Release Notes for Network Admission Control, Release 2.0

Revision 2: February 12. 2008

Contents

These release notes pertain to Cisco's Network Admission Control, Release 2.0 network solution. This document contains the following sections:

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

Introduction

Network Admission Control, Release 2.0 (NAC 2.0) is a set of technologies and solutions. It uses the network infrastructure to enforce security policy compliance on devices that try to access network computing resources, thereby limiting damage from security threats.

Customers implementing NAC can allow network access only to compliant and trusted endpoint devices (PCs, servers, and PDAs, for example) and can restrict the access of noncompliant devices.

This document lists which Cisco components are NAC 2.0 compatible and what limitations these components have.

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

Cisco Component Versions That Support NAC

Supported Cisco Switches

These devices support either the NAC L2 IP method which uses Extensible Authentication Protocol over User Data Protocol (EAP over UDP), or the NAC L2 802.1X (EAP over IEEE 802.1X) method. These are NAC Release 2.0 devices.

Table 1 Supported Cisco Switches

Supported Switch Models	Supported Methods	Supervisor, if applicable	Operating System Image
Cisco Catalyst 2940	NAC L2 802.1X	not applicable	Cisco IOS Release 12.1(22)EA6 or later
Cisco Catalyst 2950 Cisco Catalyst 2955	NAC L2 802.1X	not applicable	Cisco IOS Release 12.1(22)EA6 or later
Cisco Catalyst 2960	NAC L2 802.1X	not applicable	Cisco IOS Release 12.2(25)SED or later
Cisco Catalyst 2970	NAC L2 802.1X	not applicable	Cisco IOS Release 12.2(25)SED or later
Cisco Catalyst 3550	NAC L2 IP NAC L2 802.1X	not applicable	Cisco IOS Release 12.2(25)SED or later
Cisco Catalyst 3550	NAC L2 802.1X	not applicable	Cisco IOS Release 12.1(22)EA6 or later

Table 1 Supported Cisco Switches (continued)

Supported Switch Models	Supported Methods	Supervisor, if applicable	Operating System Image
Cisco Catalyst 3560	NAC L2 IP NAC L2 802.1X	not applicable	Cisco IOS Release 12.2(25)SED or later
Cisco Catalyst 3750	NAC L2 IP NAC L2 802.1X	not applicable	Cisco IOS Release 12.2(25)SED or later
Cisco Catalyst 4500	NAC L2 IP NAC L2 802.1X	Sup2+, 2-Plus-TS, Sup2+10GE, IV, V, V-10GE	Cisco IOS 12.2(25)SG or later
Cisco Catalyst 4900	NAC L2 IP NAC L2 802.1X	not applicable	Cisco IOS 12.2(25)SG or later
Cisco 6500 Series Models: 6503, 6503-E, 6506, 6506-E, 6509, 6509-E, 6509-NEB, 6509-NEB-A, 651	NAC L2 IP	Supervisor 32, 720	Cisco IOS 12.2(18)SXF2
Cisco 6500 Series Models: 6503, 6503-E, 6506, 6506-E, 6509, 6509-E, 6509-NEB, 6509-NEB-A, 651	NAC L2 IP NAC L2 802.1X	Supervisor 2, 32, 720	Catalyst OS 8.5 or later

Supported Cisco Routers

These routers support the NAC L3 IP method (EAP over UDP). These are considered NAC Release 1.0 devices.

Table 2 Cisco Supported Routers

Supported Cisco Router Series	Supported Models	Operating System Image
Cisco 800 Series Routers	831, 836, 837, and 870 Series	Cisco IOS 12.3(8)T or later
Cisco 1700 Series Routers	1701, 1711, 1712, 1721, 1751, 1751-V, 1760	Cisco IOS 12.3(8)T or later
Cisco 1800 Series Routers	1841	Cisco IOS 12.3(8)T or later
Cisco 2600 Series Routers	2600XM, 2691	Cisco IOS 12.3(8)T or later
Cisco 2800 Series Routers	2801, 2811, 2821, 2851	Cisco IOS 12.3(8)T or later
Cisco 3600 Series Routers	3640/3640A, 3660-ENT Series	Cisco IOS 12.3(8)T or later
Cisco 3700 Series	3725, 3745	Cisco IOS 12.3(8)T or later
Cisco 3800 Series	3845, 3825	Cisco IOS 12.3(8)T or later
Cisco 7200 Series	All	Cisco IOS 12.3(8)T or later
Cisco 7500 Series	All	Cisco IOS 12.3(8)T or later
Cisco 7600 Series	All	Cisco IOS 12.3(8)T or later

Supported Cisco Wireless Access Points

The Cisco Wireless Access Points support the NAC L2 802.1X method.

Table 3 Supported Cisco Wireless Access Points

Cisco Wireless Access Points	Supported Models	Operating System 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

Table 3 Supported Cisco Wireless Access Points

Cisco Wireless Access Points	Supported Models	Operating System Image
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

The Cisco Wireless LAN Controllers support the NAC L2 802.1X method.

Table 4 Supported Airespace Appliances Devices

Wireless LAN Controllers Models	Cisco Unified Wireless Network Software
Cisco 2000	Release 3.1 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 Services Module (WLSM)	Release 3.1 or later
Wireless LAN Controller Module for Integrated Services Routers	Release 3.1 or later

Supported Cisco Trust Agent Release

Cisco Trust Agent (CTA) 2.0.0.30.

Supported Cisco Secure Access Control Server Release

- Cisco Secure Access Control Server (ACS) 4.0.1.27 for Windows
- Cisco Secure Access Control Server (ACS) Solution Engine
  - Build 4.0.1.42 for Quanta (1112)
  - Build 4.0.1.43 for HP (1111)

Supported Cisco Security Agent Releases

- Cisco Security Agent (CSA) 4.5.1.639
- Cisco Security Agent (CSA) 5.0.0.176 or later.

Supported Cisco VPN Concentrator Release

Table 5 Supported Cisco VPN Concentrator Release

Cisco VPN Concentrator	Supported Models	Operating System version
3000 series	3005 to 3080	Version 4.7 or later

Known Component Problems

This section describes problems known to exist in release Network Admission Control, Release 2.0.

Note A "—" in the Explanation column means that no information was available at the time of publication. You should check the Cisco Software Bug Toolkit for current information. 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 Cisco Switch Problems

Known Catalyst 2000 and 3000 Switch Problems

Unless otherwise stated, these open caveats apply to Catalyst 3750, 3560, 3550, 2970, and 2960 switches running Cisco IOS Release 12.2(25)SED or later, and Catalyst 3550, 2955, 2950, and 2940 switches running Cisco IOS Release 12.1(22)EA6 or later.

These caveats address specific behaviors of the switch that affect a NAC implementation. For a complete list of the features and caveats for a particular switch, see that device's product release notes available at http;//www.cisco.com.

References to a "supplicant" in these caveats refers to any IEEE 802.1X supplicant.

Table 6 Known Problems in Cisco 2000 and 3000 Series Switches

Bug ID	Headline	Explanation
CSCei03545	NAC L2 IP 0.0.0.0 shows up in eou table as a client for 1538M HUB.	**Note** This caveat applies to Catalyst 3750, 3560, and 3550 switches running Cisco IOS Release 12.2(25)SED or later. **Symptom** If NAC L2 IP validation is configured on a port that is attached to a Cisco 1538M Micro Hub, the Extensible Authentication Protocol over User Data Protocol (EAPoUDP) table in the **show eou all** privileged EXEC command output might have an invalid entry with the IP address 0.0.0.0. **Workaround** There is no workaround. This does not affect the switch functionality.

Table 6 Known Problems in Cisco 2000 and 3000 Series Switches (continued)

Bug ID	Headline	Explanation

CSCei05652	HRPC dot1x request handler traceback from unqueue failure.	**Symptom** On Catalyst 3750 switches, NAC L2 802.1X validation repeatedly occurs on many IEEE 802.1X-enabled ports. During validation a message such as this might appear:
		`-Process= "HRPC dot1x request handler", ipl= 0, pid= 89 (l3a3-9)`
		`-Traceback= 9D0118 E97FA4 92024C 438C84 439360 45F150 4E451C 4E46FC79D6A8 7978EC (l3a3-9)`
		`May 26 17:57:03.204: %SYS-2-NOTQ: unqueue didn't find 3DECB98 in queue 1F266A4 (l3a3-3)`
		Workaround There is no workaround. This problem does not affect the switch functionality.

CSCei08901	NAC L2 IP:stack master reloaded under stress.	**Note** This caveat applies to Catalyst 3750, 3560, and 3550 switches running Cisco IOS Release 12.2(25)SED or later.
		Symptom If the Extensible Authentication Protocol over User Datagram Protocol (EoU) table has many host entries and you enter the **clear eou all** privileged EXEC command, messages such as this might appear:
		`4d01h: %SM-4-BADEVENT: Event 'eouHold' is invalid for the current state 'eou_abort': eou_auth 8.0.7.170`
		`-Traceback= 6DB0E4 158F74 419B4 41D58 448B4 44AF0 3F27C0 3ECA14 This may be followed by a software-forced reload of the switch.`
		After the message appears, the switch might unconditionally force a system reload.
		Workaround The workaround is to use the **clear eou ip** privileged EXEC command to remove specific IP hosts from the EoU table.

Table 6 Known Problems in Cisco 2000 and 3000 Series Switches (continued)

Bug ID	Headline	Explanation
CSCei31359	SU05:DAI w/IP address validation discards NAC:NAC L2 IP ARP probes.	**Note** This caveat applies to Catalyst 3750, 3560, and 3550 switches running Cisco IOS Release 12.2(25)SED or later. **Symptom** If dynamic Address Resolution Protocol (ARP) inspection is enabled on the access VLAN for the NAC host and the IP address validation option is configured, the Extensible Authentication Protocol over User Data Protocol (EoU) session for NAC ends 2 minutes after validation occurs. **Workaround** Use one of these workarounds: • Disable the IP address validation option. • Use an ARP access control list (ACL) to allow the IP address 0.0.0.0 but to block the IP address 255.255.255.255. The ARP ACL must include this access control entry: **permit response ip any host 0.0.0.0 mac any any**
CSCei49149	Trace/TCAM msg after cl eou all(48x8 hosts from EST).	**Note** This caveat applies to Catalyst 3750, 3560, and 3550 switches running Cisco IOS Release 12.2(25)SED or later. **Symptom** After the posture of a large number of hosts have been validated, if you clear the EAPoUDP table by using the **clear eou all** privileged EXEC command, this message about the system running low on TCAM resources might appear: `%QATM-4-TCAM_LOW: TCAM resource running low for table Input ACL, resource type TCAM masks, on TCAM number 1.` **Workaround** There is no workaround.

Table 6 Known Problems in Cisco 2000 and 3000 Series Switches (continued)

Bug ID	Headline	Explanation
CSCei77557	NAC L2 IP:EoU Process trace/bogus ACS msg after cl eou all as 75 NRH.	**Symptom** If 75 nonresponsive clients are connected to Catalyst 3750 or 3560 switch and you enter the **clear eou all** privileged EXEC command, a traceback appears. **Workaround** There is no workaround. You can ignore the traceback.
CSCsb76707	Port still part of VLAN even after unconfiguring auth-fail VLAN.	**Note** This caveat applies to Catalyst 3750, 3560, 3550, 2970, and 2960 switches running Cisco IOS Release 12.2(25)SED or later. **Symptom** If an IEEE 802.1X-enabled port is authorized in the restricted VLAN, the port might remain in that VLAN even after you enter the **no dot1x auth-fail vlan** interface configuration command to disable the restricted VLAN on the port. **Workaround** The workaround is to shut down the IEEE 802.1X-enabled port by entering the **shutdown** interface configuration command before you remove the restricted VLAN configuration.
CSCsb79198	dot1x:port fail to authenticate if download acl >= 20	**Symptom** An IEEE 802.1X supplicant might fail to complete authentication if the per-user ACL is too large. During IEEE 802.1X authentication, the RADIUS server might download a per-user IP or MAC ACL to be applied to an interface as part of the Access-Accept message. If the ACL is too large, the switch might not be able to apply it, and the authentication fails and restarts. Depending upon the specific access control entries (ACEs) in the ACL, the maximum ACL size is about 20 ACEs in a Catalyst 3750 switch. **Workaround** The workaround is to reduce the size of the per-user ACLs that are downloaded as part of IEEE 802.1X authentication.

Table 6 Known Problems in Cisco 2000 and 3000 Series Switches (continued)

Bug ID	Headline	Explanation
CSCsb99249	IEEE 802.1X configured port failed to ping after host mode change.	**Symptom** On an IEEE 802.1X-enabled port that has the IEEE 802.1X control direction set to **in** (unidirectional port control), if you use the **dot1x port-control** interface configuration command to change the port mode configuration or the **dot1x host-mode** interface configuration command to change the host configuration, the host attached to the port might get authenticated but might not be able to access the network. **Workaround** The workaround is that on an IEEE 802.1X-enabled port, before you change the port mode or the host mode configuration, you should shut down the port (by using the **shutdown** interface configuration command), use the **no dot1x control-direction in,** or the **dot1x control-direction both** interface configuration commands to change the port control to bidirectional.
CSCsc16152	Client with dot1x cannot get DHCP address.	**Symptom** When a client is connected to a Catalyst 3750 member switch through an interface that is configured for IEEE 802.1X and DHCP snooping, if the client uses one MAC address for IEEE 802.1X authentication and a different MAC address for the DHCP request, the client does not receive an IP address from the DHCP server. This problem does not occur when the client is connected to a Catalyst 3750 master switch or when the client uses the same MAC address for IEEE 802.1X and DHCP requests. **Workaround** The workaround is to connect the client to the master switch in the Catalyst 3750 switches switch stack, or to disable DHCP snooping.

Table 6 Known Problems in Cisco 2000 and 3000 Series Switches (continued)

Bug ID	Headline	Explanation

CSCsc26248	SYS-2-BADSHARE: Bad refcount in mem_lock during disabling ports.	**Symptom** If a Catalyst 3750 switch configured as the master switch in a stack has a large number of IEEE 802.1X-enabled ports, a series of rapid link changes on the switch (for example, when you remove cables from these ports) might cause this message to appear and the switch to reload:
		`Oct 21 12:31:07.446: -Traceback= F8E218 2F376C 2EA71C 2EB674 18C48C 2EAD94 2E9D88 86B7E8 865A2C`
		`Oct 21 12:31:07.446: %SYS-2-BADSHARE: Bad refcount in mem_lock, ptr=38AAC10, count=0`
		Workaround There is no workaround available.

Known Catalyst 6500 Series Switch Problems

These limitations are found on Catalyst 6500 series switches running the CatOS 8.5 JAC operating system.

These caveats address specific behaviors of the switch that affect a NAC implementation. For a complete list of the features and caveats for a particular switch, see that device's product release notes at http://www.cisco.com.

Table 7 Known Problems in Catalyst 6500 Series Switches

Bug ID	Headline	Explanation
CSCei90699	ACL mgr stuck in 99% while posture validating 110 hosts.	**Symptom** With NAC L2 IP, when a host's posture is being validated, you will see high CPU utilization by the ACL manager process. This is a transient condition and is expected. **Workaround** There is no workaround.
CSCei15212	Posture validation not happening on PCs having multiple NIC	**Symptom** With NAC L2 IP, if a PC connected to the switch has more than one NIC, only one of the NICs is posture validated. **Workaround** There is no workaround.

Known Cisco Secure Access Control Server

There are NAC 2.0 features in both the Cisco Secure Access Control Server for Windows and the Cisco Secure Access Control Server Solution Engine.

Table 8 contains problems known to exist only in Cisco Secure Access Control Server Solution Engine. Table 9 contains problems known to exist in both the Cisco Secure Access Control Server Solution Engine and the Cisco Secure Access Control Server for Windows. Both versions of Cisco Secure Access Control Server are referred to as ACS.

These caveats address specific behaviors of ACS that affect a NAC implementation. For a complete list of the features as well as caveats for ACS, refer to ACS's product release notes available at http://www.cisco.com.

Table 8 Known Problems in ACS Solution Engine (ACS SE) 4.0.1

Bug ID	Summary	Explanation
CSCsd20149	After initial config from Recovery CD, no GUI access.	**Symptom** This problem occurs on ACS SE 1111 (HP), when performing a full upgrade including appliance base image. After installing from the ACS SE 1111 (HP) Recovery CD, and initial configuration completes, you cannot access the web interface. When you log in to CLI, the appliance status indicates that `pfipmon not running`. **Conditions** On ACS SE 1111 (HP), after installing from the Recovery CD, when performing a full upgrade, including the appliance base image. **Note** If you are not upgrading the appliance base image, you do not need to install from the Recovery CD. **Workaround** Use the CLI command, **`reboot`**, to restart the appliance.

Table 8 Known Problems in ACS Solution Engine (ACS SE) 4.0.1 (continued)

Bug ID	Summary	Explanation
CSCsc90467	After Install from Recovery CD, no CLI access.	**Symptom** This problem occurs on ACS SE 1111 (HP), when performing a full upgrade including appliance base image. When installing from the ACS SE 1111 (HP) Recovery CD, after installation completes, the ACS SE reboots, performs some configurations, and reboots again. The configurations that occur after the first reboot take a significant amount of time, during which there is no feedback, which is normal system behavior. After this time, the CLI Initial Configuration screen should appear, but does not. **Conditions** On ACS SE 1111 (HP), when installing from the Recovery CD, when performing a full upgrade, including the appliance base image. **Note** If you are not upgrading the appliance base image, you do not need to install from the Recovery CD. **Workaround** Switch off the appliance, and switch it on again.
CSCsc81981	CSAdmin crashed when edit the RA field after replication	**Symptom** After replication, if you edit the Remote Agent field in the Network Configuration page in the slave machine, the ACS displays the error message “Action canceled.” **Workaround** None.
CSCsc80481	Proxy distribution table prevents SNMP from working.	**Symptom** If you configure ACS SE for SNMP and enable “Accept SNMP packets from selected hosts”, and then add an entry to Proxy Distribution Table like: @cisco.com -> local ACS -> strip -> local (Default) -> local ACS -> no strip -> local, SNMP stops working and there are no more responses from ACS. **Workaround** Uncheck “Accept SNMP packets from selected hosts.”

Table 8 Known Problems in ACS Solution Engine (ACS SE) 4.0.1 (continued)

Bug ID	Summary	Explanation
CSCsc77508	Stress with EAP-TLS crashes CSAuth	**Symptom** During overnight EAP-TLS stress against CSDB with NAP and RAC, and CRL (30% of all certificates are revoked), CSAuth crashed a number of times. **Workaround** None.
CSCsc77228	RSA Token is displayed in the external User DB after Upgrade from 3.2.3	**Symptom** If, in a previous version of ACS, you added RSA SecurID Token Server to the External User Database, mapped it to a group, and selected this Database in the "Unknown User Policy", then, after upgrading to ACS 4.0, the RSA SecurID Token Server is still displayed, even though it should be deleted from everywhere inside the External User Database and not just from the Database Configuration. Moreover, the Configuration in the RSA SecurID Token Server should be placed in the RADIUS Token Server after the upgrade to 4.0. **Workaround** None.
CSCsc69997	Machine authentication failed on 2003 DC with binary comparison on	**Symptom** EAP-TLS machine authentication failed if only binary comparison selected, and 2003 DC is used as the external database. There are no problems with user authentication. **Workaround** None.
CSCsc63854	ODBC Mapping exists after restoring image created on software	**Symptom** After restoring the appliance image from the software version of ACS 4.0.1, there is still ODBC configuration in Unknown User Policy and in NAP/Authentication. **Workaround** None.

Table 8 Known Problems in ACS Solution Engine (ACS SE) 4.0.1 (continued)

Bug ID	Summary	Explanation
CSCsc52381	ACS SE: console access may not work if NTP synchronization is enabled	**Symptom** The login prompt might not appear on the CLI console after rebooting through the CLI or through the GUI; even if NTP synchronization is enabled and the NTP server address is set correctly. **Workaround** Disable NTP synchronization.
CSCsc03778	ACS SE replicated changes under Admin Control not enforced unless reboot	**Symptom** If you make a change in the Access Policy under Administration Control and then replicate the change to another appliance, the changes are not enforced on the receiving appliance. **Workaround** On the receiving (secondary) appliance, do one of the following: • Click Submit on the Access Policy page. • Reboot the secondary appliance.
CSCsc02553	GUI logging change does not affect csadmin until server restarted	**Symptom** When you change the logging level for an ACS Appliance via the GUI, you click the button to restart; however, the csadmin service is not restarted, thus the csadmin logging level will not change until the csadmin service is manually restarted. **Workaround** Restart the csadmin service manually.
CSCsb83399	ACS SE should save the FTP settings during software upgrade	**Symptom** ACS appliance does not save the defined FTP settings during software upgrade, but the defined backup scheduling is saved. This behavior will cause the backup problem after software upgrade. **Workaround** Reenter the FTP information manually after an upgrade.

Table 8 Known Problems in ACS Solution Engine (ACS SE) 4.0.1 (continued)

Bug ID	Summary	Explanation
CSCsb27597	Limitation on the custom attributes (of 31k as CSAdmin indicates)	**Symptom** In the T+ Settings per User/group Configuration page, which is accessed from the Interface Configuration page, if you add 1201st entry in the custom attribute field, the browser crashes. The custom attribute field is currently limited to 31KB (which is around 1200 attributes). **Workaround** None.
CSCsb19051	TCP checksum error from Cisco Secure ACS Solution Engine 1111	**Symptom** A Cisco Secure Access Control Server Solution Engine (ACS SE) 1111 (CSACSE-1111-UP-K9) may generate transient TCP Checksum errors which may cause error logging on other devices in the network. In particular, Cisco switches would generate the following error message: `%IP-3-TCP_BADCKSUM:TCP bad checksum.` The cause of the error is the NIC Software Driver. Not every packet being transmitted will be affected. Given that TCP will retransmit any unacknowledged packet, the system will recover. Excessive logging of the error message within the network might occur. The problem only affects TCP packets; therefore, TACACS may be affected, while RADIUS will not. This problem might also occur on an ACS SE 1112 (Quanta). **Workaround** A temporary workaround is to reload the server; but, because the problem is transient, it will likely return within days or weeks. A patch is available from TAC, which will help to reduce the amount of errors; however, since this is a network configuration problem, it cannot resolve the problem completely. Contact your TAC representative for the appropriate *TCP_checksum* patch for your platform.

Table 8 Known Problems in ACS Solution Engine (ACS SE) 4.0.1 (continued)

Bug ID	Summary	Explanation
CSCsb13998	ACS dialin authorization fails against Win2K active directory	**Symptom** When ACS is configured to obtain dialin authorization from a Microsoft Active Directory user database, the user sometimes fails with the error: "User does not have dialin permission (needed)." This defect was found in an environment where Active Directory was being replicated from an NT domain. The same errors occurred when the remote agent was installed on a Member Server or a Domain Controller. **Workaround** The problem is caused because replication does not set synchronize the userParameters and msNPAllowDialin. See MS KB article 252398 for possible workaround (run a script to synchronize the attributes).
CSCeh17104	ACS Appliance: Certain Hostname/Admin name cause losing access	**Symptom** If the administrator name is same as the hostname, there is no GUI access or CLI access. **Workaround** Ensure that the administrator name is different from the hostname.
CSCeh04327	SNMP get and get-next requests for host.hrSystemNumUsers return error	**Symptom** SNMP 'get' and 'get-next' requests for host.hrSystemNumUsers return 'Generic error'. **Workaround** None.
CSCee89510	Dates are logged in local time instead of GMT	**Symptom** NAC attributes that are in date format are in GMT time zone. When ACS logs these attributes, it converts them to ACS local time zone (the time zone of the ACS server). **Workaround** Configure ACS to use the GMT time zone.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01

Bug ID	Headline	Explanation
CSCea91690	Event Viewer errors on startup/shutdown in .NET.	**Symptom** On Windows .Net Server 2003 or Windows 2003 Enterprise Edition shutdown and startup, you might see errors that falsely indicate that ACS service have failed. At startup, you might see a dialog box that indicates that a service, such as CSLog, encountered a problem and will close. The same error is logged to Event Viewer, as in this example: `Reporting queued error: faulting application CSLog.exe, version 0.0.0.0, faulting module unknown, version 0.0.0.0, fault address 0x00000000.` In Windows Server 2003, the Service Manager queries the ACS services status during startup and shutdown, but ACS services might not have started yet or might have already stopped. Even though this is normal behavior for ACS services, Windows perceives this as an error and logs it to the Event Viewer. On startup, the user sees all errors from the event viewer. Therefore, when users log into Windows right after startup, they see errors from the previous login session. **Conditions** This behavior is observed on Windows Server 2003 only. **Workaround** *V*erify that ACS services are running by using the Control Panel.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCeb78551	When doing LEAP RADIUS proxy between a front-end ACS server and a back end ACS server, problems arise if the configuration is not correct.	**Symptom** The LEAP Server (back end ACS Server) must contain an AAA Client entry of the LEAP Proxy Server (front end ACS Server), and it must be set to use **RADIUS (Cisco IOS/PIX)**. The LEAP Server (the back end ACS Server) also must be set to use `RADIUS (Microsoft) [026/311/012] MS-CHAP-MPPE-Keys` attribute in **Interface Configuration** and in Group or User Settings (depending on the profile used). This setting is required to communicate MS MPPE keys, which LEAP usess, between the Proxy LEAP Server (front end ACS Server) and the Proxy Server (back end ACS Server). This sort of communication is encapsulated in Cisco VSA and this is the reason why the AAA Client must be **RADIUS (Cisco IOS/PIX)**. **Workaround** There is no workaround.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation

CSCec72911	Windows 2003 password aging page display issue.	**Symptom** ACS is installed on Windows 2003 Server, and the password aging feature is enabled. Only the option **generate greetings for successful logins** option in Password Aging settings is checked. After pressing **Submit** or **Submit + Restart**, for the first time ACS displays this valid error message:
		`Error: Generation of greetings on successful logins requires at least one password aging rule to be configured.`
		However on the second pressing of one of these buttons, one of these errors appears:
		`Active canceled`
		`The page cannot be displayed`
		Conditions Occurs after installation and as long as no changes are made. Occurs only when managing ACS only on the local machine by using IE 6.0.
		Workaround Restart ACS.

CSCee64596	During stress tests, ACS does not reduce the size of the CsAdmin file based on the Service Control settings.	**Symptom** Intensive use of the Logged-In Users report might lead to significant memory utilization by the CSAdmin service. **Workaround** Restart the CSAdmin service.
CSCef12461	Restoring many administrators on Windows 2000 does not restore them.	**Symptom** On Windows 2000, if you attempt to restore a database of over 500 administrators, the ACS administrators are not restored. **Workaround** Manually recreate administrators after the restoration.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCef12605	Replication with many administrators does not replicate them.	**Symptom** When ACS attempts to replicate with 500 or more administrators, administrators are not replicated even though ACS reports a successful replication. **Workaround** There is no workaround.
CSCef55730	ACS authorization passes even for a disabled user.	**Symptom** The default administrative user account defined within the CiscoWorks local (user) database (and replicated within the Cisco Secure ACS TACACS+ user database) is granted access to all installed Management Center applications, even if the user account is disabled within ACS. **Workaround** There is no workaround.
CSCef85310	Group dACL is downloaded if Users dACL content is empty.	It is possible to define an ACL with empty content. Following this defect, if a user with an empty ACL belongs to a group on which a non empty ACL is defined, then authenticates, the ACL of the group is downloaded to the device, instead of the user's. (Although the user's dACL content is not empty, it is downloaded to the device, as it should be.) **Workaround** Do not define an empty downloadable ACL.
CSCef85314	Group dACL is downloaded if Users content NAF is not suitable.	**Symptom** If a user attempts authentication to the device, which is not part of the NAF specified on the user's dACL content, the ACL of the group to which the user belongs is downloaded to the device, instead of being rejected. **Workaround** There is no workaround.
CSCef96208	ACS reports incorrect privilege level	**Symptom** ACS might report users with the incorrect authorized privilege level. In particular, when using TACACS+, users who are correctly authenticated with a privilege level of 15 are reported with a level of 1. **Workaround** None; the error is cosmetic.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCeg40355	Authentication failures when remote logging fails.	**Symptom** If an ACS server configured for remote logging does not successfully transmit an accounting log to the remote server, authentication attempts to this ACS server during this time might fail. The authentication failure might not be reported at all, or it might be reported incorrectly (as being successful). The *auth.log* file might have output similar to this during an authentication failure: `AUTH 10/13/2005 10:29:55 E 0552 19568 Timeout waiting for ack from CSlog [logger name] AUTH 10/13/2005 10:29:55 E 0559 19568 Closing CSlog connection to [logger name] AUTH 10/13/2005 10:29:55 E 0574 19568 Re-sending packet to CSLog [logger name] AUTH 10/13/2005 10:29:55 E 0546 19568 -ve ack from CSLog [logger name] AUTH 10/13/2005 10:29:55 E 0499 19568 Failed to log accounting packet to logger [logger name]` **Workaround** Disable the remote logging functionality, or correct the cause of the logging failure.
CSCeg47441	CRL not preserved when upgrading from 3.3.2 or below to 3.3.3 or later.	**Symptom** When upgrading from ACS version 3.3.1.16 to 3.3.2.2, the CRL entries are not transferred. **Workaround** Create CRL entries manually.
CSCeg50237	Overinstall causes the added AVP Attributes to disappear.	**Symptom** Adding AVP attributes and then performing Overinstall causes those attributes to disappear from the Log Attribute field. **Workaround** Add AVP attribute manually after overinstall.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCeh00074	GUI/ LDAP group mapping submission failure.	**Symptom** When adding LDAP groups to be mapped to ACS groups, the Submit operation sometimes fails and an empty list error message appears. This might occur when working on the ACS UI from a remote machine (for example, with Terminal Services), and it might appear in other group mapping pages as well. **Workaround** In the Group Mapping page, before you click **Submit**, move to another window, or click another frame in the ACS HTML interface.
CSCeh10491	Authentication errors on timeout waiting for local logging.	**Symptom** Authentication takes a lot of time when ACS is configured to log on remote ACS or to ODBC and the remote server or ODBC data source is unreachable. When all worker threads are used, ACS provides no more authentications. **Conditions** The remote ACS or ODBC data source is unreachable. **Workaround** Make the remote server or ODBC data source available for logging, or disable logging to it in ACS configuration
CSCeh24979	Users fail to authenticate when upgrading and attempting to access an obsolete database.	**Symptom** When upgrading from version ACS 3.1 or later to version 4.0 (these are 2 step upgrades) if a user is trying to authenticate to a database which was in use before the upgrade but not in use after the upgrade, the user will fail to authenticate. This information will be reported in the Failed Attempts log. **Workaround** Select User Setup and then select Remove Dynamic Users after upgrading.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCeh35121	Local logging stopped working after ODBC logging removed.	**Symptom** ODBC logging is enabled for passed and failed attempts. The ODBC data source is incorrect. After removing ODBC logging, only local logging remains, but no local logging is written. **Conditions** ODBC data source must be incorrect. **Workaround** Specify the correct ODBC data source for logging, and restart ACS.
CSCeh37907	Duplicate IP assignment due to accounting packets reordering.	**Symptom** Address assignment from IP pools is based on AccountingStart/Stop records. A duplicate IP address might be assigned to a user if an Accounting Stop packet is received out of order following a new access request by the same user. If ACS receives a late Stop packet, it might erroneously mark an IP address as free even though it has just been assigned. That might lead to a duplicate address assignment during the next connection. Such situations can happen in DSL environments where a router starts new PPP connections in less than 1 second after a previous disconnection. **Workaround** There is no workaround.
CSCeh52700	AD expired-user passed EAP-TLS authentication; should be rejected.	**Symptom** EAP-TLS authentication still passes for users in the Active Directory even if their accounts have expired. No error is given from ACS. **Conditions** EAP-TLS authentication of users in Active Directory running in Windows 2000 environment. **Workaround** There is no workaround. Windows 2003 has introduced some new attributes that should help resolve this issue in future.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCeh60564	AD locked-out User passed EAP-TLS authentication, should be rejected.	**Symptom** EAP-TLS authentication will still pass for users in Active Directory even if their account is locked out. There is no error indication from ACS. **Conditions** EAP-TLS authentication of users in Active Directory running in Windows 2000 environment. **Workaround** There is no workaround. Windows 2003 has introduced some new attributes that should help resolve this issue in future.
CSCeh64162	Supplicant attempts to authenticate using UPN format and failure.	**Symptom** If a supplicant attempts to authenticate by using EAP-FAST and supplies the username in UPN format (`user@domain.com`) and the username before the at sign (@) is different from the pre-Windows 2000 name, ACS might not be able to locate the user in Active Directory. **Conditions** ACS installed in Windows 2000/2003 Active Directory environment. Authentication with EAP-FAST and UPN usernames. **Workaround** Rename the user to have the same username as the pre-Windows 2000 one.
CSCeh68821	LDAP authentication pass after modify subtree node due to DN caching.	**Symptom** If you change the User Directory Subtree in the Common LDAP Configuration, users that are already authenticated using this Generic LDAP instance (External User Database) are not affected and continue to pass authentication, even if the users are no longer under the new User Directory Subtree. ACS does not perform a new search for the users because of the user-cached Distinguished Name. **Workaround** If you want to enforce a new search on the User Directory Subtree, delete the users from the Cisco Secure internal database.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCeh79954	EAP-TLS time of day restriction in AD does not fail user - authentication succeeds.	**Symptom** EAP-TLS authentication of users in Windows Active Directory still passes when a user's time-of-day setting (located in AD) is outside the hours they are allowed. No error is given from ACS. **Conditions** EAP-TLS authentication of users in Active Directory running in Windows 2000 or 2003 environment. **Workaround** There is no workaround.
CSCsa79327	Authentications fail for users with the euro symbol in their passwords.	**Symptom** Authentication fails for users with the euro symbol in their password. **Workaround** Change user password, and remove euro symbol.
CSCsb13998	ACS dial-in authorization fails against Windows 2000 active directory.	**Symptom** When ACS is configured to obtain dial-in authorization from a Microsoft Active Directory user database, the user sometimes fails. The message appears: `User does not have dial-in permission (needed).` **Conditions** This defect was found in an environment where Active Directory was being replicated from an NT domain. The same errors occurred when the remote agent was installed on either a Member Server or a Domain Controller. **Workaround** The problem is caused because replication does not set synchronize the `userParameters` and `msNPAllowDialin` attributes in Active Directory. See MS KB article 252398 for possible workaround. Run a script to synchronize the attributes.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCsb15116	Apply and Restart button in NAP page does not release the NAF policy.	**Symptom** When deleting a Network Access Filter that is used in a Network Access Profile setup page, an unexpected behavior occurs, and authentications fail. **Workaround** Perform one of the following: 1. Before deleting a Network Access Filter, remove it from the relevant Network Access Profiles. or 2. After deleting a Network Access Filter for each relevant Network Access Profile, click **Submit** (without performing changes) in the profile setup page.
CSCsb25151	When AAA client has multiple IP addresses, NAF for DACLs fails.	**Symptom** When a single AAA client is configured with a range or list of IP addresses in ACS solution engine, the Network Access Filter (NAF) under "Shared Profile Components" cannot correctly determine the IP address of either the Network Device Group (NDG) or the correct IP address of the AAA client. **Conditions** Must have Network Access Filtering defined and must have multiple IP addresses listed under the AAA client configuration section (under Network Setup) for the AAA client that is supposed to receive the downloadable ACL. **Workaround** Perform one of the following: • Remove all but the correct IP address from the AAA client configuration component for the NAS/NAD. or • Configure the `ip radius source interface` to point to the correct IP address.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCsb48683	Log and accounting file locking causes problems with backup software.	**Symptom** ACS diagnostic and accounting log file locking results in service problems, when the directories are backed up by certain software applications (in a reported case, Veritas software was used). **Workaround** Upgrade your backup software.
CSCsb72286	ACS RADIUS proxy uses RADIUS 1645, not current 1812.	**Symptom** Cisco Secure ACS for Windows uses port 1645 for RADIUS authentication and authorization proxy to another RADIUS server. Some AAA servers might only accept connections to port 1812. **Workaround** There is no workaround.
CSCsb93223	An internal posture validation policy is created even though a template profile cannot be configured.	**Symptom** If for any reason you cannot create a profile (for example, Global Authentication Setup is not configured properly) using the NAC 802.1X template, an internal posture validation policy is created in any case. **Workaround** There is no workaround.
CSCsb95897	ACS cannot display long list of Disabled accounts correctly.	**Symptom** ACS 3.3 HTML interface has problems in displaying Disabled accounts list if it contains several pages. **Next** is working as needed, but **Previous** is available only once. **Workaround** There is no workaround.
CSCsc00788	Password change is not supported in GTC against Windows DB.	**Symptom** Password change is not supported in EAP-GTC against the Windows database. **Conditions** EAP-GTC authentication of a user in the Windows database whose account has expired or needs to be changed. **Workaround** There is no workaround.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCsc06942	Failure when EAP-FAST/PEAP credentials or posture data size is greater than 1Kb.	**Symptom** Failure when EAP-FAST/PEAP credentials or posture data size is greater than 1Kb. **Conditions** This applies only to tunneled protocols that use fragmentation (MS-PEAP, CISCO-PEAP, and EAP-FAST). It happens only when the supplicant uses the tunneled protocol fragmentation option and only if a fragment of an EAP tunnel is larger than 1002 bytes. usually fragmentation threshold is driven from the detected MTU size (Ethernet is 1.5K). **Workaround** Set the supplicant size of the fragmentation threshold to be lower than 1002 bytes. If it cannot be configured, another option is to set the MTU size that affects this value.
CSCsc27158	Memory leak during LDAP stress–PAP authentication with legacy LDAP SSL connections.	**Symptom** A memory leak was found during stress tests of PAP authentications with LDAP server (OpenLDAP) and legacy SSL enabled (cert7.db file). For example, memory usage reached 100MB after about 1.5 million authentications. Memory is freed after ACS services are restarted. No memory leak is found when the configuration is changed to use the new SSL mechanism (select Trusted Root CA). **Workaround** In the Generic LDAP configuration in ACS, use the new SSL option (Trusted Root CA) instead of the old option (*cert7.db* file).
CSCsc27168	User authentication succeeds even though the database was not selected.	**Symptom** If the external database list in the Network Access Profile (NAP) authentication settings is empty, access requests that match the NAP authenticated in the ACS internal database. **Workaround** Before deleting external database configuration be sure that it is not used in any NAP.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCsc32154	Upgrade from 3.3 removed APT,SPT, and Reason from Logged Attributes.	**Symptom** If one or more of the APT, SPT and Reason attributes were selected to be logged in the Failed or Passed reports in ACS 3.3, after upgrading to 4.0, they do not appear in the Logged Attributes column. **Workaround** Add those APT, SPT, and Reason attributes manually to the 'Logged Attributes' column after upgrade to ACS 4.0.
CSCsc37464	Updates to external database causes dynamic users to be removed.	**Symptom** Any updates to the external database cause the dynamic users linked to that database to be removed from the user's list. **Workaround** There is no workaround. This is a usability bug.
CSCsc39979	An update to NAP deletes the external user in "Logged all users" report.	**Symptom** When a NAP is being updated, all dynamic users related to this NAP are deleted from the logged-in user list. The internally defined users are not deleted. **Workaround** There is no workaround.
CSCsc40001	Session resume in EAP-FAST-TLS does not work.	**Symptom** EAP-TLS inside EAP-FAST always assumes that the user is trying to authenticate for the first time, resulting in going to the external DB (if valid) to get the user credentials instead of permitting the user to resume a previously used TLS session. **Conditions** EAP-TLS as the inner method in EAP-FAST. **Workaround** There is no workaround.
CSCsc41129	CSAuth exceptions during EAP-TLS stress vs LDAP external db with SSL connections.	**Symptom** After a heavy load for a few hours of EAP-TLS authentications with an LDAP external database and LDAP connections over SSL (Trusted Root CA option), **CSAuth** might experience exceptions and fail. **Workaround** Restart ACS services.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCsc41623	Configuring Logs - Reset Columns erroneously populates selection lists.	**Symptom** For several report types, **Reset Columns** on the ACS HTML interface Logging configuration page sets the selected attributes to log (columns) to a different set of **Logged Attributes** than the actual default attributes initially set on a fresh ACS installation. **Conditions** In ACS, when you configure the logged information through the ACS HTML interface by clicking **System Configuration > Logging** and choosing one of the listed reports, the Reset Columns sets the selected attributes in the **Selected Attributes** list box to an incorrect set of attributes. This occurs on the following reports: • CSV Failed Attempts • CSV Passed Authentications • CSV VoIP Accounting **Workaround** Manually select and deselect attributes in the **Logged Attributes** list from the provided Attributes list. • CSV Failed Attempts–Remove the **Filter Information** • CSV Passed Authentications–Add the **cisco-av-pair** attribute. • CSV VoIP Accounting: – Add the **Call Leg Setup Time** attribute. – Add the **Gateway Identifier** attribute. – Add the **Connection Id** attribute. – Add the **Call Leg Direction** attribute. – Add the **Call Leg Type** attribute. – Add the **Call Leg Connect Time** attribute. – Add the **Call Leg Disconnected Time** attribute. – Add the **Call Leg Disconnected Cause** attribute. – Add the **Remote Gateway IP Address** attribute.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCsc41638	ACS does not check if the CA certificate that was issued to a user exists in CTL.	**Symptom** A user that presents a certificate in EAP-TLS or EAP-FAST/EAP-TLS might be authenticated even though the certificate issuer is no longer trusted by the ACS machine. **Workaround** Uncheck the CA certificate in question from the ACS HTML interface before removing the CA certificate from the machine storage.
CSCsc41673	CSAuth fails after importing Airespace NAS.	**Symptom** The **CSAuth** service occasionally fails after being restarted if **CSUtil** was running immediately beforehand, for example when running **csutil -i**. **Conditions** Starting **CSAuth** immediately after **CSUtil** has run an import causes an exception in **CSAuth** due to a race condition in **CSAuth's** internal initialization sequence. This is particularly noticeable if you are using **CSUtil** to stop **CSAuth**, perform some action, and then automatically restart **CSAuth**. **Workaround** Restart **CSAuth** manually from the Control Panel or wait for **CSMon** to detect the scenario and automatically restart **CSAuth**.
CSCsc41860	CSAuth failed when CSUtil deletes 35K NASs.	**Symptom** After a large number of AAA clients were imported to an ACS server, **CSUtil** import was used to delete 35,000 of them. After deleting the AAA clients, **CSAuth** failed. **Conditions** This defect can occur on a clean installation. **Workaround** When deleting a large number of AAA clients using CSUtil it is recommended to delete them in batches of up to 10,000 AAA clients concurrently.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCsc43287	Replication: **Admin Control > Access Policy** > port allocation not replicated.	**Symptom** After replication of Interface security settings, the HTTP port allocation settings in **Admin Control > Access Policy** are not replicated (remained default–allow any). **Workaround** Ensure that the http access policy is set correctly on the slave GUI.
CSCsc43577	CSAdmin stalls and has a memory leak.	**Symptom** CSAdmin consumes memory when updating EAP-FAST inner method GTC to MSCHAPv2, using the Network Access Profile page. **Workaround** Restart the CSAdmin Service.
CSCsc49673	UPGRADE:Add Filter aaa:service=ip_admission to Upgrade-Profile NAP.	**Symptom** After an upgrade from ACS 3.3 that includes the NAC database, a profile is created with an authorization method: PEAP–posture only. This profile does not have a filter, which causes failure of all incoming authentications except from PEAP-POSTURE. **Workaround** Add a filter of Cisco av pair `aaa:service = ip-admission` to the Upgrade-Profile. The non-posture requests are authenticated against the global settings configuration (if you ensure the **Grant access using global configuration, when no profile matches** option is selected in the created profile).
CSCsc57975	The database order inside a Network Access Profile may cause authentication to fail and provide an erroneous error.	**Symptom** When a user account in theWindows AD has expired, the user may be authenticated in another external database, which is configured sequentially after theWindows database in the authentication settings in the matched NAP. If the user exists in another database, authentication is successful. If the user does not exist in another database, an erroneous failure code "CS user unknown" (instead of "Database account expired) is displayed.

Table 9 Known Problems in both ACS 4.0.1 for Windows and ACS SE 4.01 (continued)

Bug ID	Headline	Explanation
CSCsc69976	Local logging file size and days are not displayed correctly after performing an additional action in the graphic user interface.	**Symptom** While changes are applied and in use correctly, default values are displayed after selecting Submit instead of new values. **Workaround** There is no workaround.

Known Cisco Trust Agent Problems

Table 10 contains problems known to exist in CTA 2.0.0.30. These caveats address specifid behaviors of CTA that affect a NAC implementation. For a complete list of the features as well as caveats for CTA, refer to CTA's product release notes available at http://www.cisco.com.

Table 10 Known Problems of Cisco Trust Agent V.2.0

Bug ID	Headline	Explanation
CSCef09817	Install does not complete if port conflict arises.	**Symptom** If there is a port conflict with CTA on Windows NT 4.0, during the CTA installation, the Cisco Trust Agent EOU Daemon service does not start, and the user is forced to cancel the installation. However, on Windows XP and Windows 2000 you will be able to finish the installation and see the port conflict error in the CTA log. **Conditions** Occurs on Windows NT. **Workaround** The port which CTA listened can be changed in the ctad.ini file. If the port is changed to a nonconflicting port then the install continues. To change the port number look up LocalPort in the CTA Administrators Guide.

Table 10 Known Problems of Cisco Trust Agent V.2.0 (continued)

Bug 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 effect 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.
CSCsb67286	CTA does not respond to EOU hello from switch. Put in hold state.	**Symptom** CTA does not respond to an EAP over UDP hello from the switch. The switch port is put into the held state. This problem occurs even if the Windows XP firewall has been configured to allow traffic to CTA or has been configured to allow traffic over EAP over UDP. At bootup, the Windows XP firewall loads a boot policy that blocks the EAP over UDP traffic to CTA. The boot policy is loaded even if the firewall is disabled but the firewall service is still running. This behavior occurs primarily at system boot up. You can read more about the Windows firewall at this article in the Microsoft Security Developer Center: http://msdn.microsoft.com/security/productinfo/XPSP2/networkprotection/firewall.aspx. **Conditions** Windows XP Service Pack 2 - Firewall service running. **Workaround** Change the state of the Windows XP firewall service to manual or disabled.

Table 10 Known Problems of Cisco Trust Agent V.2.0 (continued)

Bug 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.
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 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 effect the running of Cisco Trust Agent.

Table 10 Known Problems of Cisco Trust Agent V.2.0 (continued)

Bug ID	Headline	Explanation
CSCsc21188	When the CTA 802.1X Wired Client is idle, it does not respond to EAP requests from the switch.	**Symptom** When the CTA 802.1X Wired Client is idle, it does not respond to EAP requests from the switch. **Conditions** This condition occurs when a CTA machine is already connected to a port and after the port is enabled for IEEE 802.1X. **Workaround** • Reboot the client machine. When the machine starts, the IEEE 802.1X session initiates. • Click the **Connect** button on the 802.1X Wired Client connection dialog.
CSCsc25865	New notification will not overwrite old user notification on Win NT 4.0.	**Symptom** Normally, CTA deletes old notifications before displaying new notifications. However, in the case of an upgrade, the original notification might not be removed. If there is a CTA notification dialog open when CTA is upgraded, the dialog is not removed when the CTA receives the next notification. **Conditions** This occurs with a upgrade while a CTA notification is being displayed. **Workaround** Close notify dialog before upgrading.
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 popup windows box is not automatically removed from the screen. **Workaround** Users need to manually close the dialog box.

Table 10 Known Problems of Cisco Trust Agent V.2.0 (continued)

Bug ID	Headline	Explanation
CSCsc39434	CTA modules are missing from CTA log file in Windows NT 4.0 with Service Pack 6a.	**Symptom** CTA modules (CTAMSG, CTASI, CTASC) are missing from the CTA log file. This is a result of different privileges existing among CTAMsg, CTASI, CTASC, and the CTA log service. **Conditions** Windows NT with Service Pack 6a. **Workaround** There is no workaround.
CSCsc40724	A full posture is not triggered after scripting has a status change <CmdBold> ctasi <noCmdBold> <CmdArg> posture_data_file 1<noCmdArg> .	**Symptom** On Windows NT 4.0 with SP6a, using script interface with option of n=1, the script does not trigger a full posture validation at the end of the Status Query timeout. The command to result in that a status change has been detected is: `ctasi posture_data_file 1`. **Conditions** Windows NT **Workaround** There is no workaround on CTA. However, you can reduce the validation timeout on the NAD.
CSCsc43747	Fatal error displayed when uninstalling CTA.	**Symptom** The error dialog, *Fatal[c0029]: Timed semaphore failed* appears when uninstalling CTA. **Workaround** Ignore the error. It is a nonfatal dialog. It does not effect the uninstall.

Table 10 Known Problems of Cisco Trust Agent V.2.0 (continued)

Bug ID	Headline	Explanation
CSCsc59547	WINNT gives ctamsg error if the EnableNotifies parameter is enabled when the notification is sent	**Symptom** When installing CTA client on Windows NT with Service Pack 6a, the default setting for notifies is enabled. On Windows NT this setting does not display the posture status pop-up, but does cause an error with ctamsg.exe and causes a Dr. Watson window to pop up. If left unattended, these Dr. Watson Pop-ups will cause the machine to run out of virtual memory. (Closing the pop-up windows solves this problem). **Conditions** Windows NT with Service Pack 6a **Workaround** The workaround is to edit the **c:\program files\cisco systems\ciscotrustagent\ctad.ini.windows** file and set enablenotifies =0, then save the file as ctad.ini. This will disable the notify messages and cause the error pop-ups to stop displaying. In order to check the posture status of the machine, the user would have to use the clogcli utility to enable logging and verify the log file, or simply test network connectivity. **c:\program files\cisco systems\ciscotrustagent\clogcli enable** will enable logging, and the log file can be found in **c:\program files\cisco systems\ciscotrustagent \logging\logs.**

Known Cisco Security Agent Problems

This caveat addresses a specific behavior of Cisco Security Agent (CSA) that affects a NAC implementation. For a complete list of the features as well as other caveats for CSA, refer to CSA's product release notes available at http://www.cisco.com.

Table 11 Known Limitations of Cisco Security Agent

Bug ID	Headline	Explanation
CSCsc15657	CSA NAC posture plugin exception removes CSA posture plugin from correct directory.	**Symptom** CSA posture plugin reports an exception causing the plugin to be automatically copied to a non active directory by CTA. The exception is logged in the CTA logfile. **Conditions** CSA version 4.5.0.565. CTA 1.0.55, Windows XP. **Workaround** Copy CSA plugin (CiscoSecurityAgentPlugin.dll) back to correct directory: \Program Files\Common Files\PostureAgent\

Resolved Component Problems

This section describes problems that have been fixed since the first version of the *Release Notes for Network Admission Control, Release 2.0* were distributed on November 28, 2005.

Resolved Catalyst 6500 Series Switch Problems

These problems with Catalyst 6500 series switches running the CatOS 8.5 JAC operating systems were resolved in CatOS software release 8.5(2).

Table 12 Problems Resolved by CatOS 8.5(2) Operating system

Bug ID	Headline	Explanation
CSCsc31164	No syslog generated when SQ fails due to Posture change	A status query failure used to occur when a host replied with an EAP NAK message, the NAD was unable to match the status query packet sent by the host, or there was no response for the status query request from the host. This problem is resolved in software release 8.5(2).
CSCsb99920	No syslog message is generated when an EOU session is manually cleared.	This problem is resolved in software release 8.5(2).
CSCei69405	SET EOU AUTH mac-addr/ip-addr not displayed as configured	When you configured an exception list with a MAC address and mask, the subsequent **show** display output displayed the address with the mask applied. However, the display looks altered from the way it was configured. The display was also inconsistent with the way information is displayed by the **show security acl info** command. This problem is resolved in software release 8.5(2).
CSCsc14943	copy cfg all incl set eou timeout idle + set port eou cmd; produce usage	When you enter the **copy config all** command, the **set eou timeout idle** command which is not supported, appears in the configuration file. **Workaround:** Do not copy the default configuration to a file in text configuration mode. Copy non-default configurations using the **copy config** command when using text configuration mode or saving the configuration (or use binary mode). This problem is resolved in software release 8.5(2)

Table 12 Problems Resolved by CatOS 8.5(2) Operating system

Bug ID	Headline	Explanation
CSCsc32787	New command to enable sending Host IP in Calling-Station-ID attrib	The current switch implementation sends the MAC address of the host in the Calling-Station-ID attribute in the RADIUS requests to the ACS. Due to requirements from the reporting and monitoring devices, a new command, **set eou allow ip-station-id**, was created to enable sending the host IP address in the Calling-Station-ID attribute in the RADIUS requests to the ACS. This problem is resolved in software release 8.5(2).
CSCsc35238	Dot1x Auth: Invalid RADIUS Accounting messages	The switch is sending invalid RADIUS accounting messages to the ACS and the ACS is ignoring these messages due to the following issues: 1) Per RFC 2869 section 5.13, the EAP message (79) attribute should not be included in the accounting request (code=4) RADIUS messages. The switch is incorrectly including them in start and stop records (not in interim/update records). 2) Inserting the EAP message (79) attribute payload in the attributes and not populating the message authenticator (80) attribute is a violation of the RFC. The message authenticator attribute is missing from the messages when the EAP message (79) attribute is present. This problem is resolved in software release 8.5(2)
CSCsc53253	LPIP goes to abort state with CTA 2.0.0.26 when configured with lp1x	The cookie TLV received from the Hello Response packet should be included only in the first EoU validate packet and should not be included in subsequent validate retransmits. The switch is including the cookie TLV in retransmitted validate packets and the CTA is discarding the packets which is causing the switch to go to abort state. This problem is resolved in software release 8.5(2).

Resolved Cisco Secure Access Control Server Problems

Table 13 Resolved Problems in ACS

Bug ID	Headline	Explanation
CSCea91947	ACS does not authenticate Windows 2000 users when NTLMv2 is enabled on the network	**Symptom** The data from the NTLMv2's hashing function was applied to the MS-CHAP response and the Domain Controller receives a hash of the data it really needs. ACS can authenticate a MS-CHAP challenge/response only, and not a hash of it. A field notice addressed this issue: http://www-tac.cisco.com/Support_Library/field_alerts/fn62167.html **Resolution** ACS now supports NTLMv2.
CSCeb51393	Multi-admin needs to be able to add, edit, and delete downloadable ACLs.	No conflicts exist when multiple administrators try to add, edit, and delete downloadable ACLs under the shared profile components.
CSCee77099	The navigation bar (buttons) disappears after exiting from the Global Authentication Setup page	The navigation bar (button bar on the left) in the ACS web interface appears successfully after exiting from the Global Authentication page.
CSCee83677	NAC attribute type change can cause NAC GUI error	NAC errors no longer occur after an administrator changes the type of an existing NAC attribute by using the **CSUtil** (or because of backup and restore).
CSCee88908	CSLog fails if a logged attribute is deleted due to replication	The CSLog works as expected after replication.
CSCeh09266	Errors occurs while installing ACS on directory with special characters.	The percent sign (%) that caused the problem with ACS installing correctly is fixed in ACS 4.0.
CSCeh93481	Network Access Filter names and settings must be unique.	**Symptom** Network Access Profile configuration problems occured when you created a NAF with a previously used name. **Resolution** Resolved in latest release.

Resolved Cisco Security Agent Problems

These problems with Cisco Security Agent (CSA) 4.5.1.639 were resolved in release 5.0.0.176.

Table 14 Resolved Problems in Cisco Security Agent

Bug ID	Headline	Explanation
CSCeg90229	If CTA install by way of CSA fails, CSA refers to a non existent CTA log file	Cisco Trust Agent is an optional component that can be installed by Cisco Security Agent on any Windows platform. On Windows NT, the CTA installer fails because it is not a supported platform. The error message is presented in a message box and is not written to a log file.
CSCsb20867	CSA misinterprets some desired CTA behavior as malicious and prevents the behavior.	CSA attempts to prevent NAC URL redirects though this is the desired behavior. This issue has been fixed in CSA 5.0 with a default policy update. The issue is very similar to CSCsc03048 however some different files are accessed based on the system configuration.
CSCsb46561	There is no option to install CTA with a scheduled update from CSA 4.0.x to 4.5.	This defect has been fixed in 5.0 release. A check box has been added to upgrade the Cisco Trust Agent along with the CSA agent upgrade. Since this defect is fixed in V5.0, the software updates from 5.0 onwards only will have this feature. CSA 4.0.x and 4.5 Management Centers do not have this feature.
CSCsb74842	CSA's CTA install utility needs to be able to specify multiple certificates.	Up to 10 certificates can now be specified when installing CTA through CSA.
CSCsc03048	CSA security policies for Internet Explorer block NAC URL redirection	Created a new rule in the Cisco Trust Agent module to CTA to modify browser related temporary files.
CSCsc34302	CSA does not know if CTA has been uninstalled	The issue was fixed by having the agent user interface appropriately not show the NAC posture result when it detects that CTA is not installed, and by resetting the CSA internal system state whenever CTA is not detected on the system.

Table 14 Resolved Problems in Cisco Security Agent (continued)

Bug ID	Headline	Explanation
CSCsc37684	CSA security policy prevents installation of CSA plugin to CTA directory.	The Cisco Trust Agent rule module now considers the documented posture agent plugin directory to be a part of the CTA executables. CTA can now manage/move installed plugins.
CSCsc58244	CTA false positive on IE history folder creation	Added an allow rule in the Cisco Trust Agent - Windows policy to allow CTA to write to this directory: `**\History\*\MSHist*\*`

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access a central point for NAC information at this URL:

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

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users can order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—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 non-emergencies.

- Non-emergencies—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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked 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.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation 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 Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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 Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI 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.

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)—Your 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 operation 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 your network is impaired, but 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.

- 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

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication

identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems 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 Systems, 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 for networking professionals to 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

- 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
