Release Notes for Network Admission Control Framework, Release 2.1

These release notes pertain to Cisco's Network Admission Control Framework, Release 2.1 network solution.

This document contains a brief description of NAC, it lists which Cisco components are NAC 2.1 compatible, and the limitations of those components as they relate to NAC functionality.

For information about installation methods, system requirements, and changes of an individual component, see that component's release notes and documentation in the Technical Support & Documentation area of Cisco Systems's web site.

Contents

This document contains the following sections**:**

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

Network Admission Control Framework Overview

Network Admission Control (NAC) is a set of technologies and solutions built on an industry initiative led by Cisco Systems. It uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources; thereby limiting damage from emerging security threats. Customers using NAC can allow network access only to compliant and trusted endpoint devices (PCs and servers, for example) and can restrict the access of noncompliant devices.

For more information about the NAC solution, see http://www.cisco.com/go/NAC.

Benefits of NAC

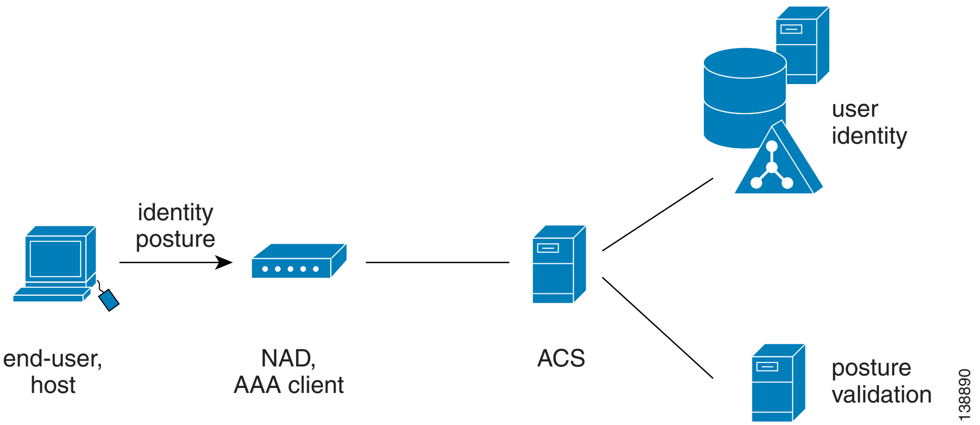
These are some of the benefits of NAC:

- **Dramatically improves network's security**—NAC ensures that all endpoints conform to the latest security policy; regardless of the size or complexity of the network. With NAC in place, you can focus operations on prevention, rather than on reaction. As a result, you can protect against worms, viruses, spyware, and malicious software before they are introduced into your network.
- **Extends the value of your existing investments**—Besides being integrated into the Cisco network infrastructure, NAC enjoys broad integration with antivirus, security, and management solutions from dozens of leading manufacturers.
- **NAC provides deployment scalability and comprehensive span of control**—NAC provides admission control across all access methods (LAN, WAN, wireless, and remote access).
- **Increases enterprise resilience**—NAC prevents noncompliant and rogue endpoints from affecting network availability.
- **Reduces operational expenses**—NAC reduces the expense of identifying and repairing noncompliant, rogue, and infected systems.

NAC Architecture Overview

Figure 1 shows the components of a typical NAC deployment.

Figure 1 Components of a Typical NAC Deployment



Typical NAC components are:

- **End-user or host**—Also known as the endpoint. The endpoint is a device such as a PC, workstation or server that is connected to a switch, access point, or router through a direct connection. In a NAC deployment, the host that is running the Cisco Trust Agent (CTA) application, collects posture data from the computer and from any NAC-compliant applications, such as Cisco Security Agent, that are installed on the computer.

  A NAC agentless host (NAH) is an endpoint that is not running the Cisco CTA application.

- **Network Access device (NAD)**—In a NAC deployment, the AAA client is called a NAD. The NAD is a Cisco network access device, such as a router or switch, which acts as a NAC enforcement point.
- **ACS**—Cisco Secure Access Control Server (ACS) performs the validation of the endpoint device by using internal policies, external policy servers, or both, to which the posture credentials are forwarded.
- **External posture validation servers**—These perform posture validation and return a posture token to ACS. In a NAC deployment with agentless hosts, you can configure ACS to invoke the services of a special type of posture

validation server, called an audit server. An audit server uses out-of-band methods, such as port scans, to validate the health of the endpoint device, and reports the result as a posture token to ACS.

- **Remediation servers**—Provide repair and upgrade services to hosts that do not comply with network admission requirements.

NAC Framework 2.1 Solution And Baseline

The NAC Framework 2.1 solution addresses a finite set of features and use cases. These features and use cases have been tested on a selected number of hardware and software components within a complete NAC Framework 2.1 environment. The use cases, features, and components that were tested together comprise the NAC Framework 2.1 baseline.

As a result of focusing our testing efforts on the NAC Framework 2.1 baseline, we are confident in the quality and effectiveness of that combination of use cases, features, and components.

Network Access Devices and Operating Systems

NAC Framework 2.1 functionality is implemented on a wide variety of Cisco devices. Specific hardware models were selected as part of a solution testing effort of features and use cases. These hardware models are listed in Table 1.

Table 1 NAC Framework 2.1 Baseline Devices and Operating Systems

NAC Framework 2.1 Baseline Network Access Device	Authentication Methods	Supervisor, if applicable	Recommended Operating System Image
Cisco Catalyst 2960 switch	NAC L2 802.1x	not applicable	Cisco IOS Release 12.2(35)SE or later
Cisco Catalyst 2970 switch	NAC L2 802.1x	not applicable	Cisco IOS Release 12.2(35)SE or later
Cisco Catalyst 3750 switch	NAC L2 IP NAC L2 802.1x	not applicable	Cisco IOS Release 12.2(35)SE or later

Table 1 NAC Framework 2.1 Baseline Devices and Operating Systems (continued)

NAC Framework 2.1 Baseline Network Access Device	Authentication Methods	Supervisor, if applicable	Recommended Operating System Image
Cisco 6500 series switch	NAC L2 IP NAC L2 802.1x	Supervisor 2, 32	Catalyst OS 8.6(1) or later
Cisco 7200 NPE-G1 router	NAC L3 IP	not applicable	Cisco IOS 12.4(11)T1 or later

In Table 1, we recommend a certain operating system to be used with each of the NADs to ensure their best performance within the NAC Framework 2.1 solution.

Required NAC Framework 2.1 Components

These components are required for the implementation of NAC Framework 2.1:

- Cisco Trust Agent, version 2.1.103.0 or later
- Cisco Trust Agent 802.1x Wired Client, version 4.0.5.5189 or later
- Cisco Secure Access Control Server for Windows, version 4.1.1.23 or later

Though other versions of these software components provide NAC functionality, these versions resolve serious defects and have been tested in the NAC Framework 2.1 environment. Previous versions of these software components are not supported.

Other NAC Framework 2.1 Components

These components are part of the NAC Framework 2.1 Baseline:

- Cisco Security Agent (CSA), version 5.1.
- Cisco IP Phone 7960.

Support for NAC Framework Environments that Deviate from the Baseline

For existing customers with ongoing NAC Framework pilot programs, we will work within their environment and make our best effort to ensure the success of their NAC Framework deployment. If problems arise which we know can be solved by upgrading or changing a component to one included in the baseline, we will advise our customers to do so.

New customers to the NAC Framework 2.1 solution will be advised to adopt the software versions of the components listed earlier before implementation.

NAC 2.1 Framework Baseline Features Available in NAC L2 802.1x Environments

The NAC components below are required to use the features described in this section:

- Network access is controlled by a switch.
- The switch ports are configured for IEEE 802.1x traffic.
- The Cisco Trust Agent (CTA) and CTA 802.1x Wired Client are installed on the end points seeking access to the network.
- An ACS server is configured to perform authentication and posture validation.

ACS Failover

Cisco Secure Access Control Server (ACS) machines can be installed redundantly. Network traffic from the switch to the current ACS can failover to the alternate ACS in these circumstances:

- There is no network connectivity between the switch and the current ACS.
- The current ACS server is not responding for some reason, and the RADIUS session is timing out.

Agentless Host Handling and MAC Authentication Bypass

If CTA and the CTA 802.1x Wired Client are not installed on a device seeking to gain network access, that device will not be able to authenticate itself or provide a posture to ACS. It is most likely that ACS will be configured to deny network access to any device that can not provide authentication or posture information.

When the switch determines that the CTA 802.1x Wired Client is not installed on the device, it uses the MAC authentication bypass feature to give it access to the network.

If the device's Machine Access Control (MAC) address is known, it can be added to a list of MAC addresses maintained on the ACS server or an external LDAP database. When the device seeks access to the network and fails because it does not have the CTA 802.1x Wired Client installed, the switch tries to verify the device's MAC address as one that can bypass authentication. If the MAC address is on the MAC authentication bypass list, the switch can verify the device and allow it on the network without authentication or posture assessment.

This feature is designed to address these use cases:

- MAC Authentication Bypass used as a fallback position when 802.1x client is not present on the host.
- An external LDAP database is used to maintain the list of MAC address for the MAC authentication bypass feature.
- MAC address authentication using ACS internal database to maintain the list of MAC address.

Authentication Methods

User and machine authentication is configured using the CTA 802.1x Wired Client and Cisco Secure Access Control Server (ACS) and enforced by the switch.

User Authentication

NAC Framework 2.1 allows you to authenticate users' security credentials before they are allowed on the network. These are the security credentials that can be validated:

- Username and password maintained in Microsoft Active Directory.

- Username and password stored in ACS
- User-certificate

The user authentication methods are designed to address these use-cases:

- Allow for a user to be authenticated by a "single sign on" (SSO). The user needs only to enter their Microsoft Active Directory (AD) username and password at the "graphical identification and authentication" (GINA) login in order to be authenticated on the network.
- Allow SSO on a host with multiple Microsoft user profiles in use.
- Pass users Group Policy Objects (GPOs) after successful SSO authentication.
- Authenticate the user based on a user name and password maintained separately from Microsoft AD.
- Pass users GPOs after successful authentication using username and password maintained separately from Microsoft AD.
- Allow user authentication with a user certificate.
- Use EAP-MSCHAPv2 or EAP-TLS as the "inner method" of the EAP-FAST authentication protocol.
- Allow for the expiration of the user PAC.
- Allow user certificates to be passed through outer EAP-FAST tunnel.
- Allow user certificates to be used in PAC provisioning.
- Allow the use of chained user certificates.
- Allow for the expiration of user certificates.

Machine Authentication

You may require a hardware device to be authenticated before it is allowed on the network. These are the security credentials that can be validated:

- Machine password
- Machine certificate

The machine authentication methods are designed to address these use-cases:

- Allow machine authentication using a machine password.
- Allow machine authentication with a machine certificate.

- Allow machine authentication only.
- Pass the host the proper GPOs after successful machine authentication.
- Allow machine PAC provisioning to be performed using a valid machine certificate, machine password, or as a result of successful user authentication.
- Allow machine certificates to be passed through outer EAP-FAST tunnel.
- Allow the use of chained machine certificates.
- Allow for the expiration of machine certificates.

Combinations of User and Machine Authentication

You can require a combination of both user and machine authentication.

Machine Authentication Only

This feature allows a computer to be authenticated using only the machine's credentials. Once the machine is powered up, and before the user logs in, the machine's credentials are sent for authentication. After the user logs in at the GINA login, the machine credentials are sent again as part of user authentication process.

Configurable 802.1x Timeout Settings

Use the "dot1x timeout" command on the switch stack or on a standalone switch to set IEEE 802.1x timers that regulate these functions:

- The number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. This can be configured in IOS and CatOS.
- The number of seconds that the switch ignores Extensible Authentication Protocol over LAN (EAPOL) packets from clients that have been successfully authenticated during this duration. This can be configured on IOS only.
- The number of seconds between re-authentication attempts. This can be configured in IOS and CatOS.

- The number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server. This can be configured in IOS and CatOS.
- The number of seconds that the switch waits for the retransmission of packets by the switch to the IEEE 802.1x client. This can be configured in IOS and CatOS.
- The number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. This can be configured in IOS and CatOS.

Use Cisco's Command Lookup Tool for a complete description of the "dot1x timeout" command.

IP Telephone and Device Mobility

User authentication, machine authentication, and MAC authentication bypass features function properly on a computer which is connected to the PC port on an IP Phone.

Machine Access Restrictions with AD Groups

Machine access restrictions (MAR) feature acts as an additional means of controlling authorization for Windows-authenticated EAP-TLS, EAP-FASTv1a, and Microsoft PEAP users, based on machine authentication of the computer used to access the network.

After successful machine authentication, ACS caches the value that was received in the Internet Engineering Task Force (IETF) RADIUS Calling-Station-Id attribute (31). When a user authenticates with an EAP-TLS, EAP-FASTv1a, or Microsoft PEAP end-user client, ACS searches the cache of Calling-Station-Id values from successful machine authentications for the Calling-Station-Id value received in the user authentication request.

If the machine has been previously authenticated, ACS assigns the user to a user group. If the machine has not been previously authenticated ACS assigns the user to the user group specified by **Group map for successful user authentication without machine authentication** list. This can include the **<No Access>** group. The user's access is then defined by their group profile settings.

However, user profile settings always override group profile settings. If a user profile grants an authorization that is denied by the group specified in the **Group map for successful user authentication without machine authentication** list, ACS grants the authorization.

VLAN Assignment

A host can be assigned to a particular VLAN, such as a corporate VLAN, a guest VLAN, or a remediation VLAN based on the host's posture and authentication information. To use this feature, network access must be managed by a switch and its ports must be configured to send and receive IEEE 802.1x traffic.

The VLAN assignment feature is designed to assign hosts to one of these VLANs:

- Guest VLAN
- AAA Failed VLAN
- Critical-Authentication VLAN
- Passed Authentication VLAN
- Failed Authentication VLAN

NAC Framework 2.1 Baseline Features Available in NAC L2 IP and NAC L3 IP Environments

ACS Failover

Cisco Secure Access Control Server (ACS) machines can be installed redundantly. Network traffic from the switch or router to the current ACS can failover to the alternate ACS in these circumstances:

- There is no network connectivity between the switch or router and the current ACS.
- The current ACS server is not responding for some reason, and the RADIUS session is timing out.

Agentless Host Handling and EAP over UDP Bypass

If CTA is not installed on a device seeking to gain network access, that device will not be able to provide posture credentials to ACS. It is most likely that ACS will be configured to deny network access to any device that can not provide posture information.

When the NAD determines that CTA is not installed on the device, it uses the EoU bypass feature to give the device access to the network.

If the device's Machine Access Control (MAC) address or IP address are known, they can be added to an exception list maintained on the NAD, the ACS server or an external database. When the device seeks access to the network and fails because it does not have CTA installed, the NAD tries to verify the device's MAC address or IP address from the exception list. If the device's MAC address or IP address is on the exception list, the device's identity can be verified and the device can be allowed on the network without posture assessment.

This feature is designed to address these use cases:

- Agentless host can be added to the EOU MAC address exception list in an EOU environment.
- MAC address authentication using ACS internal database to maintain MAC address exception list.

Client Authorization During AAA Failure with Default Switch Policy

This feature applies in NAC L2 802.1x and NAC L2 IP environments. If the ACS is down and can not authenticate a session or determine a posture, the switch grants or denies network access based on the customer's default security policy which is stored on the switch.

EAP over UDP Triggering Using DHCP Snooping and ARP Inspection

NAD monitors DHCP (Dynamic Host Configuration Protocol) requests or ARP (Address Resolution Protocol) requests to initiate an EAP over UDP session. This is a feature of a NAC L2 IP environment.

EAP over UDP Triggering Using IP and Interesting Traffic from IP Admission Access List

The NAD initiates an EAP over UDP session if any traffic traverses the IP admission interface. You can also use an IP admission access list to allow or prevent certain traffic from triggering the EAP over UDP session. For example you might want to exclude ICMP traffic from triggering an EAP over UDP session. This is a feature of a NAC L3 IP environment.

EAP over UDP Triggering Using IP Device Tracking

IP device tracking is a feature of a switch. You must enable the IP device tracking feature to use NAC L2 IP validation.

When IP device tracking is enabled, and a host is detected by the switch, the switch adds an entry to its IP device tracking table. If NAC L2 IP validation is enabled on an interface, adding an entry to the IP device tracking table initiates EAP over UDP session so that posture assessment can be performed.

IOS Routers and Switches Support Non-Responsive Host or Agentless Host Handling

Network access devices (NADs) running the IOS operating system can participate in the investigation of “non-responsive” hosts. The NAD performs a URL redirect to a Web server where the user downloads an ActiveX or Java applet that scans the non-responsive host.

“Non-responsive” hosts are hosts that cannot provide posture credentials for any reason, such as Cisco Trust Agent (CTA) has not or can not be installed on the host. Without CTA installed, the host cannot respond to a NAC challenge.

IP Telephone and Device Mobility

The computer connected to the PC port on an IP phone will get posture validated successfully.

Session Management with EAP over UDP Timers

A switch or router queries the host and CTA indicates if status of the host has changed. It also perform session verification with a session timeout. If CTA does not respond to the session verification, the EOU session will timeout.

Status Query Challenge

Upon expiration of the status query timer, a status query challenge is sent to the host. If CTA indicates to the NAD there is a change in posture, the NAD starts posture revalidation.

URL-Redirection, Access Control Lists, and Browser Auto-Launch

The URL-redirection feature is intended for hosts requiring remediation. If a host requires remediation, the ACS would download an Access Control List (ACL) specifying the URL of the remediation server. All HTTP traffic from the host would be redirected to the remediation server.

The browser auto-launch feature provides a way to launch a browser window and direct it to a URL if a specific posture validation rule is triggered. This URL may provide system or application updates to the user or it may be a means to provide information or notices.

NAC Framework 2.1 Compatibility with Legacy 802.1x Supplicants

If Cisco Trust Agent (CTA) is installed on a host running Windows XP Professional with Service Pack 2, which has an 802.1x supplicant integrated in the Windows operating system, authentication and posture tasks are divided between the Microsoft (MS) 802.1x supplicant and CTA. This feature is designed to address these use cases:

- User authentication is performed using PEAP and MSCHAPv2 by the Microsoft 802.1x supplicant. Posture validation is performed in an EAP over UDP session and managed by CTA.
- The network access policy is applied by VLAN assignment determined by the MS 802.1x session and Access Control Lists are pushed to the switch using the NAC L2 IP session.
- VLAN assignment can be determined by authentication managed by MS 802.1x supplicant or by posture managed by the NAC L2 IP session.
- This mixed environment can manage a AAA failure scenario using one of these features:
  - Client Authorization During AAA Failure with Default Switch Policy
  - ACS Failover

NAC Framework 2.1 Baseline Features Implemented on ACS

These are the NAC Framework 2.1 features that are implemented on Cisco Secure Access Control Server.

ACS Replicates Configuration Changes on Primary Server to Secondary Server

A change to the configuration on the primary ACS can be replicated on the secondary ACS server. Replication can be performed manually or it can be scheduled.

Browser Auto-Launch with UserNotificationTLV

The browser auto-launch feature provides a way to launch a browser window and direct it to a URL if a specific posture validation rule is triggered. This URL may provide system or application updates to the user or it may be a means to provide information or notices.

External LDAP Database Has Failed or is Unreachable

When ACS uses an external LDAP database for MAC Authentication Bypass (MAB) and there is a failure in verifying a valid MAC address and group, ACS assigns this MAC address to a pre-configured group and receives the authorization policy for that group.

When the external LDAP server becomes available, ACS uses configured Authorization policy to assign the corresponding RADIUS Authorization Components (RAC) which contains VLAN, timer, and other settings.

For the devices that were previously added to the unauthenticated MAC address group, their MAC addresses are reassessed at the end of a session timeout and they are reauthenticated.

External Policy Validation Server (HCAP) Has failed or is Unreachable

If an external policy server is down, then a posture token can be assigned to the corresponding vendor’s application until the policy server is restored.

Microsoft Active Directory Has Failed or is Unreachable

These features are designed for a network environment using redundant Microsoft Active Directory (AD) servers:

- If no AD server responds to the authentication request, the host will be authenticated by the secondary domain controller without causing interruptions on the host. The CTA 802.1x Wired Client indicates that the host has been authenticated.
- If both AD servers fail during an 802.1x authentication session, the host will be put in a "AAA fail" VLAN.
- If both AD servers fail during authentication, the host is put in a "AAA fail" VLAN. When an AD server recovers, existing clients are re-authenticated automatically and newer clients are authenticated successfully. The CTA 802.1x Wired Client indicates that the host has been authenticated.

Single Sign-on Access Allowed and GPOs Executed for a User Accessing Multiple Domains

Users can be authenticated by single sign-on on more than one domain if the domain on which ACS is installed has two-way trust established with the other domains, and if Microsoft Active Directory manages both domains.

After users are authenticated in either domain, they will receive their appropriate GPOs.

NAC Framework 2.1 Baseline Features Implemented on CTA

These features are available in NAC L2 802.1x, NAC L2 IP, and NAC L3 IP environments.

Asynchronous Posture Status Query

This asynchronous posture status query is implemented in two different ways on NAC L2 802.1x networks. This feature can not be used on NAC L2 IP or NAC L3 IP networks.

- CTA can be configured to query posture plugins at regular intervals to determine if there has been a change to their application's status. If a posture plugin alerts CTA that there has been a change in posture status, CTA alerts the network access device which triggers a re-posturing of the host.
- Some posture plugins monitor the status of their applications and report status changes to CTA upon detection. Such plugins are considered "asynchronous" plugins. When CTA receives the status change from an asynchronous plugin, CTA alerts the network access device, which triggers a re-posturing of the host. For example, the posture plugin for Cisco Security Agent (CSA) detects when the CSA security has been turned off.

Status Query Challenge

In the case of NAC L2 IP or NAC L3 IP network admission methods, upon expiration of the status query timer, a status query challenge is sent to the host. If CTA indicates to the NAD there is a change in posture, the NAD starts posture revalidation.

Posture Notification

Once the posture of the host has been determined, the user receives a pop-up message in a browser window reporting the results. The browser window may contain a **clickable URL** which can direct a user to information or remediation.

Instead of receiving a pop-up window with a clickable URL, a browser window, pointing to a specific URL, can be launched automatically and presented to the user. This is referred to as the "Browser auto-launch" feature.

Posture Validation

Posture is the result of an evaluation of the operating system and applications that are installed on a host. Cisco Trust Agent (CTA) gathers posture credentials from the host and forwards them to Cisco Secure Access Control Server (ACS) for evaluation. After ACS calculates the posture of the entire host, it informs the network access device of the result. Based on the posture the NAD enforces an access control rule for the host. A "Healthy" posture will receive full network access, while a "Quarantine" posture may send the host to a remediation VLAN where its operating system or applications may be updated.

NAC 2.1 Limitations

Cisco Trust Agent 2.1 No Longer Supports Windows NT

CTA 2.1 does not support Windows NT 4.0 Server or Windows NT 4.0 Workstation. CTA 2.0 was the last release to support Windows NT 4.0.

Known Defects in NAC 2.1 Components

This section describes problems known to exist in the various components that comprise the Network Admission Control 2.1 release.

Note A "—" in the Explanation column means that no information was available at the time of publication. For the latest information on these defects logon to Cisco.com and launch the Cisco Software Bug Toolkit. To access the Cisco Software Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl. (You will be prompted to log in to Cisco.com.)

Known Defects in Catalyst 8.6(1) Operating System

Table 2 describes defects found on Catalyst 6500 series switches running the CatOS 8.6(1) operating system. For a complete list of the features and defects for CatOS 8.6(1), refer to the CatOS's product release notes available at http://www.cisco.com.

Table 2 Known Defects in Catalyst 8.6.1 Operating System

Bug ID	Headline	Explanation
CSCsd43177	URL-redirect does not work with ports other than http server port 80.	**Symptom** URL-Redirect is not working on port other than http server port 80. **Conditions** Occurs in Catalyst 8.6.1 operating system. **Workaround** None. URL-Redirect is supported only on http port 80 only.
CSCse29446	URL-redirect string in policy does not accept "?" character. Editing command should be made visible.	**Symptom** URL-Redirect string in exception policy does not accept "?" char. **Conditions** Occurs in Catalyst 8.6.1 operating system. **Workaround** Disable editing with the **set editing disable** command. This is a hidden command.
CSCsg78223	Port Security with Aux VLAN on Dot1x port - Port shuts down on 2nd MAC address	**Symptom** When a second MAC address is seen on a Data VLAN, the port shuts down and thereby affects voice traffic. **Conditions** Occurs in Catalyst 8.6.1 operating system. Port security and authentication features are enabled on the port. **Workaround** None.

Table 2 Known Defects in Catalyst 8.6.1 Operating System (continued)

Bug ID	Headline	Explanation
CSCsg79868	Host behind phone - phone traffic on native VLAN after port disable / enable	**Symptom** Host behind phone - phone traffic on native VLAN after port disable/ enable with port security enabled. Port gets shutdown **Conditions** Occurs in Catalyst 8.6.1 operating system. Aux VLAN is configured and port security is enabled with **set port security mod/port maximum 3** command. **Workaround** Power off and power on the phone.
CSCsg94068	Spantree forwarding on multiple VLANs	**Symptom** Spanning tree forwarding on multiple VLANs **Conditions** Occurs in Catalyst 8.6.1 operating system. This is seen with 802.1x / MAB during reauthentication when a different VLAN/PVLAN is assigned. This can also happen with a 802.1x/MAB authentication port when module is powered down and up or Online Insertion and Removal of module is done. **Workaround** None. This is a display problem and will not affect traffic.
CSCsh06794	TAL-Misleading Errmsg Dot1x port is not private capable, config VLAN change	**Symptom** Changing PVLAN configuration from command line interface on an authenticated PVLAN port does not update the NVRAM. Traffic may also be affected. Misleading message "Dot1x port is not private VLAN capable" may be printed. **Conditions** Occurs in Catalyst 8.6.1 operating system. **Workaround** There is no workaround.

Table 2 Known Defects in Catalyst 8.6.1 Operating System (continued)

Bug ID	Headline	Explanation
CSCsh34895	MAB remains in “authenticated critical” state after reauthentication	**Symptom** MAB / EOU remains in authenticated critical after reauthentication. **Conditions** Occurs in Catalyst 8.6.1 operating system. **Workaround** This is a display problem and reauthentication happens except that the critical status of the port is not cleared. Initialize MAB / EOU on port.
CSCsh48166	DAI on ports not functioning with IPSG when DAI is enabled first	**Symptom** Dynamic ARP Inspection (DAI) is not functioning on ports with IP Source Guard (IPSG). **Conditions** Occurs in Catalyst 8.6.1 operating system. DAI is enabled before IPSG on CatOS 8.6.1. **Workaround** Enable IPSG first before enabling DAI on ports.
CSCsh52990	IP Phone ACE not present in TCAM on reset, with auto-save	**Symptom** IP Phone bindings are not reflected in TCAM after switch reset. **Conditions** Occurs in Catalyst 8.6.1 operating system. DHCP snooping auto-save is enabled. **Workaround** There is no workaround.
CSCsh70693 (CSCsh46541)	HA -PVLAN Dot1x Crash in Security_Rx on standby	**Symptom** Clearing Primary or secondary VLAN on a 802.1x / MAB authenticated port may result in a crash. Same can happen when assigning a PVLAN from command line interface to a 802.1x/MAB authenticated port. **Conditions** Occurs in Catalyst 8.6.1 operating system. **Workaround** Clear the mapping of the PVLAN to the auth port before clearing / assigning the PVLAN.

Table 2 Known Defects in Catalyst 8.6.1 Operating System (continued)

Bug ID	Headline	Explanation
CSCsh72654	EOU exception hosts not getting assigned URL string with MAC masks	**Symptom** EOU exception hosts not getting assigned URL string with MAC masks **Conditions** Occurs in Catalyst 8.6.1 operating system. Mac mask is configured with values in the mask field. For instance When mac address and mask is 00-12-79-cd-88-69 00-00-00-00-00-FF, host goes to exception state but URL-Redirect string is not applied. **Workaround** For above MAC mask, the correct mask is 00-12-79-cd-88-00 00-00-00-00-00-FF (the last 2 bytes of MAC add should be 00)
CSCsh75713	Configuration loss in critical authentication feature after upgrading from 8.5.8 to 8.6.1	**Symptom** Configuration loss in critical authentication feature on upgrade from 8.5.8 to 8.6.1. **Conditions** Occurs in Catalyst 8.6.1 operating system. **Workaround** 8.5(8) command line interface for 802.1x critical authentication are deprecated. So critical authentication has to be reconfigured using the **set port critical mod/port enable/disable** command.

Known Defects in CTA 2.1 Posture Agent

Table 3 describes problems known to exist in the posture agent functionality of Cisco Trust Agent, Release 2.1.103.0. This section excludes defects of the 802.1x Wired Client component of CTA 2.1. For a complete list of the features and defects for CTA, refer to CTA's product release notes available at http://www.cisco.com.

Table 3 Known Defects in the CTA 2.1 Posture Agent Client

Defect ID	Headline	Explanation
CSCsc18885	Erroneous log entry, claiming "Failed to read Registry Key" in CTA log.	**Symptom** When a user performs a fresh installation, upgrade, or reinstallation of Cisco Trust Agent with logging enabled, an **erroneous** log message is generated. This message is similar to this message: `2 12:00:00.000 11/11/2005 Sev=Critical/1 PSDaemon/0xE3C0001A Failed to Read Registry Key, error code 2` **Conditions** This erroneous log message is generated when the Cisco Trust Agent Version 2.0.0.30 is Installed, Reinstalled, or Upgraded with logging enabled. This **erroneous** log message was observed on the following platforms: Windows NT 4.0, Window 2000 and Windows XP. **Workaround** No workarounds are available. Note that this log message is erroneous and does not affect the running of Cisco Trust Agent.

Table 3 Known Defects in the CTA 2.1 Posture Agent Client (continued)

Defect ID	Headline	Explanation
CSCse27741	CTA uses wrong root certificate when an expired certificate exists along with working certificate.	**Symptom** Existing customer certificates work with some authentication protocols but not EAP over UDP (NAC-L3-IP or NAC-L2-IP). The certificates are valid and are stored in the correct locations. This message is in the ACS Failed Attempts log: “EAP-TLS or PEAP authentication failed during SSL handshake.” **Conditions** The existing certificate is part of a certificate chain in which the root certificate is expired. The expired root certificate has the same subject name as the valid certificate and both certificates coexist in CTA client’s certificate store. **Workaround** Remove this expired root certificate from the user certificate store.
CSCsg08764	CTAstat incorrectly reports operational status for plugin	**Symptom** ctastat reports that a posture plugin is working correctly when some other system behavior, such as a failed authentication, indicates that a plugin might not be working correctly. **Conditions** Any condition where the plugin is not working correctly or it is missing; for example, corrupted or missing .dll or .so file, missing .inf file, the plugin was installed in the wrong directory, or the plugin is corrupted etc. **Workaround** Enable logging on the client in order to capture information about the failed plugin.

Table 3 Known Defects in the CTA 2.1 Posture Agent Client (continued)

Defect ID	Headline	Explanation
CSCsg26209	CTA does not support downgrade of posture plugins	**Symptom** A posture plugin for a third-party application does not respond at all or does not respond with values for all posture attributes. In the CTA log files you may see these messages like "client not installed," "client is running the wrong version," or "client communication error." **Conditions** The third-party client application has been downgraded, and though the corresponding downgraded plugin has been dropped into the Cisco Trust Agent plugins/install directory, CTA has not installed it because the previous plugin has a higher version number. **Workaround** Uninstall the higher revision of the plugin then install the version of the plugin that corresponds to the downgraded application's version. **Note** You can verify the version numbers of the plugin and application by viewing their properties.

Known Defects in CTA 802.1x Wired Client

Table 4 lists the defects in the CTA 802.1x Wired Client 4.0.5.5189. This version was released with CTA 2.1. The CTA 802.1x Wired Client may also be referred to as the "supplicant." For a complete list of the features and defects for the CTA 802.1x Wired Client, refer to the CTA 2.1 product release notes available at http://www.cisco.com.

Table 4 Known Defects in the CTA 2.1 802.1x Wired Client

Defect ID	Headline	Explanation
CSCsb47789	TLS alert bad_certificate(42) should be unknown_ca(48)	**Symptom** The CTA 802.1x Wired Client sends an incorrect error code to the ACS. The 802.1x Wired Client sends bad_certificate(42) when it should send unknown_ca(48). This error gets logged on the ACS and might mislead ACS administrators. The result is an incorrect log on the ACS, but it does not affect the functionality of the 802.1x Wired Client nor ACS. **Conditions** A valid certificate chain or a partial chain was received, but the certificate was not accepted because the CA certificate could not be located or could not be matched with a known, trusted CA **Workaround** There is no workaround.

Table 4 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCsb88110	The 802.1x Wired Client pop up box is hidden during bootup with multiple interfaces.	**Symptom** When booting up a PC with multiple interfaces (four), with the 802.1x Wired Client installed, a user enters his username on first popup box and then his password. However, the second popup box does not appear. The 802.1x Wired Client is waiting for the password to be entered for the second popup box. Then the third popup box appears. The forth popup box does not appear but the 802.1x Wired Client waits for the password to be entered. **Conditions** This occurs with multiple interfaces that are all getting authenticated. **Workaround** Set the EnableLogonNotifies attribute to 0 in the ctad.ini for CTA.
CSCsc31219	User credentials dialog does not close upon failure to connect.	**Symptom** If the network client fails to provide a posture at Layer 2, and ACS fails to set a policy for the network client, and if the user enters incorrect credentials, the user credentials dialog box is not automatically removed from the screen. **Workaround** Users need to manually close the user credentials dialog box.

Table 4 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCsc39374	RSA 5.2 new pin mode does not work with CTA 802.1x Wired Client	**Symptom** User authentication fails. **Conditions** RSA 5.2 is used for authentication. This is the behavior the user experiences: 1. User is prompted for username. 2. User is prompted for password. User enters RSA tokencode here. 3. User responds with “y” at the prompt to create a new PIN. 4. The user is then prompted for username two times, until the connection fails. **Workaround** There is no workaround.
CSCsd60058	Dot1X, EAP-MSCHAPv2 password change fails when password complexity requirement is enforced	**Symptom** Password Complexity requirements are not displayed on the supplicant UI, leading to password change failure with simple passwords. **Conditions** ACS configured for EAP-MSCHAPv2 as inner authentication method does not send enough information to the client, this is why the password change process has failed. This results in using non-complex or non-confirming password as the new password and leads to password change failure and 802.1x authentication failure. **Workaround** Disable the password complexity rule on AD or use a complex enough password which confirms to the Corporate Password policy.

Table 4 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCse35094	Password entered in supplicant Credentials popup is not used.	**Symptom** Password entered in supplicant Credentials popup is not used for authentication. **Conditions** With machine and user authentication enabled, the password entered in supplicant Credentials popup is not used for authentication. **Workaround** There is no workaround.
CSCse35113	CTA 802.1x Wired Client can indicate that the ethernet interface is authenticated and connected when it is not.	**Symptom** With IEEE 802.1x authentication configured, the CTA 802.1x Wired Client status shows that the client is authenticated and connected to the network when it is not. **Conditions** This error can happen when you try to reconnect after a failed authentication. **Workaround** The incorrect connection status will time out in about one minute.

Table 4 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCse54397	CTA 802.1x Wired Client delays 802.1x authentication after returning from hibernation.	**Symptom** While client is coming out of hibernation state the supplicant needs to initiate a IEEE 802.1x connection for either machine or user authentication. The time it takes for supplicant to initiate for IEEE 802.1x authentication may vary form 15-to-80 seconds. **Conditions** The CTA 802.1x Wired client eventually initiates IEEE 802.1x authentication but the time it takes varies between 15-to-80 seconds after the network interface comes up. This delay depends on various factors like Operating system, PC hardware configuration, and the context of the machine, for example, is the user logged into desktop or not. **Workaround** Wait for the CTA 802.1x Wired Client to initiate IEEE 802.1x authentication after the interface comes up or open the CTA 802.1x Wired Client main window, select the network adapter you use to connect to the network, click Disconnect, and then click Connect.

Table 4 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCse77264	CTA 802.1x Wired Client fails to launch after a reboot	**Symptom** This problem occurs intermittently. Reboot the client on which CTA and 802.1x Wired Client is installed. You see the following behaviors: • 802.1x Wired Client user interface does not prompt for password. • User does not see posture popup message after logging in. • CTA 802.1x Wired Client user interface cannot be seen, and its icon is not visible in the system tray. • Navigating Start > Program Files > Cisco Systems > Cisco Systems, Inc. Cisco Trust Agent 802.1x Wired Client > Cisco Trust Agent 802.1x Wired Client Open does not launch the 802.1x Wired Client. • The Windows Services control panel indicates that all the CTA related services are running. • Stopping the “Posture Server Daemon” takes an unusually long time, and fails. • Client needs to be rebooted to fix this. **Conditions** Behavior was detected on Windows 2000 Professional with Service Pack 4. 802.1x Wired Client is configured to prompt for user password. **Workaround** There is no workaround.

Table 4 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCse93282	MSCHAP authentication uses system credentials with a specific profile	**Symptom** 1. Reboot client. 2. Login using Microsoft GINA. 3. CTA 802.1x Wired Client prompts for authentication credentials. 4. Provide a nonexistent username. 5. Client will posture and authenticate using the GINA/System user account. It works like an SSO scenario. **Conditions** ACS is configured to use EAP-MSCHAPv2 (ONLY) as inner authentication method. ACS uses Windows Active Directory as back-end user database. The client uses an authentication profile with these attributes: • Request password when needed. • Use client certificate during machine authentication and user authentication. • Never validate Trusted Servers. • Use anonymous as identity. • Automatically establish machine connection. **Workaround** There is no workaround.

Table 4 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCsf24460	CTA 802.1x Wired Client EAP-FAST Inner identity in UPN format should include domain.	**Symptom** ACS initiates a domain controller lookup of a username in UPN format that either fails or takes a long time to complete. **Conditions** The CTA 802.1x wired client removed the domain from the username, and ACS does the lookup in a Windows multi-domain architecture where the domain portion of the UPN username is needed to clarify the username. **Workaround** None, other than re-architect the Windows network to avoid multi-domain lookups.
CSCsf29511	Under high CPU of PC situation, CTA cannot respond IEEE 802.1x packet	**Symptom** Under high CPU utilization on a PC, CTA cannot respond IEEE 802.1x packet. **Conditions** High CPU utilization on the PC because of resource depletion or other issues. This occurs on Windows PCs where the CTA 802.1x Wired Client has also been installed. **Workaround** Make sure all logging levels for CTA are set to the lowest value or even turned off. Try adding more memory or increase CPU on machine. Try eliminating applications that are using the device’s resources.
CSCsf29547	CTA 802.1x Wired Client remains in connecting state when certificate is revoked.	**Symptom** When the machine certificate has been revoked, the connection does fail, but the CTA 802.1x Wired Client continues to try to re-connect. This results in the supplicant staying in a constant “yellow” state. **Conditions** CTA 802.1x Wired Client is configured for machine authentication only and it uses a revoked machine certificate. **Workaround** There is no workaround.

Table 4 Known Defects in the CTA 2.1 802.1x Wired Client (continued)

Defect ID	Headline	Explanation
CSCsf32767	CTA 802.1x Wired Client sends wrong password after Active Directory password change.	**Symptom** IEEE 802.1x user authentication may fail if user has to change Active Directory password. **Conditions** Using single sign-on with CTA 802.1x Wired Client, the user is prompted to change their Active Directory password. CTA 802.1x Wired Client sends the old password and User authentication fails. **Workaround** Reboot or logoff the user and attempt a login with the new/correct Active Directory credentials.
CSCsg14487	Password is cached even when GTC is configured	**Symptom** OTP passwords are cached after a successful connection attempt until the subsequent connections (3 attempts) have failed authentication. **Conditions** GTC is enabled on ACS. **Workaround** Click “clear credentials” button in Network Configuration Summary window prior to making a connection attempt.
CSCsg23722	User not allowed to change incorrect username right away.	**Symptom** When an invalid username is entered in the supplicant popup the user is not given the opportunity to change it for about 30 seconds. The popup's that appear for about 30 seconds only allow you to enter the password. **Conditions** This only occurs when the host is configured for machine and user authentication without single sign on and EAP-GTC is user for an inner authentication method. **Workaround** After about 30 seconds, the user receives another popup dialog box where they can enter the correct username.

Table 4 ***Known Defects in the CTA 2.1 802.1x Wired Client (continued)***

Defect ID	Headline	Explanation
CSCsg34154	CTA 802.1x Wired Client does not re-start authentication after aborted CSA downgrade.	**Symptom** PC wired interface does not re-authenticate after an aborted CSA downgrade. **Conditions** Only observed during aborted CSA downgrade. **Workaround** Open wired client GUI and click Connect.
CSCsh17908	Windows CTA 802.1x Wired Client conflicts with some Smart Card software	**Symptom** Users receive the error message "The system cannot log you on due to the following error: The handle is invalid." when they attempt to connect with some smartcard software after installing CTA with the 802.1x Wired Client **Conditions** The issue has been observed in an environment using the CTA 802.1x Wired Client distributed with CTA 2.0.1.14 in conjunction with third-party smartcard software. Installation of CTA on this system interferred with Windows authentication using this software. **Workaround** Current version of Cisco SSC 802.1x client combined with the non-802.1x CTA client worked in this environment.
CSCsh39205	Cancelled shutdown causes supplicant icon to disappear	**Symptom** The Cisco Trust Agent 802.1x wired client icon no longer appears in the Windows system tray. **Conditions** User has cancelled a Windows shutdown sequence, logged off, and re-logged in to Windows with a different user account. **Workaround** There is no workaround.

Known Defects in ACS 4.1

Table 5 describes defects in specific behaviors of ACS for Windows 4.1 and the ACS Solution Engine 4.1. These defects in ACS 4.1 may affect a NAC 2.1 implementation. For a complete list of the features and defects for ACS, refer to ACS's product release notes available at http://www.cisco.com.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1

Defect ID	Headline	Explanation
CSCeg50237	Overinstall causes the added AVP Attributes to disappear.	**Symptom** Adding AVP attributes and then performing an overinstall causes those attributes to disappear from the Log Attribute field. **Workaround** There is no workaround.
CSCsc32125	After replication, NAC is not functional until service is restarted.	**Symptom** Posture Failed for EAP-FAST & PEAP, Layer 2 & Layer 3 Authen-Failure-Code = "EAP type not configured" **Conditions** These conditions will reproduce the symptom: 1. Restore DBdump provided to master and slave (already with certs and config for EAP-FAST). 2. Replicate (all except network config). 3. Revalidate posture. **Workaround** Enter system | service control | restarted.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCsd28533	EAP-FAST with EAP-TLS inner method failed to authenticate with ACS v4.0	**Symptom** EAP-FAST with EAP-TLS Inner method failed to authenticate (phase 0-PAC provisioning) with ACS v4.0 when using Aironet Desktop Utility (ADU) version v3.0.0.190 and Driver version v3.0.0.66. **Conditions** These conditions will reproduce the symptom: 1. Request one user certificate from CA server and configure the EAP-FAST with EAP-TLS as inner method. Note that the username of the certificate must be the same one as the Windows login username. Also we enable automatic PAC provisioning. 2. The ADU will fail to do the authentication. The log from ACS 4.0 shows "EAP type not configured". 3. If we authenticate to the AP by EAP-TLS & WPA with the same user certificate, the authentication will pass. 4. Also, if we get the user PAC manually and use the stored PAC with EAP-TLS as inner method, the authentication will pass. **Workaround** Generate PAC manually and use the stored PAC with EAP-TLS as inner method, the authentication will pass.
CSCse25423	Bypass Info & extBDinfo fields in the passed\failed reports are empty	**Symptom** Bypass Info & extBDinfo fields in the passed authentication and failed attempts page in reports and activity are empty. **Conditions** These conditions will reproduce the symptom: 1. Select the Bypass Info & extBDinfo attributes in logging page under system configuration page for both passed authentication and failed attempts. 2. Submit 3. Preform MAB request. **Workaround** There is no workaround.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCse45366	EAP-FAST reauthentication records in ACS as new user	**Symptom** After successful authentication using EAP-FAST protocols and CTA 802.1x Wired Client, the next reauthentication records in ACS show as a new user. Configured ACS (using RADIUS Authorization Components (RAC)) to download attribute 27 (session time) and every 30 seconds the CTA 802.1x Wired Client tries to reauthenticate with same user name. What happened is that in ACS (group setup or user setup) appears that there are 91 users but when pressing **show users** in this group you see only one user. **Conditions** These steps will reproduce the symptom: 1. Enable EAP-FAST protocol in ACS in global authentication and NAP 2. Configure RAC with attribute 27 (session time) to 30 sec. 3. Perform full authentication **Workaround** There is no workaround.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCse47038 (CSCsf9755)	Invalid MAC address format with mixed delimiters - MAB request granted	**Symptom** MAB request which contains an invalid MAC address format - with mixed delimiters is searched in both internal and external LDAP. If similar MAC address exists, the request is granted. **Conditions** These steps reproduce the symptom: - Send MAB request with the following MAC addresses: 00:00-55.551111 (00-00-55-55-11-11 is valid internal) 00-Ab:Cd.Ef-7777 (00-AB-CD-EF-77-77 is valid LDAP) Mixed delimiters are regarded as valid MAC format in run-time & searched in internal / LDAP DBs. Same MAC addresses with mixed delimiters are considered as invalid if attempted to be configured in GUI (as internal address) - Configuration is rejected and this is correct behavior. **Workaround** Use valid MAC format
CSCse52036	LPIP posture for Cisco:HIP causes Internal Failure	**Symptom** Attempting Performance evaluation of 3750 with Cisco: PA, HOST and HIP rules activated cause a large percentage (50% or more) clients to fail with Authen-Failure-Code of Failure message of “Internal Failure.” **Workaround** There is no workaround.
CSCsf10732	Many Internal Errors and context list overflows under CiscoPEAP heavy load.	**Symptom** While running Cisco PEAP against CSDB, logs contain many error messages and Also Failed Attempts.csv contains many internal error messages. This happened after number of short and long term periods of heavy load. **Workaround** There is no workaround.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCsf11087	Attributes not showing in Passed Auth report for Linux client	**Symptom** Cisco:PA attributes are not showing up in the Passed Authentication Report for a Linux client with CTA 2.1.0.10 installed. The attributes are showing up in the AUTH.log file and are showing up for a Windows XP client on the same network. **Conditions** These steps will reproduce the symptom: 1. In System Configuration-->logging-->Passed Authentication select Cisco:PA attributes 2. Click submit 3. Performs authentication using Linux client with CTA 2.1.0.10 4. Check pass authentication log in reports and activity page **Workaround** There is no workaround.
CSCsf32284	NAC-L3:EAP-TLV can be sent although CSRADIUS did not send access accept	**Symptom** NAC-L3:EAP-TLV can be sent although CSRADIUS did not send access accept. **Conditions** Create NAC policy for NAC-L3-IP, the template will also create a RADIUS Authorization Component (RAC), notification for system restart will appear. --DONT RESTART -- I've used a E2E real env, and as a result pass auth record was added (in reports) but SPT column is empty, CSauth report for access accept and start authorization part. CSRADIUS doesn't send access accept packet, but EAP-TLV is being sent back to the CTA 802.1x Wired Client which results in PA msg popup. Template should create a disable NAP in this case or initiated a system restart as part of the procedure. **Workaround** There is no workaround.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCsg12943	csauth faulting application 4503 switch NAC L2 IP clientless stress game.dll	**Symptom** csauth faulting application when running NAC L2 IP on approximately 90 clients using 4503 switch Version 12.2 **Conditions** 1. Configure ACS for NAC L2 IP and PEAP protocol. 2. 4503 switch is configured to allow clientless. **Workaround** There is no workaround.
CSCsg19044	ACS syslog and ODBC configuration is missing in the listing for Trend, McAfee, and Qualys.	**Symptom** Under system configuration, logging configuration, configure failed attempts or passed attempts for syslog and ODBC. The attributes for Trend, Qualys and McAfee are not listed in either column but are listed under the CSV configuration. **Conditions** When adding third party vendors credentials using csutil -addAVP command, these credentials will not appear in syslog or ODBC. **Workaround** There is no workaround.

CSCsg32655	MAC Authentication Bypass Request hangs when username attribute contains valid user in ACS DB	**Symptom** When Sending MAB request using WinRadius with the following attributes, MAB request hangs - "Failed Attempts" CSV report indicates "internal error"
		`service-type=10;`
		`calling-station-id=<MAC address defined in ACS internal db>;`
		`username=<valid user defined in ACS internal DB>;`
		`password=<valid password for the user>`
		Conditions
		1. Enable MAB in NAP configuration.
		2. Enable MAB and configure MAC address ACS internal db.
		Workaround MAB request should not contain valid ACS user.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCsg40727	**Headline** RDMS fails account action 220 250 with Synchronization Partners **Symptom** - NDG is not getting added to "Synchronization Partners", but an additional (duplicated) entry is getting added to "primary" - AAA-Client may can not be deleted anymore afterwards **Conditions** Account-Action-File: SequenceId,Priority,UserName,GroupName,Action,ValueName,Value1,Value2,Value3,DateTime,MessageNo,ComputerNames,AppId,Status 1,0,testUser01,foobar,100,,foobar,,,26/08/1998 00:00,0,,,0 9,0,testUser09,foobar,100,,foobar,,,26/08/1998 00:00,0,,,0 10,0,testUser10,foobar,100,,foobar,,,26/08/1998 00:00,0,,,0 11,0,,foobar,170,,exec,,,,,,,0 12,0,,foobar,172,priv-lvl,exec,,15,,,,,013,0,,,220,chimpanzee070707,9.9.9.9,cisco,VENDOR_ID_CISCO_RADIUS,,,,,0 14,0,,,250,monkeycage,,,,,,,,0 15,0,,,252,chimpanzee070707,monkeycage,,,,,,,0 **Workaround** There is no workaround.	
CSCsg42483	No Access-Rejected is being sent by ACS when Cisco PEAP TLS fails	**Symptom** Currently ACS doesn't replies with Access-Rejected when any error happens at time of authentication, like certificate is revoked, or bad certificate. Authentication fails on supplicant due to Time-Out happened. **Conditions** These conditions will reproduce the symptoms: 1. Enable PEAP-TLS protocol in ACS 2. Revoked user certificate in CA server 3. Configure CRL in ACS 4. Perform user authentication **Workaround** There is no workaround.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCsg50297	Session timeout with EAP-FAST	**Symptom** Timeout after period specified in the Radius attribute not working. 4.1 build 18 & 19 with EAP-FAST as authentication protocol, no NAD but with NAP and external AD, authentication with pac was already made. **Conditions** Wireless Client Aironet Desktop Utility (ADU) & ACU configure to use EAP-FAST, (the user is already connected with PAC) AP configure to use authenticator from server ACS configure in the user group setting. Setup: 1. “Cisco Aironet RADIUS Attributes” ([5842\001] 2. “IETF RADIUS Attributes” ([027] Session-Timeout).
CSCsg53828	CSRADIUS fails to initialize correctly on machine reboot.	**Symptom** ACS does not process Authentication requests. The symptom is seeing continuous Authentication Failure messages for ACS's own RADIUS interface. **Conditions** This defect comes into play when more than one interface is enabled. The reason for two interfaces is to enabled SYSLOG and keep syslog and RADIUS traffic segregated. When two interfaces are used this way, ACS (specifically the CSRADIUS service) does not restart properly if the host machine is rebooted. This appears to be a bug seen in ACS v3. SYSLOG support appeared in ACS 4.1 **Workaround** Restart (stop/start) ACS or restart (stop/start) the CSRADIUS Service.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCsg56677	After upgrade re-authenticate EAP-FAST user with UPN or SAM format fails	**Symptom** When authenticating user with SAM/UPN format (Domain\username or username@domain) on ACS 4.0.1.49 or ACS 4.1, it succeeds at the first time and also after trying to re-authenticate with the same PAC. However, if we try to upgrade ACS 4.0 (i.e. 4.0.1.27, 4.0.1.42/43/44) to build 4.0.1.49 or to ACS 4.1, we will see that the re-authentication (i.e. stateless session resume) will fail with the error - “Access denied: fast-reconnect was successful but user was not found in cache”. This bug has the same behavior as describe in CSCsd82223, but after performing the above upgrade. **Conditions** These conditions will recreate the symptom: 1. First try to authenticate EAP-FASTv1a user with UPN format against ACS on build 4.0.1.27. 2. After a successful authentication, try to re-authenticate the user (without UPN format). 3. In this case the authentication fails with message: “Access denied: fast-reconnect was successful but user was not found in cache”. 4. Install new machine with build 4.0.1.48, and repeat steps one and two. 5. This time the authentication succeed. 6. Try to Upgrade the previous ACS (the one with build 4.0.1.27) to build 4.0.1.48 and repeat step 2 (only reauthentication). 7. The reauthentication will fail with the same message error as describe in step 3. **Workaround Case #1**: Customers using Manual PAC provisioning. Advise a customer to re-provision PACs with correct usernames (i.e. usernames containing domains).

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation

CSCsg56677
(continued)
		Workaround Case #2: Customers using Automatic PAC provisioning.
		Advise a customer to do the next workaround:
		1. Set the next values for the EAP-FAST settings (see EAP-FAST Configuration page):
		`Active master key TTL = 1 hours`
		`Retired master key TTL = 2 hours`
		`Tunnel PAC TTL = 30 minutes`
		`Authorization PAC TTL = 10 minutes`
		Notes:
		• Active master and Retired master key TTLs are changed to force invalidation of PACs issued by ACS 4.0 (i.e. 4.0.1.27, 4.0.1.42/43/44).
		• Tunnel PAC and Authorization PAC TTLs are changed due to limitation that their values must be less then Active master and Retired master key TTLs.
		• IMPORTANT: When customer's environment contains several ACS servers, this change must be applied on ALL ACS servers configured as EAP-FAST master server and then this change should be replicated to corresponding slave ACS Servers. This change will lead to re-provisioning of ALL PACs.
		2. It is safe to change these EAP-FAST settings back a day after this change was applied/replicated to ALL ACS servers in the customer's environment. The default values for them are:
		`Active master key TTL = 1 months`
		`Retired master key TTL = 3 months`
		`Tunnel PAC TTL = 1 weeks`
		`Authorization PAC TTL = 1 hours`

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCsg62239	Binary garbage is sent to syslog - indicative of bad or corrupt pointer.	**Symptom** Binary text output appears in SYSLOG output. **Conditions** Random. **Workaround** There is no workaround.
CSCsg85463	After Active Directory password change by dial-up network (DUN), old and new password are valid	**Symptom** After password change against Active Directory, the old and new passwords are valid for authentication **Conditions** S27 build 23 with RA 1. Create a new user in AD (demands a password change). 2. Authenticate using a DUN (MSCHAPv2) using user login name. 3. The user passed authentication a. No log was entered to 'change password' log b. The user can authenticate both with old and new passwords **Workaround** There is no workaround.
CSCsg85469	After AD password change by DUN auth is failed	**Symptom** The password change passed successfully when using a pre-windows 2000 (user61) but UPN format (user61@dom213.acs.net) failed. No password change was performs in S27. **Conditions** These conditions will recreate the symptom: 1. Create a new user in AD (demands a password change). 2. Authenticate using a DUN using user login name with domain name like: user61@dom213.acs.net. a. The user do not passed authentication b. No password change was done **Workaround** There is no workaround.

Table 5 Known Defects in ACS for Windows and the ACS Solution Engine 4.1 (continued)

Defect ID	Headline	Explanation
CSCsg95223	Upgrade from 4.0.1 to 4.1.1.23 fails to import NAC profiles and rule	**Symptom** Symptom: ACS 4.0.1.27 was upgraded to 4.1.1.23 and none of the NAC features were imported. The network access profiles and posture validation rules missing from the previous version. **Conditions** Upgrading to 4.1.1.23 when NAP and Posture validation are configured **Workaround** There is no workaround.
CSCsh48625	ACS RADIUS error 2162 - switch isn't sent RADIUS Authorization Components (RAC)/DACL client revokes token	**Symptom** The system posture token is empty which means that from the application posture token, ACS is not evaluating system posture token or it is not forwarding it to the switches. Its one thing that the RAC lookup fails and it is different thing that system posture token is not calculated. **Conditions** This can be reproduced by sending 10 clientless with audit sessions a couple times. CSAuth crashes as in defect CSCsg12943. **Workaround** Reboot ACS.

Known Defects in CSA 5.1

Table 6 describes defects found in Cisco Security Agent (CSA) 5.1. For a complete list of the features and defects for CSA, refer to CSA's product release notes available at http://www.cisco.com.

Table 6 Known Defects in Cisco Security Agent 5.1

Bug ID	Headline	Explanation
CSCsh98406	CSAMC v5.1.0.8 is not reporting root kit attributes to ACS	**Symptom** Attempting to perform a physical memory access will not cause the ACS "HIP:CSAStates" to contain the substring of "rootkit_detected". **Conditions** Deploying the rule: "SET DETECTED ROOTKIT UNTRUSTED" when an enforcement action of the type "deny" and <all applications> attempt to "access physical memory" and then attempting to perform a physical memory access will not cause the ACS "HIP:CSAStates" to contain the substring of "rootkit_detected". **Workaround** There is no workaround for CSA 5.1. **Note** This defect has been fixed in CSA 5.2.

Getting Information About Defects Resolved by NAC 2.1

To learn about the resolution of a specific defect, use the Cisco Software Bug Toolkit to find that information.

Step 1 Click on this link to launch the Cisco Software Bug Toolkit: http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl.

Step 2 Enter your CCO password when prompted.

Step 3 Type the number of the defect in the **Enter Known Bug ID** field.

Step 4 Click **Search**.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is s a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html