

Cisco Network Admission Control and Microsoft Network Access Protection

Configuration and Troubleshooting Guide

Version 1.0



Introduction

The purpose of this guide is to provide the details necessary for configuring and testing the Cisco[®] Network Admission Control (NAC) and Microsoft Network Access Protection (NAP) integration solution (referred to here as NAC-NAP). This guide provide configuration details for all components of the NAC-NAP solution, including the Microsoft Vista client, Cisco Secure Access Control Server (ACS) for Windows, Cisco network access devices (NADs), Microsoft Network Policy Server (NPS), and required components.

Cisco Network Admission Control and Microsoft Network Access Protection Integration Overview

The Cisco NAC and Microsoft NAP solutions together provide the capability to gather identity and posture information from an endpoint, determine the security policy compliance of the endpoint, provide remediation services, and enforce network access policies based on the compliance of the endpoint.

With the integration of these two solutions, an administrator can verify the health status of a Microsoft Vista client, provide remediation capabilities, and provide dynamic policy enforcement on the network infrastructure.

The NAC-NAP solution components include Cisco Secure Access Control System (ACS) version 4.2, Cisco 802.1X-capable Catalyst Switches, Microsoft Network Policy Server (NPS), and Microsoft NAP-enabled Vista operating system. The Cisco NAC Appliance does not support NAP at this time and is not part of the solution.

- For additional information about the Cisco NAC solution, see <u>http://www.cisco.com/go/nac.</u>
- For additional information about the Microsoft NAP solution, see http://www.microsoft.com/nap.

Topology

The initial deployment examples include the following components for NAC-NAP (Figure 1): Microsoft Windows 2003 Server running Cisco Secure ACS, Microsoft Active Directory, certificate authority (CA), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), a Cisco switch, a Microsoft Vista client, and Microsoft Windows Server 2008 running Microsoft NPS, Host Credential Authorization Protocol (HCAP), and Microsoft Internet Information Server (IIS). This setup includes support for IEEE 802.1x assessment methods and HCAP integration between Cisco Secure ACS and Microsoft NPS. Note that when the HCAP server is installed on Windows Server 2008, the Microsoft NPS and IIS components are also installed.

This topology also includes support for IEEE 802.1x (NAC Layer 2 IEEE 802.1x) network connection methods. Cisco Secure ACS acts as the Cisco network policy server. The Microsoft NPS acts as the posture validation server. The Microsoft NPS and the Cisco Secure ACS communicate posture data through HCAP.



Figure 1. Basic Topology for NAC-NAP Interoperability Architecture

Configuration Scenarios

IEEE 802.1x Method

The IEEE 802.1x deployment scenario uses IEEE 802.1x with Extensible Authentication Protocol– Flexible Authentication via Secure Tunneling (EAP-FAST) as the assessment method and provides policy enforcement through dynamic VLAN assignment on the switch. Initially, two VLANs will be configured on the switch for support with IEEE 802.1x: a healthy VLAN and a quarantine VLAN (Figure 2).





After the client is connected to the switch port, IEEE 802.1x authentication will occur when a link is detected and before the IP address is assigned to the client. After the initial IEEE 802.1x authentication between the client and the switch, the client will authenticate to Cisco Secure ACS using the EAP-FAST protocol. Cisco Secure ACS will be configured to receive the Windows health information using EAP-FAST and will send this to the Microsoft NPS over the HCAP protocol.

The initial policy to determine client health will be evaluation of whether Microsoft Windows Firewall is enabled on the Vista client. If Microsoft NPS determines that the firewall is enabled, a posture state of healthy is reported to the Cisco Secure ACS over HCAP. Because the host is deemed to be compliant, or "healthy," the healthy policy will be assigned to the client. With this policy, the client will dynamically be placed in the healthy VLAN and granted full network access. If Microsoft NPS determines that the firewall is disabled, two options are available. The host can be quarantined indefinitely, until the firewall is manually reenabled and the client health state changes to healthy; or the firewall can be enabled automatically through Microsoft NPS remediation, and the client status will change from quarantine to healthy automatically.

NAC-NAP Network Hardware Requirements

Supported Cisco Catalyst Switch Platforms

Table 1 lists the Cisco Catalyst[®] switch platforms that NAC-NAP supports.

Table 1. Switch Platforms Supported by NAC-NAP

Platform (Supervisor)	ОЅ Туре	OS Version
Cisco Catalyst 6500 Series Supervisor Engines 32 and 720	Cisco IOS [®] Software	Cisco IOS Software 12.2 (33) SXH or later
Cisco Catalyst 6500 Series Supervisor Engines 2, 32, and 720	Cisco Catalyst OS	Cisco Catalyst OS 8.6 (1) or later
Cisco Catalyst 4500 Series Supervisor Engine II- Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE	Cisco IOS [®] Software	Cisco IOS Software 12.2 (37) SG or later
Cisco Catalyst 4900 Series Switches	Cisco IOS [®] Software	Cisco IOS Software 12.2 (35) SE or later
Cisco Catalyst 3570 and 3560 Series Switches	Cisco IOS [®] Software	Cisco IOS Software 12.2 (35) SE or later
Cisco Catalyst 2960 Series Switches	Cisco IOS [®] Software	Cisco IOS Software 12.2 (35) SE or later

For more information, please refer to following release note

http://www.cisco.com/en/US/netsol/ns812/networking_solutions_sub_solution_home.html.

NAC-NAP Client Requirements

Table 2 lists the requirements for NAC-NAP clients.

Table 2. Client Requirements

Platform	Version	Cisco Requirement	Comments
Windows	Vista (Business, Enterprise, Ultimate)		Service Pack 1 is a prerequisite for the NAC-NAP interoperability architecture. Service Pack 1 adds critical enhancement to supplicants, and those features are required for NAC-NAP interoperation.
		Cisco EAP-FAST Module	For the NAC-NAP interoperability architecture, Windows Vista must have the Cisco EAP-FAST software module installed.

Note: Cisco Trust Agent is not required for clients with the Microsoft Vista OS.

NAC-NAP Server Requirements

The minimum number of computers need for this testing is three. The recommended machine configurations are summarized in Table 3. The addition of more machines can make testing and debugging easier.

Table 3.	Server	Requirements

Server Type	OS	Function	
Domain controller	Windows Server 2003 or 2008	The domain controller provides Microsoft Active Directory policy, DHCP server, DNS server, and root CA.	
Microsoft NPS	Windows Server 2008	Microsoft NPS is the policy configuration point for NAP health validation.	
Cisco Secure ACS 4.2	Cisco Secure ACS installed on a domain member server running on Microsoft Windows 2000 Server, Windows Server 2003, Windows Server 2008, or Cisco Secure ACS Solution Engine Version 4.2	Cisco Secure ACS is the central policy configuration point for NAC-NAP integration. Cisco Secure ACS will provide secure connection to clients and proxy health information to Microsoft NPS.	

Admission Control Predeployment Checklist

This checklist provides a guide to the components, technologies, and organizational efforts required for a successful NAC-NAP deployment.

Security Policy Creation and Maintenance

- What are your current security policies for each of these domains?
- Who (and what) is responsible for policy creation? Policy enforcement?
- What is the quorum for making changes?
- · Will network access authorizations be based on identity or posture, or both?
- What is your policy on unmanaged and nonstandard machines on your network (labs, guests, consultants, extranets, kiosks, etc.)?
- How will you handle acquisitions that may have a different network infrastructure and policy?

Public Key Infrastructure

- Have you already deployed an enterprise public key infrastructure (PKI)? Windows 2000 Server or later, a CA vendor, or other?
- If not, will you install and manage one or purchase individual certificates from a CA vendor?
- Do you understand the long-term support, migration, and scaling requirements of selfsigned certificates?

Directory Services

- Do you or will you require identity for network authorization?
- Have you already deployed directory services: Microsoft Active Directory, LDAP, or other?
- Will your existing installation scale to support the added queries or are more servers needed?

Network Access Devices

- A NAD acts as a policy-enforcement point for the authorized network access privileges that are granted to a host. Does your existing hardware support the desired NAC functions? Do you need to upgrade?
- Is a new Cisco IOS Software or Cisco Catalyst OS license required for the security (crypto) images?
- Do these NADs have enough memory for the larger Cisco IOS Software security images?
 Do you need a memory upgrade?
- Can these NADs run the NAC-supported versions of Cisco IOS Software and Cisco Catalyst OS or is another NAD required?

Hosts and Other Network-Attached Devices

- Do you already use IEEE 802.1x supplicants from Microsoft, Cisco, or some other vendor on a platform other than Windows Vista?
- Will an IEEE 802.1x upgrade require a supplicant purchase, OS upgrade, or hardware upgrade (printers, etc)?
- Do you need wired or wireless IEEE 802.1x supplicant functions? (The Cisco free supplicant is wired only.)

 Which authentication types are required? (The NAC-NAP Version 1 solution supports only EAP-FAST with EAP–Transport Layer Security [EAP-TLS], EAP–Generic Token Card [EAP-GTC], and EAP–Microsoft Challenge-Handshake Authentication Protocol Version 2 [EAP-MSCHAPv2] inner authorization methods.)

Nonresponsive Hosts

- Do you have nonresponsive hosts (NRHs)? Generally, an NRH is a host that does not have an IEEE 802.1x supplicant or NAP agent running to perform posture validation.
- Have you identified all of the NRH device types in your network:
 - No IEEE 802.1x supplicant (unsupported or hardened OS)
 - NAP agent disabled or not supported (unsupported OS or network boots)
 - · Otherwise unmanaged or uncontrolled devices (guests, labs, etc.)
- What is your authorization strategy for NRHs?
- Do you need to upgrade to IEEE 802.1x capabilities in your hardware or OS?
- Will you use whitelisting in Cisco Secure ACS (MAC authentication bypass [MAP] and MAC or IP wildcards)?
- Do you know the administrative and management costs of a MAP, host registration, and guest system?

Cisco Secure ACS

- Do you already use Cisco Secure ACS? Will you need to upgrade or purchase it?
- How many Cisco Secure ACSs will you need to scale the deployment based on your organization size, availability requirements, revalidation frequency, and policy size?
- How will you replicate the Cisco Secure ACS database and configuration changes: manually, periodically, scheduled, or instantly?
- Will any load-balancing hardware or software be necessary to handle a high volume of concurrent authorizations?

Third-Party Software Integration

- What existing desktop security software do you want to integrate with NAC-NAP?
- · What new client software do you want to deploy because of NAC-NAP?
- Do you have the required version for NAC integration? Or is an upgrade, new purchase, or replacement required?

Patch Management

- What update, patch, or remediation software do you currently use, if any?
- Does this update software integrate with NAC-NAP?
- Will you have a remediation website for communicating the posture status to unhealthy or nonresponsive hosts?
- Will you distribute software to employees and guests from this site? How will you handle licensing?

Monitoring, Reporting, and Troubleshooting

- What is your existing monitoring and reporting framework?
- Will NAC logs and events integrate? Or is something additional needed?
- Do you have sufficient long-term storage space for all of these new logs and events?

Communications

- Have you communicated the solution to the organization for the various stages: awareness (need and benefits), readiness (what and when), and adoption (monitoring and enforcement)?
- How will you communicate: email, internal news, remediation website, support desk, etc.?

Support Desk

- · Have you set up staff training for the new technology and processes?
- How will the support staff troubleshoot support calls related to NAC-NAP?
- What application development is required to resolve NAC-related issues?
- Have you reviewed the troubleshooting steps (list of required logs for opening cases, etc.)?

Configuration for NAC-NAP Integration

The following sections provide the details necessary for configuring all the Cisco NAC and Microsoft NAP solution components in the scenarios described here.

The following servers and other hardware are required and will need to be installed and configured for the NAC-NAP interoperability solution:

- Cisco Secure ACS 4.2 for Windows (Microsoft Windows Server 2008, Windows Server 2003, or Windows 2000 Server)
- Microsoft Windows Server 2008 (HCAP server including Microsoft NPS and IIS)
- Microsoft Windows Vista (Service Pack 1 is required)
- NAC-compatible Cisco Catalyst switch (such as the Cisco Catalyst 3750 Series Switch)

In addition, the network device will need to be configured to support the NAC-NAP solution. In the lab, a switch will be used for to implement IEEE 802.1x for wired connections.

Cisco Secure ACS Base Configuration

The NAC-NAP configuration will begin with the Cisco Secure ACS to establish the base functions to develop policies for the solution. After installing Cisco Secure ACS, use the following steps to create the Cisco Secure ACS configuration for NAC-NAP.

Network Configuration

Task 1: Configure AAA Clients

On the Network Configuration page, you can add and configure authentication, authorization, and accounting (AAA) clients (network access devices, such as switches and wireless access points) and remote AAA servers.

- Step 1. On the Network Configuration screen, click the hyperlink under Network Device Group. Click (Not Assigned) and move to the (Not Assigned) AAA Client screen.
- Step 2. Configure the AAA clients by clicking the Add Entry button. You can define all NADs as a single AAA client using IP address wildcards. Shared Secret is an identical key string that you define for a switch RADIUS configuration. For Authenticate Using, be sure to select RADIUS (Cisco IOS/PIX 6.0). The following screenshot shows a sample configuration.

AAA Client Setup for NAD			
AAA Client IP Address	*.*.*	•	
Shared Secret	cisco1	cisco123	
Network Device Group	(Not Assigned)		
RADIUS Key Wrap			
Key Encryption Key		000000000000000000000000000000000000000	
Message Authenticator Code Key 0000000000000000000000000000000000			
Key Input Format		○ ASCII ③ Hexadecimal	
Authenticate Using	RADIU	IS (Cisco IOS/PIX 6.0)	
🔲 Single Connect TACA	CS+ AAA C	lient (Record stop in accounting on failure)	
🗹 Log Update/Watchdo	g Packets f	from this AAA Client	
🔽 Log RADIUS Tunneling) Packets fi	rom this AAA Client	
📃 Replace RADIUS Port	info with U	sername from this AAA Client	
🔲 Match Framed-IP-Add	dress with u	user IP address for accounting packets from this AAA Client	

Step 3. Click Submit + Apply to save the changes.

Note: AAA client definitions with wildcards cannot overlap with other AAA client definitions, regardless of the authentication types. When adding more AAA clients with a different authentication type, avoid using wildcards and specify the AAA client IP address as needed.

Task 2: Configure AAA Servers

The AAA server information is populated with the hostname and IP address of the device on which Cisco Secure ACS is installed. In this configuration guide, the server name **id-acs** and IP address **10.1.100.2** are configured. If the server has been assigned a different name, it will be displayed as the AAA server name with current active IP address.

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

Step 1. Configure the Key setting for the AAA server as shown in the following screenshot. Choose Network Configuration > Network Device Group > (Not Assigned) and click the AAA server name hyperlink id-acs. This shared secret key is used by the remote AAA server and Cisco Secure ACS to encrypt the data. The key must be configured identically in the remote AAA server and the local Cisco Secure ACS, including case sensitivity.

AAA Server IP Address	10.1.100.2
Кеу	cisco123
Network Device Group	(Not Assigned)
Log Update/Watchdog Packets from thi	s remote AAA Server
Log Update/Watchdog Packets from thi AAA Server Type	s remote AAA Server CiscoSecure ACS
Log Update/Watchdog Packets from thi AAA Server Type Traffic Type	s remote AAA Server CiscoSecure ACS 💌 inbound/outbound
Log Update/Watchdog Packets from thi AAA Server Type Traffic Type AAA Server RADIUS Authentication Port	s remote AAA Server CiscoSecure ACS inbound/outbound 1645

AAA Server Setup for id-acs

Note: You can optionally assign the Cisco Secure ACS to a previously configured network device group (NDG). When adding a Cisco Secure ACS to a network device group, make sure that shared secret for NDG matches the Cisco Secure ACS's shared secret.

Interface Configuration

In the Interface Configuration section, you can configure options such as the RADIUS attribute dictionary, NDG, replication, and the HCAP interface for communication with Microsoft NPS running on Windows Server 2008. The items configured in the Interface Configuration section, such as RADIUS attributes, must be enabled here to be available in other parts of the Cisco Secure ACS configuration.

Task 1: Configure RADIUS Attributes

You configure the RADIUS attributes in the Interface Configuration section. Note that the RADIUS Cisco IOS/PIX6.0 menu appears only after you add the AAA client with the RADIUS Cisco IOS/PIX6.0 authentication type on the Network Configuration screen.

Step 1. Choose Interface Configuration from the main menu, choose RADIUS (IETF), and select the attributes shown in the screenshot. Then choose RADIUS Cisco IOS/PIX6.0 and select the attribute shown in the screenshot. Only the attributes checked are necessary for NAC. All other attributes should by unchecked to save time in later configuration steps.

	Options	
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 necessary only for VLAN assignments. Attributes 27 and 29 are used for IEEE 802.1X reauthentication.

Step 2. Choose Interface Configuration > Advanced Options and enable the attributes shown here.

Advanced Options
Default Time-of-Day / Day-of-Week Specification
Group-Level Shared Network Access Restrictions
Group-Level Network Access Restrictions
Group-Level Password Aging
Vetwork Access Filtering
Max Sessions
ACS internal database Replication
RDBMS Synchronization
Vetwork Device Groups
Microsoft Network Access Protection Settings

Advanced Options 🤶
Note: Only the selected options will appear in the user interface.
Per-user TACACS+/RADIUS Attributes
User-Level Shared Network Access Restrictions
User-Level Network Access Restrictions
🗌 User-Level Downloadable ACLs
🗹 Default Time-of-Day / Day-of-Week Specification
☑ Group-Level Shared Network Access Restrictions
Group-Level Network Access Restrictions
🗖 Group-Level Downloadable ACLs
Group-Level Password Aging
✓ Network Access Filtering
🔽 Max Sessions
🗖 Usage Quotas
Distributed System Settings
ACS internal database Replication
RDBMS Syndigronization
IP Pools
☑ Network Device Groups
Voice-over-IP (VoIP) Group Settings
Voice-over-IP (VoIP) Accounting Configuration
Microsoft Network Access Protection Settings

Note: Microsoft Network Access Protection Settings needs to be checked in this section to enable the HCAPv2 interface so you can configure the Microsoft NPS address.

System Configuration

Task 1: Set Up Cisco Secure ACS Certificate and Root CA Certificate

Configure Cisco Secure ACS with a server certificate for establishing client trust when challenging the client for its credentials. For authenticated in-band PAC provisioning for EAP-FAST, the client must have a certificate that matches the one installed in Cisco Secure ACS.

Note: Using a production PKI and certificates signed by a production CA or registration authority is highly recommended for the most scalable NAC deployments. This part of NAC implementation has been significantly compressed and abbreviated; you will need to use an existing PKI (internal or outsourced) to securely identify the Cisco Secure ACS infrastructure to endpoint devices.

The following steps show how to request the Cisco Secure ACS certificate from a locally configured Microsoft root CA server and install it on Cisco Secure ACS as the server certificate. If the CA server is not available in the testing environment, Cisco Secure ACS can generate a self-signed certificate. Please proceed to Step 14 if you want to use a self-signed server certificate generated on Cisco Secure ACS. Step 14 shows how to create and install a self-signed certificate.

Step 1. Choose System Configuration > ACS Certificate Setup > Generate Certificate Signing Request. Fill out the required field as shown here and click the Submit button.

Generate new re	quest 🔡
Certificate subject	cn=id-acs
Private key file	c:\certs\id-acs.pvk
Private key password	•••••
Retype private key password	•••••
Key length	2048 bits 💌
Digest to sign with	SHA1 🕶

Examples of field values for the certificate signing request (CSR) are shown here.

Generate Certificate Signing Request	
Certificate subject cn=your_acs_ name	
Private key file	C:\%your_cert_dir%your_private_key_name
Private key password your_private_key_password	
Retype private key password your_private_key_password	
Key length	2048 bits
Digest to sign with	SHA1

After you submit your request, your CSR is displayed in the right frame of your browser console.

P	low your certificate signing request is ready. You can copy/paste it to any certification authority enrollment tool.		
	BEGIN CERTIFICATE REQUEST		
	MIICuzCCAaMCAQAwETEPMAOGA1UEAxMGaWQtYWNzMIIBIjANBgkghkiG9wOBAQEF		
	AAOCAQ8AMIIBCqKCAQEAv74hGyrfJuUAbNwnD0v5BeaF0j/c4+p5hvcUfJBxaFP6		
	FNFn61WG3+Hh+dNvtXsYSOb9T1Ot8CIawQMMA3g4TpUHE+ErEQp2mppHszKVTvcx		
	XQJ1kbW/ccYzYh5+kPUpFW1YW7X8fcwxRM8GzPWDa+hNhGjWtJpLFhYkinKjea2V		
	OECzomrvLSmy8sRtFNLEPbiVaQWIDRZY9BA9zcvl+nK2rJ12u/BJixZnMibJRv24		
	rBe6aXR5oW7vPZCOVE6tCFAYiyjlrnAGqQBzdXq/mTzUkYBGrxpo52Oe93CivCed		
	8GtTpfoi55PK07RhRYe98xlqb8nbPKg5XCi8ur4cqwIDAQABoGUwYwYJKoZIhvcN		
	AQKOMVYwVDALBgNVHQ8EBAMCBaAwHQYDVROOBBYEFNo5o+5eaOsNM1W/75VgGJCv		
	2 AcJMBMGA1UdJQQMMAoGCCsGAQUFBwMBMBEGCWCGSAGG+EIBAQQEAwIGQDANBqkq		
	hkiG9w0BAQUFAAOCAQEAI+4LaYKk8PUvF0d8tMELDtDXxYBMSr+fXdanixw8x/uU		
	aOro3nvIYZ9nrqxitqTuJzUb42z7rD7iyDACoRxxDnhGJrBSobvWd+/rzfp23cnH		
	3qOqyS8TpAIW19PqB7GcBpAzIcOZaCKSWB11XXsqubzN6XqVW2+KvGEcjJdQnsYb		
	OR/+LdnTCFoK6hN6FpBQ/t0Gs04ZtA3mJDhJ76/ApG1GDeTxw9pJ1UqW0h2GwnJ+		
	153b4UONTZxK3xkRUAI360rC/1MqLpsIPy/y+hxmEiQ4iH1qnuIYKQWnX26jkKmC		
	1NFTxNR5yckadVxWAvK7Evn9tUE511t90Gok7nZurQ==		
	END CERTIFICATE REQUEST		

Step 2. Now send the CSR to the Microsoft CA server. Copy your CSR to a temporary text file. Then access your CA server using Microsoft Internet Explorer (IE). The local Microsoft CA server can be accessed through the following URL: http://your_ca_server/certsrv/

Welcome	
Use this Wel certificate, yo messages, a	site to request a certificate for your Web browser, e-mail client, or other program. By using u can verify your identity to people you communicate with over the Web, sign and encrypt d, depending upon the type of certificate you request, perform other security tasks.
You can also certificate rev	use this Web site to download a certificate authority (CA) certificate, certificate chain, or cation list (CRL), or to view the status of a pending request.
For more info	mation about Certificate Services, see Certificate Services Documentation.
Select a tas	
Request a	certificate
View the	tatus of a pending certificate request
Download	a CA certificate, certificate chain, or CRL

- Step 3. Click Request a certificate > advanced certificate request > Submit a certificate request by using a base-64-3ncoded CMS or PKCS #10, or submit a renewal request by using a base-64-encoded PKCS #7 file.
- Step 4. Paste your copied CSR from the Cisco Secure ACS web console to the **Saved Request** text box. For **Certificate Template**, choose **Web Server**; then click **Submit**.

Microsoft Certific:	ate Services ID-CA	Ноп
Submit a Certific	cate Request or Renewal Request	
To submit a saveo generated by an e	request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request o xternal source (such as a Web server) in the Saved Request box.	or PKCS #7 renewal request
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	HICEOCCAagCAQAFJEUMBIGAIUEAXHLaWCFUMB HDEVCCAagCAQAFJEUMBIGAIUEAXHLaWCFUMB DEPSAQUAHAEDBAWAgGKACASSATLE HB7FgZTF85pdlaj41GooPvmjEJ3dL1TJ/EDg9BuX F/GaWZgymlq18cEROKWju6qkBpe9cPiuxw7Tiftbb C Browse for a file to inserf	
Certificate Templa	te:	
	Web Server	
Additional Attribut	95:	
Attributes:	< ×	
	Submit >	

Step 5. Select **DER encoded** to download your Distinguished Encoding Rules (DER) encoded certificate to your certificate directory on Cisco Secure ACS (or you may need to download the certificate to your Cisco Secure ACS Solution Engine server). Name the downloaded certificate to distinguish it from the root CA server of this Microsoft CA server. Alternatively, you may want to save the CA certificate in both **DER** and **Base 64** encoding methods and then save them both with appropriate names.

Certificate	lssued	
The certifica	te you requested was issued to you.	
	⊙ DER encoded or ○ Base 64 encoded	
. Contra	Download certificate	

- Step 6. (Optional) When you are accessing the CA web enrollment console, we recommend that you download the CA server root certificate and save it along with the Cisco Secure ACS certificate for future use. To download the CA root certificate, access your CA server with IE and click Download a CA certificate, certificate chain, or CRL under Select a task section of Welcome page.
- Step 7. Make sure you choose the current CA server and then click Download certificate.
- Step 8. Now you have a root CA certificate, Cisco Secure ACS certificate, and associated private key saved on your Cisco Secure ACS. You have to install those certificates and the private key on Cisco Secure ACS. First install the root CA certificate on Cisco Secure ACS. Choose System Configuration > ACS Certificate Setup > ACS Certification Authority Setup. Specify the location of the CA certificate and click the Submit button.



- Step 9. After you add the new CA certificate, restart Cisco Secure ACS. Choose **System Configuration > Service Control** and click **Restart**.
- Step 10. 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, locate the name of your CA in the list, and check the box next to it and click Submit to save the changes.

Edit the Certificate Trust List (CTL)

- Step 11. Changing the CTL requires a Cisco Secure ACS restart; **choose System Configuration** > Service Control and click the Restart button.
- Step 12. Choose **Install Certificate**. Specify the location of the Cisco Secure ACS certificate and click the **Submit** button.

Install New Certificate	
Read certificate from file	
Certificate file:	c:\certs\id-acs.cer
Private key file:	c:\certs\id-acs.pvk
Private key password:	cisco123

Install ACS Certificate			
Ins	stalled Certificate Information	?	
Issued to:	id-acs		
Issued by:	ID-CA		
Valid from:	February 21 2008 at 11:08:05		
Valid to:	February 20 2010 at 11:08:05		
Validity:	ок		

- Step 13. After a successful installation of the Cisco Secure ACS certificate, you must restart Cisco Secure ACS. Choose System Configuration from the main menu, select Service Control, and click the Restart button. This completes the Cisco Secure ACS certificate installation process.
- Step 14. (Optional) Choose System Configuration > ACS Certificate Setup > Generate Certificate Signing Request. Fill out the required fields as shown here and click the Submit button.

Generate new self-sign	ed certificate	?
Certificate subject	cn=id-acs	
Certificate file	::\certs\id-acs-self.cer	
Private key file	::\certs\id-acs-self.pvk	
Private key password	•••••	
Retype private key password	******	
Key length	2048 bits 💌	
Digest to sign with	SHA1 💌	
Install generated certificate		

Note: Self-signed server certificates generated on Cisco Secure ACS should be used for lab testing purposes only. This certificate is valid for one year only, and the administrator is advised to not deploy a self-signed certificate for any production use.

Task 2: Set Up Global Authentication

Cisco Secure ACS supports many protocols for securely transferring credentials from the host to the Cisco Secure ACS for authentication and authorization. You must tell Cisco Secure ACS which protocols are allowed and what the default settings are 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. Choose System Configuration > Global Authentication Setup.
- Step 2. Select the global authentication parameters shown here to make them available for the network access profile authentication configuration. Note that Protected EAP (PEAP) and its inner authentication methods are also selected. PEAP is not required for NAC-NAP integration. Those methods can be disabled in the network access profile.

Global Authentication Setup

	tion
PEAP	
Allow EAP-MSCHAPv2	
Allow EAP-GTC	
Allow Posture Validation	
Allow EAP-TLS	
Select one or more of the following	g options:
🗹 Certificate SAN comparison	
🗹 Certificate CN comparison	
🗹 Certificate Binary compariso	in
EAP-TLS session timeout (minutes): 120
Cisco client initial message:	
PEAP session timeout (minutes):	120
Enable Fast Reconnect:	
EAP-FAST Configuration	
EAP-TLS	
Allow EAP-TLS	
Select one or more of the following	g options:
Select one or more of the following Certificate SAN comparison	g options:
Select one or more of the following Certificate SAN comparison Certificate CN comparison	g options:
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso	g options:
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes	g options: in): [120]
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication:	g options: in): 120 for setting username
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: Ouse Outer Identity	g options: in): 120 for setting username
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: Ouse Outer Identity Ouse CN as Identity	g options: in): 120 for setting username
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: OUse Outer Identity OUse CN as Identity OUse SAN as Identity	g options: in): 120 for setting username
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: OUse Outer Identity OUse CN as Identity OUse SAN as Identity LEAP	g options: in): 120 for setting username
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: Use Outer Identity Use CN as Identity Use SAN as Identity LEAP Allow LEAP (For Aironet only)	g options: in): 120 for setting username
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: Use Outer Identity Use CN as Identity Use SAN as Identity LEAP Allow LEAP (For Aironet only) EAP-MD5	g options: in): 120 for setting username
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: Use Outer Identity Use CN as Identity Use SAN as Identity EAP-MD5 Allow EAP-MD5	g options: in); 120 for setting username
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: Use Outer Identity Use CN as Identity Use SAN as Identity LEAP Allow LEAP (For Aironet only) EAP-MD5 Allow EAP-MD5 Allow EAP-MD5	g options: in): 120 for setting username
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: Use Outer Identity Use CN as Identity Use SAN as Identity LEAP Allow LEAP (For Aironet only) EAP-MD5 Allow EAP-MD5 Allow EAP-MD5 MS-CHAP Configu	g options: in): 120 for setting username : 20 iration
Select one or more of the following Certificate SAN comparison Certificate CN comparison Certificate Binary compariso EAP-TLS session timeout (minutes Select one of the following options during authentication: Use Outer Identity Use CN as Identity Use SAN as Identity LEAP Allow LEAP (For Aironet only) EAP-MD5 Allow EAP-MD5 AP EAP request timeout (seconds) MS-CHAP Configu Allow MS-CHAP Version 1 Authe	g options: in): 120 for setting username : 20 iration

- Step 3. Click **Submit + Restart** to save these changes.
- Step 4. Choose **EAP-FAST Configuration** to open the **EAP-FAST Configuration** page. Select the parameters shown here

EAP-FAST Setti	ngs	
EAP-FAST		
Allow EAP-FAST		
Active master key TTL	1	months 💌
Retired master key TTL	з	months 🖌
Tunnel PAC TTL	1	weeks 💌
Client initial message:		
Authority ID Info:	CIS	со
Allow full TLS renegotiation in c	ase of	F Invalid PAC
🗹 Allow anonymous in-band PAC p	rovisi	oning
🗹 Enable anonymous TLS rene	gotiat	ion
Allow authenticated in-band PA	C prov	/isioning
🗹 Accept client on authentica	ted pr	rovisioning
Require client certificate for	provi	sioning
When receiving client certificat following lookup methods:	e, sel:	ect one of the
○ Certificate SAN lookup		
⊙ Certificate CN lookup		
🗹 Allow Machine Authentication		
Machine PAC TTL	1	weeks 💌
☑ Allow Stateless session resume		
Authorization PAC TTL	1	hours 🖌
Allowed inner methods	().	1940 - 1940 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 -
EAP-GTC		
EAP-MSCHAPv2		
EAP-TLS		
Select one or more of the following methods:) EAP-	TLS comparisor
🗹 Certificate SAN comparison		
🗹 Certificate CN comparison		
🗹 Certificate Binary compariso	n	
EAP-TLS session timeout (minutes)) 120	
EAP-FAST master server		
Actual FAR-FAST server status	Mas	ter

EAP-FAST Configuration

Step 5. Click **Submit + Restart** to save these changes.

Task 3: Configure Attributes for Logging

In this task, you will turn on the Cisco Secure ACS logs needed for monitoring and troubleshooting. Cisco Secure ACS logs provides records of access requests from clients and hints about why authentication failed if something goes wrong. You should always turn on the appropriate log options when initially configuring Cisco Secure ACS.

Note: To log any attribute values from hosts other than NAC attribute values, you must first import the attribute definitions into Cisco Secure ACS and then select them for logging.

Step 1. To specify which log files are enabled and which event attributes are recorded within them, choose **System Configuration > Logging**.

The recommended log files and their logged attributes for NAC are shown here. Make sure logging for CSV Failed Attempts, CSV Passed Authentications, and CSV RADIUS Accounting are all turned on.

CSV Failed Attempts	CSV Passed Authentications	CSV 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
 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
• EAP Type	• EAP Type	 Framed-IP-Address
 EAP Type Name 	EAP Type Name	 NAS-Port
 Network Access Profile Name 	 Network Access Profile Name 	 NAS-IP-Address
 Shared RAC 	 Outbound Class 	Class
Downloadable ACL	Shared RAC	 Termination-Action
 System-Posture-Token 	Downloadable ACL	 Called-Station-Id
 Application-Posture-Token 	 System-Posture-Token 	 Acct-Delay-Time
Reason	 Application-Posture-Token 	Acct-Authentic
	Reason	 Acct-Terminate-Cause
		 Event-Timestamp
		 NAS-Port-Type
		 NAS-Port-Id
		AAA Server
		ExtDB Info
		 Network Access Profile Name
		 cisco-av-pair
		Access Device

Administration Control Configuration

Task 1: Add Remote Administrator Access

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

Step 1. Choose Add Administrator and in the Administration Control section add the information shown here.

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

Shared Profile Components Configuration

Shared profile components are configurations that can be reused across many different network access profiles for filtering within Cisco Secure ACS or for network authorization within RADIUS. These need to be defined before you configure the network access profiles.

Note: Network access profiles are introduced in Cisco Secure ACS 4.0. They enable you to create and map individual authentication, posture validation, and authorization components depending on the access method being used.

Among the most useful shared profile components are the RADIUS authorization components (RACs).

Task 1: Configure RADIUS Authorization Components

RACs are sets of RADIUS attributes that are applied to NADs during network authorization. After you group a set of RADIUS attributes in a RAC, you can make the RAC available when configuring network access profiles and use it as an enforcement command for the NAD, sent in the RADIUS Access Accept packet.

Step 1. To configure RACs, choose Shared Profile Components > RADIUS Authorization Components and click the Add button for each new RAC you want to create. Each RAC can contain one or more vendor RADIUS attributes, including Cisco IOS/PIX 6.0 and IETF.

Note: The session timeout value used for NAC deployments can significantly affect Cisco Secure ACS performance. We strongly recommended that you adjust the timeout value for the scale of your network and the Cisco Secure ACS transaction capacity.

Attribute	Vendor	Use Case	Definition
Session Timeout (27)	IETF	IEEE 802.1x	Reauthentication timer value in second
Termination Action (29)	IETF	IEEE 802.1x	RADIUS-Request (1) means that posture revalidation takes place without any session termination. If this value is set to Default (0) or not sent, the session is terminated upon revalidation timer expiration.
Tunnel-Type	IETF	IEEE 802.1x	Tunnel-Type (802) defined in RFC 3580
Tunnel-Medium-Type	IETF	IEEE 802.1x	Tunnel-Medium-Type (VLAN) defined in RFC 3580
Tunnel-Private-Group-ID	IETF	IEEE 802.1x	Tunnel-Private-Group-ID defined in RFC 3580. This attribute is used to tell the NAD which local VLAN the switch should assign to a port to which a user is connected. Cisco NADs accept both strings (VLAN name) and integers (VLAN ID) in this attribute. This attribute needs to be sent along with attributes 64 and 65.

Step 2.	Specify RAC entries, attribute assignments, and values. Create these RAC configurations
	for a IEEE 802.1x scenario (NAC Layer 2 IEEE 802.1x).

RAC Name	Vendor	Assigned Attributes	Value
802.1x_Compliant_User	IETF	Session-Timeout (27)	3600
	IETF	Termination-Action (29)	RADIUS-Request
	IETF	Tunnel-Type (64)	VLAN
	IETF	Tunnel-Medium-Type (65)	802
	IETF	Tunnel-Private-Group-ID (81)	healthy
802.1x_Compliant_Machine	IETF	Session-Timeout (27)	3600
	IETF	Termination-Action (29)	RADIUS-Request
	IETF	Tunnel-Type (64)	VLAN
	IETF	Tunnel-Medium-Type (65)	802
	IETF	Tunnel-Private-Group-ID (81)	asset
802.1x_Quarantine	IETF	Session-Timeout (27)	60
	IETF	Termination-Action (29)	RADIUS-Request

RAC Name	Vendor	Assigned Attributes	Value
	IETF	Tunnel-Type (64)	VLAN
	IETF	Tunnel-Medium-Type (65)	802
	IETF	Tunnel-Private-Group-ID (81)	quarantine

Step 3. For the IEEE 802.1x scenario, you should have three RACs total. Now the Cisco Secure ACS service needs to compile those RACs. Choose **System Configuration > Service Control > Restart** to compile the RACs.

RADIUS Authorization Components		
Name	Description	
802.1x Compliant Machine		
802.1x Compliant User		
802.1x Quarantine		

Group Setup Configuration

Cisco Secure ACS can enforce policy for users by applying authorization rules (dynamic VLAN assignment) per group. You can configure these groups locally on the Cisco Secure ACS; however, they can be mapped to a set of groups in an external database, such as Active Directory. For instance, if **user1** belongs to the Active Directory Domain user group, this user can be assigned to VLAN 10 if authentication succeeds. If **user2** belongs to the Cisco Secure ACS local database, this user can be assigned to VLAN 30 in the same way. There is also a way to assign policy per user; however, this method does not scale in a large enterprise environment.

Task 1: Set Up User Groups

This documentation uses an Active Directory environment as the user authentication database; therefore, in this test you will create three Cisco Secure ACS local groups, with two of them mapped to Active Directory user groups.

Step 1. By default, Cisco Secure ACS already has 500 user groups. You will start by renaming four of these groups. Choose Group Setup from the main Cisco Secure ACS menu. From the Group pull-down menu, choose 1: Group 1 and click Rename Group. Type AD_User and click Submit. Repeat those steps for each of the other groups using the group names shown here.

Group Number	Group Name
1: Group 1	AD_User
2: Group 2	AD_Asset
4: Group 4	Local_User
5: Group 5	Quarantine



Task 2: Set Up Users

Although the user is authenticated against Active Directory, a user account can be created locally on Cisco Secure ACS.

- Step 1. Choose User Setup, for User, enter Vista, and click the Add/Edit button. Under User Setup for User: vista (New User), enter cisco123 as the user's password.
- Step 2. In the **Group to which the user is assigned** drop-down menu, assign the user to the **Local_User** group. Scroll to the bottom and click the **Submit** button.

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

External User Database Configuration

For Cisco Secure ACS to authenticate the user and device against Active Directory, Cisco Secure ACS needs to be running on a domain member server. Active Directory in the Windows domain can be configured in the external user database. In this section, you will set up three items: you will configure unknown-user policy, map the Cisco Secure ACS local group to the Active Directory security group, and set up Windows database options in detail.

Task 1: Configure Unknown-User Policy

In this task, unknown-user policy is configured to find the correct database when a user is not found in the Cisco Secure ACS local database.

- Step 1. Choose External User Database > Unknown User Policy.
- Step 2. Click Check the following external user database.
- Step 3. Use the arrow button to move **Windows Database** from the **External Databases** box to the **Selected Database** and then click **Submit**.

Task 2: Map Database Groups

In this task, Cisco Secure ACS local groups are mapped to Active Directory user groups on in a domain.

- Step 1. Choose External User Database > Database Group Mappings.
- Step 2. Under Unknown User Group Mappings, click Windows Database.
- Step 3. Click **New configuration** to select your domain. In this task, use domain name ID, so in the **Detected Domains** list, select **ID** (or your domain) and click **Submit**.
- Step 4. Click ID and start Cisco Secure ACS local group and NT group mappings. Click Add mapping and under NT Groups select Domain User and then click Add to selected. In the ACS group list, select AD_User and click Submit.
- Step 5. Repeat these steps with the entries shown here to map the NT groups to Cisco Secure ACS local groups.

NT Groups	Cisco Secure ACS Groups
Domain Computers	AD_Asset

Note: Domain computer accounts are used to authenticate devices using IEEE 802.1x against Active Directory.

Task 3: Configure External User Database

In this task, more detailed options for the specific user database are configured.

- Step 1. Choose External User Database > Database Configuration > Windows Database and click the Configure button to configure more detailed options for the Windows Active Directory database.
- Step 2. Under Windows User Database Configuration, unselect Verify that "Grant dialin permission to user" setting has been enabled from within the Windows User Manager for users configured for Windows User Database authentication.

With this option disabled, Cisco Secure ACS will not check the **Allow access** remote access permission in the Active Directory user account properties. The following screenshot shows the user account properties on the Active Directory Users and Computers management console.

Note: This feature is disabled here for testing purpose only. You should revisit and evaluate this setting when deploying Cisco Secure ACS to a production network.

General Address Account Profil	rvices Profile	COM+
Member Of Dial-in E	Invironment	Sessions
Remote Access Permission (Dial-in or VF () <u>Allow access</u> () <u>D</u> eny access	'N]	
C Control access through Remote Acce	ess Eolicy	
☐ Verify Caller-ID:	1	
Callback Options	3	1
• No <u>C</u> allback		
○ Set by Caller (Routing and Remote A	ccess Service only	ı)
C Always Callback to:	[
🗖 Assign a Static IP Address	1 a a	12
- C Applu Static Boutes		
* where more more a	Static Ro	utes
Define routes to enable for this Dial-in connection.		

- Step 3. Select Use the next sequential External Database in the Selected Databases list in case of an "External DB user invalid or bad password" error.
- Step 4. Under **Configure Domain List**, use the arrow button to move your domain name, in this case, the domain name **ID**, from the **Available Domains** list to **Domain List**.
- **Note:** If you are in a single domain, this operation is optional.



Step 5. Under MS-CHAP Settings, select both MS-CHAP version 1 and MS-CHAP version 2.

Step 6. Under Windows EAP Settings, select Enable password change inside PEAP or EAP-FAST.

	Windows EAP Settings
V	Enable password change inside PEAP or EAP-FAST.
Mar	chine Authentication.
V	Enable PEAP machine authentication.
	Enable EAP-TLS machine authentication.
	Enable machine access restrictions.
	Aging time (hours):
	Group map for successful user authentication without machine authentication: (No Access>
	User Groups that are exempt from passing machine authentication: Available User Groups Selected User Groups
	Default Group emp_grp guest_grp temp_grp asset_grp woice Group 7

Step 7. Under Windows Authentication Configuration, select Default: "CISCO" as the workstation name and select Enable nested group evaluation during group mapping.

	Windows Authentication Configuration
Use	this table to configure a different workstation name rather than a CISCO workstation account for ACS authentications to Windows Active Directory.
۲	Default: "CISCO"
0	Local: id-acs
0	User defined workstation name
	Enable nested group evaluation during group mapping.

	[a]
Submit	Cancel

Posture Validation Configuration

Microsoft NPS provides posture validation and basic remediation services for the NAC-NAP solution. All statement of health (SoH) information from the client will be received by Cisco Secure ACS and forwarded to Microsoft NPS over HCAP for compliance checking. The result of the compliance check in Microsoft NPS will be sent back to Cisco Secure ACS over HCAP, and a NAC policy will be assigned based on the result.

Task 1: Set Up Cisco Secure ACS External Posture Validation

External posture server validation will be configured to forward Microsoft Vista client statement of health information from Cisco Secure ACS to Microsoft NPS for posture validation.

Step 1. Choose Posture Validation > External Posture Validation Setup.

Step 2. Under External Posture AAA Servers, click Add Server.

Note: Be sure to select External Posture AAA Servers, not External Posture Servers. External Posture Servers allows you to configure posture servers, which are HCAPv1 capable. External Posture AAA Servers provides an interface to the Microsoft NPS which is HCAPv2 compliant.

- Step 3. In the Name field, add the hostname of the Microsoft NPS. In this example, the name for the Microsoft NPS is **ID-NPS**.
- Step 4. Select Primary Server Configuration.
- Step 5. Enter the URL (https://x.x.x.x/hcap/hcapext.dll) that will be used for communication between Cisco Secure ACS and the Microsoft NPS. In this example, the URL has been configured as the following: https://10.1.100.10/hcap/hcapext.dll
- Step 6. Do not configure any username or password. The username and password are optional and should be used if these credentials are required by the IIS server.
- Step 7. The default **Timeout (Sec)** value of **10** can be used. This value sets the interval between primary server failure and failover to the secondary server.
- Step 8. To enable encrypted communication between Cisco Secure ACS and Microsoft NPS, an HTTPS connection can be established using a server certificate. Select the trusted root CA used for both Cisco Secure ACS and Microsoft NPS. In this example, the **Trusted Root CA** value is **ID-CA**. In the test environment, Secure Sockets Layer (SSL) communication can be turned off by changing the URL as described in Step 5 to http://x.x.x.x/hcap/hcapext.dll (the "s" is removed from https://).
- Step 9. Select all the attributes in the Available Fwd Attributes box and use the arrow button to move them to the Selected Fwd Attributes box. The attributes include Endpoint-ID, Endpoint-IP-Address, Endpoint-Location, User-Group, and User-Name.

	Add/E	dit External Posture AAA Server	?
Name	ID-	VPS	
Description	Ext	ernal NPS Server	
	URL Username	https://10.1.100.10/hcap/hcapext.dll	
Primary Server configuration	Password Timeout (Sec)	10	
	Trusted Root CA	ID-CA	~
Secondary Server Configuration	URL Username Password Timeout (Sec) Trusted Root CA	10 none selected	×
	Availab	e Fwd Attributes Selected Fwd Attributes Endpoint-ID Endpoint-ID-Address Endpoint-Location User Group User Name	
	I	Submit Delete Cancel	

The following table shows the available attributes used in NAC-NAP IA and their definitions.

Attributes	Definition
Endpoint-ID	End host MAC address
Endpoint-IP-Address	End host IP address if available
Endpoint-Location	Flag to differentiate policy on Microsoft NPS; Location-Group can be configured in the network access profile on Cisco Secure ACS when configuring posture
User-Group	Cisco Secure ACS local group name that specifies the group to which the user is assigned
User-Name	Authenticated username

Completion of Common Cisco Secure ACS Configuration for IEEE 802.1x Scenario Initial Cisco Secure ACS configuration for IEEE 802.1x is now complete. Additional configuration, including posture validation setup for IEEE 802.1x network access profiles, is discussed in the following sections.

Task 1: Complete the Configuration

Before proceeding to the next configuration discussion, change the logging level on Cisco Secure ACS and restart Cisco Secure ACS service.

Step 1. Choose System Configuration > Service Configuration. Under Services Log File Configuration, change the level of detail to Full. Click the Restart button to restart all Cisco Secure ACS services.

Windows Server 2008 Configuration

In this document ID-NPS runs on Windows Server 2008 and hosts Microsoft NPS and the HCAP server, which provides client health validation for Cisco Secure ACS.

Note: In this document, Active Directory is running on Windows Server 2003. The CA service runs on the same server. Because some of the operations in this document require certificates for Windows Vista or Windows Server 2008 through web enrollment, we have applied the following hotfix on Windows Server 2003: <u>http://support.microsoft.com/kb/922706</u>

Task 1: Obtain a Computer Certificate for SSL

To provide SSL authentication for HCAP, the server running Microsoft NPS uses a computer certificate that is stored in its local computer certificate store. Microsoft Certificate Manager will be used to obtain a computer certificate. Do not perform this procedure if your server already has a certificate for SSL encryption.

Note: To request an SSL certificate using the following procedure, the server must be joined to a domain with an available enterprise CA.

- Step 1. Choose Start > Run, and in the Open field enter mmc. This operation opens a window called Console1.
- Step 2. From the File menu, choose Add/Remove Snap-in.
- Step 3. In the Add or Remove Snap-ins dialog box, click Certificates, click Add, select Computer account, click Next, and then click Finish. Then click OK to close the dialog box.
- Step 4. In the left pane, double-click **Certificate**, right-click **Personal**, point to **All Tasks**, and then choose **Request New Certificate**.
- Step 5. The Certificate Enrollment dialog box, opens. Click Next.
- Step 6. Select the Computer check box as shown here and then click Enroll.

ou can request the following types	of certificates. Select the certificates you want to requ	est, and then dick Enroll.
Computer	i) STATUS: Available	Details®

Step 7. Verify that **Succeeded** is displayed to indicate the status of certificate installation and then click **Finish**.

Step 8. Close the Console1 window.

Note: Your server may have more than one certificate in the local certificate store. Before choosing an SSL certificate, you can view the properties of these certificate by clicking a certificate in the list, then clicking **Properties**, and then clicking the **Detail** tab. A certificate used for SSL authentication must have a **Subject** field value that corresponds to the fully qualified domain name of the HCAP server (for example, **ID-NPS.id.local**), and an **Enhanced Key Usage** (EKU) field value of **Server Authentication**. The certificate must also be sent from a root CA that is trusted by the client computer. The computer certificate provisioned in this procedure meets these requirements.

Task 2: Run the Role Management Tool to Install the HCAP Server

This Role Management Tool (RMT) also installs the Microsoft NPS and IIS components. The screenshots in this section show the RMT installation of the HCAP server.

Step 1. To activate the RMT wizard, click **Add Roles** in the server manager user interface. The following screenshot shows the wizard's introductory page. Click **Next** to see the roles that can be installed on the server.

Add Roles Wizard	
Before You	u Begin
Before You Begin Server Roles Confirmation Progress Results	This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site. Before you continue, verify that: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The latest security updates from Windows Update are installed If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again. To continue, dick Next.
	☐ Skip this page by default
	< Previous Next > Instal Cancel

Step 2. The following screenshot shows the roles that can be selected on the server. Select the **Network Policy and Access Services** role and click **Next**.

Select Server Ro Select Server Roles Kett Server Roles Network Policy and Access Services Role Services Confirm Installation Selections Installation Progress Installation Results	Select one or more roles to install on this server. Rele Active Directory Certificate Services Active Directory Roleration Services Active Di	Description: Network Policy and Access Services provides support for routing LAN and WAN network traffic, creating and enforcing network resources over VPN and dial-up connections.
	More about server roles	

Step 3. The following screenshot shows the introductory page for the **Network Policy and** Access Services role. Click Next.



Step 4. Select Host Credential Authorization Protocol to install the HCAP server.

Select Role Serv	ices	
Before You Begin Select Server Roles Network Policy and Access Services Role Services Confirm Installation Selections Installation Progress Installation Results	Select the role services to install for Network Policy and Acc Role services: Network Policy Server: Routing and Remote Access Services Routing Health Registration Authority Health Registration Authority Host Credential Authorization Protocol	ess Services: Description: (FGP) behaves as a connection point between Cisco Access Control Server and the Microsoft Network Policy Server, allowing the Microsoft Network Policy Server to validate the machine's posture in a Cisco 802. IX environment



Add Roles Wizard		X
Select Role Serv	ices	
Before You Begin Select Server Roles Network Policy and Access Services Role Services Server Authentication Certificate Web Services Confirm Installation Selections Installation Progress Installation Results	Select the role services to install for Network Policy and Acc Role services:	ess Services: Description: Host Credential Authorization Protocol (HCAP) behaves as a connector point between Cisco Access Control Server and the Microsoft Network Policy Server to additute the machine's posture in a Cisco 802. 3X environment.
	< Previous	Next > Install Cancel

Step 6. Installation of HCAP requires dependent role services and features that will be installed automatically for the administrator. The following screenshot shows the dialog box listing all the dependent role services and features required for the HCAP server. Click Add Required Role Services.



Step 7. The following screenshot shows the **Server Authentication Certificate** page, which allows the administrator to use an existing certificate. Select **ID-NPS.id.local** from the existing certificate list and click **Next**.

Before You Begin Server Roles Network Policy and Access Services Role Services Server Authentication Certificate Web Server (TIS)	 When communicating with clents, HCAP can use the secure solders Layer (SL) protocol to enryph rebonds traffic. Choose a server authentication certificate suitable for SSL encryption to add to the default site in Tritement Information Services (IIS). Choose an existing certificate for SSL encryption (recommended) This option is recommended for most production scenarios. You should use a certificate issued by an external certification authority (CA) or you can use a certificate issued by your own internal CAI fitte CA is tructed by deints connecting to this server. The subject name of the certificate must match the host name of this server. 				
Role Services	Issued To	Issued By	Expiration Date	Intended Purpose	Properties
Ionfirmation	ID-NPS.id.local	ID-CA	7/4/2009	Client Authentication,	Import
lesults					Refresh
	 Create a self-signed This option is recommunity instal C Don't use SSL or chose 	certificate for SSL mended for small- I the certificate or ose a certificate fi	encryption scale deployments on clients that commu or SSL encryption la of want to use SSL.	r test scenarios only. After in nicate with this server. ter or if you plan to request a cer	stalling HCAP, you tificate from a CA
	This option is recom and import it later.	nended if you do			

Step 8. Click Next on the Web Server (IIS) screen to get to the Select Role Services page.

Add Roles Wizard		×
Web Server (IIS)	
Before You Begin Select Server Roles Role Services Role Services Server Authentication Certificate Web Server (115) Role Services Confirm Installation Selections Installation Progress Installation Results	Introduction to Web Server (IIS) The twb Server (IIS) role enables sharing of information on the Internet, an intranet, or an extranet. It is a unified Web plotterm that integrates IIS 7.0.80x PLTY, Windows Communication Foundation, and Windows SharePoint Services. IIS 7.0.80x PLTY, Windows Communication Foundation, and Windows SharePoint Services, IIS 7.0.80x PLTY, Windows Communication Foundation, and Windows SharePoint Services, IIS 7.0.80x PLTY, Windows SharePoint Services, and delegated administration. Things to Kote ① Using Windows System Resource Management (WSRM) can help ensure equitable servicing of web server traffic especially when there are multiple roles or workloads on this computer.	
	< Previous Next > Install Cancel	

Step 9. The following screenshot shows the role services that are being installed on the server. Click **Next**.

Add Roles Wizard		
Add Roles Witzard Select Role Servi Before You Begin Select Server Roles Network Policy and Access Services Role Services Server Authentication Certificate Web Server (115)	CES Select the role services to install for Web Server (IIS): Role services: Bit Web Server Web Server State Content V State Content V Default Document V Declary Browsing V Declary Browsing	Description: Web Server provides support for HTML Web arise and optional support for ASP.Net, ASP, and Web server ASP.Net, ASP, and Web server descriptions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web shared
Role Services Confirm Installation Selections Installation Results : Installation Results :	Application Development Application Development App ARET NET Extensibility AP CGI VISAPIExtensions ISAPI Filters Server Side Includes Methods and Disprositis VITTP Logging Visaping Tools Request Monitor VITTP Cogging Custom Logging Custom Logging	applications.
	More about role services < Previous	Next > Install Cancel

Step 10. The following screenshot shows the confirmation page before installation begins. Click **Install** to start the installation.

Before You Begin Select Server Roles	To install the following roles, role services, or features, click Install.	
Network Policy and Access Services	Network Policy and Access Services	<u>^</u>
Role Services Server Authentication Certificate Web Server (IIS)	Network Policy Server Host Credential Authorization Protocol SSL Certificate: Use selected certificate	
Role Services Confirm Installation Selections	Web Server Cormon HTTP Features Static Content	
Installation Progress	Default Document	
Installation Results	Directory Browsing HTTP Errors HTTP Redirection Application Development	_
	ISAPI Extensions Health and Diagnostics HTTP Logging Logging Tools Request Monitor	
	Tracing Security Basic Authentication	¥

Step 11. The following screenshot shows the installation progress.

	The following folds, fold as wees, of features are being instance.	
elect Server Roles	Network Policy and Access Services	
Role Services	Web Server (IIS)	
Server Authentication Certificate	Windows Process Activation Service (WPAS)	
Neb Server (IIS)		
Role Services		
Confirm Installation Selections		
nstallation Progress		
nstallation Results		
installation Results		
Installation Results		
Installation Results		

Step 12. The following screenshot shows that the installation has succeeded and that the HCAP server and its dependent components are installed.



Step 13. Open the Microsoft NPS Management Console, choose Start > Run, and in the Open field enter nps.msc. Then click OK. The following screenshot shows NPS Management Console.

Network Policy Server		
Elle Action View Help		
🍋 🤿 📶 🔲 🖬		
NPS (Local) RADIUS Clients and Servers	Policies	
RADIUS Clients Remote RADIUS Server Groups	Connection Request Policies	
Connection Request Policies Network Policies Health Policies	Connection request policies allow you to desi remote RADIUS servers. For NAP VPN or 80	gnate whether connection requests are processed locally or forwarded to 2.1X, you must configure PEAP authentication in connection request policy.
Metwork Access Protection System Health Validators Remediation Server Groups Accounting	Configure Connection Request Policies	Learn more
	Network Policies	
	Network policies allow you to designate who they can or cannot connect.	is authorized to connect to the network and the circumstances under which
	Configure Network Policies	Learn more
	Health Policies	
	Health policies allow you to designate the con network. Deploy health policy by configuring health policy to the Health Policies condition	ifiguration required for NAP-capable client computers to access the System Health Validators, creating a health policy, and then adding the n network policy.
	Configure Health Policies	Learn more
	1.	

Network Policy Server Configuration

The Microsoft NPS service on Microsoft NPS needs to be configured for the test lab. There are four configuration steps:

- Configure connection request policy (CRP)
- Configure system health validators (SHVs)
- · Configure health policies
- · Configure network policies

All configuration steps are performed using the Microsoft NPS Microsoft Management Console.

Task 1: Configure Connection Request Policy

Client authentication methods are evaluated in CRP for this test lab.

- Step 1. Double-click Connection Request Processing and then click Connection Request Policies.
- Step 2. In the middle pane, under **Name**, right-click **Use Windows authentication for all users** and then click **Delete**. When a dialog box appears asking you to confirm the deletion, click **OK**. You will create a new connection request policy.
- Step 3. Right-click Connection Request Policies, point to New, and then choose Custom.
- Step 4. In the New Connection Request Policy Properties box, on the Overview tab, for Policy name, type HACP. From the Type of network access server pull-down menu, choose HCAP Server. Your screen should look like the following screenshot. Click Next.

	Specify Connection Request Policy Name and Connection Type	
M	You can specify a name for your connection request policy and the type of connections to which the policy is applied.	
Policy name	c.	
HCAP		
Type or Vendo Type of ne Type of ne HCAP Se Vendor sp 10	e of hetwork access server that senas the connection request to NPS. You can select either the network access server server twork access server:	

Step 5. In the **New Connection Request Policy Properties** box, click **Add** to add the conditions for the CRP to match.

New Connectio	n Request Poli	cy					×
	Specify C Specify the cor A minimum of	conditions nditions that deter one condition is n	rmine whether this equired.	s connection rec	uest policy is ev	aluated for a cor	nnection request.
Conditions:							
Condition	1	Value					
Condition de	scription:						
					A <u>d</u> d	<u>E</u> dit	<u>R</u> emove
				<u>P</u> revious	Next	Einish	Cancel

Step 6. In the **Select Conditions** dialog box that opens, you can select the conditions for the CRP. For this task, select the **Day and Time Restriction** condition to permit connections.

<u>189</u>	Tunnel Type The Tunnel Type condition restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP.	
Day an	d time restrictions	
ť	Day and Time Restrictions Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.	
dentity	/ Туре	
J	Identity Type The Identity Type condition restricts the policy to only clients that can be identified through the specified mechanism, such as NAP statement of health (SoH).	
RADIU	S Client Properties	
<u> </u>	Calling Station ID The Calling Station ID condition specifies the network access server telephone number dialed by the access client.	•

Step 7. The **Day and time restrictions** dialog box that opens permits all requests from the Cisco Secure ACS. Select a range as shown in the screenshot, click **Permitted**, and click **OK**.

Note: This is an example, and administrators can use whatever conditions apply to their specific deployments.



Step 8. Click the Add button again and this time choose HCAP Location Groups; then click Add.

HCAP			
	Location Groups the HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.		
User			
<u>87</u>	User Name The user name that is used by the access client in the RADIUS message. This attribute is a character string that typically contains a realm name and a user account name.		
Conne	ection		
N	Access Client IPv4 Address The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADUS client.		
	Access Client IPv6 Address The Access Client IPv6 Address condition specifies the IPv6 address of the Access Client that is requesting access		

Step 9. In the Location Groups window, type the HCAP location group name: for example, NAC-NAP-IA. Microsoft NPS can use the HCAP location group name to identify HCAP requests by the specific Cisco Secure ACS. The same string is configured in the Posture section of the network access profile in the Cisco Secure ACS configuration.

Location Groups	<u>×</u>
Specify the name of the Host (groups required to match this p	Credential Authorization Protocol (HCAP) location olicy.
NAC-NAP-IA]
	OK Cancel

Step 10. This task set up two conditions. Make sure you have the two entries for **Conditions** and then click **Next**.

ew Connection Request Poli	cyX
Specify C Specify the cor A minimum of	conditions nditions that determine whether this connection request policy is evaluated for a connection request, one condition is required.
Conditions:	Value
Decation Groups Day and time restrictions	NAC-NAP-IA Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursd
Condition description:	Add Edit Bernove
	Previous Next Einish Cancel



lew Connection Request Polic	y X
Specify C	onnection Request Forwarding
The connection	request can be authenticated by the local server or it can be forwarded to RADIUS servers in a
remote RADIUS	server group.
Settings:	Specify whether connection requests are processed locally, are forwarded to remote
Forwarding Connection	RADIUS servers for authentication, or are accepted without authentication.
Recuest	Authenticate requests on this server:
Authentication	To award requests to the following remote RADIUS server group for authentication:
Connection	New
Accounting	Accept users without validating credentials
	Previous Next Einish Cancel

Step 12. Ensure that **Override network policy authentication settings** is not checked. The authentication settings should be set up in the network policies.

w Connecti	ion Request Policy
	Specify Authentication Methods
R	Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP.
Uverride	e network policy authentication settings
These auth connection	entication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X s with NAP, you must configure PEAP authentication here.
EAP Type	are negotiated between NFS and the cliencum the order in which they are haved.
	Move Up Move Down
<u>A</u> dd	Edit Remove
Microso	ure authentication methods: aft Encrypted Authentication version 2 (MS-CHAP- <u>v</u> 2)
	r can o <u>h</u> ange password after it has expired of Encycled A development MS, CUART
L Use	r can change password after it has expired
Engrypi	ted authentication (CHAP)
	ypted authentication (PAP, SPAP) lients to connect without reportation an arthentication method.
	איז
	Previous Next Finish Cancel

Step 13. On the **Configure Settings** page, click **Next**. Click **Finish** to complete the configuration of the CRP.

Task 2: Configure System Health Validators

Network health requirements are defined by SHVs. For the test lab, the Windows Security Health Validator will require only that Windows Firewall is enabled.

- Step 1. Double-click Network Access Protection and then click System Health Validators.
- Step 2. In the middle pane, under Name, double-click Windows Security Health Validator.
- Step 3. In the Windows Security Health Validator Properties dialog box, click Configure.
- Step 4. Clear all check boxes except **A firewall is enabled for all network connections**, as shown in the following screenshot.

dows Vista Windows XP	
e the settings below to define a Windows Security Health your network.	Validator policy. Your selections define the requirements for client computers connecting
earn more	
Firewall	
A firewall is enabled for all network connections	
Virus Protection	
An antivirus application is on	Antivirus is up to date
Spyware Protection	
An antispyware application is on	Antispyware is up to date
Automatic Updating	
Automatic updating is enabled	
Security Update Protection	
Restrict access for clients that do not have all available	le security updates installed
Important and above	
Specify the minimum number of hours allowed since th	e client has checked for new security updates:
By default, clients can receive security updates from f both of the following sources.	Microsoft Update. If additional sources are required for your deployment, select one or
🗖 Window Server Update Services	🔽 Windows Update

Step 5. Click **OK** to close the **Windows Security Health Validator** dialog box and then click **OK** to close the **Windows Security Health Validator Properties** dialog box.
Task 3: Configure Health Policies

Health policies classify the client health status. The test lab defines a compliant and noncompliant health state.

- Step 1. Double-click Network Access Protection.
- Step 2. Right-click System Health Validator Templates and then click New.
- Step 3. In the Create New SHV Template dialog box, under Name, type Compliant.
- Step 4. Under Template type, verify that Client passes all SHV checks is selected.
- Step 5. Under Select which SHVs must pass, select the Windows Security Health Validator check box, as shown in the following screenshot.

ate Ne	w SHV Template	
Settings	1	
Create	a health validation template for a network po	licy.
Name:		
Compli	ant	
Templa	e type:	
Client p	asses all SHV checks	•
Select	which SHVs must pass:	
Name	Windows Conversity Unable Vehides	
	windows Security Realth Validat	
L		
•		>
	OK (Cancel Apply

Step 6. Click OK.

- Step 7. Right-click System Health Validator Templates and then click New.
- Step 8. In the Create New SHV Template dialog box, under Name, type Noncompliant.
- Step 9. Under Template Type, choose Client fails one or more SHV checks.
- Step 10. Under Select desired SHVs, select the Windows Security Health Validator check box, as shown in the following screenshot.

Create New SHV Template	×
Settings	
Create a health validation template for a network policy.	
Name:	
Noncompliant	
Template type:	
Client fails one or more SHV checks	
Select desired SHVs:	
Name	
Vindows Securty Health Validat	
OK Cancel Apply	

Step 11. Click OK.

Task 4: Configure Network Policies

Network policies evaluate information contained in client authorization requests and grant network access based on the results. Network policy determines whether a client complies with health policy and returns the appropriate posture token to Cisco Secure ACS using HCAP. If the client is determined to be noncompliant with health policy, then a quarantine state is sent to Cisco Secure ACS, which can optionally be updated to a compliant state.

- Step 1. Click Network Policies.
- Step 2. Delete the two default policies under **Name** by right-clicking the policies and then choosing **Delete**. Click **OK** to confirm each deletion.
- Step 3. Right-click Network Policies, point to New, and choose New Network Policy.
- Step 4. In the **New Network Policy window**, under **Policy name**, name the new network policy; in this example, type **Full-Access**. **Select Type of network access server** and choose **HCAP Server** from the pull-down menu. Then click **Next**.

New Network	Policy	×
-	Specify Network Policy Name and Connection Type	
	You can specify a name for your network policy and the type of connections to which the policy is applied.	
Policy name	x	
Full-Access		
Network conn	rection method	
Select the typ type or Vendo	e of network access server that sends the connection request to NPS. You can select either the network access server r specific.	
Type of n	etwork access server:	
HCAP Se	erver 🛛 🖌	
C Vendor sp		
10		
	Previous Next Einish Cancel	1
		4



/-	Health Policies The Health Policies condition restricts the policy to only clients that meet the health criteria specified in the health
	NAP-Capable Computers The NAP-Capable Computers condition specifies that connecting computers either are or are not capable of participating in NAP. This capability is determined by whether the client computer sends a statement of health to
17	Operating System The Operating System condition specifies the operating system, role, and architecture required for client computer configuration to match this policy.
0	Policy Expiration The Policy Expiration condition specifies when the network policy expires and is no longer evaluated by NPS. This condition is used with the NAP Enforcement setting that allows clients full network access for a limited time. If used for this policy, configure another NAP network policy for after the expiration time.
onne	ction
	Access Client IPv4 Address The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access

Step 6. From the **Health Policies** pull-down menu, choose **Compliant**, which was created in the previous task (Task 3). Click **OK** to go back to the **Select Condition** page and click **Next**.

- Step 7. In the Specify Access Permission window, choose Access granted and click Next.
- Step 8. In the **Configure Authentication Methods** window, deselect everything and select **Perform machine health check only**. Note that Microsoft NPS is used as the HCAP server, not the authentication server. Microsoft NPS is only performing a health check.

ew Network Po	olicy		×
	Configure Authentication M Configure one or more authentication metho authentication, you must configure an EAP ty Protected EAP in connection request policy, y	lethods ads required for the connection request to match ype. If you deploy NAP with 802.1X or VPN, you which overrides network policy authentication so	1 this policy. For EAP must configure ettings.
EAP types are ne	gotiated between NPS and the client in the ord	er in which they are listed. Move Up Move Down	
Add	Edit <u>Remove</u>		
Microsoft En User can Microsoft En User can User can User can	crypted Authentication version 2 (MS-CHAP ±2) change password after if has expired crypted Authentication (MS-CHAP) change password after if has expired theretication (CHAP)	(
Unencrypted	I authentication (PAP, <u>S</u> PAP) to connect without negotiating an authentication bins health check only.	in method.	

Step 9. In the Configure Constraints window, click Next and leave all options unchanged.

Step 10. In the Configure Settings window, first remove all predefined Standard RADIUS attributes (Framed-Protocol and Service-Type). Microsoft NPS communicates to Cisco Secure ACS using the HCAP protocol; therefore, no RADIUS attributes are involved. Then click NAP Enforcement in the settings list on the left side of the window. In NAP Enforcement settings pane that appears on the right, select Allow full network access and leave everything else deselected.

in meen on it is oney		
Configure NPS applies s are matched.	Settings ings to the connection request if all of the network policy co	nditions and constraints for the policy
f conditions and constraints ma Settings:	h the connection request and the policy grants access, settings	are applied.
RADIUS Attributes Standard Standard Vendor Specific Network Access Protection NAP Enforcement Extended State Routing and Remote Access Multilink and Bandwith Allocation Protocol (BAP)	Specify whether you want to enforce Network Access F Allow full network access Allows unrestricted network access for clients when the policy. Use this option for reporting mode. C Allow full getwork access for a limited time Allows unrestricted network access suitil the specific date and time, health policy is enforced and non-cord the restricted network. Date: 3/10/2008 Time C Allow full mitted access	Protection for this policy. the connection request matches ed date and time. After the specified mpliant computers can access only 8:26:59 PM restricted network for undates
 IP Filters Encryption IP Settings 	Non-compilant clients are allowed access only to a r Remediation Server Group and Troubleshooting URL To configure a Remediation Server Group, a Troubles Configure.	shooting URL, or both, click

- Step 11. Click Next and then click Finish to complete the Full-Access network policy.
- Step 12. Repeat Steps 1 through 9 for a network policy named Restricted-Access. In the Specify Condition window, select Health Policies and then choose Noncompliant, which was created in the previous task (Task 3).
- Step 13. In the Configure Settings window for a network policy named Restricted-Access, remove all predefined standard RADIUS attributes (Framed-Protocol and Service-Type). In the NAP Enforcement settings pane, select Allow limited access, and in the Auto remediation section, deselect Enable auto-remediation of client computers. Be sure to deselect the autoremediation in this section; otherwise, the NAP system changes the computer state (firewall state) immediately after IEEE 802.1x connection, and checking the switch port state (healthy or changed to quarantine VLAN) is difficult.

onfigure the settings for this netwo conditions and constraints match t	k policy. he connection request and the policy grants access, settings are applied.
RADIUS Attributes	C Allow full network access for a limited time
Vendor Specific	Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.
Network Access Protection	Date: 7/17/2008 💌 Time: 1:15:49 PM 🚟
Extended State	C Allow limited access Non-compliant clients are allowed access only to a restricted network for updates.
Routing and Remote Access Multilink and Bandwidth Allocation	Remediation Server Group and Troubleshooting URL To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.
Protocol (BAP)	Configure
IP Filters	Enable auto-remediation of client computers
IP Settings	in this policy.

Step 14. After configuring the **Configure Settings** window options, click **Next** and then click **Finish** to complete network policy configuration. This completes the Microsoft NPS setup.

Windows Vista Client Configuration

NAC-NAP interoperability architecture requires a client computer running Windows Vista. The Windows Vista configuration consists of three steps:

- Enable Network Access Protection Agent and Wired Autoconfiguration Service
- · Enable EAP enforcement client and Windows Security Center
- Install and configure the Cisco EAP-FAST Module

Task 1: Enable Network Access Protection Agent and Wired AutoConfig Service

The Network Access Protection Agent and Wired AutoConfig Services are the two main services that need to be enabled for NAP using IEEE 802.1x technologies. By default, these services are turned off and need to be manually turned on. Also, the service type needs to be set to Automatic so that these services are enabled on the next reboot of Windows Vista. Follow these steps to enable both NAP Agent and Wired AutoConfig services.

- Step 1. Choose Start > All Programs > Accessories, right-click Command Prompt, and choose Run as Administrator.
- Step 2. Type services.msc and press the Enter key. This operation opens a Services window.
- Step 3. In the list of services, right-click **Network Access Protection** Agent and choose **Properties**.
- Step 4. For Startup type, choose Automatic.
- Step 5. Under Service status, click Start, wait for the service to start, and then click OK.
- Step 6. In the list of services, right-click Wired AutoConfig and choose Properties.
- Step 7. For Startup type, choose Automatic.
- Step 8. Under Services status, click Start, wait for the service to start, and then click OK.
- Step 9. Close the services window.

Task 2: Enable EAP Quarantine Enforcement Client and Windows Security Center In addition to NAP Agent and Wired AutoConfig, EAP Quarantine Enforcement Client and Windows Security Center need to be enabled. The following steps show how to enable these essential clients.

- Step 1. Choose Start > All Programs, Accessories, right-click Command Prompt, and choose Run as Administrator.]
- Step 2. Type mmc and press the Enter key. This operation opens a window called Console1.
- Step 3. From the File menu, choose Add/Remove Snap-in.
- Step 4. Select NAP Client Configuration and then click Add.
- Step 5. In the NAP Client Configuration dialog box, click OK to accept the default selection Local computer (the computer on which this console is running).
- Step 6. Select Group Policy Object Editor and then click Add.
- Step 7. Click Finish to accept the default Group Policy Object selection Local Computer.
- Step 8. In the Add or Remove Snap-ins dialog box, click OK.
- Step 9. In the left pane of the Console1 window, double-click **NAP Client Configuration (Local Computer)** and then click **Enforcement Clients**.
- Step 10. In the middle pane, right-click EAP Quarantine Enforcement Client and then click Enable.
- Step 11. In the left pane, double-click Local Computer Policy, double-click Computer Configuration, double-click Administrative Templates, double-click Windows Components, and then click Security Center.
- Step 12. In the middle pane, double-click Turn on Security Center (Domain PCs only).
- Step 13. Select Enabled and then click OK.
- Step 14. Close the Console1 window.
- Step 15. Click No when prompted to save the console settings.

Note: Enable the NAP agent service on Vista. At the command prompt, enter the following command: net start napagent.

Note: Enable the NAP quarantine enforcement client (QEC) on Vista. At the command prompt, enter the following command: netsh nap cli set enforcement ID = 79623 ADMIN = "ENABLE".

Task 3: Install and Configure the Cisco EAP-FAST Module

These are the steps required to install and enable the Cisco EAP-FAST Module (IEEE 802.1x) on the Vista client.

- Step 1. First, obtain EAP-FAST Module through Microsoft Windows Update. The EAP-FAST files will be installed in C:\program files\Cisco Systems\Cisco EAP-FAST Module.
- Step 2. Choose Start > All Programs, Accessories, right-click Command Prompt, and choose Run as Administrator.
- Step 3. Next to Open, type control netconnections and then click OK.
- Step 4. Right-click Local Area Connection on the Network Connections screen and select properties.
- Step 5. Select the Authentication tab.

Note: This tab becomes available only when Wired AutoConfig service is started. If you do not see the Authentication tab, check the service status.

- Step 6. Select the Enable IEEE 802.1x authentication check box.
- Step 7. Under Choose a network authentication method, select Cisco EAP-FAST.
- Step 8. On the **Connection** tab, select **Use anonymous outer identity** and use the default identity of **anonymous**.
- Step 9. Select the Use Protected Access Credential option and select Allow automatic PAC provisioning. A protected access credential (PAC) authority will not be available at this point. You will first need to provision a PAC during the initial client authentication,
- Step 10. Select Validate Server Certificate and select the appropriate CA from the Trusted Root CA drop-down list. If your trusted root CA is not in the list, select the Validate Server Certificate check box and deselect the Do not prompt user to authorize new servers or trusted certification authorities check box. The next time the user is authenticated successfully, the trusted root CA certificate will be provisioned, with a prompt to verify the provisioned certificate.
- Step 11. On the User Credentials tab, the default setting Use Windows user name and password should be selected. If you are testing with a username and password that differs from the one used in the Windows logon, choose Prompt automatically for username and password.
- Step 12. Select the Authentication tab. For Authentication method, select EAP-MSCHAPv2. Also select the Allow fast reconnect and Enable posture validation options.

Configuration of IEEE 802.1x on the Cisco IOS Software Switch

In this section, you will configure the components to enable the base functions of IEEE 802.1x on a switch running Cisco IOS Software.

Task 1: Configure AAA on the NAD

Follow these steps to enable AAA for NAC Layer 2 802.1x on a Cisco IOS Software switch for NAC.

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

Cat3560(config)#aaa new model

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

Cat3560(config)#aaa authentication dot1x 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.

Cat3560(config)#aaa authorization network default group radius

Step 4. Configure the switch to use RADIUS for IEEE 802.1x accounting using the aaa accounting dot1x default start-stop group radius command.

Cat3560(config)#aaa accounting dot1x default start-stop group radius

Step 5. Verify that the VLANs and VLAN interfaces listed here have been preconfigured on the switch for NAC L2 802.1x.

VLAN Name	VLAN	Subnets
healthy	10	10.1.10.x/24
guest	20	10.1.20.x/24
quarantine	40	10.1.40/x/24
asset	50	10.1.50.x/24
voice	99	10.1.99.x/24

vlan 10
name healthy
!
vlan 20
name guest
!

```
vlan 40
name quarantine
1
vlan 50
name asset
1
vlan 99
name voice
T.
interface Vlan10
description healthy VLAN
ip address 10.1.10.254 255.255.255.0
ip helper-address 10.1.200.1
ı.
interface Vlan20
description guest VLAN
 ip address 10.1.20.254 255.255.255.0
 ip helper-address 10.1.200.1
!
interface Vlan40
description quarantine VLAN
ip address 10.1.40.254 255.255.255.0
ip helper-address 10.1.200.1
1
interface Vlan50
description asset VLAN
ip address 10.1.50.254 255.255.255.0
ip helper-address 10.1.200.1
1
interface Vlan99
description voice VLAN
 ip address 10.1.99.254 255.255.255.0
 ip helper-address 10.1.200.1
```

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

Cat3560(config)#dot1x system-auth-control

Step 7. Enable IEEE 802.1x on Fast Ethernet 1/1.

```
Cat3560(config-if)#dot1x port-control auto
Cat3560(config-if)#dot1x pae authenticator
Cat3560(config-if)#dot1x timeout reauth-period server
Cat3560(config-if)#dot1x reauthentication
Cat3560(config-if)#spanning-tree portfast
```

Network Access Profile Configuration for NAC L2 802.1x

In the following section, you will configure a network access profile (authentication, posture validation, and authorization) to support NAC L2 802.1x. Cisco Secure ACS supports two methods of configuring network access profiles.

- Add an empty profile and configure all the necessary information.
- Use the template profiles to customize the network access profile desired with the base information included in the template.

Cisco Secure ACE provides eight predefined network access profile templates:

- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x
- Microsoft IEEE 802.1x
- Wireless (NAC L2 802.1x)
- Agentless Host for L2 (802.1x fallback)
- Agentless Host for L3
- Agentless Host for L2 and L3

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

In this section of the lab, you use the NAC L2 802.1x network access profile template to create a base profile; you then make the necessary changes to customize this template.

- Step 1. Choose Network Access Profiles from the main menu and select Add Template Profile.
- Step 2. Create a Network Access Profile for IEEE 802.1x by selecting the NAC L2 802.1x template from the Template drop-down menu. Select Active to enable the profile.

	Create Profile from Template	
Name:	NAC-802.1x	
Description:		
Template:	NAC L2 802.1x	
Antium		

Step 3. Click Submit.

Task 2: Configure the Profile

Now you can configure the NAC-802.1x network access profile.

Step 1. On the **Network Access Profiles** screen, select the **NAC-802.1x** link for the new IEEE 802.1x profile.

		Network Access Profi	iles	?
	Name	Policies	Description	Active
0	NAC-802.1x	Protocols Authentication Posture Validation Authorization		YES

Step 2. Verify that the profile includes the following elements in **Rule Elements Table** under Advanced Filtering:

[026/009/001]cisco-av-pair	not-exist	aaa:service
[006]Service-Type !=10		

These elements should be automatically populated when the profile is created from the template.

Rule Elemen	ts Table:	
[026/009/0 [006]Servio	01)cisco-av-pair not-exist aaa:se se-Type != 10	rvice
	remove	
Attribute	[001]User-Name	•
Operator	=	•
Value		
Asenair-Value	10	

- Step 3. On the **Network Access Profiles** screen, select the **Protocols** link for the new IEEE 802.1x profile.
- Step 4. Notice that a portion of the EAP-FAST configuration is already selected as part of the base template. Leave the default EAP-FAST configuration as is except under **Posture** Validation, select **Optional** and choose **Quarantine** as the token from the drop-down list.

Note: This setting is very important; if a Vista client requests access and can provide only a user or machine identity credential and cannot provide SoH information (for instance, the NAP agent is not running), then this setting can still give the user access to the quarantine VLAN, instead of rejecting network access entirely.

Protocols Settings for NAC-802.1x	
Populate from Global	
Authentication Protocols	
Allow PAP	
Allow CHAP	
Allow MS-CHAPv1	
Allow MS-CHAPv2	
Allow Agentless Request Processing	

	EAP Configuration
	w RADIUS Key Wrap
PEAP	
	v EAP-MSCHAPv2
	W EAP-GTC
	v Posture Validation
Allov	v EAP-TLS
EAP-FA	ST
Allov	V EAP-FAST
💿 Use	PACs
	Allow full TLS renegotiation in case of Invalid PAC
<u> </u>	Allow anonymous in-band PAC provisioning
	Enable anonymous TLS renegotiation
¥ .	Allow authenticated in-band PAC provisioning
	Accept client on authenticated provisioning
	Require client certificate for provisioning
¥.	Allow Stateless session resume
3	Authorization PAC TTL 1 hours
O Do N	lot Use PACs
	Require client certificate
	Disable Client Certificate Lookup and Comparisons
	Assign Group 0: Default Group
When re	ceiving client certificate, select one of the following lookup methods:
OC	ertificate SAN lookup
() C	ertificate CN lookup
Allowed	inner methods
~	EAP-GTC
¥	EAP-MSCHAPv2
	EAP-TLS
Posture	Validation:
0	None
0	Required
0	Optional - Client may not supply posture data. Use token Quarantine 💌
0	Posture only

Step 5. Click Submit.

- Step 6. Select the **Authentication** link from the Network Access Profile screen for the profile you created.
- Step 7. Under Credential Validation Databases, use the arrow buttons to move Windows Database from Available Databases to Selected Databases. You are going to authenticate the user and machine using the IEEE 802.1x protocol against Microsoft Active Directory.



CLDAP Server:	Not Selected 💌						
	MAC Address	es	User Group				
● Internal ACS DB	No MA	No MAC Group Mappings					
	A	dd Delete					
1	Default Action						
If Agentless request was n	ot assigned a user-group:	0: Default	Group 🗸				
If Agentless request was n	ot assigned a user-group: OID Comparison	0: Default	Group 💌				
If Agentless request was n	OID Comparison	0: Default	Group 💌				
If Agentless request was n	OID Comparison	0: Default	Group 💌				
If Agentless request was n If Agentless request was n Enter OIDs seperated by o OMatch OIDs for 'AND' cor OMatch OIDs for 'OR' conc	OID Comparison or assigned a user-group: OID Comparison comma ndition set	0: Default	Group 💌				
If Agentless request was n If Agentless request was n Enter OIDs seperated by c Match OIDs for 'AND' con Match OIDs for 'OR' conc	OID Comparison comma ndition set	0: Default	Group				
If Agentless request was n If Agentless request	OID Comparison OID Comparison comma ndition set	0: Default	Group 💌				
If Agentless request was n If Agentless request	OID Comparison OID Comparison comma ndition set	D: Default	Group 🔽				

- Step 8. Click Submit to apply change.
- Step 9. On the **Network Access Profile** screen, select the **Posture Validation** link for the profile you created.
- Step 10. Under **Posture Validation Rule**, click **NAC-SAMPLE-POSTURE-RULE** link and click **Delete**. This rule is automatically generated when a NAC-802.1x profile is created using the template, and you are not going to use this rule in this task.
- Step 11. Click the Add Rule button for the Statement of Health Posture Validation Rule.
- Step 12. In the Name field, type the name of the policy. In this example, the name is ID-NPS.

- Step 13. In the Action section, enter a name for End Point Location. In this example, the name is NAC-NAP-IA. Remember that this value needs to be match the HCAP location ID that was configured in the Microsoft NPS connection request policies. Please refer to Network Policy Server Configuration, Task 1 Step 9 section to make sure the same Location Group string is used in the NPS configuration.
- Step 14. Select External Posture Validation Server. In this example, the name is the name of our Microsoft NPS ID-NPS.
- Step 15. Select the Reject User box. The Failure Posture Token should be dimmed.

Remember that the **Reject User** option for **Failure Action** can be turned off when the selected Microsoft NPS becomes available if Cisco Secure ACS can still send at least a posture token (in this case, a quarantine token) back to the NAD. For testing purposes, you will disable this feature and fail authentication when Microsoft NPS is not available.

		St	atement of Health Posture Validation Rule for N	AC-802.1x	ૢ
Name:		NAP-	SOH-POLICY		
			Action		
End Poir	nt Locati	on: NAC-N	IAP-IA		
		~ ~ ~	Select External Posture Validation Serve	r	
Select	Name	Description	Server Details	Failure Action	Failure Posture Token
c	ID-NPS		Primary https://10.1.100.10/hcap/hcapext.dll Secondary	🗖 Reject User	Quarantine 💌
S Healthy	ystem f	Posture Toke	System Posture Token Configuration URL Red	direct	
Checku	р				
Transiti	ion				
Quaran	tine				
Infecte	d		ſ		
Unknow	/n				
1					
			Submit Delete Cancel		

Step 16. For System Posture Token Configuration, type your remediation URL under URL Redirect. Upon quarantine, user HTTP traffic is redirected to this URL for further user notification purposes.

Step 17. Click the Submit button.

Note: We recommend the use of Failure Posture Token instead of Reject User in Failure Action. If the client responds with an empty SoH, meaning that no posture information is available on Vista, the system returns the configured token instead of rejecting the access request. It is highly likely that clients will not send SoH if the NAP agent is not configured properly or if dot3svc starts before NAP service.

Task 3: Configure Authorization section of the NAC-802.1x Profile

In the Authorization section of the profile, you can configure conditional authorization rules for the profile. For instance, you can configure authorization rule such as if the authentication request is for a user belongs to group A, and also if the health condition is healthy then apply the healthy authorization rule, otherwise go to next line for more restricted authorization rule. Following steps show how to build the conditional authorization rules for NAC-802.1x profile.

- Step 1. Select the Authorization link for the NAC-802.1x profile.
- Step 2. Enable authorization as shown in following screenshot. This configuration specifies the following conditions:
 - If the user is successfully authenticated against Active Directory, and if the user's Active Directory group is mapped to Cisco Secure ACS local group AD_User, and if SoH evaluation by Microsoft NPS returns the Healthy token, then send authorization rule 802.1x_Compliant_User.
 - If a device is successfully authenticated against Active Directory, and if the device's Active Directory group is mapped to Cisco Secure ACS local group AD_Machine, and if SoH evaluation by Microsoft NPS returns the Healthy token, then send authorization rule 802.1x_Compliant_Machine.
 - If a user or device is authenticated successfully against Active Directory but SoH evaluation by Microsoft NPS returns the Quarantine token, then send authorization rule 802.1x_Quarantine.
 - If none of these conditions match, then reject authentication.

	Cor	ndition			Action						
	User Group	ļ.	System Posture Token	e Deny Access	Shared RAC		Downloadable ACL				
) C	1: AD_User	~	Healthy 🖌		802.1x_Compliant_User	~	~				
D	2: AD_Asset	~	Healthy 🖌		802.1x_Compliant_Machine	~					
•	Any	~	Quarantine 💌		802.1x_Quarantine	~					
f a c natc	condition is not def hed condition:	ined or	there is no			4					
] In] In	clude RADIUS attrib clude RADIUS attrib	outes fr outes fr	om user's group om user record								
			,								

Step 3. Click Submit.

Task 6: Test Basic Client Authentication to Cisco Secure ACS

In this task, basic authentication between the client and Cisco Secure ACS will be performed. This will verify basic user authentication is occurring prior to validating posture information from the client to Microsoft NPS.

- Step 1. On the Windows Vista client, choose Start > All Programs > Accessories, right-click Command Prompt, and choose Run as Administrator. In the Command Prompt console, type control netconnections to display the Network Connections window.
- Step 2. In the Network Connections window, right-click Local Area Connection and select properties. If the user access control (UAC) asks permission to continue, click Continue and type your local administrator credential if necessary.
- Step 3. Click the **Authentication** tab. (If this tab is not available, you need to enable the Wired AutoConfig supplicant service.)
- Step 4. Verify that **Cisco: EAP-FAST** is selected as the network authentication method and then click the **Settings** button.

- Step 5. Click the Authentication tab for EAP-FAST Properties.
- Step 6. Uncheck Enable Posture Validation.

Note: Cisco Secure ACS is configured to accept access from a client that cannot provide any SoH information but return the quarantine token. If authentication succeeds with a valid user ID and password, the client PC should be assigned to the quarantine VLAN, in this case VLAN 40, and DHCP IP address scope 10.1.40.x/24 should be assigned to it.

Step 7. After successful authentication is confirmed, return EAP-FAST configuration to the original setting; that is, enable **Posture Validation** on the **Authentication** tab.

Basic authentication for EAP-FAST is complete.

Testing the NAC IEEE 802.1x Function

This section helps you verify that IEEE 802.1x (NAC L2 802.1x) is configured and functioning properly. Authentication will occur between the client and Cisco Secure ACS over EAP-FAST. The health information from the Vista client will be gathered by Cisco Secure ACS and forwarded to Microsoft NPS over HCAP for verification and compliance checking. On the basis of these results, a posture token and accompanying policy will be downloaded to the switch from Cisco Secure ACS and assigned to the client session. With IEEE 802.1x, a specific VLAN quarantine client is assigned to the port as an enforcement mechanism. (See Figure 2 at the beginning of this guide.)

To be considered healthy and to be placed in the healthy role, the Vista client must correctly return the required SoH information to Cisco Secure ACS and Microsoft NPS. The system health requirements specified in Microsoft NPS must be met for the client to be passed an application posture token of "healthy." In the example topology, Fast Ethernet port 0/1 is configured for IEEE 802.1x (NAC L2 802.1x).

Task 1: Test Scenario 1

In test scenario 1, shown here, user authentication is performed as well as posture validation for the client.

Test Scenario 1								
Scenario	User authentication and posture validation							
Description	Perform user authentication and posture validation for the client using IEEE 802.1x							
Authentication context	User							
VLAN settings	 Port VLAN: VLAN 1 (default) User VLAN: VLAN 10 (VLAN name = healthy) 							

- Step 1. On the Windows Vista Client, choose Start > All Program > Accessories > Command Prompt. At the Command Prompt console, type control netconnections.
- Step 2. In the **Network Connections** window that opens, right-click **Local Area Connection** and select **properties**. If the UAC asks permission to continue, click **Continue** and type your local administrator credential, if necessary.
- Step 3. Select the **Authentication** tab. (If this tab is not available, you need to enable the Wired AutoConfig supplicant service.)

- Step 4. Verify that **Cisco: EAP-FAST** is selected as the network authentication method and then click the **Settings** button.
- Step 5. On the User Credentials tab, select Prompt automatically for username and password.
- Step 6. Connect the client to the switch port Fast Ethernet 0/1. Alternatively, enter the shut and then the **no shut** command in the interface. On the client, you should see a credential request from the supplicant similar to the one in the following screenshot.





Step 7. Click the notification icon, and you will be prompted to enter user credentials.

Step 8. Enter the user credentials for authentication. In this example, the username is **user1**, and the password is **cisco123**.

<u>je-</u>	<u>User-</u> Name	<u>Group-</u> <u>Name</u>	<u>Caller-ID</u>	NAS- Port	NAS-IP- Address	Network Access Profile Name	Shared RAC	Downloadable ACL	<u>System-</u> Posture- Token	Application- Posture- Token	<u>Reason</u>	EAP Type	EAP Type Name
ок	ID\user1	AD_User	00-0D-60-FC- 9C-38	50001	10.1.100.254	NAC- 802.1x	802.1x_Compliant_User	n	Healthy	xe	Posture State=1 Extended State=0 returned by: Evaluated by policy: ID-NPS	43	EAP- FAST

Step 9. View the Cisco Secure ACS **Passed Authentication** log to verify successful client authentication and policy assignment.

Step 10. On the switch, enter the show dot1x interface FastEthernet 0/1 details command to verify the current status of the client.

PAE	= AUTHENTICATOR
PortControl	= AUTO
ControlDirection	= Both
HostMode	= SINGLE_HOST
ReAuthentication	= Enabled
QuietPeriod	= 60
ServerTimeout	= 30
SuppTimeout	= 30
ReAuthPeriod	= (From Authentication Server)
ReAuthMax	= 2
MaxReq	= 2
TxPeriod	= 30
RateLimitPeriod	= 0
Dotlx Authenticator Clie	nt List
Domain	= DATA
Domain Supplicant	= DATA = 000d.60fc.9c38
Domain Supplicant Auth SM State	<pre>= DATA = 000d.60fc.9c38 = AUTHENTICATED = JDLE</pre>
Domain Supplicant Auth SM State Auth BEND SM State	<pre>= DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE</pre>
Domain Supplicant Auth SM State Auth BEND SM State Port Status	<pre>= DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED</pre>
Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod	<pre>= DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600</pre>
Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction	<pre>= DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate</pre>
Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction TimeToNextReauth	<pre>= DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate = 3593</pre>
Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction TimeToNextReauth Authentication Method	<pre>= DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate = 3593 = Dot1x</pre>
Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction TimeToNextReauth Authentication Method Posture	<pre>= DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate = 3593 = Dot1x = Healthy</pre>
Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction TimeToNextReauth Authentication Method Posture Authorized By	<pre>= DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate = 3593 = Dot1x = Healthy = Authentication Server</pre>

Step 11. Enter the show vlan command to verify that the switch port has been placed in the correct VLAN.

VLAN	Name	Status	Ports
1	default	active	Fa0/7
10	healthy	active	Fa0/1, Fa0/2
20	guest	active	
30	contractor	active	
40	quarantine	active	
50	asset	active	
99	voice	active	Fa0/1, Fa0/2

Task 2: Test Scenario 2

In test scenario 2, shown here, user authentication is performed as well as posture validation for the client, but this time you will disable Windows Firewall to verify that the basic quarantine and remediation functions are working.

Test Scenario 2								
Scenario	User authentication and noncompliant posture validation							
Description	Perform user authentication and posture validation for the client using IEEE 802.1x when Windows Firewall is disabled							
Authentication context	User							
VLAN settings	 Port VLAN: VLAN1 (default) User VLAN: VLAN 10 (VLAN name = healthy) Quarantine VLAN: VLAN 50 (VLAN name = quarantine) 							

- Step 1. Choose Start > All Programs > Accessories, right-click Command Prompt, and choose Run as administrator. Type your administrative credential at the UAC prompt and click Continue.
- Step 2. Type **netsh firewall set opmode disable** to disable Windows Firewall. As soon as the command above is issued, the NAP agent is notified that the health state has changed, and it will initiate an EAPoL-Start 802.1x control packet to trigger IEEE 802.1x reauthentication with new health information. As a result of reauthentication, the client is now considered noncompliant; therefore, it is placed in the quarantine VLAN, and the user is notified that the computer does not meet the requirements of the network policy, as shown here.



Step 3. Click this balloon message. Another window appears detailing why the computer does not meet the requirements of the network policy.



Step 4. In this test, Microsoft NPS is configured to perform autoremediation when Windows Firewall is disabled. As a result, when Microsoft NPS detects that the client Windows Firewall is disabled, it tries to reenable the firewall as a remediation process. You will see this process right after you disable Windows Firewall. When the firewall is forcefully enabled as a remediation process, the user will be notified that the remediation process is complete in a balloon message as shown here.



Step 5. Click this balloon message. Another window appears detailing the remediation process, as shown here.



Step 6. View the Cisco Secure ACS **Passed Authentication** log. You can now see that the client was quarantined once and then placed back in the healthy VLAN immediately after Microsoft NPS performed the remediation process.

÷	<u>Time</u>	Message- Type	<u>User-</u> Name	<u>Group-</u> <u>Name</u>	Caller- ID	NAS- Port	NAS-IP- Address	Network Access Profile Name	Shared RAC	<u>System-</u> Posture- Token	<u>Reason</u>	EAP Type	EAP Type Name	PEAP/EAP EAST- Clear- Name
2008	12:47:41	Authen OK	ID\user1	. AD_User	00-1C- 25-14- 79-E2	50001	10.1.100.254	NAC- 802.1x	802.1x_Compliant_User	. Healthy	Posture State=1 Extended State=0 returned by: Evaluated by policy: ID-NPS	43	EAP- FAST	anonymous
2008	12:47:40	Authen OK	ID\user1	AD_User	00-1C- 25-14- 79-E2	50001	10.1.100.254	NAC- 802.1x	802.1x_Quarantine	Quarantine	Posture State=2 Extended State=0 e returned by: Evaluated by policy: ID=NDS	43	EAP- FAST	anonymous

Step 7. Notice in Reason field of the Cisco Secure ACS Passed Authentication log that the Posture State value changed from 2 to 1. Posture State=2 means that the SoH information sent from the client PC did not meet the policy requirements configured on Microsoft NPS. Posture State=1 means that the client passed all health checks on Microsoft NPS.

Task 3: Test Scenario 3

In test scenario 3, shown here, both computer and user authentication is performed as well as posture validation for the client. By default, the IEEE 802.1x supplicant on the Vista client will attempt both machine and user authentication.

Test Scenario 3				
Name	Computer and user authentication IEEE 802.1x and posture validation			
Description	Perform computer and user authentication and posture validation for the client			
Authentication context	machineOrUser (default)			
VLAN settings	 Port VLAN: VLAN1 (default) Computer VLAN: VLAN50 (VLAN name = asset) User VLAN: VLAN 10 (VLAN name = healthy) 			

Step 1. Verify that machine authentication is enabled in Cisco Secure ACS by navigating on the Cisco Secure ACS web console to System Configuration > Global Authentication Setup > EAP-FAST Configuration.

Step 2. In the EAP-FAST settings, verify that Allow Machine Authentication is enabled.

C cortinoato on lookup	
Allow Machine Authentication	
Machine PAC TTL	1 weeks 💌
Allow Stateless session resume	
Authorization PAC TTL	1 hours 🖌
Allowed inner methods	
EAP-GTC	
EAP-MSCHAPv2	
EAP-TLS	

Step 3. Verify that your Vista supplicant configuration is set to perform both machine and user authentication by entering the following command at the command prompt in Vista:

netsh lan show profile

```
Profile on interface Local Area Connection
_____
Applied: User Profile
   Profile Version
                      : 1
                      : Wired LAN
   Туре
   AutoConfig Version
                      : 1
   802.1x
                      : Enabled
   802.1x
                      : Not Enforced
   EAP type
                      : Cisco: EAP-FAST
   802.1X auth credential : Machine or user credential
   Cache user information : No
```

- Step 4. Reboot your Windows Vista machine and wait for the CTRL + ALT + DELETE message to appears.
- Step 5. On the switch, enter the **show dot1x interface FastEthernet 0/1 details** command to verify the current status of the client.

Cat3560#show dot1x int B	CastEthernet 0/1 details
Dotlx Info for FastEther	met0/1
 PAE	= AUTHENTICATOR
PortControl	= AUTO
ControlDirection	= Both
HostMode	= SINGLE_HOST
ReAuthentication	= Enabled
QuietPeriod	= 60
ServerTimeout	= 30
SuppTimeout	= 30
ReAuthPeriod	= (From Authentication Server)
ReAuthMax	= 2
MaxReq	= 2
TxPeriod	= 30
RateLimitPeriod	= 0
Dotix Authenticator Clie	ent List
Domain	= DATA
Supplicant	= 000d.60fc.9c38
Auth SM State	= AUTHENTICATED
Auth BEND SM State	= IDLE
Port Status	= AUTHORIZED

ReAuthPeriod	=	60
ReAuthAction	=	Reauthenticate
TimeToNextReauth	=	50
Authentication Method	=	Dotlx
Posture	=	Quarantine
Authorized By	=	Authentication Server
Vlan Policy	=	40

Step 6. Enter the **show vlan** command to verify that the switch port has been placed in the correct VLAN.

Cat35	560#show vlan		
VLAN	Name	Status	Ports
1	default	active	Fa0/7
10	healthy	active	Fa0/2
20	guest	active	
30	contractor	active	
40	quarantine	active	Fa0/1
50	asset	active	
99	voice	active	Fa0/1, Fa0/2

Step 7. Notice that although machine authentication succeeds, the Vista client is placed in quarantine VLAN 40. This behavior occurs because the Windows Vista supplicant service starts much earlier than the NAP agent. When authentication requests SoH information, the NAP agent is not available, and therefore no SoH information is sent to Cisco Secure ACS. Cisco Secure ACS performs authentication first against Active Directory; however, because there is no SoH information, it uses the Posture Optional method and immediately assigns the Quarantine token.

osture Validation:		
○ None		
O Required		
⊙ Optional - Client may not supply posture data. Use token	Quarantine	~
○ Posture only		

This behavior is why the NAD receives the quarantine VLAN for machine authentication. As soon as the NAP agent starts, it reevaluates the system and tries to reauthenticate the device. The following are the results of the **show dot1x interface FastEthernet0/1 detail** command after the NAP agent starts upon successful machine authentication, and also after the successful user authentication.

PAE	= AUTHENTICATOR
PortControl	= AUTO
ControlDirection	= Both
HostMode	= SINGLE_HOST
ReAuthentication	= Enabled
QuietPeriod	= 60
ServerTimeout	= 30
SuppTimeout	= 30
ReAuthPeriod	= (From Authentication Server)
ReAuthMax	= 2
MaxReq	= 2
TxPeriod	= 30
RateLimitPeriod Dotlx Authenticator Clie	= 0 ent List
RateLimitPeriod Dotlx Authenticator Clie Domain	= 0 ent List = DATA
RateLimitPeriod Dotlx Authenticator Clie Domain Supplicant	= 0 ent List = DATA = 000d.60fc.9c38
RateLimitPeriod Dotlx Authenticator Clie Domain Supplicant Auth SM State	<pre>= 0 ent List = DATA = 000d.60fc.9c38 = AUTHENTICATED</pre>
RateLimitPeriod Dot1x Authenticator Clie Domain Supplicant Auth SM State Auth BEND SM State	<pre>= 0 ent List = DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE</pre>
RateLimitPeriod Dotlx Authenticator Clie Domain Supplicant Auth SM State Auth BEND SM State Port Status	<pre>= 0 ent List = DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED</pre>
RateLimitPeriod Dotlx Authenticator Clie Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod	<pre>= 0 ent List = DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600</pre>
RateLimitPeriod Dotlx Authenticator Clie Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction	<pre>= 0 ent List = DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate</pre>
RateLimitPeriod Dotlx Authenticator Clie Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction TimeToNextReauth	<pre>= 0 ent List = DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate = 3472</pre>
RateLimitPeriod Dotlx Authenticator Clie Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction TimeToNextReauth Authentication Method	<pre>= 0 ent List = DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate = 3472 = Dot1x</pre>
RateLimitPeriod Dotlx Authenticator Clie Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction TimeToNextReauth Authentication Method Posture	<pre>= 0 ent List = DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate = 3472 = Dot1x = Healthy</pre>
RateLimitPeriod Dotlx Authenticator Clie Domain Supplicant Auth SM State Auth BEND SM State Port Status ReAuthPeriod ReAuthAction TimeToNextReauth Authentication Method Posture Authorized By	<pre>= 0 ent List = DATA = 000d.60fc.9c38 = AUTHENTICATED = IDLE = AUTHORIZED = 3600 = Reauthenticate = 3472 = Dot1x = Healthy = Authentication Server</pre>

Dotlx Info for FastEtherr	net0/1
PAE	= AUTHENTICATOR
PortControl	= AUTO
ControlDirection	= Both
HostMode	= SINGLE_HOST
ReAuthentication	= Enabled
QuietPeriod	= 60
ServerTimeout	= 30
SuppTimeout	= 30
ReAuthPeriod	= (From Authentication Server)
ReAuthMax	= 2
MaxReq	= 2
TxPeriod	= 30
RateLimitPeriod	= 0

Domain	= DATA
Supplicant	= 000d.60fc.9c38
Auth SM State	= AUTHENTICATED
Auth BEND SM State	= IDLE
Port Status	= AUTHORIZED
ReAuthPeriod	= 3600
ReAuthAction	= Reauthenticate
TimeToNextReauth	= 3139
Authentication Method	= Dotlx
Posture	= Healthy
Authorized By	= Authentication Server
Vlan Policy	= 10

Here is the Cisco Secure ACS log showing the flow of those authentications by device and user.

<u>User-Name</u>	<u>Group-</u> <u>Name</u>	<u>Caller-</u> <u>ID</u>	NAS- Port	NAS-IP- Address	Network Access Profile Name	Shared RAC	Downloadable ACL	<u>System-</u> Posture- Token	Application- Posture- Token	Reason
ID\user1	AD_User	00-0D- 60-FC- 9C-38	50001	10.1.100.254	NAC- 802.1x	802.1x_Compliant_User		Healthy	τ.	Posture State=1 Extended State=0 returned by: Evaluated by policy: ID-NPS
host/vista01.id.local	AD_Asset	00-0D- 60-FC- 9C-38	50001	10.1.100.254	NAC- 802.1x	802.1x_Compliant_Machine	5	Healthy	680	Posture State=1 Extended State=0 returned by: Evaluated by policy: ID-NPS
host/vista01.id.local	AD_Asset	00-0D- 60-FC- 9C-38	50001	10.1.100.254	NAC- 802.1×	802.1x_Quarantine		Quarantine	- X7	Posture State=2 Extended State=0 returned by: Evaluated by policy: ID-NPS

Task 4: Test Scenario 4

In test scenario 4, shown here, Fast Ethernet port 0/1 is configured to perform NAC Layer 2 IEEE 802.1x (EAP-FAST) authentication. By default, the IEEE 802.1x supplicant on the client will attempt both machine and user authentication. The supplicant configuration on the Vista client will need to be modified to perform only machine authentication.

Test Scenario 4				
Name	Computer authentication IEEE 802.1x and posture validation			
Description	erform machine authentication and posture validation			
Authentication context	Machine			
VLAN settings	 Port VLAN: VLAN1 (default) Computer VLAN: VLAN 50 (VLAN name = asset) 			

Step 1. The profile can be edited using a text editor or an Extensible Markup Language (XML) editor. To export the default configuration profile, use following command:

```
netsh lan export profile folder="path_to_xml_file"
interface="interface_name"
```

Example: netsh lan export profile folder="c:\profiles" interface="LAN"

Use the following command to reimport the configuration profile after editing is completed:

netsh lan add profile filename="path_to_xml_file" interface="interface_name"

Example: netsh lan add profile filename="c:\profiles\LAN.xml" interface="LAN"

- Step 2. On the Windows Vista Client, choose Start > All Program > Accessories > Command Prompt. In the command prompt console, type netsh to enter netsh command mode.
- Step 3. Type **Ian** and **show profile**. Verify that the output from the previous task shows the values shown here.

```
Profile on interface Local Area Connection
_____
Applied: User Profile
   Profile Version
                      : 1
                      : Wired LAN
   Type
                      : 1
   AutoConfig Version
   802.1x
                      : Enabled
   802.1x
                      : Not Enforced
   EAP type
                      : Cisco: EAP-FAST
   802.1X auth credential : Machine or user credential
   Cache user information : No
```

Step 4. Enter the command shown here to export the profile (for this operation, the wired interface name is Local Area Connection; if the name of your interface is different, change the name here accordingly). After you export the profile, exit the netsh command line by typing bye and then start editing the XML profile with Notepad or some other text editor.

```
netsh lan>export profile folder=. interface="Local*"
Interface: Local Area Connection
Profile File Name: .\Local Area Connection.xml
1 profile(s) were exported successfully.
netsh lan>bye
C:\Users\user1.ID>notepad "Local Area Connection.xml"
```

Step 5. When editing the Local Area Connection.xml file, add <authMode>machine</authMode> immediately before the <EAPConfig> element in this XML file as shown here.

```
--- Skipped ---
<OneX xmlns="http://www.microsoft.com/networking/OneX/v1">
<cacheUserData>false</cacheUserData>
<authMode>machine</authMode>
<EAPConfig>
--- Skipped ---
```

- Step 6. After editing the XML file, save the change and close the text editor. Go back to the command prompt console and enter **netsh lan** mode.
- Step 7. Type the following command to add the edited profile to the interface:

```
netsh lan>add profile filename="Local Area Connection.xml"
interface="Local*"
```

The profile was added successfully on the interface Local Area Connection.

Step 8. Verify your change in **authMode** so that only machine authentication is enabled.

```
netsh lan>show profile
Profile on interface Local Area Connection
_____
Applied: User Profile
   Profile Version
                     : 1
                     : Wired LAN
   Type
   AutoConfig Version
                     : 1
   802.1x
                     : Enabled
   802.1x
                     : Not Enforced
                     : Cisco: EAP-FAST
   EAP type
   802.1X auth credential : Machine credential
   Cache user information : No
```

- Step 9. Reboot your Windows Vista machine and wait for the CTRL + ALT + DELETE message to appear.
- Step 10. On the switch, enter the **show dot1x interface FastEthernet 0/1** details command to verify the current status of the client.

```
Cat3560#show dot1x int FastEthernet 0/1 details
Dot1x Info for FastEthernet0/1
_____
PAE
                      = AUTHENTICATOR
PortControl
                      = AUTO
ControlDirection
                     = Both
HostMode
                      = SINGLE_HOST
                     = Enabled
ReAuthentication
QuietPeriod
                      = 60
                      = 30
ServerTimeout
```

SuppTimeout	= 30
ReAuthPeriod	= (From Authentication Server)
ReAuthMax	= 2
MaxReq	= 2
TxPeriod	= 30
RateLimitPeriod	= 0
Dot1x Authenticator Clies	nt List
Domain	= DATA
Supplicant	= 000d.60fc.9c38
Auth SM State	= AUTHENTICATED
Auth BEND SM State	= IDLE
Port Status	= AUTHORIZED
ReAuthPeriod	= 60
ReAuthAction	= Reauthenticate
TimeToNextReauth	= 50
Authentication Method	= Dotlx
Posture	= Quarantine
Authorized By	= Authentication Server
Vlan Policy	= 40

Step 11. Enter the **show vlan** command to verify that the switch port has been placed in the correct VLAN.

Cat3	560#show vlan				
VLAN	Name	Status	Ports		
-					
1	default	active	Fa0/7		
10	healthy	active	Fa0/2		
20	guest	active			
30	contractor	active			
40	quarantine	active	Fa0/1		
50	asset	active			
99	voice	active	Fa0/1, Fa0/2		

Step 12. Notice that although machine authentication succeeds, the Vista client is placed in quarantine VLAN 40. This behavior occurs because the Windows Vista supplicant service starts much earlier than the NAP agent. When authentication requests SoH information, the NAP agent is not available, and therefore no SoH information is sent to Cisco Secure ACS. Cisco Secure ACS performs authentication first against Active Directory; however, because there is no SoH information, it uses the Posture Optional method and immediately assigns the Quarantine token. This behavior is why the NAD receives the quarantine VLAN for machine authentication. As soon as the NAP agent starts, it reevaluates the system and tries to reauthenticate the machine. Here are the results of the show dot1x interface FastEthernet0/1 detail command after the NAP agent starts.

Note: This is the setting for machine authentication only. Therefore, IEEE 802.1x authentication is not triggered upon Windows user logon.

Dotlx Info for FastEther	net0/1
PAE	= AUTHENTICATOR
PortControl	= AUTO
ControlDirection	= Both
HostMode	= SINGLE_HOST
ReAuthentication	= Enabled
QuietPeriod	= 60
ServerTimeout	= 30
SuppTimeout	= 30
ReAuthPeriod	= (From Authentication Server)
ReAuthMax	= 2
MaxReq	= 2
TxPeriod	= 30
RateLimitPeriod	= 0
Dot1x Authenticator Clie	nt List
Domain	= DATA
Supplicant	= 000d.60fc.9c38
Auth SM State	= AUTHENTICATED
Auth BEND SM State	= IDLE
Port Status	= AUTHORIZED
ReAuthPeriod	= 3600
ReAuthAction	= Reauthenticate
TimeToNextReauth	= 3472
Authentication Method	= Dotlx
Posture	= Healthy
Authorized By	= Authentication Server
Vlan Policy	= 50

Tuning the Windows Vista Supplicant Function

The Single Sign On feature is added to the Windows Vista supplicant on both the wireless interface (introduced in the release version of Vista) and wired interface (supported on Service Pack 1 [SP1]). With this feature, supplicant behavior can be optimized to run more synchronously with the Microsoft Windows startup process, making IEEE 802.1x deployment much easier than before.

Two types of authentication are introduced with the Single Sign On feature: PreLogon and PostLogon. With PreLogon, Single Sign On (IEEE 802.1x user authentication using the Windows domain credential) is performed before the user logs on. With this authentication method, Windows can make sure that network authentication establishes a network connection with the user credential before initiating user domain logon.

With the PostLogon authentication method, Single Sign On (IEEE 802.1x user authentication) is performed immediately after the user logs on. This type of authentication is preferred for authentication with a user certificate, since the user certificate is typically stored in a specific user account, which requires user logon to access.

For information about the options you can use to tune Single Sign On elements, see http://msdn2.microsoft.com/en-us/library/ms706527.aspx. These elements can be configured by editing the XML profile, adding **singleSignOn** elements and subelements.

The following is a sample profile, with **singleSignOn** set to **preLogon** mode.

```
<?xml version="1.0" ?>
- <LANProfile
xmlns="http://www.microsoft.com/networking/LAN/profile/v1">
- <MSM>
- <security>
  <OneXEnforced>false</OneXEnforced>
  <OneXEnabled>true</OneXEnabled>
- <OneX xmlns="http://www.microsoft.com/networking/OneX/v1">
  <cacheUserData>false</cacheUserData>
  <supplicantMode>compliant</supplicantMode>
  <authMode>machine</authMode>
- <singleSignOn>
 <type>preLogon</type>
 <maxDelay>10</maxDelay>
  <allowAdditionalDialogs>true</allowAdditionalDialogs>
  <maxDelayWithAdditionalDialogs>10</maxDelayWithAddtionalDialogs>
  <userBasedVirtualLan>true</userBasedVirtualLan>
  </singleSignOn>
- <EAPConfig>
----- omitted ------
 </EAPConfig>
  </OneX>
 </security>
  </MSM>
  </LANProfile>
```

These elements can also be configured with group policy on Windows Server 2003 or 2008. The next task describes a feature that allows the administrator to configure supplicant behavior as well as EAPHost options remotely on Windows Server 2003 or 2008 using group policy. The task focuses on deployment options for the Cisco EAP-FAST Module.

Task 1: Configure Supplicant with Group Policy

Many elements and options of supplicant as well as EAPHost components (including the Cisco EAP-FAST Module) can be remotely configured and provisioned using Windows Server 2003 or 2008. This documentation assumes that Active Directory is running on Windows Server 2003. By default, Windows Server 2003 domain policy does not contain the schema needed to configure the Windows Vista supplicant and EAPHost. You need to follow the steps presented here to make those configuration options available on Windows Server 2003.

- Step 1. On a server running Windows Server 2003, copy the adprep directory, located in <yourDVDdrive>:\sources\adprep on the Windows Server 2008 DVD, to a temporary directory on your local system. (You can create a temporary directory named temp on your C drive on a server running Windows Server 2003 and copy adprep to the directory.)
- Step 2. On Windows Server 2003, launch the command prompt (choose Start > All Programs > Accessories > Command Prompt) and open the adprep directory you just copied from Windows Server 2008 DVD (cd c:\temp\adprep).
- Step 3. The **adprep** directory contains a program called **adprep.exe**. You will use this program to extend your Active Directory schema. Note that this command will be applied to your Active Directory schema, so use this command with caution. We highly recommended that you test this upgrade in your testing environment first. At the command prompt, enter the following command:

C:\temp\adprep\adprep.exe /forestprep

- Step 4. At the command prompt, you will be asked to confirm the command and change. Confirm the command by typing C and pressing the **Enter** key.
- Step 5. On the Windows Vista SP1 client where the Cisco EAP-FAST Module is installed, you need to install another program called Group Policy Management Console (GPMC), so you can make changes to Active Directory group policy. By default, GPMC is not installed on Windows Vista SP1. From Windows Vista SP1, GPMC is included in a package called Remote Server Administrator Tool (RSAP), which can be found as KB941314 at the Microsoft website. You have to install RSAP first and enable GPMC as a Windows component. Download the RSAP installer to the desktop. Click Windows6.0-KB941314-x86 installer and follow the instructions to complete RSAP installation.
- Step 6. After installing RSAP, choose Start > Control Panel > Programs > Programs and Features and select Turn Windows features on or off. Then choose Remote Server Administration Tools > Feature Administration Tools and select Group Policy Management Tools. Click OK to enable GPMC.]
- Step 7. With GPMC installed, you can browse Group Policy on your Active Directory domain from Windows Vista SP1. Start GPMC by choosing Start > All Programs > Accessories > Run and typing gpmc.msc. On the User Account Control screen, click Continue to display the Group Policy Management screen. (This example assumes that you are running this program from an account with administrative privileges.)
- Step 8. As shown in the following screenshot, browse to your domain and select Default Domain Policy. On the right pane of the screen, select the Settings tab and right-click Computer Configuration (Enabled). In the context menu, choose Edit.

Image: Statum, Vance Watsdam, May	B Group Policy Management					
Image: Section 1.1 Image: Section 1.1 Image: Section	Ag File Action View Window Help			10		
Proving Markage Image: An and Decay Index (Markage) Image: An and Anandor (Markage) Image: An and Anandor (Markage) Image: An and Ananandor (Markage) Image: An an a	** 200 8 8 0					
Image: Control and Cont	In Group Policy Management	Default Domain Policy				
Image: Second	A Forest id.local Domains ID Id.local B Default Domain Policy	Score Details Sethig: Delegation				
distribution branching in general constants in g		Default Domain Ballow				
Introduction Second Introduction <td>Data collected on 8/25/2007 5:15:47 AM</td> <td></td> <td>store of</td>		Data collected on 8/25/2007 5:15:47 AM		store of		
Bount Conclusion Bount Conclusion Con	Software Installation	Computer Configuration (Enabled)		tide		
 J damp Kalo Qakuta Sanda Sanda Sa) 🔯 Domain Controllars	Windows Settings		tais		
Year Security Staticity Security Staticy Security Staticy Year Year Security Security Staticy Year Year Security Security	Group Policy Objects	Scripts		tex		
tion p king kaladag Group King Kaladag Group King Kaladag Group King Kaladag Ka	Ell Ster	Security Settings		bala		
Comp Patry Reads Account Philosoftward Ladout Patry data Load Philosoftward Control data Web Start Philosoftward Patry data Mark for Philosoftward Patry data Web Conference data Reads Filter Philosoftward data Web Start data Reads Filter Philosoftward data Web Start data Reads Filter Philosoftward data Philosoftward Patry data Philosoftward Philosoftward data Septimic data	Croup Policy Moduling	Account Policies/Password Poli	koy	1000		
Accourt Philosof Voltem Data Werders Kleward (2021) 11 Tele Data Werders Kleward (2021) 12 Tele Data Kalek for philosof Philosof Data Data Werders Kleward (2021) 12 Tele Data Data Werders Kleward (2021) 12 Tele Data Data Werders Kleward (2021) 12 Tele Data Data Werders Kleward (2021) 12 Tele Kleward (2021) 12 Data Data Werders Kleward (2021) 12 Tele Kleward (2021) 12 Data Data Werders Kleward (2021) 12 Tele Kleward (2021) 12 Data Data Werders Kleward (2021) 12 Tele Kleward (2021) 12 Data Data Werders Kleward (2021) 12 Tele Kleward (2021) 12 Data Data Data Werders Kleward (2021) 12 Tele Kleward (2021) 12 Data Data Data Werders Kleward (2021) 12 Tele Kleward (2021) 12 Data Data Data Werders Kleward (2021) 12 Tele Kleward (2021) 12 Data Data Data	Croup Policy Raturs	Account Policies/Account Lock	senit Policy	states		
Lead Points-Rised Quite Educe Value (or phosen Through Quite) Ball Nalue (or phosen Through Quite) Ball Week (or phosen Through Quite) Ball Week (or phosen Through Quite) Ball Week (or phosen Through Quite) Ball Second Quite) Ball Neek (or phosen Through Quite) Ball Neek (or phosen Through Quite) Ball Neek (or phosen Through Quite) Ball Second Quite) Ball		Account Policies/Nerberos Poli-	cy .	1000		
Wedess Headed 0011 Factor 676 Marke fory Michaed/Factor 666 Uvor Carly Angenetic Standard 666 Wedens Simpler 666 Wedens Simpler 6662 Singlet 6662		Local Policies/Security Options		show		
Nate: Key Holoson/Tocogn Intelligence I		Wireless Network (802.11) P *		dew		
Pack by Product/Total of Unror Carportine (Total of Production Simple) Constraints (Statical Section Simple) <thconstraints (Statical Section Simple) Constraints</thconstraints 		Public Key Policies/Encrypti	101.	stars		
Unor Configuration Stanlarg Comp Section Solution Solution <t< td=""><td rowspan="4"></td><td>Public Key Policies/Trusted</td><td>Pice</td><td>these</td></t<>		Public Key Policies/Trusted	Pice	these		
Wenders Startung Corp Section Salet, 34		User Configuration (Enabled)	Pare ucbout.	tide		
Hence backful Service Sett 24 gins gins <thgi< td=""><td>Windows Settings</td><td>Char Section</td><td>100</td></thgi<>		Windows Settings	Char Section	100		
Singer Anton		Renote Installation Services	Select All	day		
		Sents	Refresh	den		

The Local Group Policy Editor screen will appear. Although the default domain policy is used to configure group policy in this document, we recommend that you configure a separate GPO that can be applied to only NAC-NAP computers.

Default Descrip Deling (ed.id (each Deling)					
Computer Configuration Software Settings	Default Domain Policy (ad.id.local) Policy				
Default Demain Policy (skidulcal) Policy Compute Configuration Schware Settings Windows Settings Windows Settings Script (Satury/Shudown) Big Deployed Printers Script (Satury/Shudown) Big Deployed Printers Script (Satury/Shudown) Big Deployed Printers Dig Settings Scrivers Settings Markows Settings Markows Settings Markows Printers Dig Mindows Settings Markows Printers Dig Mindows Settings Markows Printers Markows Printers Markows Printers Markows Printers Scrivers Settings Markows Settings Markows Printers Markows Printers	Default Domain Policy (adiation Select an item to view its description.	I) Policy Recomputer Configuration Suber Configuration			

Step 9. In the Local Group Policy Editor window, choose Computer Configuration > Windows Settings > Security Settings to display the Wireless / Wired Interface Policies pane.

Note: This documentation discusses only wired interface policy and its EAP-FAST configuration.

- Step 10. Right-click Wired Network (IEEE 802.3) Policies in the policy tree and choose Create a New Windows Vista Policy from the context menu
- Step 11. On the General tab, in the Policy Name field, type Wired-802.1x.

Step 12. On the Security tab, verify that Enable use of IEEE 802.1x authentication for network access is selected. From the Select a network authentication method pull-down menu, choose Cisco: EAP-FAST. Change the value for Max Authentication Failures to 3. For Authentication Mode, choose User re-authentication from the pull-down menu. This selection will enable both user and machine authentication (equivalent to the <authMode>userOrMachine</authMode> element in an XML-based profile).

Note: Max Authentication Failure is set to 1 by default. This setting prevents a user from reentering his or her credentials when invalid credentials are provided at the initial prompt.

Enable	use of IEEE 8	802.1X authentica	tion for network a	ccess
	EAP-FAST	a len activit me a k	-	Properties
Auther	ntication Mode	81		
User r	re-authenticat	ion	•	
Max A	uthentication F	Failures:		3
				Advanced

- Step 13. If you click the **Properties** button on the **Security** tab, the **EAP-FAST Configuration** screen will appear. You can configure EAP-FAST settings centrally using this group policy configuration tool. For EAP-FAST settings, follow the steps described in the "Windows Vista Client Configuration" section earlier in this document.
- Step 14. If you click **Advanced** button on the **Security** tab, you'll see the available configuration options for the supplicant. Configure the supplicant as in the following screenshot.

EEE 802.1X	
Enforce advanced 802.1X se	ettings
Max Eapol-Start Msgs:	Held Period (seconds):
3 🖆	160 <u></u>
Start Period (seconds):	Auth Period (seconds):
5 🛨	30 🛨
Eapol-Start Message:	
Transmit per IEEE 802.1X	•
ingle Sign On	
Enable Single Sign On for thi	s network
Perform immediately before	ore User Logon
C Perform immediately after	er User Logon
Max delay for connectivity(s	econds): 10 🛨
Reference Allow additional dialogs to Sign On	o be displayed during Single
🖂 This network uses differe	ent VLAN for authentication

- Step 15. As described earlier, **Single Sign On** can be configured in detail, using group policy. Use the preceding screenshot to configure your group policy setup.
- Step 16. After you finish your configuration, exit the GPMC tool.
- Step 17. After you finish configuring group policy, you can provision your configuration to the local Windows Vista machine. To do this, run the **gpupdate** tool to reflect your policy change on the domain to your local system.

Troubleshooting the NAC-NAP Solution

This section provides information about how to troubleshoot the Cisco NAC and Microsoft NAP solution. The section discusses the steps for troubleshooting problems with the client software, network hardware, and server applications. Troubleshooting guidance is provided for both the EAP over User Datagram Protocol (UDP) and the IEEE 802.1x deployment scenarios. Detailed configuration information for each of these scenarios is provided in the previous section of this document.

NAC-NAP Troubleshooting Overview

To facilitate troubleshooting, you should understand where possible failure points exist in the architecture. Figure 3 shows the possible failure points in the NAC-NAP solution architecture and the process for debugging them.



Figure 3. Possible Failure Points in the NAC-NAP Architecture

Network Access Devices

Because the NAC-NAP solution is an integration of technologies from both Cisco and Microsoft, the architecture includes many components, and failure points can exist in a component itself or in communication between components.

As shown in Figure 3, the architecture has four major components: the client computer, the network access devices (NADs), Cisco Secure ACS, and Microsoft NPS. The first component is the client software running on the Windows Vista operating system. This client software (or agent) communicates with a NAD, in this case a Cisco switch or wireless access point. The NAD forwards an authentication and access request to the policy server; Cisco Secure Access Control Server (ACS) is the policy server, which becomes a broker of both identity and posture information. Behind the Cisco Secure ACS is another policy server, the Microsoft Network Policy Server (NPS), where all the access policies are determined. This document discusses how to troubleshoot each of these components in the access method using IEEE 802.1x.

When troubleshooting the NAC-NAP solution, you should first understand how successful authentication and posture validation looks like in the log. As you have seen in the IEEE 802.1x testing section, after client user or machine credentials are authenticated successfully and SoH values are validated as compliant, the log of the successful session appears in the Cisco Secure ACS Passed Authentication log. From the Cisco Secure ACS web console, choose **Reports and Activity > Passed Authentications** on the left and click the **Passed Authentication active.csv** link. As in the following screenshot, you may see a log of a quarantined user. This user was not rejected, but was granted limited access to the network. It is very important to remember that both healthy and quarantined users and machines are listed in Passed Authentication log when authentication and posture validation succeed. When authentication is performed but you do not see any log associated with the authentication session, you need to start troubleshooting NAC-NAP.

	<u>User-</u> Name	<u>Group-</u> <u>Name</u>	Caller- ID	NAS- Port	NAS-IP- Address	Network Access Profile Name	Shared RAC	<u>System-</u> Posture- Token	<u>Reason</u>	Contraction of the second s
K	ID\user1	AD_User	00-1C- 25-14- 79-E2	50001	10.1.100.254	NAC- 802.1x	802.1x_Compliant_User	Healthy	Posture State=1 Extended State=0 returned by: Evaluated by policy: ID-NPS	
<	ID\user1	AD_User	00-1C- 25-14- 79-E2	50001	10.1.100.254	NAC- 802.1x	802.1x_Quarantine	Quarantine	Posture State=2 Extended State=0 returned by: Evaluated by policy: ID-NPS	

When you troubleshoot the NAC-NAP interoperability architecture, the Cisco Secure ACS log is a good place to start. Although the Cisco Secure ACS log does not always tell you the exact issue that is causing the authentication failure, it at least gives you some hints as to where the problem may be. This section looks at two categories of authentication failure: problems for which the Cisco Secure ACS log does not show any record of the authentication session, and problems for which the Cisco Secure ACS log shows a record of the authentication session.

Failure with No Authentication Record in Cisco Secure ACS Log

In some cases, a user may be connected to an IEEE 802.1x–enabled port but there is no Cisco Secure ACS log associated with authentication. A common cause of such a situation is an error in the authenticator (NAD) configuration. Following is a checklist of procedures to follow when there is no authentication record:

- Make sure that required AAA commands are configured properly. Required AAA commands are listed in the "IEEE 802.1x Network Access Device Configuration" section of this guide. If AAA commands are not properly configured, there will be no RADIUS communication between the authenticator and the authentication server, and hence there will be no record in the Cisco Secure ACS log.
- Make sure on the switch or access point that RADIUS servers are configured with the correct addresses and port numbers. If the switch or access point (authenticators) is not sending the authentication request packet to the correct RADIUS server (Cisco Secure ACS), then there will be no record in the Cisco Secure ACS log. If the IP address and port numbers of the RADIUS server are correct but the RADIUS shared key is incorrectly configured, there will be a record in the Cisco Secure ACS Failed Attempt log with the authentication failure code "Invalid message authenticator in EAP request."
- If you have multiple Cisco Secure ACSs in an authenticator configuration, check them all for the log. There is a chance that the log is recorded on another Cisco Secure ACS when multiple Cisco Secure ACSs are running behind a server load-balancing mechanism.

Another common error is that the IEEE 802.1x supplicant is not installed or enabled on the connecting interface. Check the output of the show command on the authenticator. In this document, the IEEE 802.1x supplicant is connected on the port Fast Ethernet 0/1. Enter show dot1x interface FastEthernet 0/1 detail to see whether any other factor is causing the problem. If
there is a client but no IEEE 802.1x supplicant running or connected, output similar to the following screenshot will be displayed.

Cat3560#show dot1x in	t fa0/1 d
PAE	= AUTHENTICATOR
PortControl	= AUTO
ControlDirection	= Both
HostMode	= SINGLE_HOST
ReAuthentication	= Enabled
QuietPeriod	= 60
ServerTimeout	= 30
SuppTimeout	= 30
ReAuthPeriod	= (From Authentication Server)
ReAuthMax	= 2
MaxReq	= 2
TxPeriod	= 30
RateLimitPeriod	= 0
Guest-Vlan	= 20
Dotlx Authenticator C	lient List Empty
Domain	= DATA
Port Status	= UNAUTHORIZED

If any other fail open IEEE 802.1x feature such as a IEEE 802.1x guest VLAN is configured on the port, then the output will be similar to the next screenshot. Guest VLAN is a feature of Cisco IOS Software for the Cisco Catalyst platform of switches; with it, any user without an IEEE 802.1x supplicant can be placed in a locally predefined VLAN (in the following output, the guest VLAN is defined as VLAN 20) so that user has at least restricted network access. The guest VLAN feature is implemented when the switch sends an EAP request and identity packet to the supplicant (sending request ReAuthMax_count with interval TxPeriod) but does receive a response from the supplicant. By default, after 90 seconds, if the supplicant does not respond, the switch assumes that there is no supplicant on the IEEE 802.1x port and assigns a predefined VLAN to this port. No RADIUS communication is involved in the guest VLAN process; therefore, no log is associated with this authentication, even though the user is granted guest VLAN access.

PAE	= AUTHENTICATOR
PortControl	= AUTO
ControlDirection	= Both
HostMode	= SINGLE_HOST
ReAuthentication	= Enabled
QuietPeriod	= 60
ServerTimeout	= 30
SuppTimeout	= 30
ReAuthPeriod	= (From Authentication Server)
ReAuthMax	= 2
MaxReq	= 2
TxPeriod	= 30
RateLimitPeriod	= 0
Guest-Vlan	= 20
Dotlx Authenticator Cli	ent List Empty
Domain	= DATA
Port Status	= AUTHORIZED
Authorized By	= Guest-Vlan
Operational HostMode	= MULTI_HOST
Vlan Policy	= 20

Failure with Authentication Record in Cisco Secure ACS Log

In many situations Cisco Secure ACS provides information about authentication failures. Although the authentication failure code (AFC; description of possible cause of authentication failure) does not indicate exactly where the problem is, the AFC makes troubleshooting much easier and helps you narrow down the root cause of the problem so that you can resolve it. This section examines possible points of failure in each component based on the Cisco Secure ACS Failed Attempt log output.

Troubleshooting Client Software

This section examines situations in which software components running on the Windows Vista client fail. When the NAP-related agent fails to respond to the request by Cisco Secure ACS, failure information will be reported in the Failed Attempt log on Cisco Secure ACS. The main NAP-related software running on Windows Vista consists of the supplicant, system health agents, NAP agent, and enforcement client.

When EAP-FAST Posture Validation Is Not Enabled

By default, the Cisco EAP-FAST Module does have posture validation enabled. When Cisco Secure ACS requests SoH information and the supplicant is not enabled to send SoH information, authentication fails. Check the EAP-FAST settings to make sure that **Enable Posture Validation** on the **Authentication** tab is selected.

AFC	Reason
Posture Validation Failure (general)	Supplicant is unable to send SoH information. General posture validation failure occurs when Cisco Secure ACS receives empty SoH. Note that the same AFC can be recorded for other reasons, such as when NAP agent is not enabled and when EAP QEC is not running.

When NAP Agent Is Not Enabled

By default, the NAP agent service is turned off. When Cisco Secure ACS requests SoH information and the NAP agent is not running, authentication fails.

AFC	Reason
Posture Validation Failure (general)	NAP agent is not running. General posture validation failure occurs when Cisco Secure ACS receives empty SoH. Note that the same AFC can be recorded for other reasons, such as when the Enable Posture Validation setting for the Cisco EAP-FAST Module is not enabled and when EAP QEC is not running.

Enter the command shown here at the command prompt to verify that the NAP agent is running. If it is running, following output is displayed.

C:\Windows\system32>sc que:	ry	nar	pagent
SERVICE_NAME: napagent			
TYPE	:	20	WIN32_SHARE_PROCESS
STATE	:	4	RUNNING
			(STOPPABLE, NOT_PAUSABLE,
ACCEPTS_SHUTDOWN)			
WIN32_EXIT_CODE	:	0	(0x0)
SERVICE_EXIT_CODE	:	0	(0x0)
CHECKPOINT	:	0x0)
WAIT_HINT	:	0x()

If the NAP agent is not running, the **netsh nap client show state** command at command prompt also returns the message "The "Network Access Protection Agent" service is not running." Enter the commands shown here at the command prompt to enable the NAP agent.

```
C:\Windows\system32>sc config napagent start= auto
C:\Windows\system32>net start napagent
```

When EAP Enforcement Client Is Not Enabled

By default, EAP QEC is turned off. When Cisco Secure ACS requests SoH information and EAP QEC is not running, authentication fails.

AFC	Reason
Posture Validation Failure (general)	EAP QEC is unable to send SoH information. General posture validation failure occurs when Cisco Secure ACS receives empty SoH. Note that the same AFC can be recorded for other reasons, such as when NAP agent is not enabled and when the Enable Posture Validation setting for the Cisco EAP-FAST Module configuration is not enabled.

Enter the command shown here at the command prompt to verify that EAP QEC is running. If it is running, the following output is displayed.

SKIPPED	
Enforcement client st	cate:
Id	= 79617
Name	= DHCP Quarantine Enforcement Client
Description	= Provides DHCP based enforcement for NAP
Version	= 1.0
Vendor name	= Microsoft Corporation
Registration date	=
Initialized	= Yes
Id	= 79618
Name	= Remote Access Quarantine Enforcement Client
Description Client	= Provides the quarantine enforcement for RAS
Version	= 1.0
Vendor name	= Microsoft Corporation
Registration date	=
Initialized	= Yes
Id	= 79619
Name	= IPSec Relying Party
Description Network Access Pro	= Provides IPSec based enforcement for
tection	
Version	= 1.0
Vendor name	= Microsoft Corporation
Registration date	=
Initialized	= No
Id	= 79621
Name	= TS Gateway Quarantine Enforcement Client

Description	= Provides TS Gateway enforcement for NAP
Version	= 1.0
Vendor name	= Microsoft Corporation
Registration date	=
Initialized	= Yes
Id	= 79623
Name	= EAP Quarantine Enforcement Client
Description	= Provides EAP based enforcement for NAP
Version	= 1.0
Vendor name	= Microsoft Corporation
Registration date	=
Initialized	= Yes
SKIPPED	

Enter the commands shown here at the command prompt to enable the NAP agent.

```
C:\Windows\system32>netsh nap client set enforcement ID = 79623
ADMIN = "ENABLE"
```

When System Health Agent Is Not Running

When for any reason the System Health Agent (SHA) is not running, the NAP agent will not send SoH information regarding this specific SHA. In this case, authentication does not fail. Instead, the user is granted limited network access until the health state becomes compliant.

AFC	Reason
None	Authentication does not fail. The information is recorded in the Cisco Secure ACS Passed Authentication log.

Enter the command shown here at the command prompt to identity the SHA that is unable to obtain health information.

```
netsh nap client >show state
System health agent (SHA) state:
_____
                              . . . . . . . . . . . . . . . .
Id
                      = 79744
Name
                      = Windows Security Health Agent
--- skipped ---
Registration date
                      =
Initialized
                      = Yes
Failure category
                     = None
Remediation state
                      = Could not update
Remediation percentage = 0
```

```
= (3237937215) - The Windows Security Health
Fixup Message
Agent failed to update the security state of this computer.
Compliance results
                       = (0xC0FF0001) - A system health component is
not enabled.
                          (0x0000000) -
                         (0x0000000) -
                          (0x0000000) -
                         (0 \times 00000000) -
                          (0x0000000) -
                          (0x0000000) -
                          (0x0000000) -
                       = (0xC0FF0023) - Windows could not enable the
Remediation results
Windows Firewall. An administrator must start it manually.
---SKIPPED---
```

A number of client events also provide information about failures. Figure 4 shows the information events logged on the client when the NAP transaction crosses the component boundaries.





Event ID	Description	
27	Indicates that an SoH was received from the SHA	
28	Indicates that the SoH was received by the quarantine enforcement client indicated in the event	
29	Indicates the SoH response from the server; also contains the client health state	
18	Indicates a NAP health state change	

All events that relate to communication between the NAP agent and SHA are documented at the following Microsoft website:

http://technet2.microsoft.com/WindowsServer2008/en/library/e85ebe50-e515-4121-84c8fcebf8d778d31033.mspx

All events that relate to communication between the NAP agent and the enforcement client are documented at the following Microsoft website:

http://technet2.microsoft.com/WindowsServer2008/en/library/77685aa1-083d-45dd-89b4a8cb67cc58fc1033.mspx When troubleshooting, the most reliable source of information is a log from the particular components. You need to know how to enable logging on a component and where the log is written.

All NAP logs on the Windows Vista client can be viewed through Event Viewer. Following are the steps to view logs.

- 1. Choose Start > All Programs > Administrative Tools and launch Event Viewer.
- Under Event Viewer (Local) on the left side of the screen, navigate to Applications and Services Logs > Microsoft > Windows > Network Access Protection, right-click
 Operational, and choose Filter Current Logs.
- 3. On the Filter tab, from the Event sources pull-down menu, choose Network Access Protection.
- 4. In the Include/Excludes Event IDs section, type 6-10, 12, 28, 29 to filter events to those related to NAP in the text box and click OK.

When Supplicant Fails

As discussed previously, if the supplicant fails to respond to the authentication request, there will be no report in the Cisco Secure ACS Failed Attempt log, since there will be no IEEE 802.1x communication if the supplicant does not exist. Enter the commands shown here at the command prompt to verify that the supplicant service is started and running.

Enter this command to verify the state of EAPHost service:

```
C:\Windows\system32>sc query eaphost

SERVICE_NAME: eaphost

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE,

ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0
```

Enter this command to verify the state of IEEE 802.1x supplicant service for the wired interface:

```
C:\Windows\system32>sc query dot3svc
SERVICE_NAME: dot3svc
TYPE : 20 WIN32_SHARE_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE,
ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
```

Enter this command to verify the state of IEEE 802.1x supplicant service for the wireless interface:

C:\Windows\system32>sc query wlansvc			
TADE	: 20 WIN32_SHARE_PROCESS		
STATE	: 4 RUNNING		
	(STOPPABLE, NOT_PAUSABLE,		
ACCEPTS_SHUTDOWN)			
WIN32_EXIT_CODE	: 0 (0x0)		
SERVICE_EXIT_CODE	: 0 (0x0)		
CHECKPOINT	: 0x0		
WAIT_HINT	: 0x0		

Note: Wired AutoConfig service is disabled by default and must be manually started. The commands shown here enable the supplicant and configure service so that it starts automatically when the client PC is booted.

```
C:\Windows\system32>sc config dot3svc start= auto
C:\Windows\system32>sc config wlansvc start= auto
C:\Windows\system32>net start dot3svc
C:\Windows\system32>net start wlansvc
```

When EAP-FAST Module Is Not Installed

The Cisco EAP-FAST Module provides additional an EAP method for Windows Vista. EAP-FAST is the only EAP method that is supported by the NAC-NAP integration architecture. The Cisco EAP-FAST Module is not shipped with Windows Vista; instead, it is provisioned through Windows Update. If the EAP-FAST is not installed on the Vista client and the Vista client tries to connect to a NAC-NAP enabled network, the AFC shown here is reported to the Cisco Secure ACS Failed Attempt log.

AFC	Reason
EAP_PEAP Type not configured	The Cisco EAP-FAST Module is not installed; therefore, the supplicant cannot negotiate the EAP type suggested by Cisco Secure ACS because no other EAP method is enabled on Cisco Secure ACS to accept the requested access. When the supplicant is enabled on Windows Vista, Microsoft: Protected EAP (PEAP) is enabled by default.

To view the EAP-FAST settings for IEEE 802.1x, enter **control netconnections** at the command prompt; then open **Network Connections**, right-click **Local Area Connection**, and choose **properties** from context menu.

In the Local Area Connection Properties window, look for Cisco: EAP-FAST on the Choose a network authentication method drop-down box on the Authentication tab; if you see it, the EAP-FAST module is successfully installed. If you do not see the Authentication tab in the Local Area Connection Properties window, go back to Task 1 in the section "Configuring the Windows Vista Client" and configure and start Wired AutoConfig service.

vetworking	Authentication	Sharing
Select th this Ethe	iis option to provii met adapter.	de authenticated network access for
Choose	le IEEE 802.1X a a network auther	authentication ntication <u>m</u> ethod:
Cisco: E	AP-FAST	▼ <u>S</u> ettings…
to thi	s network	
¹ To thi	s network	

On the Authentication tab, choose Cisco: EAP-FAST from the Choose a network authentication method drop-down menu and click the Settings button. The EAP-FAST Properties window appears.

Connection	User Credentials Authentication About	
Use and	onymous outer identity anonymous	ĩ
V lise P	Protected Access Credentials (PAC)	
	low automatic PAC provisioning	
PAC	Authority:	
<u></u>		ŕ
Nor	ne 👻 Limport	
- IN GARA		
	ate server certificate	
	onnect to only these servers:	
Trus	ted Root Certificate Authority	
	Class 3 Public Primary Certification Authority	
	GTE CyberTrust Global Root	
	ID-CA	
	Microsoft Root Authority	
	Microsoft Root Certificate Authority	
	Thawte Server CA	
	to not prompt user to authorize new servers or trusted certification authorities	į.,

EAP-FAST will attempt to download a protected access credential (PAC) to the client during the initial client authentication attempt. Prior to this initial client attempt, you will notice that no PAC is available for selection in the **PAC Authority** pull-down menu.

If the initial authentication is successful, a PAC will be provisioned to the client. The user will be notified in the balloon message that additional information is required to connect to the network.

_	MA
	Additional information is required to connect to the network ×
	84% C < 11

If user clicks this balloon message, another message box appears asking the user if he or she wants to accept the PAC from the PAC authority. If the user clicks yes, then the PAC will be saved, and your EAP-FAST Properties window will now show the PAC authority name and the trusted root CA server.

Connection	User Credentials Authentication Abo	ut	
🔽 Use and	nymous outer identity anonymous		
Use E	rotected Access Credentials (PAC)		
VA	low automatic PAC provisioning		
PAC	Authority:		
(m)			Turnet
[ID-	105	•	Tubol t
	Class 3 Public Primary Certification Author Equifax Secure Certificate Authority	ity	*
	GTE CyberTrust Global Root		_
	ID-CA		100
	Microsoft Root Authority Microsoft Root Certificate Authority		
	Thawte Server CA		÷
1000	a pet prempt upor to putherize new repue	rs or trusted certifica	tion authorities.
	The prompt user to authorize new serve		
D	not prompt user to authorize new serve		

View the Cisco Secure ACS report to verify successful client authentication and policy assignment. In the example shown here, the client was successfully authenticated, assigned a PAC, and assigned a policy of "Healthy" based on the client status.

<u>User-</u> Name	Group- Name	Caller- ID	NAS- Port	NAS-IP- Address	Network Access Profile Name	Shared RAC	Downloadable <u>ACL</u>	<u>System-</u> Posture- <u>Token</u>	Application- Posture- Token	Reason	EAP Type	EAP Type Name	PEAP EA Cle Na
user1	AD_User	00-1C- 25-14- 79-E2	50001	10.1.100.254	NAC- 802.1x	802.1x_Compliant_User	ñ	Healthy	'n	Posture State=1 Extended State=0 returned by: Evaluated by policy: ID-NPS	43	EAP- FAST	anony

Troubleshooting IEEE 802.1x Authenticator

IEEE 802.1x provides client authentication to the network devices. The IEEE 802.1x method relies on EAP-FAST as the transport protocol. When troubleshooting a problem with IEEE 802.1x, information can be gathered from the Vista client, the network device, Cisco Secure ACS, and Microsoft NPS.

The IEEE 802.1x method can carry user identification and SoH information between the client and the network devices and servers in a single transaction. After the client is authenticated, the client health state is determined and a network access policy is assigned on the network device. In the case of IEEE 802.1x, this policy is enforced on the NAD through the use of dynamic VLANs, which are assigned through RADIUS attributes from Cisco Secure ACS to the switch.

IEEE 802.1x Logging and Debugging on a Switch

The IEEE 802.1x log and debugging information on the switch provides a lot of useful information for troubleshooting and verifying IEEE 802.1x sessions and status. You should enable the RADIUS IEEE 802.1x Accounting features to log IEEE 802.1x information.

You can view the IEEE 802.1x settings for an interface along with the current IEEE 802.1x state information for the interface by entering the show dot1x interface x/x/x details command.

Cat3560#show dot1x int f	Cat3560#show dot1x int fa0/1 d				
Dotlx Info for FastEther	Dotlx Info for FastEthernet0/1				
PAE	= AUTHENTICATOR				
PortControl	= AUTO				
ControlDirection	= Both				
HostMode	= MULTI_HOST				
ReAuthentication	= Disabled				
QuietPeriod	= 60				
ServerTimeout	= 30				
SuppTimeout	= 30				
ReAuthPeriod	= (From Authentication Server)				
ReAuthMax	= 2				
MaxReq	= 2				
TxPeriod	= 30				
RateLimitPeriod	= 0				
Dotlx Authenticator Clie	nt List				
Domain	= DATA				
Supplicant	= 0016.41ae.8b1b				
Auth SM State	= AUTHENTICATED				
Auth BEND SM State	= IDLE				
Port Status	= AUTHORIZED				
Authentication Method	= Dotlx				
Posture	= Healthy				
Authorized By	= Authentication Server				
Vlan Policy	= 10				

In the output in the preceding screenshot, you can see that the client connected to interface 0/1 has been authenticated and authorized on the port with a posture of healthy. The VLAN that has been assigned is 10, the healthy VLAN.

By entering the **show vlan** command, you can see that interface FastEthernet 0/1 has been placed in VLAN 10.

Cat3	Cat3560#show vlan				
VLAN	Name	Status	Ports		
1	default	active	Fa0/2, Fa0/3, Fa0/4,		
Gi0/	1				
10	healthy	active	Fa0/1, Fa0/5, Fa0/6		
20	contractor	active			
30	guest	active			
40	quarantine	active			
50	asset	active			
99	voice	active			

Other useful IEEE 802.1x Cisco IOS Software commands include the following:

```
debug dot1x {all | errors | events | feature | packets | registry |
state-machine}
no debug dot1x {all | errors | events | feature | packets | registry
| state-machine}
```

Options	Description	
all	Display all IEEE 802.1x authentication debug messages	
errors Display IEEE 802.1x errors debug messages		
events	events Display IEEE 802.1x event debug messages	
feature	feature Display IEEE 802.1x feature debug messages	
packets Display IEEE 802.1x packet debug messages		
registry Display IEEE 802.1x registry invocation debug messages		
state-machine Display debug messages for state-machine-related events		

When troubleshooting the RADIUS protocol, the following debug command are useful:

debug radius {accounting authentication brief elog fail retransmit verbose <cr>}</cr>	.over
no debug radius {accounting authentication brief elog failover retransmit verbose <cr>}</cr>	

Options Description	
accounting Display RADIUS accounting packet debug message only	
authentication Display RADIUS authentication packet debug message only	
brief Display RADIUS I/O transaction only	
elog Display RADIUS event logging	

Options Description	
failover Display debug message on packets sent upon RADIUS failover	
retransmit Display debug message on retransmission of RADIUS packet	
verbose Display all debug messages including those for nonessential RADIUS debugging	

Authorization Failures on Authenticator (Switch)

One common problem that can be difficult to troubleshoot is authorization failure. IEEE 802.1x authorization occurs when the switch or access point receives the last RADIUS packet, called access-accept. Usually the RADIUS access-accept packet contains all the RADIUS attributes that are necessary to enforce authorization on the client PC. RADIUS attributes used for authorization can be the VLAN ID and name and the reauthentication timer value. Authorization failure occurs when the RADIUS server sends authorization to an authenticator (switch or access point) and the authenticator does not understand or is unable to apply enforcement on the port.

The two most common authorization failures result from lack of authorization command and authorization mismatch.

When Authorization Command Is Not Configured

If the command aaa authorization network default group radius is not configured, all the authorization criteria carried by the RADIUS attributes will fail. Common RADIUS attributes that will be ignored are:

- Session-Timeout (27)
- Termination-Action (29)
- Tunnel-Type (64)
- Tunnel-Medium-Type (65)
- Tunnel-Private-Group-ID (81)

If the switch port is configured with IEEE 802.1x and also configured to receive VLAN (through attributes 64, 65, and 81) and the reauthentication timer (through attributes 27 and 29), the port will be assigned to VLAN 0, and no reauthentication timer will be assigned to the port: that is, reauthentication will never happen on this port. The following log shows VLAN assignment failure.

```
Feb 27 15:55:16.659: dot1x-ev:dot1x_sendRespToServer: Response sent
to the server from 000d.60fc.9c38
Feb 27 15:55:16.668: dot1x-ev:dot1x_vlan_assign_authc_success called
on interface FastEthernet0/1
Feb 27 15:55:16.676: dot1x-ev:dot1x_vlan_assign_authc_success:
Successfully assigned VLAN 0 to interface FastEthernet0/1
Feb 27 15:55:16.676: dot1x-ev:dot1x_switch_supplicant_add: Adding
000d.60fc.9c38 on FastEthernet0/1 in vlan 1, domain is DATA
Feb 27 15:55:16.676: dot1x-ev:dot1x_switch_addr_add: Added MAC
000d.60fc.9c38 to vlan 1 on interface FastEthernet0/1
```

Following is the output of the **show dot1x int fa0/1 detail** command when authorization failure occurs. Notice that **ReAuthPeriod** is now set to 0, and **TimeToNextReauth** is also **0**. VLAN assignment fails, and VLAN policy becomes inapplicable. Also note that authentication succeeds, and the port status is **AUTHORIZED** even if authorization fails.

ID-3560#show dot1x int fa)/:	1 d
skipped		
Dot1x Authenticator Client	: 1	List
Domain	=	DATA
Supplicant	=	000d.60fc.9c38
Auth SM State	=	AUTHENTICATED
Auth BEND SM State	=	IDLE
Port Status	=	AUTHORIZED
ReAuthPeriod	=	0
ReAuthAction	=	Terminate
TimeToNextReauth	=	0
Authentication Method	=	Dotlx
Authorized By	=	Authentication Server
Vlan Policy	=	N/A

This type of authorization failure can be easily found by checking the authenticator configuration in detail. However, this problem is difficult to troubleshoot from the Cisco Secure ACS log, because the AAA server sends an access-accept packet to its RADIUS client (NAD) but never receives acknowledgment back from the RADIUS client. That is, after the RADIUS access-accept packet is sent to the NAD, successful authentication is logged on Cisco Secure ACS, and the network administrator is usually confused as to why the client cannot get on to the network.

When Authorization Mismatch Occurs

Authorization mismatch occurs when the RADIUS attribute sent from the AAA server cannot be matched to the value on the NAD. A common scenario of authorization mismatch is VLAN mismatch upon authorization. For instance, if RADIUS is configured to send the VLAN name HEALTHY, and if a VLAN named Healthy_VLAN exists but not a VLAN named HEALTHY, then authorization fails because there is no matched VLAN on the local switch. As a result, the port becomes unauthorized and is closed. Again this authorization failure will never be reported back to Cisco Secure ACS. The Cisco Secure ACS log shows a successful authentication session. Currently only Cisco Catalyst 3000 Series Switches with Cisco IOS Software Release 12.2(44)SE or later will generate a syslog message noting this authorization failure. Other platforms do not send syslog messages; therefore, you must turn on debugging on the switch for troubleshooting. Following is the syslog message generated on the Cisco Catalyst 3000 Series with Cisco IOS Software.

Feb 27 16:39:40.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up Feb 27 16:39:41.477: %DOT1X_SWITCH-5-ERR_RADIUS_VLAN_NOT_FOUND: Attempt to assign non-existent VLAN wrong_vlan to dot1x port FastEthernet0/1 Feb 27 16:39:41.930: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up Failure in Communication with RADIUS Server

The common failures on the authenticator are related to the RADIUS protocol communication between the authenticator (NAD) and the authentication server (Cisco Secure ACS). A common problem occurs when an invalid RADIUS shared secret is used on either the NAD or Cisco Secure ACS. The error code shown here is reported in the Cisco Secure ACS Failed Attempt log.

AFC	Reason
Invalid message authenticator in EAP request	Message authenticator (attribute 80) is a hashed checksum of the access-request packet using a shared secret as the key. Invalid message authenticator usually means that the shared secret configured on either NAD or Cisco Secure ACS is invalid or does not match on both. Check or r-configure the shared secret on both NAD and Cisco Secure ACS to resolve the problem.

Troubleshooting with Cisco Secure ACS Passed Authentication Log

When a client establishes a secure EAP-FAST connection to Cisco Secure ACS and properly authenticates, an entry is created in the Passed Authentication log. The log entry enables you to view basic client information such as the username, IP address or MAC address (caller-id), posture token that is assigned, reason description, network access profile assigned, RAC, and additional information.

The following screenshot shows an example of the Cisco Secure ACS Passed Authentication log for a Vista client. In this case, the client has authenticated and matched the IEEE 802.1x network access profile and has been assigned a healthy posture token and accompanying policy.

	Date 🕈	<u>Time</u>	<u>Message-</u> <u>Type</u>	<u>User-</u> Name	Group- Name	Caller- ID	NAS- Port	NAS-IP- Address	Access Profile Name	Shared RAC	<u>System-</u> Posture- <u>Token</u>	Reason	EAP Type	EAP Type Name	FAST- Clear- Name
(03/17/2008	09:40:15	Authen OK	ID\user1	AD_User	00-1C- 25-14- 79-E2	50001	10.1.100.254	NAC- 802.1x	802.1x_Compliant_User	Healthy	Posture State=1 Extended State=0 returned by: Evaluated by policy: ID-NPS	43	EAP- FAST	anonymous

It is possible for a Passed Authentication log entry to be created for a client assigned to a quarantine state. When the client has authenticated, a log entry is placed in the Passed Authentication report, but the posture token assigned is a quarantine token. Remember that just because a client is authenticated does not mean that it should be assigned a healthy policy. In the following screenshot, the Vista client has authenticated but is assigned a quarantine token. If you look at the Microsoft NPS policy, it states that the Windows Firewall must be enabled for the client to be assigned a healthy policy. In this case, the firewall was disabled on the client, and as a result the client was assigned a quarantine policy.

Date 🕈	<u>Time</u>	Message- Type	<u>User-</u> Name	<u>Group-</u> <u>Name</u>	<u>Caller-</u> ID	NAS- Port	NAS-IP- Address	Network Access Profile Name	Shared RAC	<u>System-</u> Posture- Token	<u>Reason</u>	EAP Type	EAP Type Name	PEAP/EAP- FAST- Clear- Name
03/17/2008	09:40:15	Authen OK	ID\user1	AD_User	00-1C- 25-14- 79-E2	50001	10.1.100.254	NAC- 802.1x	802.1x_Compliant_User	Healthy	Posture State=1 Extended State=0 returned by: Evaluated by policy: ID-NPS	43	EAP- FAST	anonymous

Depending on the configuration options selected in the external posture validation policy created in the network access profile, a client may also fail authentication when the external posture validation server (Microsoft NPS) is unavailable, as shown here.



If the Microsoft NPS and the Cisco Secure ACS lose communication, you can select the option to assign the client a default posture token, which can either grant full or limited network access while the server communication is unavailable, as shown here.

Date 🕈	<u>Time</u>	<u>Message-</u> Type	<u>User-</u> Name	<u>Group-</u> Name	<u>Caller-</u> ID	NAS- Port	NAS-IP- Address	Network Access Profile Name	Shared RAC	<u>System-</u> Posture- <u>Token</u>	<u>Reason</u>	EAP Type	EAP Type Name	PEAP/EAP- FAST- Clear- Name
03/17/2008	10:39:16	Authen OK	ID\user1	AD_User	00-1C- 25-14- 79-E2	50001	10.1.100.254	NAC- 802.1×	802.1x_Quarantine	Quarantine	Statement of Health rule failed with server= ID-NPS return a defualt token.	43	EAP- FAST	anonymous

The Cisco Secure ACS **Reports and Activities** menu brings you to a page where you can find the available log messages. These logs are useful for viewing both passed authentications and failed attempts from the Cisco Secure ACS web console. Detailed debug logs are available in the directories listed here.

AFC	Reason
Authentication Logs	C:\Program Files\CiscoSecure ACS v4.2\CSAuth\Logs\AUTH.log
RADIUS Logs	C:\Program Files\CiscoSecure ACS v4.2\CSRadius\Logs\RDS.log
CSV Files	C:\Program Files\CiscoSecure ACS v4.2\Logs\

All the logs that are required for troubleshooting and support can be dumped into a CAB archive file and saved in the following directory: C:\Program Files\CiscoSecure ACSv4.2\Utils\Support\Package.Cab.

Choose System Configuration > Support and select Collect Log Files, Collect User Database, and Collect Previous Days Logs and enter the number of days for which you need to collect the logs. Then click Run Support Now to create the Package.cab archive log file.

When creating the Package.Cab file using this support tool, be aware that all Cisco Secure ACS services are stopped. Be cautious when exporting log files on Cisco Secure ACS.

Troubleshooting Microsoft Network Policy Server

The NAC-NAP IEEE 802.1x session will fail if Microsoft NPS is misconfigured. Event logs are useful for gathering information about and troubleshooting a failure on Microsoft NPS.

Event Logs

The event viewer on Microsoft NPS is used to view logs related to Microsoft NPS events. On Microsoft NPS, choose Event Viewer (Local) > Custom View > Server Roles > Network Policy and Access Services. This custom view will include events for HCAP, Microsoft NPS, and access auditing. This custom view is created automatically when the Microsoft NPS role is installed.

wer (Local) Netwo	rk Policy and	Access Services 2,764 Events				A	ctions	
m Views	764 Events					- 1	etwork Policy and Acc	
erver Roles		Date and Time	Source	Event ID	Task Category	- 4	Open Saved Log	
Web Server	ormation	3/17/2008 12:33:49 PM	HCAP	2	None	-	Create Custom View	
AP Inf	ormation	3/17/2008 12:13:06 PM	HCAP	22	None		Import Custom View	
PS Inf	ormation	3/17/2008 12:13:06 PM	Microsoft Win	6278	Network Policy			
AP Inf	ormation	3/17/2008 12:13:06 PM	Microsoft Win	6272	Network Policy		Filter Current Custo	
s inf	ormation	3/17/2008 12:13:04 PM	HCAP	22	None		Properties	
Logs	ormation	3/17/2008 12:13:04 PM	Microsoft Win	6276	Network Policy		0 - 1	
pplication I Inf	ormation	3/17/2008 12:13:04 PM	Microsoft Win	6272	Network Policy		Hind	
ecurity D Inf	ormation	3/17/2008 12:12:14 PM	HCAP	22	None	- I F	Save Events in Cust	a
up 🚺 Inf	ormation	3/17/2008 12:12:14 PM	Microsoft Win	6278	Network Policy		Export Custom View	
ystem 🚺 🚺 Inf	ormation	3/17/2008 12:12:14 PM	Microsoft Win	6272	Network Policy		CAPOT COBRONN VIEW	с.
orwarded Events	ormation	3/17/2008 12:12:09 PM	HCAP	22	None		Copy Custom View	
ations and Services Logs	ormation	3/17/2008 12:12:09 PM	Microsoft Win	6278	Network Policy		Attach Task To This	
riptions Inf	ormation	3/17/2008 12:12:09 PM	Microsoft Win	6272	Network Policy	- 18	1000	
(i) Inf	ormation	3/17/2008 12:12:07 PM	HCAP	22	None		View	•
(i) Inf	ormation	3/17/2008 12:12:07 PM	Microsoft Win	6276	Network Policy		Refresh	
(i) Inf	ormation	3/17/2008 12:12:07 PM	Microsoft Win	6272	Network Policy			
(i) Inf	ormation	3/17/2008 12:11:54 PM	HCAP	22	None		Help	•
(i) Inf	ormation	3/17/2008 12:11:54 PM	Microsoft Win	6278	Network Policy	E	vent 2. HCAP	
(i) Inf	ormation	3/17/2008 12:11:54 PM	Microsoft Win	6272	Network Policy			
(i) Inf	ormation	3/17/2008 12:07:24 PM	HCAP	22	None		Event Properties	
(i) Inf	ormation	3/17/2008 12:07:24 PM	Microsoft Win	6278	Network Policy	- 3	Attach Task To This	6
Event	2, HCAP				3	<	Save Selected Event.	
Gen	eral Details					8	Сору	•
	1						Refresh	
T	te HCAP Serve	r stopped successfully.					Help	,
. In	n Namer	System						
		HCAD	Langed	2/17/2009 12:22	40 014			
20			roddra:	372772000 12:33.				
Eve	ent ID:	2	Task Category:	None		1		

The example in the following screenshot shows an entry in the log for the Vista client that was authenticated successfully and granted full network access (healthy token). An HCAP log is also generated containing information about the values that are returned to Cisco Secure ACS.

General Details Friegdly View C XML View System SubjectUserName SubjectUserName SubjectUserName SubjectUserName SubjectUserName SubjectMachineName SubjectMac
System System System System SubjectUserSid SubjectUsecESid SubjectUserSid SubjectUserSid SubjectUserSid S
None (0x0 -)

Successful HCAP R	lesponse was returned.			
HCAP client host n HCAP client IP add Request ID: 0x5 Version: 2 User Name: ID\use User Groups: Endpoint ID: 00-1C Endpoint Location: Endpoint Location:	name: - rress: 10.1.100.2 r1 -25-14-79-E2 : NAC-NAP-IA ress: -			
Endpoint IPv6 Add Posture State retur	ress: - ned: 1			
Endpoint IPv6 Add Posture State retur Extended State retu	ress: - ned: 1 arned: 0			
Endpoint IPv6 Add Posture State retur Extended State retu	ress - ned: 1 urned: 0			•
Endpoint IPv6 Add Posture State retur Extended State retu Log Na <u>m</u> e:	System	logande	2/17/0009 10-56-27 АМ	•
Endpoint IPv6 Add Posture State retur Extended State retu Log Name: Source: Source:	ress - ned: 1 irmed: 0 System HCAP 22	Logge <u>d</u> :	3/17/2008 10:56:37 AM	▲
Endpoint IPv6 Add Posture State retur Extended State retu Log Name: jource: jource: jvent ID: evel:	ress - ned: 1 irmed: 0 System HCAP 22 Information	Logged: Task Category: Keywords:	3/17/2008 10:56:37 AM None	•
Endpoint IPv6 Add Posture State retur Extended State retur Source: Source: Event ID: Level: User:	ress - ned: 1 urned: 0 System HCAP 22 Information NT AUTHORITYJUSR	Logge <u>d:</u> Task Category: <u>K</u> eywords: Computer:	3/17/2008 10:56:37 AM None ID-NPS.id.local	•
Endpoint IPv6 Add Posture State retur Extended State retur Log Name: Source: Event ID: Event ID: Event: User: OpCode:	ress - ned: 1 urned: 0 System HCAP 22 Information NT AUTHORITY/JUSR Info	Logge <u>d:</u> Task Category: <u>K</u> eywords: Computer:	3/17/2008 10:56:37 AM None ID-NPS.id.local	•

In the next example, a log entry for the same Vista client has been created. Because Windows Firewall was disabled, the client was assigned a restricted access policy (quarantine token) until the firewall is reenabled.

System		
EventData		
SubjectUserSid SubjectUserName	S-1-5-21-3670840749-1484431986-3346287640-1117	
SubjectDomainName	ID	
FullyQualifiedSubjectUs	erName ID\user1	
SubjectMachineSID	5-1-5-21-3670840749-1484431986-3346287640-1126	
SubjectMachineName	Vista03.id.local	
FullyQualifiedSubjectM	achineName ID\VISTA03\$	
MachineInventory	6.0.6001 1.0 x86 Domain Controller	
CalledStationID		
CallingStationID	00-1C-25-14-79-E2	
NASIPv4Address	10.1.100.10	
NASIPv6Address	-	
NASIdentifier		
NASPortType	5/	
NASPort	8	
ClientName		
ClientIPAddress	Barry Control of Contr	
ProxyPolicyName	HCAP	
NetworkPolicyName	Restrict-Access-Policy	
AuthenticationProvider	Windows	
AuthenticationServer	ID-NPS.id.local	
AuthenticationType	Unauthenticated	
EAPType		
AccountSessionIdentifie	er -	
QuarantineState	Quarantined	
ExtendedQuarantineSta	ite -	
QuarantineSessionID	{517A3B89-7372-4D37-9438-4F2F9748D148} - 2008-03-17 17:56:02.124Z	
QuarantineHelpURL	2	18
QuarantineSystemHealt	hResult Windows Security Health Validator NonCompliant No Data None (0x:0ff0001 - A system health component is not enabled) (0x0 -) (0x0 -) (0x0 -) (0x0 -) (0x0 -) (0x0 -)	

Successful HCAP F	Response was returned.			
HCAP client host r HCAP client IP adc Request ID: 0x3 Version: 2 User Name: ID\use User Groups: Endpoint ID: 00-1C Endpoint Location Endpoint IPv6 Add Endpoint IPv6 Add	name: - tress: 10.1.100.2 r1 25-14-79-E2 : NAC-NAP-IA ress: - tress: -			
Extended State retu	ned: 2 urned: 0			+
Extended State retu	neo: 2 urned: 0 System			•
Extended State retu Log Na <u>m</u> e: Source:	nea: 2 imed: 0 System HCAP	Logge <u>d</u> :	3/17/2008 10:56:02 AM	•
Extended State retu .og Na <u>m</u> e: Source: Event ID:	System HCAP 22	Logge <u>d</u> : Task Category:	3/17/2008 10:56:02 AM None	•
Extended State retu Log Name: Source: Event ID: Level:	system HCAP 22 Information	Logge <u>d:</u> Task Category: Keywords:	3/17/2008 10:56:02 AM None	•
Log Name: Source: Event ID: Event ID: Event ID: Event ID:	System HCAP 22 Information NT AUTHORITYJUSR	Logged: Task Category: Keywords: Computer:	3/17/2008 10:56:02 AM None ID-NPS.id.local	•
Log Name: Source: Event ID: Level: User: QpCode:	System HCAP 22 Information NT AUTHORITY/JUSR Info	Logge <u>d:</u> Task Category: <u>K</u> eywords: Computer:	3/17/2008 10:56:02 AM None ID-NPS.id.local	•

The critical event IDs are 6278 (healthy) and 6276 (quarantined). With those event IDs, you can identify the health state as well as find detailed information about the client. More information is available at the following URL:

http://technet2.microsoft.com/windowsserver2008/en/library/3bfa69a6-26a3-4796-a50b-168f7f5e48731033.mspx?mfr=true

Verification That HCAP Is Running on Microsoft NPS

When a client tries to authenticate, w3wp.exe will be listed in the task list. You can verify the current state of this service by entering the following command at the command prompt:

tasklist | findstr -1 w3wp.exe

If this commend does not return any value, repeat it right after authentication occurs and you will get a result similar to the screenshot shown here.



Troubleshooting NAP

For NAP-related components, both logging and tracing information is available for use in troubleshooting. Tracing information will typically be collected only if you contact Microsoft for support. This section describes how to find the logs for the NAP components.

Event Logs

NAP logging is enabled by default, and events are stored in the following log:

Event Viewer\Applications and Services logs\Microsoft\Windows\Network Access Protection\Operational

Tracing

NAP tracing files can be created and forwarded to the Microsoft development team to diagnose problems. To enable tracing, do the following:

- 1. Open a command prompt in an elevated mode.
- If the directory %systemroot%\tracing\nap does not exist, create it with the command mkdir %systemroot%\tracing\nap.
- 3. At the command prompt, enter logman start qagentrt -p {b0278a28-76f1-4e15-b1df-14b209a12613} 0xFFFFFFF 9 -o %systemroot%\tracing\nap\qagentrt.etl -ets.
- 4. Run the scenario to capture the trace.
- 5. To stop tracing, at the command prompt enter logman stop qagentrt -ets.
- Copy %systemroot%\tracing\nap\qagentrt.etl to another folder so that it can be sent to Microsoft.

Troubleshooting Microsoft Network Policy Server

Accounting Logs

Accounting log files are enabled by default. The location of the Microsoft NPS accounting logs is **%windir%\system32\logfiles**. Microsoft NPS accounting can be managed from the accounting node in the Microsoft NPS snap-in.

Event Logs

Event logging for Microsoft NPS is enabled by default, and events are visible in the system log. You can send the event log with any other information when a problem occurs.

Tracing

Microsoft NPS tracing files do not require symbol files to read and can be used for troubleshooting. Tracing files are located in **the %windir%\tracing** folder and are called **ias*.log**. To enable tracing, do the following:

- 1. At the command prompt in an elevated mode, run **netsh ras set tracing * enable**. This command will start tracing.
- 2. Restart Microsoft NPS.
- 3. At the command prompt, enter net stop ias.
- 4. At the command prompt, enter net start ias.
- 5. Reproduce the problem. This will generate a trace file of the problem.
- 6. Copy %windir%\tracing\IAS*.log to another folder so that it can be sent to Microsoft.
- 7. At the command prompt, enter netsh ras set tracing * disable.

- 8. Restart Microsoft NPS.
- 9. At the command prompt, enter net stop ias.
- 10. At the command prompt, enter net start ias.

Troubleshooting HCAP Server

Event Logs

Event logging for HCAP server is enabled by default, and events are visible in the system log. You can send the event log with any other information when a problem occurs.

Tracing

HCAP server tracing files can be created and forwarded to the Microsoft development team to diagnose problems. Tracing files are located in the **%systemroot%\tracing\hcapext** folder and are called **hcapext.etl**. To enable tracing, do the following:

- At the elevated command prompt, enter logman start hcapext -p {af000c3b-46c7-4166-89ab-de51df2701ee} 0xFFFFFFF 9 -o %systemroot%\tracing\hcapext\hcapext.etl -ets.
- 2. Reproduce the problem. This will generate the trace file of the problem.
- Copy %systemroot%\tracing\hcapext\hcapext.etl to another folder so that it can be sent to Microsoft.
- 4. To stop tracing, at the command prompt enter logman stop hcapext -ets.

Troubleshooting Wireless AutoConfig Service

Event Logs

Wireless AutoConfig event logging is enabled by default, and events are stored in the following logs:

Event Viewer\Applications and Services logs\Microsoft\Windows\WLAN-Autoconfig\Operational

Tracing

WLAN AutoConfig tracing files do not require symbol files to read and can be used for troubleshooting. Tracing files are located in the **C:\Windows\tracing\wireless** folder. To enable tracing, do the following:

- 1. From an elevated command prompt, enter **netsh WLAN set tracing yes**. This will start tracing.
- 2. Reproduce your problem.
- 3. To disable tracing, at the command prompt enter **netsh WLAN set tracing no**. After executing this command, wait for control to return to the command window (postprocessing converts the files into readable text).
- 4. Copy the entire C:\Windows\tracing\wireless folder, including all subdirectories, to another folder so that it can be sent to Microsoft.

Troubleshooting Wired AutoConfig Service

Event Logs

Wired AutoConfig event logging is enabled by default, and events are stored in the following logs:

Event Viewer\Applications and Services logs\Microsoft\Windows\Wired-Autoconfig\Operational

Tracing

Wired AutoConfig tracing files do not require symbol files to read and can be used for troubleshooting. Tracing files are located in the **C:\Windows\tracing\wired** folder. To enable tracing, do the following:

- 1. From an elevated command prompt, enter Netsh LAN set tracing yes. This will start tracing.
- 2. Reproduce your problem.
- 3. To disable tracing, at the command prompt enter **netsh LAN set tracing no**. After executing this command, wait for control to return to the command window (postprocessing converts the files into readable text).
- Copy the entire C:\Windows\tracing\wired folder, including subdirectories, to another folder so that it can be sent to Microsoft.

Troubleshooting Cisco EAP-FAST Module

Tracing

Follow these steps to configure and start logging when gathering logs for the Cisco EAP-FAST Module:

- 1. Choose Start > All Programs > Accessories.
- 2. Right-click **Command Prompt** and choose **Run as Administrator**.
- 3. At the prompt, enter the following command to configure and start logging: wevtutil.exe si Cisco-EAP-FAST/Debug /e:true Network Policy Server.
- 4. Reproduce the problem with the Cisco EAP-FAST Module.
- 5. At the prompt, enter the following command to stop the logging: wevtutil.exe sl Cisco-EAP-FAST/Debug /e:false.
- Browse to C:\Windows\System32\Winevt\Logs\ and you can find the log file Cisco\EAP-FAST%4Debug.etl.

Note: After the .etl file is obtained, you can view this log with Event Viewer. After logging is turned off, all the internal buffers for logs are flushed. Also, you must stop logging before you can analyze the .etl file. If you must shut down the device on which logging was running before logging finishes, logging resumes after you reboot. If logging is started either automatically or manually, however, the logs are cleared.



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore

Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco Stadium/Vision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks: Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncoS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCOone, IX, ProConnect, ScriptShare, SenderBase, SMARTinet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0903R)

Printed in USA

C07-491725-01 05/09