



Release Notes for NAC/NAP Interoperability Architecture 1.0

These release notes pertain to the Network Admission Control (NAC)/Network Access Protection (NAP) interoperability architecture, Release 1.0 by Cisco Systems, Inc., and Microsoft Corporation.

Contents

This document contains:

- [NAC/NAP Overview](#)
- [Features of NAC/NAP](#)
- [Supported Cisco Component Versions](#)
- [External Software Requirements](#)
- [Obtaining NAC/NAP](#)
- [Important Notes](#)
- [Known Defects in NAC Components](#)
- [Related Documentation](#)
- [Obtaining Documentation](#)

NAC/NAP Overview

The NAC/NAP solution components include Cisco Secure Access Control Server (ACS) version 4.2, Cisco 802.1x-capable Catalyst switches, Microsoft Network Policy Server (NPS), and Microsoft NAP-enabled Vista desktops.

The Cisco NAC appliance does not support NAP at this time and is not part of the solution.

The NAC/NAP interoperability architecture:

- Gathers identity and posture information from an endpoint.
- Determines the security policy compliance of the endpoint.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- Provides remediation services.
- Enforces network access policies based on the compliance of the endpoint.

NAC/NAP verifies the identity and health status of a Windows Vista client, provides remediation capabilities, and dynamically enforces access policies on the network infrastructure.

For additional information about the Cisco NAC solution, go to:

http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

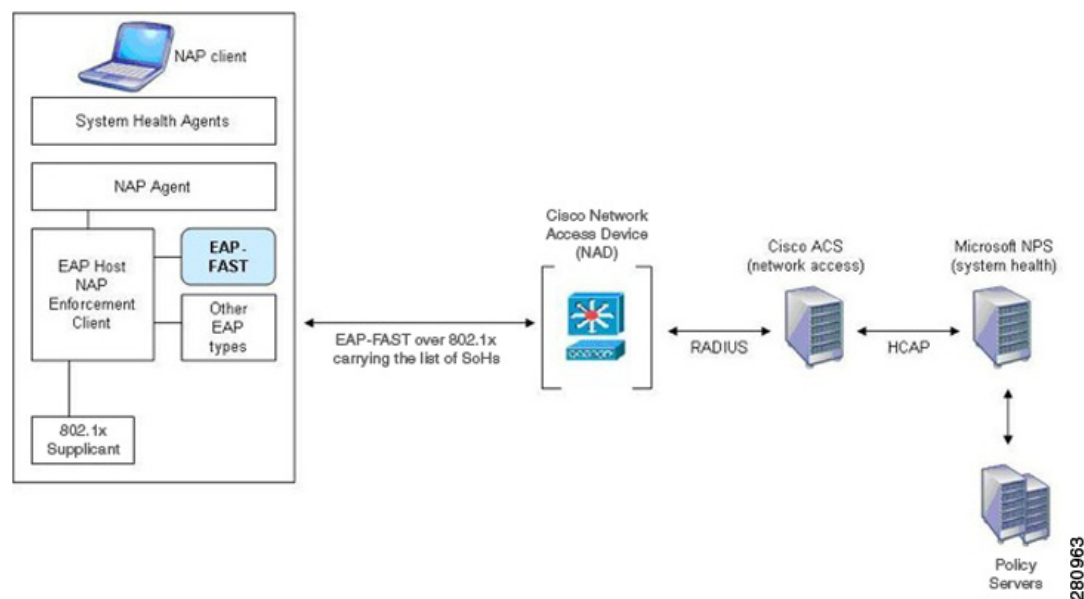
For additional information about the Microsoft NAP solution, go to:

<http://www.microsoft.com/technet/itsolutions/network/nap/default.msp>

NAC/NAP Interoperability Architecture

Figure 1 shows the components of the NAC/NAP Interoperability Architecture.

Figure 1 NAC/NAP Interoperability Architecture



The EAP-FAST module on Windows Vista, NAD (Cisco switches and access points), and ACS components belong to Cisco.

The NAP Client, NAP agent, and NPS components belong to Microsoft.

Table 1 describes the components in NAC/NAP Interoperability Architecture.

Table 1 NAC/NAP Interoperability Architecture Components

Component	Description
NAP Client	A computer that runs Windows Vista or Windows Server 2008. The NAP client sends its health credentials in the form of Statements of Health (SoHs) to Access Control Server (ACS).
NAP Agent	A process that runs on a NAP client. The NAP agent sends a list of SOHs to ACS.

Table 1 **NAC/NAP Interoperability Architecture Components (continued)**

Component	Description
NAD	A NAD, such as a switch or a wireless access point, that acts as a NAC enforcement point. In a NAC/NAP deployment, the AAA client is called a NAD.
ACS	A AAA server that uses internal policies, external policy servers, or both to validate the client's identity and health status. ACS sends an access profile to the NAD, which grants access privileges to the client based on the authentication and authorization results.
NPS	A Network Policy Server (NPS) is a Microsoft server that performs posture validation for a NAP client. NPS returns the posture assessment result to ACS. Also provides remediation services if needed.
Policy Server	A Microsoft or third-party policy server that provides the current state of system health for an NPS.

Features of NAC/NAP

This section describes the new features that Cisco components support in the NAC/NAP environment:

- [SoH in Host Credentials Authorization Protocol, version 2 Support](#)
- [Posture Optional Configuration Support](#)
- [Authenticated In-Band PAC Provisioning Support](#)
- [EAP Type in NAC/NAP Environment](#)
- [EAP-FAST Enhancement for Anonymous TLS Renegotiation](#)
- [EAP-FAST Module on Windows Vista with Service Pack 1 Platform](#)

SoH in Host Credentials Authorization Protocol, version 2 Support

NPS supports the Host Credentials Authorization Protocol (HCAP), version 2, to receive a list of SOHs from ACS and return a list of SOH Response (SOHRs) back to ACS.

Posture Optional Configuration Support

NAC/NAP deployment requires posture optional configuration in ACS. A posture optional setting prevents a machine or user from failing authentication during computer bootup process, if the NAP agent service has not yet started. If the authentication fails, the NAP agent does not send SOH information to ACS.

Authenticated In-Band PAC Provisioning Support

NAC/NAP 1.0 supports authenticated in-band Protected Access Credential (PAC) provisioning.

PACs are strong shared secrets that enable ACS and an EAP-FAST end-user client to authenticate each other, and establish a Transport Layer Security (TLS) tunnel for use in EAP-FAST phase <2>.

The in-band provisioning mode operates inside an authenticated tunnel before the client authenticates the server. This method minimizes the risk of exposing the user's credentials.

For a description of the in-band PAC provisioning method, see the “About PACs” section in Chapter 9, *System Configuration: Authentication and Certificates of the User Guide for Cisco Secure Access Control Server 4.2*.

EAP Type in NAC/NAP Environment

EAP-FAST is the only EAP type that NAC/NAP supports. EAP-FAST is enhanced to support SoH information. You can use any of the following EAP inner methods:

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

EAP-FAST Enhancement for Anonymous TLS Renegotiation

EAP-FAST is a tunneling protocol that works in two phases:

- Provisioning
- Authentication

In the Server-Unauthenticated provisioning phase, an anonymous TLS handshake occurs between the client and ACS to establish a protected tunnel. ACS provisions a PAC and sends an access-reject message (failure) to the client.

In the authentication phase, the client again starts a new authentication with ACS using the PAC received in the provisioning phase.

This EAP-FAST enhancement combines the provisioning and authentication phases into a single phase, bypassing the failure state. After the provisioning phase, the authentication does not fail. Instead, the client initiates a TLS renegotiation, followed by a new authentication. Upon successful authentication, ACS grants the client network access.

For a description of the EAP-FAST enhancement for anonymous TLS renegotiation, see the “EAP-FAST for Anonymous TLS Renegotiation” section in Chapter 9, *System Configuration: Authentication and Certificates of the User Guide for Cisco Secure Access Control Server 4.2*.

EAP-FAST Module on Windows Vista with Service Pack 1 Platform

The EAP-FAST module is installed through Microsoft Windows Vista Update. For information on EAP-FAST installation, refer to Microsoft's *NAP Design Guide* and *NAP Deployment Guide*.

Supported Cisco Component Versions

The following sections list the hardware and software that you can use in the NAC/NAP environment:

- [Supported Cisco Switches](#)
- [Supported Cisco Wireless Access Points](#)
- [Supported Cisco Wireless LAN Controllers](#)
- [Supported Cisco Wireless LAN Service Module](#)
- [Supported EAP-FAST Module](#)
- [Supported Cisco Secure Access Control Server Release](#)

Supported Cisco Switches

[Table 2](#) lists the devices that support the NAC L2 802.1x (EAP over IEEE 802.1x) method:

Table 2 *Supported Cisco Switches*

Supported Switch Models	Supervisor, if applicable	Operating System Image
Cisco Catalyst 2960	All	Cisco IOS, Release 12.2(35)SE or later
Cisco Catalyst 3560 and 3570	All	Cisco IOS, Release 12.2(35)SE or later
Cisco Catalyst 4500	Sup II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, V-10GE	Cisco IOS, Release 12.2(37)SG or later
Cisco Catalyst 4900	All	Cisco IOS, Release 12.2(37)SG or later
Cisco Catalyst 6500	Sup 2, 32, 720	CatOS 8.6(1) or later
Cisco Catalyst 6500	Sup 32, 720	IOS 12.2(33)SXH or later

Supported Cisco Wireless Access Points

[Table 3](#) lists the Cisco Wireless Access Points that support the NAC L2 802.1x method:

Table 3 *Supported Cisco Wireless Access Points*

Cisco Wireless Access Points	Supported Models	Cisco IOS Image
350 series	All	12.3(7)JA1 or later
1100 series	All	12.3(7)JA1 or later
1130 AG series	All	12.3(7)JA1 or later
1200 series	All	12.3(7)JA1 or later
1230 AG series	All	12.3(7)JA1 or later
1240 AG series	All	12.3(7)JA1 or later

Supported Cisco Wireless LAN Controllers

Table 4 lists the Cisco Wireless LAN Controllers that support the NAC L2 802.1x method:

Table 4 *Supported Cisco Wireless LAN Controllers*

Wireless LAN Controller Models	Cisco Unified Wireless Network Software
Cisco 2000	Release 3.1 or later
Cisco 2100	Release 4.0 or later
Cisco 4100	Release 3.1 or later
Cisco 4400	Release 3.1 or later
Wireless Services Module (WiSM)	Release 3.1 or later
Wireless LAN Controller Module for Integrated Services Routers	Release 3.1 or later

Supported Cisco Wireless LAN Service Module

Table 5 lists the Cisco Wireless Service Module that supports the NAC L2 802.1x method:

Table 5 *Supported Cisco Wireless LAN Service Module*

Wireless Service Modules	Cisco IOS Image
Wireless LAN Services Module (WLSM)	Release 1.4.1 or later

Supported EAP-FAST Module

Cisco EAP-FAST module, version 2.2.8, supports NAC/NAP 1.0. The EAP-FAST 2.2.8 is available for 32-bit and 64-bit platforms.

You must install the EAP-FAST 2.2.8 on Windows Vista with Service Pack 1 applied. The following editions of Windows Vista support the EAP-FAST module:

- Windows Vista Enterprise
- Windows Vista Business
- Windows Vista Ultimate



Note

The EAP-FAST module is only available through the Microsoft Windows Vista Update Service in the form of an optional driver package installation.

Supported Cisco Secure Access Control Server Release

ACS 4.2 (124), supports NAC/NAP 1.0.

External Software Requirements

To deploy NAC/NAP, you need:

- Client operating system—Windows Vista (Enterprise, Business, or Ultimate edition) with Service Pack 1 applied.
- Server—Windows Server 2008.
- EAP-FAST Module for Windows Vista. See [Supported EAP-FAST Module](#) for more information.

Obtaining NAC/NAP

This initial NAC/NAP release is a limited offering from Cisco and Microsoft.

If your organization has an immediate need to evaluate or deploy the NAC/NAP solution in your environment, contact your Cisco sales representative.

Important Notes

This section contains:

- [Important Notes for Cisco IOS](#)
- [Important Notes for EAP-FAST](#)

Important Notes for Cisco IOS

The following information applies to Cisco IOS, Release 12.2(35)SE2, which runs on Catalyst switches 2960, 3560, and 3570:

A device attached to Multi-Domain Authentication-enabled port with Guest VLAN, but no MAC Authentication Bypass (MAB), shows up as a dot1x authenticated device

When MAB is not enabled and the switch obtains the MAC address from the port, the port status indicates a device authenticated by dot1x.

To prevent this behavior, enable MAB, or set the *tx-period* to one second.

Important Notes for EAP-FAST

The following information applies to EAP-FAST, version 2.2.8:

After authentication fails, the next authentication attempt starts in about 20 minutes

If your authentication fails because of identity failure, explicit EAP failure, or UI failure, you must wait for 20 minutes before you can log in again.

This condition occurs because the Vista supplicant goes into a 20-minute wait period (block) when your authentication fails.

When the Vista supplicant receives an explicit EAP-Failure message from the AAA server, it starts the blocking timer (the default value is set to 20 minutes). During this blocking-timer period, the Vista supplicant does not initiate EAPOL-Start, or respond to EAP-ID Request from NAD.

This condition also exists on a wireless supplicant in Windows Vista.

To get around this wait period:

- For wired interfaces, physically disconnect and reconnect the cable; or, disable and re-enable the affected adapter.
- For wireless interfaces, you can manually change the EAP-FAST profile. Add the *maxAuthFailures* element and set its value to 3.

User authentication is not performed when Remote Desktop is used

When you use Remote Desktop, profiles that are configured for automatic connection undergo machine authentication instead of user authentication.

If you start authentication manually, user authentication occurs as expected.

Known Defects in NAC Components

This section contains the [Known Defects in Cisco Secure Access Control Server 4.2](#).

For a complete list of bugs on individual components of the NAC security solution, refer to that component's release notes on Cisco.com.

Known Defects in Cisco Secure Access Control Server 4.2

Table 6 lists the known defects in Cisco Secure Access Control Server for Windows and Solution Engine 4.2. These defects in ACS can affect a NAC implementation:

Table 6 Known Defects in ACS for Windows and ACS Solution Engine 4.2

Defect ID	Headline	Explanation
CSCsf26433	Machine PAC should not be generated when anonymous in-band is enabled.	Symptom When “Allow anonymous in-band PAC provisioning”, GTC, and MS-CHAPv2 are enabled in ACS EAP-FAST configuration, then during authentication, ACS provides a machine PAC to the supplicant. However, according to the EAP-FAST System Functional Specification (SFS) for ACS 4.0, this option should not be supported. Conditions This condition occurs when you choose the following options: 1. Enable EAP-FAST. 2. Enable Allow anonymous in-band PAC provisioning. 3. Enable GTC and MS-CHAPv2. 4. Allow machine authentication. Workaround Choose System Configuration > Global Authentication Setup > EAP-FAST Configuration and uncheck Allow Machine Authentication check box.
CSCsf31776	Full <i>Auth.log</i> shows HCAP Endpoint-ID TLV MAC address with period.	Symptom MAC address shown in <i>Auth.log</i> contains a period (.) as separator. Conditions During NAC/NAP authentication, in <i>Auth.log</i> file, the HCAP Endpoint-ID TLV appears with a MAC address that contains a period in place of a dash. Workaround None.

Table 6 Known Defects in ACS for Windows and ACS Solution Engine 4.2 (continued)

Defect ID	Headline	Explanation
CSCsf31786	Specifying only secondary External Posture AAA Server shows incorrect error in report.	Symptom Authentication fails and returns the failure code, “Could not communicate with external policy server-wrong HCAP version”. Conditions When you configure only a secondary External Posture AAA server, the authentication fails with a failure code, “Could not communicate with external policy server-wrong HCAP version”. This failure code is ambiguous. Workaround None.
CSCsg14041	HCAP Full Detail shows System Posture Response and Request as unknown.	Symptom The HCAP Full Detail log in the <i>Auth.log</i> file shows the System Posture Response and Request as unknown types. Workaround None.
CSCsg50817	The Reason field is not displayed in the Failed Attempts report.	Symptom The Reason field is empty in the Failed Attempts report. Conditions This condition occurs when NAC-NAP validations fail. For example, there is an error when you access the external posture AAA server. Workaround None.
CSCsg62239	Binary garbage is sent to syslog, indicative of bad or corrupt pointer.	Symptom Binary text appears in syslog output. Conditions This condition occurs randomly. Workaround None.

Table 6 Known Defects in ACS for Windows and ACS Solution Engine 4.2 (continued)

Defect ID	Headline	Explanation
CSCsg81878	ACS generates an authorization PAC when only Allow Posture Validation is enabled.	Symptom ACS generates an authorization PAC when you enable only Allow Posture Validation in ACS EAP-FAST configuration. Conditions This condition occurs when you choose the following options: 1. Enable only Allow Posture Validation. 2. Enable Allow Stateless session resume. ACS generates an authorization PAC for the supplicant during posture validation. Workaround Choose System Configuration > Global Authentication Setup > EAP-FAST Configuration and uncheck the Allow Stateless session resume check box.
CSCsh82218	No failed report when quarantine and extended state values are invalid.	Symptom ACS does not generate a Failed Authentication report when NAC/NAP authentication fails. Conditions When the client sends invalid quarantine and extended state values, the NAC/NAP authentication fails and there is no Failed Authentication report. Workaround None.
CSCsh94935	The reason message in Passed Authentication for SOH fail or open is ambiguous.	Symptom An ambiguous error message, "Statement of Health rule failed with server= NPS_Dummy return a default token" appears when supplicant does not acknowledge SOH request. Conditions When you configure SOH PV rule, and the supplicant does not acknowledge ACS SOH request, or responds with an empty SOH fail or open default token, the token is returned correctly. However, the Reason field in the Passed Authentication report is ambiguous. Workaround None.

Table 6 Known Defects in ACS for Windows and ACS Solution Engine 4.2 (continued)

Defect ID	Headline	Explanation
CSCsi13512	ACS does not send an Access-Reject message when the user ID and initiator ID in a received PAC do not match.	Symptom ACS does not send an Access-Reject message when the user ID and initiator ID in a received PAC do not match. Conditions This condition occurs when you configure ACS as follows: 1. Enable EAP-FAST. 2. Enable anonymous in-band PAC provisioning or authenticated in-band PAC provisioning. 3. Enable any of the configurable inner methods (GTC, MS-CHAPv2 or EAP-TLS). When the supplicant sends the request, during the second authentication, the username value in the authentication message is different from the one that the PAC created. Workaround None.
CSCsi84065	ACS does not accept a user name that contains a pound sign (#).	Symptom An external user with a username that contains a pound sign cannot log into ACS. Workaround None.
CSCsi184885	ACS requests NAC-TLV even if not configured in NAP - Posture Optional broken.	Symptom ACS requests NAC-TLV even if NAC is not configured in NAP. Conditions This condition occurs when ACS is configured only with NPS configuration, but requests for NAC-TLV. Workaround None.
CSCsm35834	The Reason field is not populated during Posture Optional.	Symptom The Reason field in <i>Passed Attempts.csv</i> log file does not appear when you enable Posture Optional setting. Workaround None.

Related Documentation

- *Cisco Network Admission Control and Microsoft Network Access Protection Integration Deployment Guide*
http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns812/guide_c07-491729.html
- *Cisco Network Admission Control and Microsoft Network Access Protection Troubleshooting Guide*
http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns812/guide_c07-491725.html
- *Cisco Secure Access Control Server Configuration Guide for NAC/NAP Interoperability*
<http://cisco.com/en/US/docs/security/nac-nap/1.0/config/guide/acskonfnacnap10.html>
- *EAP-FAST for Windows Vista Administrator Guide*
http://cisco.com/en/US/docs/wireless/wlan_adapter/eap_types/fast/admin/guide/FAST_admin.html
- *Release Notes for Cisco Secure ACS 4.2*
http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html
- *Supported Interoperable Devices and Software Tables for Cisco Secure ACS Release 4.2*
http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/device/guide/sdt42.html
- *Documentation Guide for Cisco Secure ACS 4.2*
http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html
- *Installation Guide for Cisco Secure ACS for Windows 4.2*
http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html
- *User Guide for Cisco Secure Access Control Server 4.2*
http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/ACS4_2UG.html
- *Cisco Secure ACS Online Troubleshooting Guide, 4.2*
http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/trouble/guide/ACSTrbG42.html
- Microsoft NAP Documentation
<http://technet2.microsoft.com/windowsserver2008/en/library/97fc1222-2fa2-413d-92d3-bbff79c4a4fb1033.mspx?mfr=true>

Obtaining Documentation

For information on obtaining documentation and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, 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, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, 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)

© 2008 Cisco Systems, Inc. All rights reserved.