network access device because the supplicant does not have the correct credentials for machine authentication. You should be aware that this causes the 802.1x state machine on the switch to move the port into the *held* state, which prevents the switch from accepting any EAPOL-Starts from the client. If the supplicant sends an EAPOL-Start while the switch is in the *held* state, the end-user could experience a slower than normal login experience. The supplicant has to wait to complete the user login until the switch moves the 802.1x state machine to a *connecting* state and accepts the EAPOL-Starts from the supplicant to initiate a successful 802.1x exchange.

Verify NAC L2 802.1x Functionality

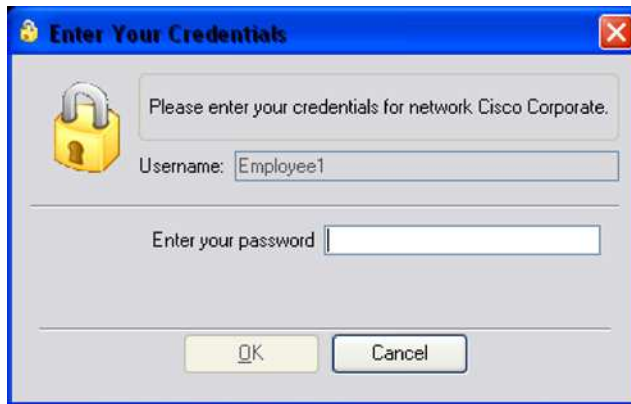
This section helps you validate that NAC L2 802.1x is configured properly, that you are being passed the correct posture token from ACS, and that the correct VLAN assignment from ACS is being applied on the NAD.

To be considered healthy and to be placed in the healthy role, the client must correctly pass back the required credential information to the NAD and then to ACS. The posture validation requirements for each credential created in the previous Network Access Profile section must be met for the client to be passed an application posture token of *healthy*. The credentials include **Cisco Trust Agent**, the agent version is $\geq 2.0.0.30$, and the OS-Type contains **Windows XP**.

Note: It is important to remember that the client only passes to ACS the credentials that ACS is specifically requesting.

Step 1. First, re-enable the switchport to which the client is connected by issuing the `no shut` command.

Step 2. On the client, you should see a credential request from the supplicant similar to this:



Step 3. Issue the `show dot1x all` command to verify the status of the client.

```
NAC4948#sh dot1x all
Dot1x Info for interface GigabitEthernet 1/1
-----
Supplicant MAC 000d.80cd.cda6
  AuthSM State      = AUTHENTICATED
  BendSM State      = IDLE
  Posture            = Healthy
  ReAuthPeriod      = 3600 Seconds (From Authentication Server)
  ReAuthAction       = Terminate
  TimeToNextReauth  = 3570 Seconds
PortStatus          = AUTHORIZED
MaxReq              = 2
MaxAuthReq          = 2
HostMode            = Single
PortControl         = Auto
ControlDirection    = Both
QuietPeriod         = 60 Seconds
Re-authentication   = Enabled
ReAuthPeriod        = From Authentication Server
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
TxPeriod            = 30 Seconds
Guest-Vlan          = 0
```

Step 4. Verify that the client switch port has been placed in the correct VLAN.

```
NAC4948#sh vlan
```

VLAN	Name	Status	Ports

1	default	active	Ge1/5, Ge1/6, Ge1/7, Ge1/8 Ge1/9, Ge1/10, Ge1/13, Ge1/15 Ge1/16, Ge1/17, Ge1/18, Ge1/19 Ge1/20, Ge1/21, Ge1/22, Ge1/23 Ge1/24, Gi1/2
10	employees	active	Ge1/3
20	contractors	active	
30	utilities	active	
40	guests	active	
50	healthy	active	Ge1/1
60	checkup	active	
70	transition	active	
80	quarantine	active	
90	infected	active	
100	unknown	active	Ge1/4, Ge1/11, Ge1/14
110	voice	active	
200	servers	active	Ge1/12
255	nads	active	

Step 5. You can see the client switch port has been placed in VLAN 50 (healthy). You could also use the following interface command to view the switch port information for the interface:

```
NAC4948#sh int GigE 1/1 switchport
Name: Ge1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 50 (healthy)
...
```

Step 6. On the client, CTA will provide a pop-up message similar to the following:



Step 7. On ACS, verify the client information in the appropriate report. Because it appears that we have correctly established communications between the client and ACS, the most appropriate report to check is Passed Authentications.

Suppose the client is not given a token of *Healthy* and is given a *Quarantine* token instead. What are some of the ways to troubleshoot this?

First, force the client into a Quarantine role. You can do this by configuring a posture validation rule in ACS that you know will cause the client will fail.

Step 8. Change the minimum version of the trust agent being requested for a healthy posture status.

```
Cisco:PA:PA-Name contains Cisco Trust Agent
Cisco:PA:PA-Version >= 3.0.0.0
```

Because we are running CTA version 2.0.0.30, the client should fail this rule.

Step 9. Enable the following debug: debug dot1x events

Step 10. Enter the dot1x initialize interface x/x command to restart the authentication process.

```
00:55:00: dot1x-ev:auth_initialize_enter:000d.60cd.cda6: Current ID=0
00:55:00: dot1x-ev:dot1x_update_port_direction: Updating oper direction for Gel/1
(admin=Both, current oper=Both)
00:55:00: dot1x-ev:dot1x_update_port_direction: New oper direction for Gel/1 is Both
00:55:00: dot1x-ev:dot1x_port_cleanup_author: cleanup author on interface
GigabitEthernet1/1
00:55:00: dot1x-ev:dot1x_update_port_status: Called with host_mode=0 state
UNAUTHORIZED
00:55:00: dot1x-ev:dot1x_update_port_status: using mac 000d.60cd.cda6 to send port to
unauthorized on vlan 80
00:55:00: dot1x-ev:Found a supplicant block for mac 000d.60cd.cda6 1E113F0
00:55:00: dot1x-ev:dot1x_port_unauthorized: Host-mode=0 radius/guest vlan=80 on
GigabitEthernet1/1
```

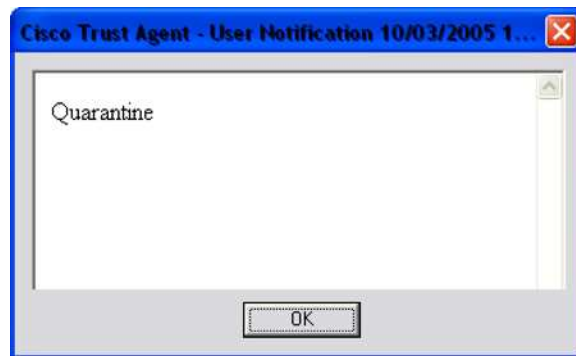
Step 11. Notice that the client has now been placed in VLAN 80, the quarantine VLAN.

```
NAC4948#sh dot1x int
NAC4948#sh dot1x interface GigE 1/1
Supplicant MAC 000d.80cd.cda6
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
Posture           = Quarantine
ReAuthPeriod      = 3600 Seconds (From Authentication Server)
ReAuthAction      = Reauthenticate
TimeToNextReauth  = 3482 Seconds
PortStatus        = AUTHORIZED
MaxReq            = 2
MaxAuthReq        = 2
HostMode          = Single
PortControl       = Auto
ControlDirection  = Both
```

```
QuietPeriod      = 60 Seconds
Re-authentication = Enabled
ReAuthPeriod     = From Authentication Server
ServerTimeout    = 30 Seconds
SuppTimeout      = 30 Seconds
TxPeriod         = 30 Seconds
Guest-Vlan       = 0
```

In the sample output, the client was authenticated correctly because the correct username and password were entered. However, the client failed one of the credential checks, and, as a result, was placed in a quarantine role.

Step 12. On the client, CTA will provide a pop-up message similar to the following:



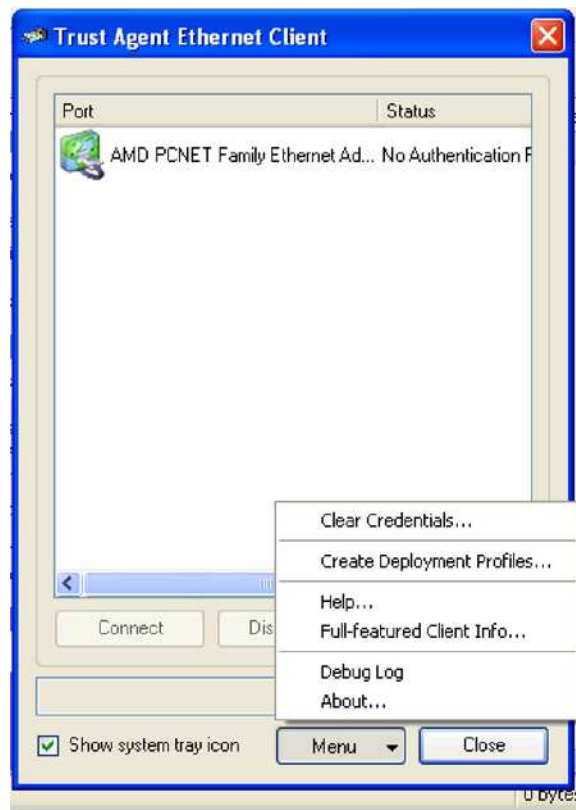
Step 13. View the ACS reports to gather information on why the client was quarantined.

By viewing the report information, you should be able to see where the problem was encountered and start the troubleshooting process.

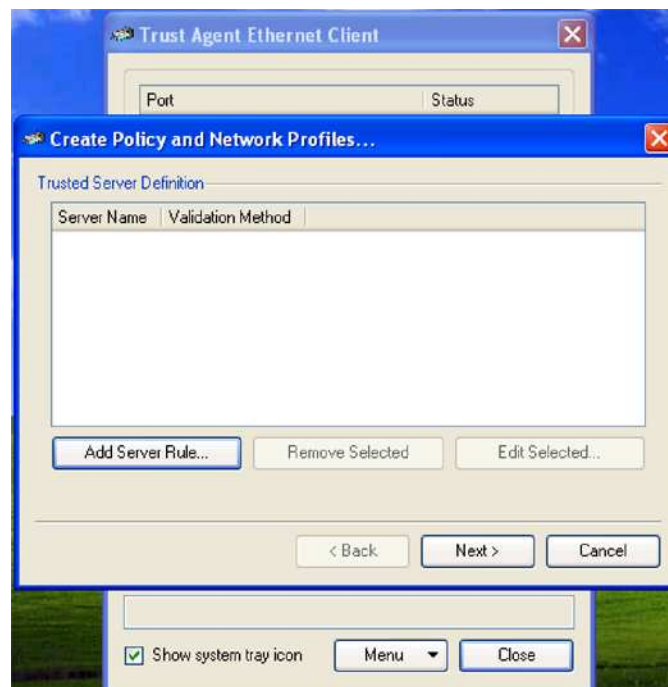
Configuring Supplicant Single Sign-On

CTA Supplicant Configuration

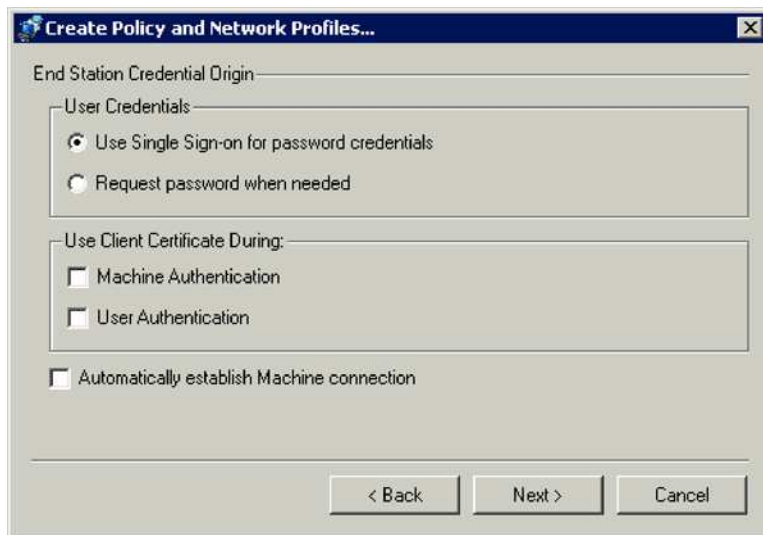
When configuring NAC L2 802.1x with the CTA supplicant most policy is defined on the server. There are a few options on the client that are available to you. The options are set by using XML files. You can create the XML files by installing the CTA supplicant on an administrative workstation. On this workstation, you should access the **Trust Agent Ethernet Client Open** menu option. On the CTA supplicant GUI, you will find an option **Create Deployment Profiles** under the Menu button.



This brings up the wizard for creating the deployment profiles. The first screen of the wizard is the Trusted Server Definition dialog.



You can use this dialog to define ACS servers that you trust, either through validation of the certificate that they present or through the PAC that they present. This is done in Phase 1 of EAP-FAST to validate the credentials that the ACS server sends to the client to establish the SSL tunnel.

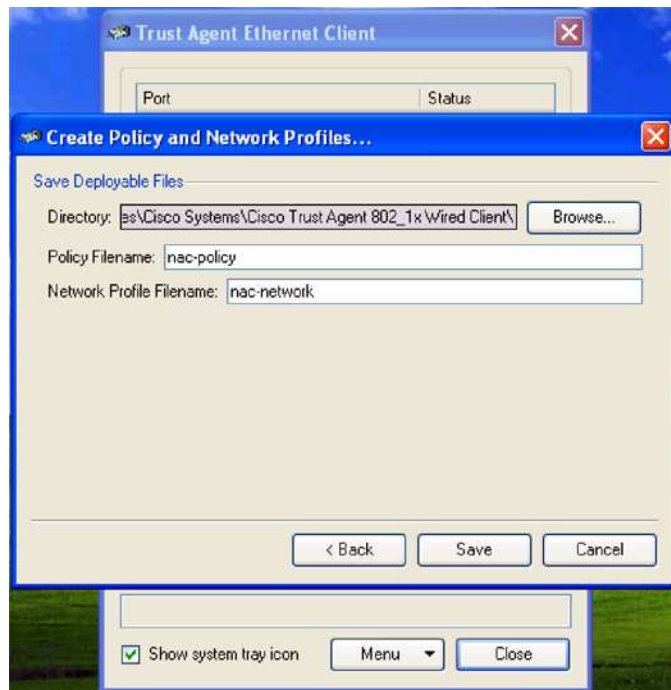


The dialog is divided into three parts. The first part instructs the supplicant on how to acquire user credentials. The client can either try to leverage the username and password of the user login through the single sign-on radio button, or it can prompt you for password credentials.

The second section of the dialog is used to determine how to use any certificates with the supplicant if they are available on the host. You can use certificates for user or machine authentication. This dialog is assuming that a certificate has already been provisioned to the host, either for machine or user identity.

The third section, **Automatically establish Machine Authentication**, is enabled by default and can be unchecked and turned off for the purposes of this configuration guide.

After defining the origin of the end station credentials, you see the dialog to save the two XML files that define the deployment profiles. You can choose where you would like to create the network profile file and the policy file.



We expect that you already have preferred methods of moving files to end-user stations (for example, Microsoft's SMS).

- Export the CTA Client installation file to the end-user's machine.
- Execute the installation file on the end-user machine. Do not restart the machine.
- Export the policy and profile configuration files into the following folders created by the installer:
- **IMPORTANT:** if updating an existing client, the newly deployed configuration files must replace any existing ones. There can only be one.xml file in each of the specified folders. Move these files into the <install directory>\profiles\policies and <install directory>\profiles\networks folders.

Note: The default <install directory> is: Program Files\Cisco Trust Agent Ethernet Client\ policy configuration file: <install directory>\profiles\policies network configuration file: <install directory>\profiles\networks.

Restart the end-user's machine. The End-User CTA Client is automatically started and operational per the deployed configuration files.

Considerations for Hosts Without Supplicants

Not every host that connects to a NAC L2 802.1x network will have a supplicant, so there are several IBNS (Identity Based Networking Services) features that have been developed for these types of hosts. It should be clear that these are IBNS features and are not directly developed for NAC. However, they have relevance for handling agentless hosts in a NAC-enabled network. The IBNS features covered provide the ability to assign an host with no 802.1x supplicant to a VLAN designated for guest access and the ability to authenticate a host based on the MAC address.

Guest VLANs for Non-802.1x Hosts

A guest VLAN enables the non-802.1x capable hosts to access the networks that use 802.1x authentication. You can use the guest VLANs while you are upgrading your system to support 802.1x authentication.

When you configure a VLAN as an 802.1x guest VLAN, all the non-802.1x capable hosts are put in this VLAN. You can configure any VLAN (except for the private VLANs and RSPAN VLANs) as a guest VLAN. If a port is already forwarding on the guest VLAN and you enable 802.1x

support on the network interface of the host, the port is immediately moved out of the guest VLAN, and the authenticator waits for authentication to occur.

Enabling 802.1x authentication on a port starts the 802.1x protocol. If the host fails to respond to the packets from the authenticator within a certain amount of time, the authenticator puts the port in the guest VLAN.

The guest VLANs are supported in both single-authentication mode and multiple-host mode.

Guidelines for 802.1x Authentication with the Guest VLANs on Windows XP Hosts

This section describes the usage guidelines for configuring 802.1x authentication with the guest VLANs on Windows-XP hosts:

- If a guest VLAN is enabled on a port, that port cannot be configured as a unidirectional port, and conversely, a unidirectional port cannot be configured in a guest VLAN.
- If the host fails to respond to the authenticator, the port remains in the connecting state for 180 seconds. After this time, the login/password window does not appear on the host. The workaround is to have the user disconnect and then reconnect the network interface cable.
- The hosts that respond with an incorrect log in or password fail authentication. The hosts that fail authentication are not put in the guest VLAN. The first time that a host fails authentication, the quiet-period timer starts, and no activity occurs for the duration of the quiet-period timer. When the quiet-period timer expires, the host is presented with the log in and password window. If the host fails authentication for the second time, the quiet-period timer starts again and no activity occurs for the duration of the quiet-period timer. The host is presented with the log in and password window a third time. If the host fails the third time, the port is put in the connecting and unauthorized states. The workaround is to have the user disconnect and then reconnect the network interface cable.

If a host does not respond to the username and password authentication requests from the Authenticator Port Access Entity, it is placed in a guest VLAN.

Task 1: Enable Guest VLAN Support on the Interface

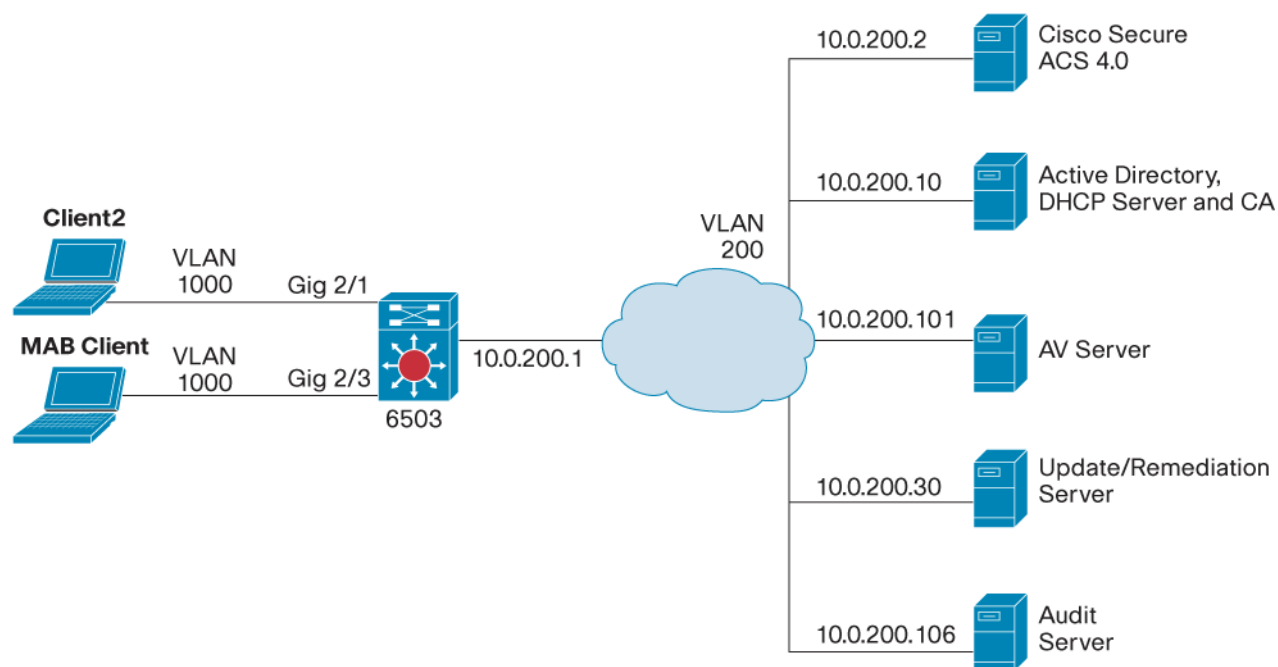
```
IOS-Switch(config)# interface gigabitethernet1/1
IOS-Switch(config-if)# dot1x guest-vlan 40
```

Verify that the supplicant service is stopped or that the supplicant is uninstalled. Make sure that the Windows wireless zero config service is stopped. After you do that, verify that the supplicantless device is placed in the guest VLAN.

NAC L2 IP CatOS SWITCH CONFIGURATION

This section of the document covers configuration for NAC L2 IP and NAC L2 802.1x on a CatOS switch. Figure 6 provides a reference for this section.

Figure 6. Reference Network for CatOS



Task 1: Configure NAC L2 IP

Step 1. Enable the RADIUS on the switch.

```
Console> (enable) set radius server 10.0.200.20 primary
Console> (enable) set radius key cisco123
```

Step 2. Enable EAPoUDP for NAC L2 IP on the switch.

```
Console> (enable) set eou enable
```

Step 3. Enable EAPoUDP for the L2IP port that requires posture validation.

```
Console> (enable) set port eou 2/1 auto
```

Step 4. Remove any previous security ACLs.

```
Console> (enable) clear security acl all
```

Step 5. Configure this Policy-Based ACL. This ACL should be used as a reference point.

```
Console> (enable)!Permit ARP
Console> (enable) set security acl ip nac permit arp
Console> (enable) set security acl ip nac permit arp-inspection any any
Console> (enable)!Permit DHCP Snooping
```



```

Console> (enable) set security acl ip nac permit dhcp-snooping
Console> (enable)!Permit DNS
Console> (enable) set security acl ip nac permit udp any any eq 53
Console> (enable)!Create an entry that allows access for healthy hosts access and that
Console> (enable) matches the healthy policy group name defined in ACS.
Console> (enable) set security acl ip nac permit ip group Healthy_hosts any
Console> (enable)!Create an entry that allows limited access for quarantine hosts
access and that matches the quarantine policy group name defined in ACS.
Console> (enable) set security acl ip nac permit ip group Quarantine_hosts 10.0.200.0
0.0.0.255
Console> (enable) set security acl ip nac permit ip 10.0.200.0 0.0.0.255 group
Quarantine_hosts
    !Permit quarantine hosts the ability to communicate with the default gateway
Console> (enable) set security acl ip nac permit ip group Quarantine_hosts host 10.9.1.1
Console> (enable)!Allow the default gateway to communicate with quarantine hosts
Console> (enable) set security acl ip nac permit ip host 10.9.1.1 group
Quarantine_hosts
Console> (enable)!Allow EOU
Console> (enable) set security acl ip nac permit eapoudp
Console> (enable)!Allow DHCP
Console> (enable) set security acl ip nac permit udp any eq 67 any
Console> (enable) set security acl ip nac permit udp any eq 68 any

```

Step 6. Commit the security ACLs, and apply to the desired VLANs

```

Console> (enable) commit security acl all

```

Step 7. Map the security ACL to the default L2 IP VLAN (1000).

```

Console> (enable) set security acl map nac 1000

```

Note: Enter **show security acl info all** to see the configured security ACL

Step 8. Verify NAC L2 IP functionality.

```

Console> (enable) show policy group all

```

```

-----
Group Name           = Healthy
Group Id             = 1
No.of IP Addresses   = 1
Is Changed flag      = 0
Src Type             = ACL CLI
    List of Hosts in group.
    -----
    Interface        = 2/1
    IpAddress         = 10.7.50.5
    Src type          = NAC

```

Task 2: Configure NAC L2 802.1x

Because RADIUS was already enabled in the previous steps for NAC L2 IP and the VLANs for 802.1x have been preconfigured, there are very few steps required to enable NAC L2 802.1x in CatOS.

Step 1. Globally enable 802.1x authentication.

```
Console> (enable) set dot1x system-auth-control enable
```

Step 2. Enable 802.1x control on Port 2/1, our dot1x Client.

```
Console> (enable) set port dot1x 2/1 port-control auto
```

Step 3. Enable reauthentication on the port.

```
Console> (enable) set port dot1x 2/1 reauthentication
```

Step 4. Verify NAC L2 802.1x functionality.

```
Console> (enable) show port dot1x 2/1
```

```
Console> (enable) show port 2/1
```

Catalyst 6500 Guest VLAN Configuration Example

This example shows how to add port 2/1 to 802.1x guest VLAN 40.

```
Console> (enable) set port dot1x 2/1 guest-vlan 40
Port 2/1 is Multiple-authentication enabled, guest-vlan can not be enabled
6506-CatOS> (enable) set port dot1x 2/1 multiple-authentication disable
Port 2/1 Multiple-authentication option disabled
6506-CatOS> (enable) set port dot1x 2/1 guest-vlan 40
Port 2/1 Guest Vlan is set to 40
6506-CatOS> (enable) show port dot1x guest-vlan
```

Guest-Vlan	Status	Mod/Ports
40	active	2/1
none	none	2/2,3/2-48,8/1-8

Configuring MAC-Authentication-Bypass on the 6500

MAC Authentication Bypass is an IBNS feature that is configured on a per-port basis. The switch makes a RADIUS request to the ACS server with the MAC address of the host connecting to the switch. If the MAC address is found in the internal ACS database, the ACS server replies with an Access-Accept, and the host is permitted onto the network. This MAC authentication happens after 802.1x and hence *bypasses* the default 802.1x security policy of denying access for all devices that cannot complete an EAP authentication. This feature is useful for allowing N/AH access to the host. The MAC address OUI can be used to wildcard MAC addresses allowing devices with addresses within the same OUI range to access the network. This is useful for devices such as printers or terminals that do not have an 802.1x supplicant, but that need to be allowed access to the network. Because MAC Authentication Bypass is dynamic in nature you can configure it on all ports in the network and will not have to explicitly configure it on ports where printers are connected.

Note: MAC Authentication Bypass is only supported on the Catalyst 6500 at this time.

Task 1: Catalyst 6500 Configuration

The Catalyst 6500 configuration for MAC Authentication Bypass consists of a few commands. The following assumes that the necessary RADIUS configuration has been done on the Catalyst 6500 802.1x authentication. The feature must be enabled globally and then applied to the port as shown:

```
6506-CatOS > (enable) set mac-auth-bypass enable
Mac-Auth-Bypass enabled globally.

6506-CatOS > (enable) set port mac-auth-bypass 2/3 enable
Mac-Auth-Bypass successfully enabled on 2/3.
```

Task 2: ACS Configuration for MAC-Auth-Bypass

To do MAC Authentication Bypass (MAB), ACS must be configured to match against the exact MAC address of the host or against a wildcard match of the MAC address. A wildcard match is used to authenticate the OUI portion of the MAC address of the VMware image.

Step 1. Create a Network Access Profile for handling MAB requests from the Catalyst 6500. Create this NAP by selecting the NAP > Add Template Profile > Authentication Bypass (802.1x fallback).

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser's address bar displays `http://127.0.0.1:4110/`. The main content area is titled "Network Access Profiles" and includes a sidebar with navigation links: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, and External User Databases. A "Create Profile from Template" dialog box is open, featuring the following fields:

- Name:** A text input field containing "MAB_NAP".
- Description:** A large, empty text area.
- Template:** A dropdown menu showing "Authentication bypass (802.1x fallback)".
- Active:** A checkbox that is checked.

At the bottom of the dialog box are "Submit" and "Cancel" buttons.

Step 2. Enable MAC Authentication Bypass in the Network Access Profile > MAB_NAP > Authentication Settings.

The image shows the Cisco Systems Network Access Profiles configuration interface. On the left is a vertical navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, and External User Databases. The main content area is titled "Network Access Profiles" and has a black "Edit" bar at the top. Below this is a section titled "Authentication Settings for MAB_NAP" with a help icon. A "Populate from Global" button is present. The "Authentication Protocols" section contains a list of checkboxes: "Allow PAP", "Allow CHAP", "Allow MS-CHAPv1", "Allow MS-CHAPv2", and "Allow MAC-Authentication-Bypass" (which is checked). A blue link "MAC Authentication Bypass Configuration" is located below the list.

CISCO SYSTEMS Network Access Profiles

Edit

Authentication Settings for MAB_NAP

Populate from Global

Authentication Protocols

- ☐ Allow PAP
- ☐ Allow CHAP
- ☐ Allow MS-CHAPv1
- ☐ Allow MS-CHAPv2
- ☒ Allow MAC-Authentication-Bypass

[MAC Authentication Bypass Configuration](#)

Step 3. Select the Add button to create a MAC List under Network Access Profile > MAB_NAP > MAC_Authentication_Bypass_Configuration.

Step 4. After you have a MAC Group, enter the beginning of the Client interface MAC address in the MAC Addresses Text Box. If you enter 00, the comma designates to ACS that you are wildcarding the MAC address match after the entered text. For example, if you entered 00-95, you wildcard the MAC address match after the 5. You can also map the MAC addresses to a user group, in this instance the default group.

Task 3: Monitoring

After applying the configuration, you can monitor the feature with show commands as depicted below.

Step 1. The port with MAC authentication in progress:

```
6506-CatOS > (enable) sho port mac-auth-bypass 2/3
```

Port	Mac-Auth-Bypass State	MAC Address	Auth-State	Vlan
2/3	Enabled	00-00-00-00-00-00	waiting	10

Port	Termination action	Session Timeout	Shutdown/Time-Left
2/3	reauthenticate	3600	NO -

Step 2. The port after a successful authentication:

```
6506-CatOS > (enable) sho port mac-auth-bypass 2/3
Port  Mac-Auth-Bypass State MAC Address      Auth-State      Vlan
-----
2/3   Enabled              00-0a-95-dc-32-4a authenticated    50

Port  Termination action Session Timeout Shutdown/Time-Left
-----
2/3   reauthenticate      1000           NO              -
```

Step 3. VLAN assignment can be validated by looking at the output of the **show vlan** command. VLAN 50 matches the name *healthy* as described in the group IETF RADIUS attributes.

```
6506-CatOS > (enable) sho vlan 50
VLAN Name                               Status    IfIndex Mod/Ports, Vlans
-----
50   healthy                             active    68      2/3,2/47
                                           15/1

VLAN Type  SAID      MTU    Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
-----
50   enet    100050    1500   -      -      -   -      0      0

VLAN MISTP-Inst DynCreated RSPAN
-----
50   -        static    disabled
```

Step 4. Under “Reports and Activity/Passed Authentications”, there is a message that matches the following ACS log message for a successful MAC authentication.

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port
07/14/2005	21:43:10	Authen OK	00-0a-95-dc-32-4a	..	00-0a-95-dc-32-4a	201

MICROSOFT ACTIVE DIRECTORY INTEGRATION

ACS can delegate authentication decisions to external servers, including Windows, LDAP, ODBC databases, RADIUS token servers, and RSA SecurID Token Servers. You can prioritize the list of servers for authentication, and ACS tries each one sequentially until a match is found. If no match is found after trying all of the servers, the authentication fails. To configure ACS to use an external server for authentication, you must configure each type of server under **External User Databases**.

Note: Add the ACS server to the AD Domain.

Microsoft Active Directory

Note: To perform authentication with Microsoft Active Directory, the ACS server must be a member of the domain.

There are three parts to the configuration of an external user database in ACS:

1. Unknown User Policy
2. Database Group Mappings
3. Database Configuration

You must enable the use of an external database, and specify which type of database. In ACS, go to the configuration screen **External User Database > Unknown User Policy**, and choose Windows Database as shown in this figure.

Unknown User Policy
Fail the attempt
Check the following external user databases
Selected Databases:
Windows Database (Windows Database)

Note: If you specify multiple databases for authentication, ACS queries each directory server in the order specified until it receives an authoritative response. You should put the most likely directory servers higher in the list to improve response times and user experience.

In order for ACS to know how to authorize users authenticated by Microsoft Active Directory, you must map the Active Directory groups to the respective network groups in ACS as shown. This mapping is configured under **External User Database > Database Group Mappings > Windows Database > Domain**. For the reference network, the domain is named **NAC**.

Database Group Mappings
Windows Database
Domain Configurations: NAC
NT groups "Users, *" matches Cisco Secure group "Employees"
NT groups "Contractors, *" matches Cisco Secure group "Contractors"
NT groups "Guests, *" matches Cisco Secure group "Guests"

The final step in external database configuration is to specify the order of the databases that ACS uses to perform authentication against for incoming requests. The following settings are used at **External User Databases > Database Configuration > Windows Database > Configure** to use the nac.cisco.com Active Directory domain for user and machine authentication.

Dialin Permission	
Verify that <i>Grant dialin permission to user</i> setting has been enabled from within the Windows User Manager for users configured for Windows User Database authentication.	
Unknown User Policy	
Use the next sequential External Database in the Selected Databases list in case of an "External DB user invalid or bad password" error.	
Configure Domain List	
Domain List:	
NAC	
\LOCAL	
MS-CHAP Settings	
Enable password changes using MS-CHAP version 1.	
Enable password changes using MS-CHAP version 2.	
Windows EAP Settings	
Enable password change inside PEAP or EAP-FAST.	
EAP-TLS Strip Domain Name.	
Machine Authentication	
Enable PEAP machine authentication.	
Enable EAP-TLS machine authentication.	
EAP-TLS and PEAP machine authentication name prefix.	<input type="text" value="host/"/>
Enable machine	<input type="text" value="12"/>
access restrictions.	<input type="text" value=" <No Access>"/>
Aging time (hours):	
Group map for successful user authentication without machine authentication:	

Configuring User and Machine Authentication

These sections provide details on configuring ACS and the switches for the following variations of host authentication.

- user authentication
- machine authentication
- machine and user authentication

User and Machine Authentication Overview

With the notion of machine posture states in NAC-L2-802.1x, there is a possibility of multiple 802.1x authentications occurring during a machine and user authentication. This is the maximum possible machine and user authentication scenario for 802.1x transactions:

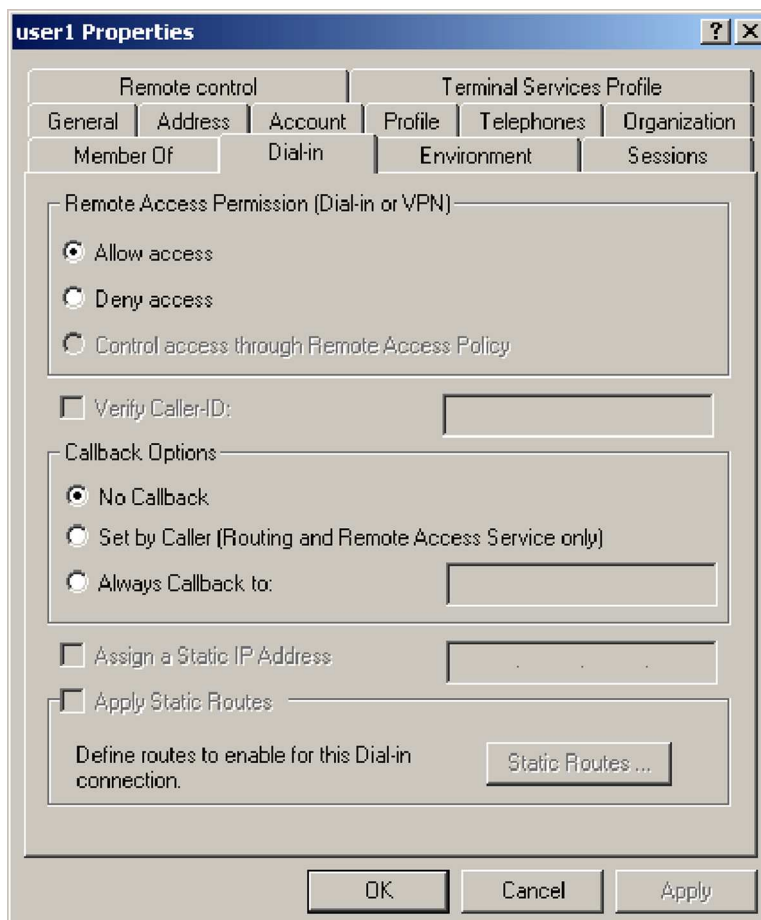
- Machine boots.
- Supplicant performs Machine Auth and posture—first 802.1x exchange.
- All services on the machine complete, thus CTA triggers a posture status change as a result of the machine changing from booting to running.

- Supplicant performs Machine Auth and posture—second 802.1x exchange.
- User logs in.
- Supplicant performs user auth and posture—third 802.1x exchange.
- Login completes, thus CTA triggers a posture status change as a result of the machine changing from running to logged in.
- Supplicant performs user auth and posture—fourth 802.1x exchange.

Task 1: Configure ACS to AD Communication

Step 1. You must add the Windows Database to the list of databases checked within the NAP > Lab_NAC_L2_802.1X > Authentication > Credential Validation Databases > Selected Databases.

Step 2. In this configuration guide and for ACS to properly exchange user and machine authentication with Microsoft Active Directory, you have to have the enable the *Allow access* for Dial-In on the user properties if you are doing user authentication and on the machine properties if you are doing machine authentication. This figure shows how to enable this setting in the *Active Directory Users and Computers Management Tool*.



To test AD integration:

Step 3. Click **Clear Credentials** on the **Menu** button of the Cisco Trust Agent supplicant GUI on the client desktop.

Step 4. To test user authentication with Active Directory, use NAC\User1 as the username and cisco123 as the password when logging in.

TROUBLESHOOTING NAC

Network Admission Control is a complex solution; however a wealth of information is available from the individual solution components. Each of these components provides show commands, reports, or logging output that helps the troubleshooter pinpoint the problem. Let's take a look at the information available from each component. We'll start with the client or host undergoing the admission control process and move towards the AAA and policy servers.

Cisco Trust Agent and CTA Supplicant Logging

CTA provides a logging daemon that is installed along with the agent during the normal setup routine. By default, this logging is not enabled after the installation process completes. The CTA logging function can be enabled a number of different ways, if you want to have the logging enabled after the installation of CTA has completed, a properly configured *ctalogd.ini* file can be included with the ctasetup executable. By default, a file named ctalogd.tmp is copied to the appropriate folder at installation time. This file can be renamed to an.ini file type, and the logging service restarted in Windows to turn on logging or logging, can also be started from the command line.

A sample of ctalogd.ini follows along with an explanation:

```
;
;This file contains Cisco Trust Agent log settings.
;To use these setting simply rename file to "ctalogd.ini"
;

;
; 0 = disable logging
; 1 = enable logging
;

[main]
EnableLog=1

;
; This section allows you to set the "verbose" levels for various
; components of the Cisco Trust Agent.
;
; 0 = disable
; 1 = log critical events only
; 2 = log critical and warning events
; 3 = log critical, warning and informational events
;

[LogLevel]
PADaemon=3
NetTrans=3
PAPlugin=3
```

```
CTAMsg=3
CTAD=3
PEAP=3
EAPTLV=3
EAPSQ=3
PPMgr=3
PSDaemon=3
HostPP=3
CTASI=3
ScriptPlugin=3
CTASC=3
CTAVSTLV=3
CTASTATE=3
```

Each of the previous ctalogd.ini entries references a specific daemon that is part of CTA. The sample file included with the installation if renamed to a .ini filetype will set each daemon's logging level to high. This is normally enough information to help with the troubleshooting activity. Setting the logging level for the various daemons to 15 enables a complete packet dump. CTA logging can also be enabled from a command prompt with this syntax:

```
ctalogd { start | stop | restart | enable [-t] | disable | clear }
```

The location where ctalogd writes the log file might also be changed. More information is available in the CTA Administrator's Guide at this following URL: http://www.cisco.com/en/US/partner/products/ps5923/products_administration_guide_book09186a008023f7a5.html

This example shows parts of a successful EoU session with the logging level set to high for the various daemons. A majority of the messages have been removed for clarity. The tab-separated fields are Sequence number, Time, Date, Severity, Daemon ID and Message.

```
103      13:49:32.095   07/08/2005   Sev=Info/4   NetTrans/0x6310000E
EAPoUDP Session 4 created for NAD 172.31.211.1, total session count: 2

109      13:49:32.305   07/08/2005   Sev=Info/5   PEAP/0x6340000D
Server certificate (/O=Cisco Systems, Inc./CN=Server) has been validated by local CA certificate
(/O=Cisco Systems, Inc./CN=Stress).

110      13:49:32.335   07/08/2005   Sev=Info/5   PEAP/0x6340000F
Server certificate matches following DN checking rule: CN*"Server", ISSUER-CN="Stress"

111      13:49:32.365   07/08/2005   Sev=Info/4   PEAP/0x63400003
PEAP handshake success

112      13:49:32.405   07/08/2005   Sev=Info/6   EAPTLV/0x63500002
EAP Identity:  PCTOO:NAC User

120      13:49:32.836   07/08/2005   Sev=Info/4   PEAP/0x63400008
PEAP received a message of: EAP Success

121      13:49:32.866   07/08/2005   Sev=Info/5   EAPTLV/0x63500004
Done with EAP-TLV processing

125      13:49:33.036   07/08/2005   Sev=Info/5   PEAP/0x6340000C
```

PEAP processing finished

```
126    13:49:33.046    07/08/2005    Sev=Info/4    PAPPlugin/0x63200001
Application Posture Result = Healthy
```

```
127    13:49:33.086    07/08/2005    Sev=Info/4    PAPPlugin/0x63200002
System Posture Result = Healthy
```

```
129    13:49:33.177    07/08/2005    Sev=Warning/2 PAPPlugin/0xA3200010
CTAPP receives UserMsg Notification: Content = healthyL2IP
```

This session shows a new EoU session creation, the CTA receiving a server certificate from ACS, the validation of that certificate as trusted and matching any certificate filtering rules. After the message of PEAP handshake success, the registered credentials are sent to ACS, where the client's posture is validated. The results are sent back to CTA.

The configuration of the CTA logging settings file can be modified from a DOS prompt with this command:

```
clogcli { enable | disable | clear | loglevel [1-3, 15] }
```

The **clogcli** command also initiates logging from the CLI. More details can be found in the CTA Administrators Guide.

A quick status of CTA on a client may be obtained with the **ctastat** command. A sample of the output is shown here. This output shows the number of times that the posture has been validated since CTA was started, the current system posture token, the results of the last status query, and any registered posture agents.

```
> ctastat.exe
CTA Statistics Reporting Tool

Cisco Trust Agent Statistics
Current Time: Mon Jul 18 08:10:59 2005

Session Information
  Session Number (Hex): 01000000
    System Posture Token Value: Healthy
      Received on: Mon Jul 18 07:50:30 2005
      Total Postures Received: 1
    Last SQ Response was "No Status Change"
    Plugin Vendor/Application: 9/1
      Application Posture Token Value: Healthy
        Received: Mon Jul 18 07:50:30 2005
      Posture Request last received: Mon Jul 18 07:50:30 2005
        Length of last response to Posture Req: 28
        Sent: Mon Jul 18 07:50:30 2005
    Plugin Vendor/Application: 9/2
      Posture Request last received: Mon Jul 18 07:50:30 2005
        Length of last response to Posture Req: 167
        Sent: Mon Jul 18 07:50:30 2005
```

NAD Logging, Show Commands, Session Control, and Debug

Cisco IOS devices and CatOS devices acting as NAC network access devices provide information through normal console and syslog functions as well as some RADIUS accounting functions. The information and the methods provided depends on how NAC has been implemented: whether you are using L2/L3-IP or L2-802.1x.

This command changes the logging level for EoU-related events to only informational. This has the effect of reporting a great deal of detail to the NAD console, the management station, or both and can be required for a complete picture from either SIMS or MARS.

eou logging

```
*Jul 18 04:12:16.878 MDT: %EOU-6-SESSION: IP=172.31.211.2| HOST=DETECTED|
Interface=GigabitEthernet1/9
*Jul 18 04:12:16.882 MDT: %EOU-6-CTA: IP=172.31.211.2| CiscoTrustAgent=DETECTED
*Jul 18 04:12:22.446 MDT: %EOU-6-POLICY: IP=172.31.211.2| ACLNAME=#ACSACL#-IP-healthy-42c46e7c
*Jul 18 04:12:22.446 MDT: %EOU-6-POLICY: IP=172.31.211.2| TOKEN=Healthy
*Jul 18 04:12:22.446 MDT: %EOU-6-POLICY: IP=172.31.211.2| HOSTNAME=PCTOO:Jane Dough
*Jul 18 04:12:22.446 MDT: %EOU-6-POSTURE: IP=172.31.211.2| HOST=AUTHORIZED|
Interface=GigabitEthernet1/9
*Jul 18 04:12:22.450 MDT: %EOU-6-AUTHTYPE: IP=172.31.211.2| AuthType=EAP
```

This command changes the station ID from a MAC address to an IP address when the NAD reports to ACS. This is useful when the client is more than a single hop away from the NAD, as the MAC address changes with each hop.

eou allow ip station-id

In an L2-802.1x NAC implementation, there is no logging available as there is with an L2/L3-IP configuration. Instead, use the 802.1x accounting features built into the NADs. Enable 802.1x accounting with this command:

aaa accounting dot1x default group radius

NAD Show Commands

A variety of show commands report the state of NAC sessions. **Show eou all** displays a simple table of the current NAC sessions present on the NAD, including information about the authentication type, the current posture token assigned to the clients, and the age of the NAC session.

show eou { all | posture token | authentication }

```
-----
Address           Interface           AuthType    Posture-Token  Age(min)
-----
172.31.211.2      GigabitEthernet1/9  EAP         Healthy        15
```

You can see detailed information about a specific NAC client and its session with the **show eou ip** or **show eou mac** command. In addition to the previously shown information, these commands also show time values, information about the URL downloads (if any) and the downloadable ACL instance that has been applied.

show eou { ip x.x.x.x | mac h.h.h.h }

```
Address           : 172.31.211.2
MAC Address       : 0004.5aa8.2bde
```

```
Interface          : GigabitEthernet1/9
AuthType           : EAP
Audit Session ID   : 00000031007C75E400000002AC1FD302
PostureToken        : Healthy
Age(min)           : 15
URL Redirect        : NO URL REDIRECT
URL Redirect ACL    : NO URL REDIRECT ACL
ACL Name           : #ACSACL#-IP-healthy-42c46e7c
User Name          : PCTOO:Jane Dough
Revalidation Period : 3600 Seconds
Status Query Period : 300 Seconds
Current State       : AUTHENTICATED
```

The ip device tracing command shows the existence of IP end stations that the IOS switch platform is aware of.

```
show ip device tracking { all | interface | ip | mac }
```

```
IP Device Tracking = Enabled
```

IP Address	MAC Address	Interface	STATE
172.31.211.2	0004.5aa8.2bde	GigabitEthernet1/9	ACTIVE

For 802.1x environments, the **show dot1x** command will displays a table of information on a per-interface basic that shows the port state, the current posture token, and timer settings.

```
show dot1x { all | interface | statistics interface }
```

```
Supplicant MAC 000f.20ca.665c
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
Posture           = Healthy
ReAuthPeriod      = 3600 Seconds (From Authentication Server)
ReAuthAction      = Reauthenticate
TimeToNextReauth  = 3590 Seconds
PortStatus        = AUTHORIZED
MaxReq            = 2
MaxAuthReq        = 2
HostMode          = Single
PortControl       = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Enabled
ReAuthPeriod      = From Authentication Server
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
```

```
Guest-Vlan          = 216
AuthFail-Vlan       = 0
AuthFail-Max-Attempts = 3
```

IOS NAD Clear Commands

NAC EoU sessions can be reset or revalidated on a session-by-session basis, in some cases, on an interface-by-interface basis, or on an entire NAD at once by using these commands.

The **clear** command completely resets the NAC sessions in question and removes all the information about those sessions. These IP end stations need to be rediscovered again to take part in NAC. The **clear** command can be applied on an entire NAD with the *all* option, a specific authentication type such as EAP, a specific interface, an single IP address or MAC address, or on a specific posture token.

```
clear eou { all | authentication | interface | ip | mac | posturetoken }
```

The **initialize** command clears all the NAC state information regarding the sessions in question. *It does not* remove the existence of those sessions. This command causes the NAD to initiate NAC communications with the clients in question.

```
eou initialize revalidate { all | authentication | interface | ip | mac | posturetoken }
```

The **revalidate** command causes the NAD to revalidate the NAC clients without clearing any of the sessions. During the revalidations, the clients still retain the network access that they had before the **revalidate** command being entered.

```
eou revalidate { all | authentication | interface | ip | mac | posturetoken }
```

NAC sessions configured with 802.1x can be reset or re-authenticated with these commands. The **initialize** command resets the 802.1x state machine on the interface and causes the client and supplicant to go through the 802.1x authentication process.

```
dot1x initialize interface
```

The **re-auth** command causes a simple re-authentication of the interface. The 802.1x state machine is not reset. takes place. If the client has currently been assigned a VLAN, that assignment remains until the re-authentication has completed.

```
dot1x re-auth interface
```

NAD Debug Commands

IOS debug commands can provide information on exactly where a NAC session is failing. These commands show a detailed trace of each of the protocols mentioned or just show that a packet was received from a particular protocol.

```
debug eou { all | events | packets }
```

```
debug dot1x { all | errors | events | packets | state-machine }
```

```
debug radius { authentication | brief | e-log }
```

CatOS NAD Show Commands

```
show eou config
```

```
show eou ip-address x.x.x.x
```

```
show eou all
```



```
show dhcp-snooping bindings

show policy group <name>

show dot1x user [ <username> | all ]

show dot1x group <group name>
```

Troubleshooting Flow

The problems associated with NAC can be generally classified into three different categories:

- **No attempts**—Problems where there is no authentication attempt made to ACS.
- **Failed attempts**—Problems where ACS has received a RADIUS authentication attempt but was unable to successfully process it and passed authentications where the result of the posture validation was incorrect or unexpected.

Troubleshooting and Interpreting the Logs and Reports

The first step in troubleshooting a NAC implementation is to check your NADs. The network access device sits between the client and the network and gives you a quick snapshot of the state of the solution. If the NAD has detected a supplicant in the case of an L2-802.1x implementation or you are getting a message of CTA detected with an L2-IP implementation, visit the ACS reports to ascertain the problem type.

No Attempts Problems

No attempts problems are characterized by the lack of a report entry in either the Failed Attempts report or the Passed Authentications report in ACS. These problems generally signify some sort of communications problem in the NAC solution. In the case of L2/L3-IP, this can be caused by the EAP-over-UDP port being blocked by a firewall on the client undergoing NAC, a firewall between the client and the network access device or an access control list on the NAD. Because this implementation of NAC communicates over IP, it can also be caused by an ACL blocking the clients access to a DHCP server. The following is the minimum recommended access that an interface access list should restrict a client to that is doing any version of NAC.

```
permit udp any eq bootpc any eq bootps
permit udp any any eq 21862
```

If the implementation is NAC L2 802.1x, this could be caused by a misconfigured switch port or a supplicant installation that did not complete properly. Both implementations depend on successful RADIUS communications with ACS. This includes the configuration of the proper RADIUS source address from the NAD in ACS. IOS or CatOS show commands determine whether or not the NAD has sensed a host on the interface or switch port in question, and whether or not the CTA or CTA supplicant is properly responding to the NAD.

Windows Service Pack II causes a *no attempt* problem if it has been installed and the Windows firewall enabled without configuring an exception for CTA. Select **Security Center** from the Windows Control Panel, and click **Manage Settings for Windows Firewall** at the bottom of the window. Select the exceptions tab, and then click **add program**. Browse for the CTA executable, and select **Ok**.

Failed Attempts Problems

Failed attempts are marked by an entry in the Failed Attempts report in ACS. These are generally caused by the authentication request matching an incorrectly configured policy, profile, or rule. These errors can also be caused by a lack of credentials being returned from the client's posture agents.

This report has a number of fields that include the IP address of the ACS server, the IP address of the NAD, the IP or MAC address of the client, and the identity of the client. This report also includes two fields that provide most of the information necessary for troubleshooting the Authen-Failure-Code and the Author-Failure-Code problems. The Reason attribute should also be included in this report, as this field is sometimes also helpful. The

following table contains the currently documented list of Authen-Failure-Codes, a reason for the AFC occurrences, and a suggested action to solve the problem.

Authen-Failure-Code	Cause	Suggested Action
Authentication protocol is not allowed for this profile.	Authentication request is matched against a network access profile but the protocol is not allowed in the profile.	Check Network Access Profile configuration and NAP Authentication configuration.
EAP-FAST anonymous in-band provisioning is not permitted.		
Error communicating with the audit server or invalid response.	When there is a problem communicating with the audit server.	Check that the audit server is running and that it is returning correctly formatted responses.
Too many audit round trips.	When there are too many round trips.	Check that the audit server is functioning properly or increase audit server timeout. You can also increase the permitted round trips in the audit policy.
MAC auth bypass is not allowed.	When a request is match against a profile but MAC auth bypass is not allowed.	
Access denied due to unmatched profile.	The access request did not match any profile in the enabled profile list.	
MAC auth bypass group is disabled.		Enable MAC auth bypass group.
Access rejected due to authorization policy.	Access was rejected because the matched authorization rule was marked with deny access.	This can also be caused by an unmatched group setting in the authorization section of the selected Network Access Profile.
Posture Validation failed due to unmatched profile.	No access profile was matched. Request fallback to global settings where no posture validation was configured.	Check Network Access Profile configuration for expected profile.
User's credentials reside in an external DB that is not configured for this profile.	User info missing from ACS user database.	Add user to ACS or configure an external database under Authentication section of NAF.
MAC auth bypass group is disabled.		
External User Not Found.	Username is not present in configured external user database.	Add user info to external user database or configure correct database for this user.
Posture Validation Failure (general).		
Users in this group are disabled.	Group set for disabled users.	Change group setting.
External DB not operational.	Unable to connect to configured external user database.	
External DB password invalid	-	-
Auth type not supported by External DB	-	-
External DB user unknown	User not present in the configured external user database.	Add user to external user database.
External DB EAP authentication failed	-	-
External DB not configured	-	-
EAP type not configured	-	-
EAP-TLS or PEAP authentication failed during SSL handshake	-	-

Authen-Failure-Code	Cause	Suggested Action
EAP-FAST user was provisioned with new PAC	-	-
EAP-FAST user PAC is invalid	-	-
EAP-FAST in-band provisioning is not permitted	-	-
Posture Validation Failure (general)	-	-
External DB user access denied (Machine Access Restriction)	-	-
Posture Validation settings contain unknown attribute(s)	-	Check posture validation settings and remove unknown attributes.
EAP-FAST anonymous in-band provisioning is not permitted	-	-
Error communicating with the audit server or invalid response	-	Check communication settings for external audit server.
MAC auth bypass is not allowed	-	-
Posture Validation Failure on Internal Policy	-	-
Posture Validation Failure on External Policy	No response received from external policy server.	-

Passed Authentications Problems

A passed authentication problem has an entry in the Passed Authentications report in ACS. These are problems where the outcome of the posture validation was unexpected or incorrect. These might not be problems specifically, but more likely are errors in the way in which ACS has been configured or a misunderstanding of the data contained in the attributes sent from the posture agents on the clients.

Properly configured passed authentications reports show similar information as the failed attempts report without the particular failure codes. Passed authentications also show the EAP type, the configured network access profile name of the profile that was selected for this authentication attempt, the application posture tokens that have been returned by the NAC policies that you have configured under the posture validation section of network access profiles, the resulting system posture token, and a reason. The reason field in the passed authentications report shows the posture validation rule set selected, the policy that resulted in the returned system posture token, and the rule in the policy that was matched. If the attribute information is included in the passed authentications report, and these values are compared against the matched rule in the selected policy, the reason why the particular token was selected can be found. The application posture token field also contains any results from external policy validation servers.

Ordering of various policies, profiles and rules in this version of ACS is very critical. ACS performs its matching on a first-match basis not a best-match. As a result of this logic, it is necessary to think through the way in which ACS checks its policies, profiles and rules. Generally the most complex policies, profiles, and rules should appear first in the ordered lists. This prevents a complex authentication request from matching a simple network access profile and an incorrect authentication from taking place.

APPENDIXES

Appendix #1: Reference Documents

- Solution Documents
 - [Implementing NAC: Phase One Configuration and Deployment](#)
 - [NAC Technical Frequently Asked Questions \(FAQ\)](#)
 - [NAC Deployment Guide](#)
- NAC Component Documents
 - [Cisco Trust Agent \(CTA\) 2.0 Administrators Guide](#)
 - Cisco Secure Access Control Server (ACS) 4 User Guide
 - o http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_book09186a0080533dd8.html
 - Cisco VPN 3000 Concentrators
 - o [NAC Administration and Configuration, v4.7.1](#)
- Protocol Documents
 - EAP Flexible Authentication via Secure Tunneling (EAP-FAST)
 - [EAP-FAST, Internet Draft, April 2005](#)
 - RFC 2246: SSL
 - RFC 2616: HTTP
 - RFC 2617: HTTP digest authentication
 - RFC 2865: Remote Authentication Dial In User Service (RADIUS)
 - [Internet Assigned Numbers Authority](#) (IANA), [Protocol Numbers and Assignment Services](#)
 - RFC 2279: UTF-8, a transformation format of ISO 10646, January 1998.

Appendix #2: NAC Attribute Reference

Attribute Namespace

All NAC attributes are addressed by using a namespace based on the vendor and application type. Although each vendor and application type are represented by numbers within the EAP exchange, they are commonly referred to in the following format:

Vendor-ID: Application-Type: Attribute

The Vendor ID is a 32-bit field containing a globally unique vendor identifier. The high-order octet is 0, and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined by the [International Assigned Numbers Authority](#). The Vendor ID for Cisco Systems is 9.

The Application Type is a 16-bit field meaning a globally unique posture application type. The application types currently defined are:

Vendor	Application Type	Application Type Name	Description
*	1	PA	Posture Agent
*	2	Host	Host information
*	3	AV	Anti-Virus
*	4	FW	Firewall
*	5	HIPS	Host Intrusion Protection Service
*	6	Audit	Audit

32768-65535—Reserved for local use (this is intended for use by customers who write custom plugins or scripts to use in a single enterprise and that need not be globally unique.)

Attribute Data Types

Data Type	Operators	Description
OctetArray	=,!=	The data contains arbitrary data of variable lengths.
Integer32	=,<,>,! =, >=, <=	32-bit signed value, in network byte order.
Unsigned32	=,<,>,! =, >=, <=	32-bit unsigned value, in network byte order.
String	=,!=, >, <, >=, <=, contains, does not contain, start with, end with, regular-expression	<p>Derived from the OctetArray data type., This is a human readable string represented using the ISO/IEC IS 10646-1 character set with the UTF-8 transformation format [UTF8].</p> <p>Note 1: For information encoded in 7-bit US-ASCII, the UTF-8 character-set is identical to the US-ASCII character-set.</p> <p>Note 2: UTF-8 might require multiple bytes to represent a single character/code point; the length of an UTF8String in octets might be different from the number of characters encoded.</p>
IPv4Address	Wildcards and mask	Derived from the OctetArray data type. The IPV4Address <i>must</i> contain four octets, with the most significant octet first. i.e. "10.11.12.13" IPV4Address= 0A 0B 0C 0D
IPv6Address	Wildcards and mask	Derived from the OctetArray data type. The IPV6Address MUST contains 16 octets, with the most significant octet first.i.e. 0A0A:0B0B:0C0C:0D0D:0E0E:0F0F:1010:1111 IPV6Address= 0A 0A 0B 0B 0C 0C 0D 0D 0E 0E 0F 0F 10 10 11 11.
Time	=,<,>,! =, >=, <=	Derived from the Unsigned32 data type. Represents the number of seconds since January 1, 1970 00:00 UTC.

Data Type	Operators	Description
Version	=, <, >, !=, >=, <=	<p>Derived from the OctetArray Data Type. The 8 octets are broken into four 2-octet sets. The two most significant octets contains the major version, the next two octets contains the minor version, the last four octets contain 2 two-octet values are defined by the vendor. Traditionally, the third octet is a revision number and the last octet has the build number.</p> <p>Example: "3.5.1.350" has the value: 00 03 00 05 00 01 01 5E</p> <p>Note: All unused fields must be set to 0.</p>

Attribute Reference

The Application-Posture-Token (APT) AVP shows the result of validating posture request-response AVPs from a particular vendor and application type. This AVP is a Posture Notification AVP and can be sent across these interfaces in the NAC solution: Client API Posture Notification request, EAP-TLV Posture-Notification request, and HCAP Posture Validation response.

The System-Posture-Token (SPT) AVP shows the overall result of validating posture request-response AVPs from one or more vendors and application types. This AVP is a Posture Notification AVP and can be sent across these interfaces in the NAC solution: Client API Posture Notification request, EAP-TLV Posture-Notification request, and HCAP Posture Validation response.

Vendor (#)	App-Type (#)	Attribute Name	Attr #	Type	Value or Format
* (any)	* (any)	Application-Posture-Token	1	Unsigned32	0 = Healthy 10 = Checkup 15 = Transition 20 = Quarantine 30 = Infected 100 = Unknown
* (any)	* (any)	System-Posture-Token	2	Unsigned32	0 = HealthySystem 10 = Checkup 15 = Transition 20 = Quarantine 30 = Infected 100 = Unknown
Cisco (9)	PA	PA-Name	3	String	Name of the Posture Agent. For Cisco, this is Cisco Trust Agent
Cisco (9)	PA	PA-Version	4	Version	Format: major.minor.revision.build
Cisco (9)	PA	OS-Type	5	String	Name of the host operating system: Windows Server 2003 Datacenter Edition Windows Server 2003 Enterprise Edition Windows Server 2003 Web Edition Windows Server 2003 Standard Edition Windows XP Home Edition Windows XP Professional

Vendor (#)	App-Type (#)	Attribute Name	Attr #	Type	Value or Format
					Windows 2000 Datacenter Server Windows 2000 Advanced Server Windows 2000 Server Windows NT Workstation 4.0 Windows NT Server 4.0 Enterprise Edition Windows NT Server 4.0 Windows NT 4.0 Windows NT 3.51 Windows 95 Windows 95 OSR2 Windows 98 Windows 98 SE Windows Me
Cisco (9)	PA	OS-Version	6	Version	Version of host operating system. Format: major.minor.revision.build.
Cisco (9)	PA	User-Notification	7	String	Value contains one or more characters for example, <i>Your anti virus signature file is out-of-date. Please update your signature file from http://www.in-companyxyz..remediation-server.com.</i>
Cisco (9)	PA	OS-Kernel	8	String	Example: Linux 2.4.20-8 i386
Cisco (9)	PA	Kernel Version	9	Version	Version of host operating system., Format: major.minor.revision.build.
Cisco (9)	PA	Action	10		URL
Cisco (9)	OS	Machine-Posture-State	11		This attribute specifies the running state of the machine. 1—Booting 2—Running 3—Logged In
Cisco (9)	OS	ServicePacks	6	String	Example: ServicePack4
Cisco (9)	OS	HotFixes	7	String	Example: KB12345 Q21345
Cisco (9)	OS	HostFQDN	8	String	Example: xp1.nac.cisco.com
Cisco (9)	OS	Package	100	Extended Query Protocol	-
* (any)	AV	Software-Name	3	String	Name of the software product
* (any)	AV	Software-ID	4	Unsigned32	Numeral identifier of the software product
* (any)	AV	Version	5	Version	Version of the software

Vendor (#)	App-Type (#)	Attribute Name	Attr #	Type	Value or Format
* (any)	AV	Scan-Engine-Version	6	Version	Version of the AV scan engine
* (any)	AV	DAT-Version	7	Version	Value contains version of AV signature file, for example, 559.0.0.0, 4.5.2.0.
* (any)	AV	DAT-Date	8	Time	Release time of AV signature file
* (any)	AV	Protection-Enabled	9	Unsigned32	0 = Disabled 1 = Enabled
* (any)	AV	Action	10	String	Format and content are vendor-specific. Maximum length to be supported is 255 characters.
Cisco (9)	HIP	CSAVersion	5	Version	CSA Version
Cisco (9)	HIP	CSAOperationalState	9	Unsigned32	0 = Disabled 1 = Enabled
Cisco (9)	HIP	TimeSinceLastSuccessfulPoll	11	Unsigned32	-
Cisco (9)	HIP	CSAMCName	32768	String	-
Cisco (9)	HIP	CSAStatus	32769	String	Possible values delimited by ' ': global_testmode_on rootkit_detected ipforwarding_on
Cisco (9)	HIP	DaysSinceLastSuccessfulPoll	32770	Unsigned32	Example: 3

Appendix #3: RADIUS Attributes for NAC

The table lists all RADIUS attributes, including Cisco vendor-specific attributes (VSAs), relevant to NAC.

NAC-L2-802.1x	NAC-L2-IP	NAC-L3-IP	#	Attribute Name	Description
√			1	User-Name	Copied from EAP Identity Response in Access Request.
	√	√	8	Framed-IP-Address	IP address of host.
	√	√	26	Vendor-Specific Cisco (9,1) CiscoSecure-Defined-ACL	ACL name. Automatically sent by ACS.
√			26	Vendor-Specific Cisco (9,1) sec:pg	Policy-based ACL assignment. Only applies to Catalyst 6000. sec:pg = <group-name>
	√	√	26	Vendor-Specific, Cisco (9,1), url-redirect	Redirection URL. url-redirect=<URL>
	√	√	26	Vendor-Specific Cisco (9,1) url-redirect-acl	Apply the named ACL for the redirect URL; ACL must be defined locally on the NAD. Only works on switches with IOS. url-redirect-acl=<ACL-Name>

NAC-L2-802.1x	NAC-L2-IP	NAC-L3-IP	#	Attribute Name	Description
√	√	√	26	Vendor-Specific Cisco (9,1) posture-token	Posture token or state name. Automatically sent by ACS.
	√	√	26	Vendor-Specific Cisco (9,1) status-query-timeout	Sets Status Query timer.
	√	√	26	Vendor-Specific Cisco (9,1) host-session-id	Session identifier used for auditing. Automatically sent by ACS.
?	√	√	26	Vendor-Specific Microsoft = 311	Key for Status Query: MS-MPPE-Recv-Key Automatically sent by ACS.
√	√	√	27	Session-Timeout	Sets Revalidation Timer (in seconds).
√	√	√	29	Termination-Action	Action on Session Timeout (0) Default: Terminate session (1) Radius-Request: Re-authenticate
√			64	Tunnel-Type	13 = VLAN
√			65	Tunnel-Medium-Type	6 = 802
√	√	√	79	EAP Message	EAP Request/Response Packet in Access Request and Access Challenge: <ul style="list-style-type: none"> EAP Success in Access Accept EAP Failure in Access Reject
?	?	?	80	Message Authenticator	HMAC-MD5 to ensure integrity of packet.
√			81	Tunnel-Private-Group-ID	VLAN name

Appendix #4: ACS Digital Certificate Enrollment with Microsoft Windows 2000 Server Certificate Authority

Public key infrastructures (PKIs) require a certificate authority (CA) for scalable certificate deployments. Both the Microsoft Windows 2000 Server and the Windows 2003 Server have an optional certificate authority component for this purpose. These steps show you how to use a Microsoft Windows 2000 Server Certificate Authority to obtain the CA certificate and to request a digital certificate.

Obtain the Certificate Authority Public Certificate

Step 1. Open a new web browser instance, and connect to your local Microsoft Windows 2000 Server Certificate Authority by using the URL <http://ca.company.com/certsrv/>. You might be prompted for a valid username and password for authorization to obtain the CA certificate.

Step 2. When authorized, you see the dialog at the right. Select **Retrieve the CA certificate**, and then click **Next**.

Step 3. You are given an option to **Install this CA certification path** directly into your computer or to download it as a file. We recommend to **Download the CA certificate** as a file so that you can save and later distribute the CA certificate to all of your ACSes and clients.

Note: You can use either DER or Base64 encoding; both formats are supported.

Step 4. You can install it into any host computer running the Windows operating system by right-clicking on the certificate and choosing **Install Certificate**. You might want to save the certificate into the **Trusted Root Certification Authorities** store.

The image displays two screenshots of the Microsoft Certificate Services web interface. The top screenshot shows the 'Welcome' page with a 'Select a task' section where 'Retrieve the CA certificate or certificate revocation list' is selected. The bottom screenshot shows the 'Retrieve The CA Certificate Or Certificate Revocation List' page with the 'Install this CA certification path' option selected.

Microsoft Certificate Services -- ca [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- ☒ Retrieve the CA certificate or certificate revocation list
- ☐ Request a certificate
- ☐ Check on a pending certificate

[Next >](#)

Microsoft Certificate Services -- ca [Home](#)

Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate: [Current \[ca\]](#)

☐ DER encoded or ☒ Base 64 encoded

[Download CA certificate](#)

[Download CA certification path](#)

[Download latest certificate revocation list](#)

Request a Digital Certificate for ACS

- Step 5.** During the configuration of your ACS for NAC, you should have generated a certificate signing request (CSR) in the **System Configuration > ACS Certificate Setup > Generate Certificate Signing Request** screen. The CSR is simply a block of encoded text for the certificate authority to digitally sign with its private key.
- Step 6.** Open a new web browser instance, and connect to your local Microsoft Windows 2000 Server Certificate Authority by using the URL <http://ca.company.com/certsrv/>. You might be prompted for a valid username and password by the CA administrator to request a new certificate.
- Step 7.** Choose **Request a certificate**, and click **Next**.
- Step 8.** Because the ACS certificate is the same as a web server, choose **Advanced Request**, and click **Next**.

Choose Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file, and click Next.

Step 9. **Select, copy (CTRL-C), and paste (CTRL-P)** all of the CSR from ACS into the form, or you can **Browse** for the CSR as a saved file to upload it.

Step 10. Choose **Web Server** as the certificate template, and add any optional attributes for signing by the CA.

Step 11. Click **Submit** to finish your certificate request. Depending upon how your CA is configured, the request will be granted automatically, or you might need to wait for the CA administrator to approve your request.

Step 12. If your request is automatically approved, you can retrieve your new ACS certificate by choosing **Download CA certificate** with either DER or Base64 encoding. This is your ACS digital certificate containing the ACS public key as signed by the CA for authenticity.

The screenshot shows the 'Microsoft Certificate Services' web interface. The title bar says 'Microsoft Certificate Services -- ca' and there is a 'Home' link. The main heading is 'Submit A Saved Request'. Below this, it says: 'Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA)'. There is a text area labeled 'Base64 Encoded Certificate Request (PKCS #10 or #7):' containing a long string of base64-encoded text. Below the text area is a 'Browse for a file to insert.' button. Underneath is a 'Certificate Template:' section with a dropdown menu set to 'Web Server'. Below that is an 'Additional Attributes:' section with a text area and a 'Submit >' button at the bottom right.

Step 13. If your request must be approved, you must wait for approval from the CA Administrator. After the approval is granted, you can download the certificate by going back to the CA at <http://ca.company.com/certsrv/> and choosing **Check on a pending certificate**.

Appendix #5: Configuring 802.1x with NAC L2 IP

802.1x with NAC L2 IP Overview

One option for deploying NAC is to leverage an existing 802.1x supplicant to verify the identity credentials of the host and to allow the device to gain access to the network. Then you can use NAC L2 IP to check the posture credentials of the host. This layered approach might be necessary for one of these reasons.

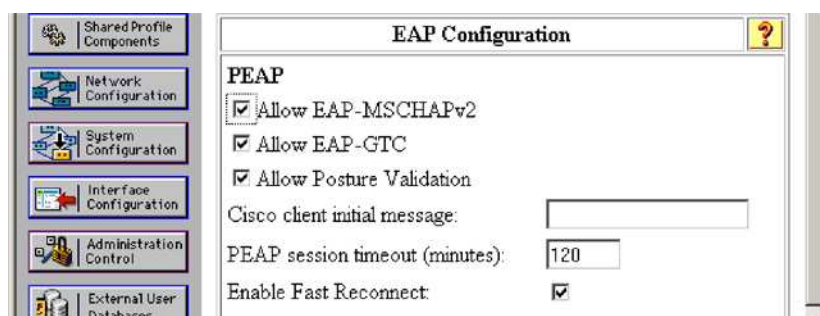
1. There is non-NAC enabled 802.1x supplicant already installed on the host, and NAC is being layered on top of the IBNS solution.
2. The network administrator requires identity and posture credential checks, but also wants to leverage the NAC audit features that are currently only supported in NAC L2 IP.

Task 1: ACS Configuration

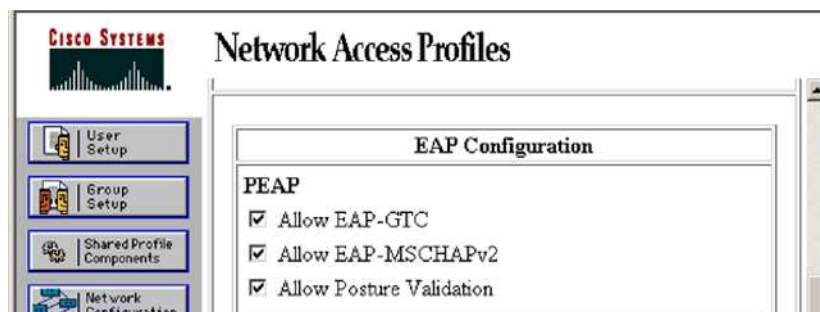
For authentication to a CiscoSecure ACS server to authenticate the 802.1x supplicant for identity credentials and CTA for posture credentials, the follow these steps:

Based on the configuration of ACS that was done in the previous section of this document, there are only a few things that need to be done to configure ACS to support authentication by the Microsoft 802.1x supplicant.

- Step 1.** First navigate to the System Configuration > Global Authentication Setup and make sure that EAP-MSCHAPv2 is selected. You must have this selected so that the EAP-MSCHAPv2 method is available in the network access profiles authentication settings. These settings are for *all* machine authentications. Therefore, you must select this method *must* if you are doing machine authentication with domain credentials (SID definition), because the authentication method for machine authentication must be the same for both machine and user authentication with the Microsoft 802.1x supplicant. If you use a third party 802.1x supplicant like Meetinghouse, you might want to select the EAP-GTC option to have that method available in the network access profiles. These settings are shown in the figure.

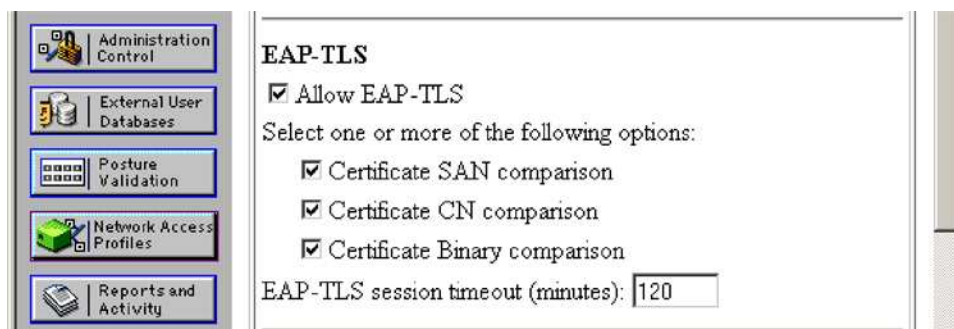


- Step 2.** Navigate to Network Access Profiles, and select the Authentication link of the NAC L2 IP network access profile. When in the NAC L2 IP authentication settings, scroll to the PEAP section in EAP Configuration, and make sure the EAP-MSCHAPv2 section is selected. Only EAP-MSCHAPv2 is relevant for the Microsoft 802.1x supplicant. If using a third-party supplicant, you can also select the EAP-GTC box to use that EAP method. The EAP selections are shown.



Note: If you would like to use EAP-TLS for authentication, you need to select the correct EAP-TLS settings within the System Configuration > Global Authentication Settings > EAP-TLS. You must select EAP-TLS, and select the correct certificate comparison options, as well as the EAP-TLS session timeout. As mentioned, these settings are for all machine authentications. Therefore, this method *must* be selected if you are doing machine authentication with certificates, because the authentication method for machine authentication must be the same for both machine and user authentication with the Microsoft 802.1x supplicant. The global EAP-TLS settings are shown here. It is very common to select all the available certificate comparison options to allow the maximum flexibility in comparing certificates.

Navigate to Network Access Profiles, and select the Authentication link of the NAC L2 IP network access profile. When in the NAC L2 IP authentication settings, scroll to the EAP-TLS section, and make sure EAP-TLS is selected.



Note: See the following document for guidelines on configuring machine and user certificates if you would like to use EAP-TLS for machine or user authentication. http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a008009256b.shtml

Task 2: Configure 802.1x with NAC L2 IP on the NAD Interface

Enabling 802.1x with NAC L2 IP requires very few steps on the switch.

Step 1. Enable 802.1x and assign an IP admission policy on the interface for the respective operating system.

For IOS:

```
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
 ip access-group 101 in
 dot1x port-control auto
 spanning-tree portfast
 ip admission NAC L2 IP
```

For 802.1x and NAC L2 IP on the Catalyst 6500 with CatOS.

```
set port dot1x 2/3 port-control auto
set port eou 2/3 auto
set spanntree portfast 2/3 enable
```

You can see that both 802.1x and NAC L2 IP have been configured on the port.

Appendix #6: Policy-Based ACL configuration

Dynamic authorization policy, in NAC2, is enforced by dynamic VLAN assignment. Any additional authorization enforcement needs to pre-exist on the switches, for instance, VACLs on the quarantine restricting access to remediation services. The one exception to this general-support model is the support on the Catalyst 6500 for the use of Policy-Based ACLs (PBACLs).

Policy-based ACLs are ACLs that are created dynamically with policy-based definitions in the ACE that represent groups of users within the infrastructure. These group definitions are expanded in the 6500 TCAM ACL implementation when the 6500 learns of a new IP address on a port. Once the 6500 learns of the new IP address, it looks at the group policy of the port and creates a specific ACE in the TCAM with the new IP address substituting for the group definition in the ACE. These group definitions are either static definitions (CLI-port based assignment) or dynamic definitions created through a RADIUS assignment.

In the context of NAC L2 802.1x the most common implementation is dynamic assignment of a port into a group based on the posture policy assigned from the ACS. PBACLs are not restricted to NAC L2 802.1x, PBACLs, are also supported with NAC L2 IP as a way to dynamically implement access control policy.

In this section, we show how the functionality of PBACLs is being used to create ACEs based on a healthy or a quarantine posture token being returned from ACS after a NAC L2 802.1x posture assessment has taken place. We are using the topology and NAC policies that were created earlier in the guide.

Specifically, group assignment is determined by the receipt of the Cisco VSA sec:pg. Earlier in the document, sec:pg definitions were created in the RADIUS Authorizations Components (RACs) for each of the posture tokens in NAC for NAC L2 IP. These same RACs can be used for NAC L2 802.1x when used with Catalyst 6500s. If the entire switching infrastructure is not Catalyst 6500s, network access filters are one way to classify a RADIUS request as coming from a 6500 and returning the appropriate sec:pg value. In practice, the network access filtering might not be necessary because a switch should ignore and drop any RADIUS attribute that it does not understand.

With this in mind, these RACs are created for all the 802.1x requests. The example shows the settings the RACs for NAC L2 802.1x can have in order to leverage PBACLs on the Catalyst 6500.

RAC Name	Assigned Attributes	Value
L2_1x_Healthy_RAC		
	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Healthy_hosts
L2_1x_Checkup_RAC		
	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Checkup_hosts
L2_1x_Transition_RAC		
	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Transition_hosts
L2_1x_Quarantine_RAC		

RAC Name	Assigned Attributes	Value
	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Quarantine_hosts
L2_1x_Infected_RAC	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Infected_hosts
L2_1x_Unknown_RAC	Session-Timeout (27)	300
	Termination-Action (29)	RADIUS-Request (1)
	cisco-av-pair (1)	sec:pg=Unknown_hosts

With these RACs PBACLs on the Catalyst 6500 must be group names that correlate to the values of sec:pg. For simplicity, only the healthy_hosts and quarantine_hosts values are used in the PBACL setup for the Catalyst 6500 in this guide.

You can see below in the PBACL, nac_pbacl, the configuration that will allow healthy_hosts to have unrestricted access to the network while quarantine_hosts will only have access to the 10.0.200.0/24 subnet which houses the remediation servers.

Note: These configurations assume that all the other NAC L2 802.1x configurations (RADIUS and 802.1x configuration) have been configured and are functioning.

These VLANs should already be configured and named on the Catalyst 6503. This is an example of how the VLAN is created and named in CatOS.

```
#assign vlan 50 and 80 to be the healthy and quarantine vlans
set vlan 50 name healthy type ethernet mtu 1500 said 100050 state active
set vlan 80 name quarantine type ethernet mtu 1500 said 100080 state active
```

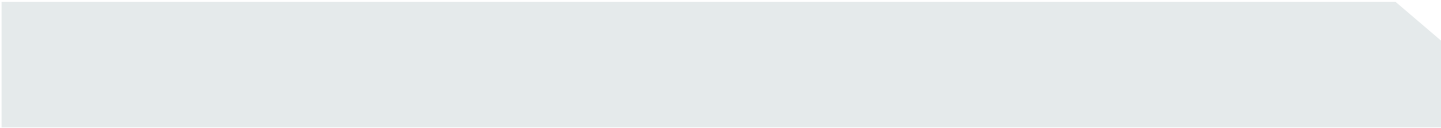
Delete any previously defined ACEs :

```
clear security acl all
```

Create the following PBACL:

```
#nac_pbacl
# allow the pbacl to inspect arp and dhcp for address information
set security acl ip nac_pbacl permit arp
set security acl ip nac_pbacl permit arp-inspection any any
set security acl ip nac_pbacl permit dhcp-snooping

# allow all vlans to access dns
set security acl ip nac_pbacl permit udp any any eq 53
```



```
# allow healthy hosts access to the network
set security acl ip nac_pbacl permit ip group healthy_hosts any
```



```

# allow quarantined hosts to access to the remediation servers and allow the
# remediation servers to communicate back to the quarantined hosts
set security acl ip nac_pbacl permit ip group quarantine_hosts 10.0.200.0 0.0.0.255
set security acl ip nac_pbacl permit ip 10.0.200.0 0.0.0.255 group quarantine_hosts

# allow quarantined hosts to communicate back and forth with the vlan's router
set security acl ip nac_pbacl permit ip group quarantine_hosts host 10.9.80.1
set security acl ip nac_pbacl permit ip host 10.9.80.1 group quarantine_hosts

# commit the security acl
commit security acl all

# map the pbacl to the healthy and quarantine vlans with statistics enabled
set security acl map nac_pbacl 50,80 statistics enable

```

These examples are show commands that depict a host that received a NAC L2 802.1x healthy posture and the subsequent contents of the Catalyst 6500 TCAM. This is followed by **show** commands that depict a host that received a NAC L2 802.1x quarantine posture and the subsequent contents of the 6500 TCAM.

In this example, a user on port 2/2 with the username cisco was authenticated, and received healthy posture, and then assigned to VLAN 50 with a group assignment of healthy_hosts. The DHCP assignment of 10.9.50.100 was snooped and added to the group table.

```
cat6500-nac (enable) show dot1x group all
```

Group Manager Info

Info of Group healthy_hosts

```
User Count = 1
```

Username	Mod/Port	UserIP	VLAN
cisco	2/2	10.9.50.100	50

Info of Group quarantine_hosts

```
User Count = 0
```

The following **show** command shows how the snooped IP address on port 2/2, 10.9.50.100 was added to the PBACL and inserted into the Catalyst 6500 TCAM with the proper substitution of the IP address for the keyword *healthy_hosts*.

```
cat6500-nac (enable) show security acl tcam interface 50
```

Input

```
IP
0. redirect arp (matches 4)
1. bridge udp any any fragment (matches 0)
2. redirect udp any any (matches 0)
3. bridge udp any any 53 (matches 17)
4. bridge ip host 10.9.50.100 any (matches 46)
   ^^^^^^^^^^^ - snooped IP address substituted for
   group "healthy_hosts"
5. deny ip any any (matches 26)
```

Output

```
IP
0. redirect (L3) arp (matches 0)
1. bridge udp any any fragment (matches 0)
2. redirect (L3) udp any any (matches 0)
3. bridge udp any any 53 (matches 0)
4. bridge ip host 10.9.50.100 any (matches 0)
   ^^^^^^^^^^^ - snooped IP address substituted for
   group "healthy_hosts"
5. deny ip any any (matches 0)
```

In the next example, a user on port 2/2 with the username cisco was authenticated, received quarantine posture, and then was assigned to VLAN 80 with a group assignment of quarantine_hosts. The DHCP assignment of 10.9.80.100 was snooped and added to the group table.

```
cat6500-nac (enable) show dot1x group all
```

Group Manager Info

Info of Group healthy_hosts

```
User Count   = 0
```

Info of Group quarantine_hosts

```
User Count   = 1
```

Username	Mod/Port	UserIP	VLAN
cisco	2/1	10.9.80.100	80

This **show** command shows how the snooped IP address on port 2/2, 10.9.80.100 was added to the PBACL and inserted into the Catalyst 6500 TCAM with the proper substitution of the IP address for the keyword *quarantine_hosts*.

```
cat6500-nac (enable) sho security acl tcam interface 80

Input
IP
0. redirect arp (matches 0)
1. bridge udp any any fragment (matches 0)
2. redirect udp any any (matches 0)
3. bridge udp any any 53 (matches 0)
4. bridge ip host 10.9.80.100 10.0.200.0 0.0.0.255 (matches 0)
    ^^^^^^^^^^^ - snooped IP address substituted for
                  group "quarantine_hosts"
5. bridge ip 10.0.200.0 0.0.0.255 host 10.9.80.100 (matches 0)
6. bridge ip host 10.9.80.100 host 10.9.80.1 (matches 0)
7. bridge ip host 10.9.80.1 host 10.9.80.100 (matches 0)
8. deny ip any any (matches 4)

Output
IP
0. redirect (L3) arp (matches 0)
1. bridge udp any any fragment (matches 0)
2. redirect (L3) udp any any (matches 0)
3. bridge udp any any 53 (matches 0)
4. bridge ip host 10.9.80.100 10.0.200.0 0.0.0.255 (matches 0)
    ^^^^^^^^^^^ - snooped IP address substituted for
                  group "quarantine_hosts"
5. bridge ip 10.0.200.0 0.0.0.255 host 10.9.80.100 (matches 0)
6. bridge ip host 10.9.80.100 host 10.9.80.1 (matches 0)
7. bridge ip host 10.9.80.1 host 10.9.80.100 (matches 0)
8. deny ip any any (matches 0)
```

Appendix #7: Microsoft Suppliant Configuration

This section is intended as a short guide on how to configure the Microsoft 802.1x suppliant. However, there are many other documents available online that also demonstrate this capability.

http://download.microsoft.com/download/b/0/e/b0e2a363-0044-4327-8f17-020818f57234/Wired_depl.doc

<http://www.microsoft.com/technet/community/columns/cableguy/cg1202.msp>

Use these instructions to set up a Windows XP or Windows 2000 client for 802.1x authentication:

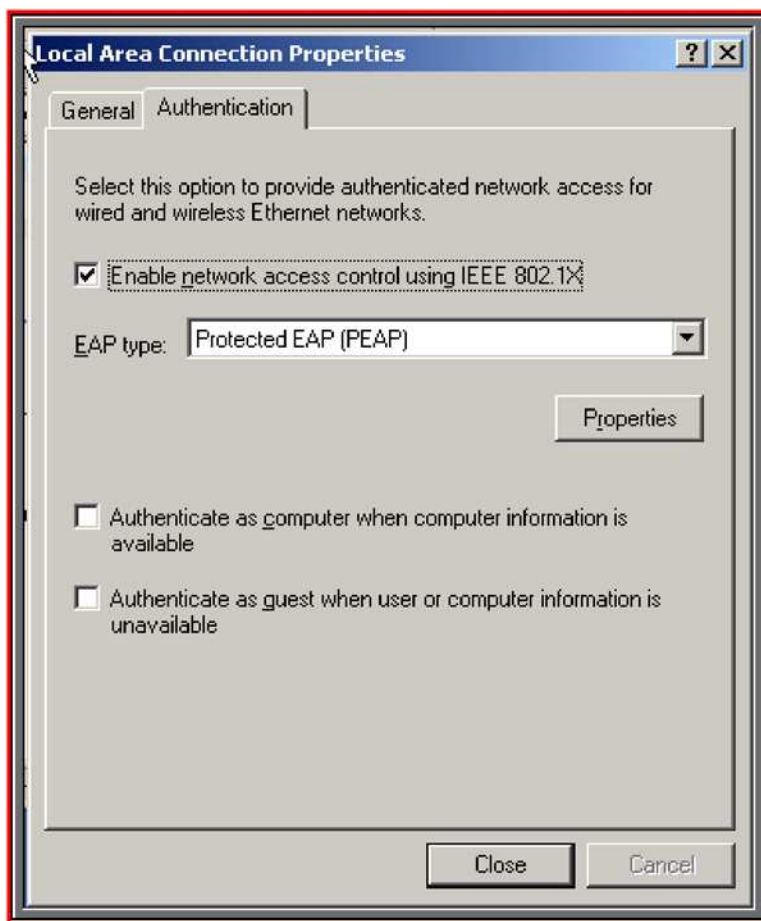
Step 1. On the end user's machine, open **Network Connections** (**Start menu > Settings > Network Connections**).

Step 2. Right click the connection, and select **Properties**.

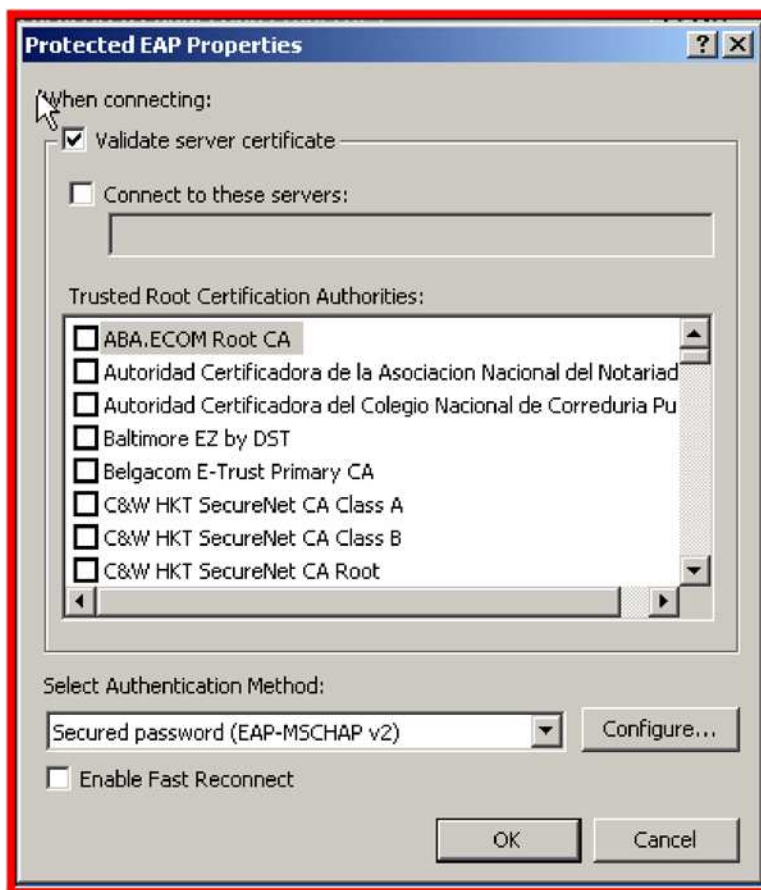
Step 3. In the General tab, verify that the *Show icon in notification area when connected* option is selected.

Step 4. In the Authentication tab, check the *Enable network access control using IEEE 802.1x* check box. Select **Protected EAP (PEAP)** as EAP type.

Step 5. Click **Properties** under the drop-down box for EAP type. The figure shows the resulting window.



Step 6. By default, the *Validate Server Certificate* box is checked. This causes the supplicant to verify that the server certificate presented has not expired, has the correct signature, and has a trusted root certificate authority. You then need to specify the server or servers to which the computer will automatically connect and the trusted root certification authorities. For simplicity and the purposes of this guide, you can leave this box is unchecked. The figure shows the Validate Server Certificate window.



Step 7. If you select the **Configure** button of the Secured password (EAP-MSCHAP v2), you could specify whether to use the user name and password (and domain, if applicable) that you enter in the Windows logon screen for authentication, and click OK. In other words, this could allow separate user authentication for network access compared to access to an Active Directory domain.

Step 8. Again for simplicity, a classic AD deployment is assumed, the default condition is demonstrated here, and is depicted in the figure below.



Step 9. Assuming the above measures have been deployed at a minimum, 802.1x authentication can successfully be deployed.

To specify that a computer attempt authentication to the network if user information or computer information is not available, you can check the **Authenticate as guest when user or computer information is unavailable** check box. This check box is checked by default. As a possible fallback mechanism to Microsoft AD, you could configure this option to allow authenticated guest accounts to login to the computer when an AD domain might not be available. The computer will try to logon to the network with a null username and password. We recommend for ACS deployments that this feature be turned off due to the way switches respond to these EAPOL frames from supplicants. With this feature enabled by default, switch ports that plug in to supplicants will stay in an *authenticating* state until correct user credentials are applied. With this feature disabled on the supplicant, a switch port will stay in “connected” state, which is expected operation.

To specify that the computer attempt authentication to the network even if a user is not logged on, check the **Authenticate as computer when computer information is available** check box. If you have it enabled on the supplicant, but *not* in ACS, authentication fails, and ports are placed in *held* state upon reboot of the supplicant (for example). This can increase login times (for a supplicant to wait until timers expire to try and re-authenticate with user credentials).

This feature can provide quicker times for logging into an Enterprise AD domain, because machine authentication should have already taken place. Specifically, upon restart or power on of a supplicant, machine authenticated occurs on a port before a logon screen even appears. When a user then logs into the machine, credentials for logging into the domain can then be accessed immediately, followed by a re-authentication of 802.1x based on the user credentials. In contrast, if the above feature is disabled, the client depends on standard user authentication (assuming it was not setup in ACS before). Logging into the domain has to time out before user credentials are authenticated. This increases authenticated login times to a domain. We recommend that you run machine authentication because it provides quicker login times to Enterprise AD domains. We also recommend that the options for authenticating to the network *as guest* not be used. (in the default condition this feature is enabled).

Appendix #8: Acronyms and Terms

Acronym	Description
ACE	Access Control Entry
ACK	Acknowledgement
ACL	Access Control List
ACS	Access Control Server
AD	Active Directory (Microsoft)
AID	Authority Identity
AP	Access Point
API	Application Programming Interface
ARP	Address Resolution Protocol
AV	Antivirus
CAM	Clean Access Manager (CCA)
CAS	Clean Access Server (CCA)
CCA	Cisco Clean Access
CDP	Cisco Discovery Protocol
CHAP	Challenge Handshake Authentication Protocol
CSA	Cisco Security Agent

Acronym	Description
CTA	Cisco Trust Agent
CTASI	CTA Scripting Interface
DB	Database
DC	Domain Controller (Microsoft)
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name Service
DoS	Denial of Service
DOT1X	IEEE 802.1X
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EAPoRADIUS	EAP over RADIUS
EAPoUDP	EAP over UDP
EOU	EAP Over UDP
FAST	Flexible Authentication Secure Tunnel
GAME	Generic Authorization Message Exchange
GINA	Graphical Identification and Authentication (Microsoft)
GPO	Group Policy Object (Microsoft)
GTC	Generic Token Card
HA	High Availability
HAL	Hardware Abstraction Layer
HCAP	Host Credential Authentication Protocol
HIPS	Host Intrusion Prevention System
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secured
IAS	Internet Access Server (Microsoft)
IBNS	Identity Based Networking Services
IDS	Intrusion Detection System
IID	Initiator Identity
IOS	Internetworking Operating System
IP	Internet Protocol
L2	Layer 2
L2TP	Layer 2 Tunneling Protocol
L3	Layer 3
LAN	Local Area Network

Acronym	Description
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MITM	Man In The Middle
MS	Microsoft
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MVAP	Multi VLAN Access Ports
NAC	Network Admission Control
NAD	Network Access Device
NAF	Network Access Filter
NAH	NAC Agentless Host
NAK	Negative Acknowledgement
NAR	Network Access Restriction
NAT	Network Address Translation
NDIS	
NDS	Netware Directory Services (Novell)
NRH	Non Responding Host
NTLM	
ODBC	Open Database Connect
OOB	Out Of Band
OS	Operating System
OTP	One Time Password
PA	Posture Attribute
PAC	Provisioned Access Credential
PACL	Port ACL
PAE	Port Access Entity
PBACL	Policy Based ACL
PEAP	Protected EAP
PKI	Public Key Infrastructure
PPTP	
PVLAN	Private VLAN
QoS	Quality of Service
RAC	RADIUS Attribute Component
RPC	Remote Procedure Call
SAML	Security Assertion Markup Language
SIMS	Security Information Management System

Acronym	Description
SLB	Server Load Balancing
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SQ	Status Query
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
TLS	Tunnel Layer Security
TLV	Type Length Value
UDP	Universal Datagram Protocol
URL	Universal Resource Locator
VACL	VLAN ACL
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VSA	Vendor Specific Attribute
VVID	Voice VLAN Identifier
WAN	Wide Area Network
WEP	Wireless Encrypted Protection
WLAN	Wireless LAN
WoL	Wake on LAN

Term	Definition
802.1X, dot1x	IEEE 802.1X. The standard for layer 2 network authentication. It should not be confused with 802.11a/b/g which is for wireless networking.
AAA	Authentication, Authorization, and Accounting. Typically this refers to authorization of users for network access including dial-up, wireless, VPN, or 802.1X. The central server that aggregates one or more authentication and/or authorization decisions into a single system authorization decision, and maps this decision to a network access profile for enforcement on the NAD.
Access-Accept	Response packet from the RADIUS server notifying the access server that the user is authenticated. This packet contains the user profile, which defines the specific AAA functions assigned to the user.
Access-Accept	Response packet from the RADIUS server notifying the access server that the user is authenticated. This packet contains the user profile, which defines the specific AAA functions assigned to the user.
Access-Challenge	Response packet from the RADIUS server requesting that the user supply additional information before being authenticated.
Access-Reject	Response packet from the RADIUS server notifying the access server that the user is not authenticated.
Access-Request	Request packet sent to the RADIUS server by the access server requesting

Term	Definition
	authentication of the user.
Accounting	Accounting in network management subsystems are responsible for collecting network data relating to resource usage.
ACE	Access Control Entry—An ACL Entry contains a type, a qualifier for the user or group to which the entry refers, and a set of permissions. For some entry types, the qualifier for the group or users is undefined.
ACL	Access Control List.
ACS	Access Control Server or Cisco Secure Access Control Server.
APT	Application Posture Token. The result of a compliance check for a given vendor's application, which represents the health of that component. All APTs from a posture validation are merged by the primary PVS to create the SPT.
APT, Application Posture Token	The result of a posture validation check for a given vendor's application.
Audit Server	The server that can determine the posture credentials of a host without relying on the presence of a PA on the host. The server must be able to determine the posture credentials of a host and act as a posture-validation server.
Authentication	In network management security, the verification of the identity of a person or a process.
Authorization	The method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.
AVP	Attribute-value pair.
CSA, Cisco Security Agent	Cisco Security Agent provides threat protection for server and desktop computing systems. It aggregates multiple security functionality, combining host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent package. As part of an overall security strategy, Cisco Security Agent enhances Network Admission Control and the SAFE blueprint and extends protection to the endpoint.
CSM	Cisco Security Manager
CS-MARS	Cisco's Mitigation and Response System (CS-MARS) family of high performance, scalable appliances for threat management, monitoring and mitigation, enable customers to make more effective use of network and security devices by combining network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification and automated mitigation capabilities.
CTA	Cisco Trust Agent. Cisco product instance of the PA. Includes a PA posture plugin.
CTA, Cisco Trust Agent	Cisco's implementation of the posture agent is called the CTA and includes the embedded wired-only supplicant
CTASI	CTA Scripting Interface
DAI	Dynamic ARP Inspection
DHCP Snooping	<p>DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table.</p> <p>DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the</p>

Term	Definition
	end user and trusted interfaces connected to the DHCP server or another switch. DHCP snooping builds a DHCP binding table containing client IP address, MAC address, port, VLAN number, lease and binding type. The feature can be enabled on a particular VLAN on the switch. The switch intercepts all DHCP messages bridging within the Layer 2 VLAN domain.
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a TLS based RFC3748 compliant EAP method. EAP-FAST uses symmetric key algorithms to achieve a tunneled authentication process. The tunnel establishment relies on a Protected Access Credential (PAC) that can be provisioned and managed dynamically by EAP-FAST through AAA server.
EAP-FAST	EAP Flexible Authentication via Secure Tunneling.
EAP-GTC	EAP Generic Token Card
EAPOL	EAP over LAN
EAP-TLS	EAP Transport Layer Security
Endpoint	Any machine attempting to connect or use the resources of a network.
EoU, EAPoUDP	Extensible Authentication Protocol over User Datagram Protocol.
GAME	Generic Authorization Message Exchange.
GINA	Graphical Identification and Authentication (Microsoft)
HCAP	Host Credential Authorization Protocol.
Host	Another name for an endpoint device
Host	Any machine that attempts to connect to or use the resources of a network. Also referred to as a "host".
IID, Initiator Identity	For machine authentication, the IID is the FQDN of the host. (i.e. jdoe-pc.cisco.com). For user authentication the IID is a username. (i.e. jdoe)
MAB	MAC Authentication Bypass (MAC-Auth-Bypass)
Machine Authentication	The machine identity used for authentication is the actual name of the computer as it exists in the Active Directory. The credentials used to authenticate the computer can be password-based or PKI certificate-based, depending on the EAP type used.
MSCHAPv2	
NAC	Network Admission Control. NAC is a Cisco Systems sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms. NAC is part of the Cisco Self-Defending Network, an initiative to increase network intelligence in order to enable the network to automatically identify, prevent, and adapt to security threats.
NAC L2 802.1X	Cisco implementation of the 802.1X protocol on CatOS and IOS switches.
NAC L2 IP	Layer 2 EAP over UDP support for Cisco switches
NAC L3 IP	Layer 3 EAP over UDP support for Cisco routers
NAD	Network Access Device. A network access device acts as a policy enforcement point for the authorized network access privileges granted to an endpoint device.

Term	Definition
NAD, Network Access Device	A network access device acts as a policy-enforcement point for the authorized network-access privileges that are granted to a host.
NAF, Network Access Filter	A NAF is a named group of any combination of one or more of the following network elements: IP addresses, AAA clients (network devices), or Network device groups (NDGs). Using a NAF to specify a downloadable IP ACL or Network Access Restriction based on the AAA clients by whom the user may access the network saves you the effort of listing each AAA client explicitly.
NAH	NAC Agentless Host
NAH, NAC Agentless Host	A host that does not have an 802.1X supplicant or CTA installed to perform posture validation.
NDG, Network Device Group	A collection of network devices that act as a single logical group.
NRH	Non-Responsive Host
PA	Posture Agent. An application that serves as the single point of contact on the endpoint for aggregating posture credentials from potentially multiple posture plugins and communicating with the network. Cisco's posture agent is the Cisco Trust Agent (CTA).
PA, Posture Agent	An application that serves as the single point of contact on the host for aggregating posture credentials from potentially multiple posture plugins and securely communicating them to the network.
PAC	Protected Access Credential
PDP, Policy Decision Point	Provides facilities for policy management and conditional filters.
PEAP	Protected EAP
PEAP-GTC	
PEP, Policy Enforcement Point	ACS acts as the policy enforcement point for policy management.
plugin, posture plugin	A third-party DLL that provides host posture credentials to a posture agent on the same endpoint for endpoint posture validation and network authorization.
Posture	Current host status and configuration. This can include things like antivirus levels, hotfixes, OS types, etc.
posture agent	An application that serves as the single point of contact on the endpoint for aggregating posture credentials from potentially multiple posture plugins and communicating with the network. Cisco's posture agent is the Cisco Trust Agent (CTA).
posture credentials	State information of an endpoint device at a given point in time representing hardware and software (OS and application) information.
posture credentials	State information of a network endpoint at a given point in time that represents hardware and software (OS and application) information.
posture plugin	A third-party DLL that provides host posture credentials to a posture agent on the same endpoint for endpoint posture validation and network authorization.
posture validation	The authorization of an endpoint device's posture credentials by one or more posture validation servers and their associated compliance policies.
posture validation	The authorization of a network endpoint's posture credentials by one or more posture-

Term	Definition
	validation servers and their associated compliance policies.
posture validation server	A posture validation server acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials against a set of policy rules.
PP	Posture Plugin.
PV	Posture Validation. Validates the collection of attributes that describe the general state and health of the user's machine (the "host").
PV	Posture Validation. Validates the collection of attributes that describe the general state and health of the user's machine (the "host").
PVS, Policy Server, Vendor Policy Server, Posture Validation Server, External Posture Validation Server	A Cisco or third-party server used to perform posture validation. A posture-validation server acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials against a set of policy rules.
PVS, Posture Validation Server, Policy Server, Vendor Policy Server, External Posture Validation Server	A Cisco or third-party server used to perform posture validation. A posture-validation server acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials against a set of policy rules.
RAC	RADIUS Attribute Component.
RADIUS	Remote Authentication Dial-In User Service is a widely deployed protocol enabling centralized authentication, authorization, and accounting for network access.
SCM	Switchport Configuration Manager
SDM	Security Device Manager
SPT	System Posture Token. The result of aggregating one or more application posture tokens into a single compliance result for an endpoint device. This is the final posture state resulting from the posture validation of an endpoint.
SPT, System Posture Token	The result of aggregating one or more application posture tokens into a single posture validation result for an Host.
Token: Check-up	Host is within policy but an update is available. Used to proactively remediate a host to the Healthy state.
Token: Healthy	Host is compliant; no restrictions on network access.
Token: Infected	Host is an active threat to other hosts; network access should be severely restricted or totally denied all network access.
Token: Quarantine	Host is out of compliance; restrict network access to a quarantine network for remediation. The host is not an active threat but is vulnerable to a known attack or infection
Token: Transition	Host posturing is in process; give interim access pending full posture validation. Applicable during host boot when all services may not be running or audit results are not yet available.
Token: Unknown	Host posture cannot be determined. Quarantine the host and audit or remediate until a definitive posture can be determined. May also
User Authentication	Method in which user information is verified over 802.1X at the time of login. User

Term	Definition
	Authentication can be performed through either the users active directory (domain) credentials or through credentials provided with a client-side certificate.
VSA, Vendor Specific Attribute	Most vendors use the VSA to support value-add features.



Corporate Headquarters

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

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

206616.F_ETMG_KL_1.06