Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(3)

Revised: November 25, 2010, OL-14508-01

Contents

These release notes provide late-breaking and release information for Cisco® NAC Appliance, formerly known as Cisco Clean Access (CCA), release 4.1(3). This document describes new features, changes to existing features, limitations and restrictions ("caveats"), upgrade instructions, and related information. These release notes supplement the Cisco NAC Appliance documentation included with the distribution. Read these release notes carefully and refer to the upgrade instructions prior to installing the software.

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

Cisco NAC Appliance Releases

Cisco NAC Appliance Version	Availability
4.1.3.2 (Windows Agent Only)	April 7, 2008
4.1.3.1 (Mac OS X Agent Only)	February 21, 2008
4.1.3.1 ED	February 18, 2008
4.1.3.10 (Cisco NAC Web Agent Only)	January 24, 2008
4.1.3.1 (Windows Agent Only)	January 15, 2008
4.1(3) ED	December 20, 2007

Note Any ED release of software should be utilized first in a test network before being deployed in a production network.

Cisco NAC Appliance Service Contract/Licensing Support

For complete details on service contract support, new licenses, evaluation licenses, legacy licenses and RMA, refer to the *Cisco NAC Appliance Service Contract / Licensing Support*.

System and Hardware Requirements

This section describes the following:

- System Requirements
- Hardware Supported
- Supported Switches for Cisco NAC Appliance
- VPN and Wireless Components Supported for Single Sign-On (SSO)

System Requirements

See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for system requirement information for the Clean Access Manager (CAM), Clean Access Server (CAS), and Cisco NAC Appliance Agents.

Hardware Supported

This section describes the following:

- Cisco NAC Network Module
- NAC-3300 Series Appliances
- Important Installation Information for NAC-3310

- Additional Hardware Support Information

Cisco NAC Network Module

Release 4.1(3) supports the Cisco NAC Appliance network module (NME-NAC-K9) on the next generation service module for the Cisco 2811, 2821, 2851, 3825, and 3845 Integrated Services Routers (ISRs). The Cisco NAC Network Module for Integrated Services Routers supports the same software features as the Clean Access Server on a NAC Appliance, with the exception of high availability. NME-NAC-K9 does not support failover from one module to another.

For hardware installation instructions (how to install the NAC network module in an Integrated Service Router), refer to the following sections of the *Cisco Network Modules Hardware Installation Guide*.

- Installing Cisco Network Modules in Cisco Access Routers
- Connecting Cisco Network Admission Control Network Modules

For software installation instructions (how to install the Clean Access Server software on the NAC network module) refer to *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*.

Note If introducing the Cisco NAC network module to an existing Cisco NAC Appliance network, you must upgrade all CAM/CAS appliances to release 4.1(2) or later for compatibility.

While upgrading to release 4.1(3) and later is not required to support Cisco NAC network modules, if you are supporting 64-bit Windows Vista client systems, you must upgrade to release 4.1.2.1 or later.

NAC-3300 Series Appliances

Release 4.1(3) supports Cisco NAC Appliance 3300 Series platforms.

Customers have the option to upgrade NAC-3310, NAC-3350, or NAC-3390 MANAGER and SERVER appliances to release 4.1(3) using a single upgrade file, **cca_upgrade-4.1.3.x.tar.gz**.

CD installation of release 4.1(3) is also supported:

- For NAC-3310 and NAC-3350, the **cca-4.1_3-K9.iso** file is required for new CD installation of the Clean Access Server or Clean Access Manager.

  Note The NAC-3310 appliance requires special installation directives, as well as a firmware upgrade. Refer to Important Installation Information for NAC-3310, page 4 for details.

- For NAC-3390, a separate ISO file, **supercam-cca-4.1_3-K9.iso**, is required for CD installation of the Clean Access Super Manager.

  Note Super CAM software is supported only on the NAC-3390 platform.

Release 4.1(3) and Cisco NAC Profiler

Release 4.1(3) includes the Cisco NAC Profiler Collector component that resides on Clean Access Server installations.

Refer to the *Release Notes for Cisco NAC Profiler* for updated product information.

See also Known Issues with Cisco NAC Profiler Release 2.1.7, page 88.

Important Installation Information for NAC-3310

- NAC-3310 Required BIOS/Firmware Upgrade, page 4
- NAC-3310 Required DL140 or serial_DL140 CD Installation Directive, page 4

NAC-3310 Required BIOS/Firmware Upgrade

The NAC-3310 appliance is based on the HP ProLiant DL140 G3 server and is subject to any BIOS/firmware upgrades required for the DL140 G3. Refer to *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for detailed instructions.

NAC-3310 Required DL140 or serial_DL140 CD Installation Directive

The NAC-3310 appliance (MANAGER and SERVER) requires you to enter the **DL140** or **serial_DL140** installation directive at the "boot:" prompt when you install new system software from a CD-ROM. For more information, refer ro Known Issue with NAC-3310 CD Installation, page 87.

Additional Hardware Support Information

See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for details on:

- Cisco NAC Appliance 3300 Series hardware platforms
- Supported server hardware configurations
- Pre-installation instructions for applicable server configurations
- Troubleshooting information for network card driver support

See Troubleshooting, page 109 for further details.

Supported Switches for Cisco NAC Appliance

See *Switch Support for Cisco NAC Appliance* for complete details on:

- Switches and NME service modules that support Out-of-Band (OOB) deployment
- Switches/NMEs that support VGW VLAN mapping
- Known issues with switches/WLCs
- Troubleshooting information

VPN and Wireless Components Supported for Single Sign-On (SSO)

Table 1 lists VPN and wireless components supported for Single Sign-On (SSO) with Cisco NAC Appliance. Elements in the same row are compatible with each other.

Table 1 VPN and Wireless Components Supported By Cisco NAC Appliance For SSO

Cisco NAC Appliance Version	VPN Concentrator/Wireless Controller	VPN Clients
4.1(3)	Cisco WiSM Wireless Service Module for the Cisco Catalyst 6500 Series Switches	N/A
	Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs)[1]	N/A
	Cisco ASA 5500 Series Adaptive Security Appliances, Version 8.0(3)7 or later[2]	AnyConnect
	Cisco ASA 5500 Series Adaptive Security Appliances, Version 7.2(0)81 or later	• Cisco SSL VPN Client (Full Tunnel) • Cisco VPN Client (IPSec)
	Cisco WebVPN Service Modules for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers	
	Cisco VPN 3000 Series Concentrators, Release 4.7	
	Cisco PIX Firewall	

[1] For additional details, see also Known Issue with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs), page 88.

[2] Release 4.1(3) supports existing AnyConnect clients accessing the network via Cisco ASA 5500 Series devices running release 8.0(3)7 or later. For more information, see VPN SSO Enhancement to Support Existing Clientless SSL VPN Users Launching the AnyConnect Client from a WebVPN Portal, page 16 and CSCsi75507.

Note Only the SSL Tunnel Client mode of the Cisco WebVPN Services Module is currently supported.

For further details, see the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(3)* and the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(3)*.

Software Compatibility

This section describes software compatibility for releases of Cisco NAC Appliance:

- Software Compatibility Matrixes
- Determining the Software Version

For details on Clean Access Agent and Cisco NAC Web Agent client software versions and AV integration support, see:

- Cisco NAC Appliance Agents, page 25
- Clean Access Supported AV/AS Product List, page 32

Software Compatibility Matrixes

This section describes the following:

- Release 4.1(3) Compatibility Matrix

- Release 4.1(3) CAM/CAS Upgrade Compatibility Matrix
- Release 4.1(3) Clean Access Agent Upgrade Compatibility Matrix

Release 4.1(3) Compatibility Matrix

Table 2 shows Clean Access Manager and Clean Access Server compatibility and the Clean Access Agent version supported with each CCA 4.1(3) release (if applicable). CAM/CAS/Clean Access Agent versions displayed in the same row are compatible with one another. Cisco recommends that you synchronize your software images to match those shown as compatible in the table.

Table 2 Release 4.1(3) Compatibility Matrix

Clean Access Manager [1]	Clean Access Server [1]	Cisco NAC Appliance Agents [2]		
		Windows [3]	Mac OS X [4]	Web Agent [5]
4.1.3.1 [6]	4.1.3.1 [6]	4.1.3.2 4.1.3.1 4.1.3.0	4.1.3.1 4.1.3.0	4.1.3.10 4.1.3.9
		4.1.2.x 4.1.1.0 4.1.0.x [7]	4.1.2.x 4.1.1.0 4.1.0.x [7]	-
				-
4.1(3)	4.1(3)	4.1.3.2 4.1.3.1 4.1.3.0	4.1.3.1 4.1.3.0	4.1.3.10 4.1.3.9
			4.1.2.x 4.1.1.0 4.1.0.x [7]	-
				-

[1] Make sure both CAS and CAM are of same version.

[2] See Cisco NAC Appliance Agents, page 25 for details on version updates for each Windows/Mac OS X/Web Agent.

[3] Version 4.1.3.0 and later of the Windows Clean Access Agent is compatible with the 4.1(3) CAM and 4.1(3) and later CAS releases. See Cisco NAC Appliance Agents, page 25 for details and caveats resolved for each Agent version.

[4] Mac OS X Clean Access Agent supports authentication only (no posture assessment) and auto-upgrade starting from version 4.1.3.0. See Mac OS X Clean Access Agent Version 4.1.3.0, page 29 for details.

[5] Cisco NAC Web Agent 4.1.3.9 is a new user access option introduced in release 4.1(3). See Cisco NAC Web Agent Enhancements, page 30 for more information.

[6] Cisco NAC Appliance Release 4.1.3.1 is a general and important bug fix release that resolves issues as described in Enhancements in Release 4.1.3.1, page 10.

[7] Cisco strongly recommends running version 4.1.3.0 of the Clean Access Agent with release 4.1(3) of the CAM/CAS. If necessary, release 4.1(3) allows administrators to optionally configure the 4.1(3) CAM/CAS to allow 4.1.0.x Agent authentication and posture assessment (Windows only). Note that by default, 4.1.0.x Agents are not allowed to log into a 4.1(3) Cisco NAC Appliance system. However, an Agent upgraded to 4.1.3.0 and later can still log into a 4.1(0) CAM/CAS. See *4.1.0.x Agent Support on Release 4.1(1)* in the 4.1(1) release notes for details.

Release 4.1(3) CAM/CAS Upgrade Compatibility Matrix

Table 3 shows 4.1(3) CAM/CAS upgrade compatibility. You can upgrade/migrate your CAM/CAS from the previous release(s) specified to the latest release shown in the same row. When you upgrade your system software, Cisco recommends you upgrade to the most current release available whenever possible.

Table 3 Release 4.1(3) CAM/CAS Upgrade Compatibility Matrix

Clean Access Manager		Clean Access Server	
Upgrade From:	To:	Upgrade From:	To:

4.1(2)+
4.1(1)
4.1(0)+ [1]
4.0(x)
3.6(x)
3.5(7)+ [2]
	4.1.3.1 [3]
	4.1(3)
		4.1(2)+
		4.1(1)
		4.1(0)+ [1]
		4.0(x)
		3.6(x)
		3.5(7)+ [2]
			4.1.3.1 [3]
			4.1(3)

[1] Release 4.1(0), 4.1.0.1, and 4.1.0.2 do not support and cannot be installed on Cisco NAC Appliance 3300 Series platforms.

[2] "In-place" upgrade from version 3.5(11) to 4.1(3) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(3) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(3). (See CSCsl76977.)

[3] Cisco NAC Appliance Release 4.1.3.1 is a general and important bug fix release that resolves issues as described in Enhancements in Release 4.1.3.1, page 10.

Release 4.1(3) Clean Access Agent Upgrade Compatibility Matrix

Table 4 shows Clean Access Agent upgrade compatibility when upgrading existing versions of the Agent after 4.1(3) CAM/CAS upgrade. You can auto-upgrade any 3.5.1+ Windows Agent directly to the latest 4.1.3.x Windows Agent. You can auto-upgrade Mac OS X Agents starting from version 4.1.3.0 and later.

Note The temporal Cisco NAC Web Agent is updated on the CAM under **Device Management > Clean Access > Updates > Update** only; auto-upgrade does not apply.

Refer to the "Cisco NAC Appliance Agents Systems Requirements" section of the *Supported Hardware and System Requirements for Cisco NAC Appliance* for additional compatibility details.

Table 4 Release 4.1.3.x Agent Upgrade Compatibility Matrix

Clean Access Manager	Clean Access Server	Clean Access Agent [1, 2, 3]		
		Upgrade From:	To Latest Compatible Windows Version:	To Latest Compatible Mac OS X Version:
4.1.3.1 4.1(3)	4.1.3.1 4.1(3)	4.1.2.x 4.1.1.0 4.1.0.x [4]	4.1.3.2 4.1.3.1 [5] 4.1.3.0	4.1.3.1 [6] 4.1.3.0
		4.0.x.x 3.6.x.x 3.5.1 and later	4.1.3.1 [5] 4.1.3.0	—

[1] Clean Access Agent versions are not supported across major releases. Do not use 4.1.3.x Agents with 4.0(x) or prior releases. However, auto-upgrade is supported from any 3.5.1 and later Agent directly to the latest 4.1.3.x Agent.

[2] See Cisco NAC Appliance Agents, page 25 for details on version updates for each Windows/Mac OS X/Web Agent.

[3] For checks/rules/requirements, version 4.1.1.0 and later Clean Access Agents can detect "N" (European) versions of the Windows Vista operating system, but the CAM/CAS treat "N" versions of Vista as their US counterpart.

[4] Cisco strongly recommends running the latest 4.1.3.x version of the Clean Access Agent with release 4.1(3) of the CAM/CAS. If necessary, release 4.1(3) allows administrators to optionally configure the 4.1(3) CAM/CAS to allow 4.1.0.x Agent authentication and posture assessment. Note that by default, 4.1.0.x Agents are not allowed to log into a 4.1(3) Cisco NAC Appliance system. However, an Agent upgraded to 4.1.3.0 and later can still log into a 4.1(0) CAM/CAS. See *4.1.0.x Agent Support on Release 4.1(1)* in the 4.1(1) release notes for details.

5. Windows Clean Access Agent version 4.1.3.1 resolves caveat CSCsm05207. See Windows Clean Access Agent Version 4.1.3.1, page 27 and Resolved Caveats - Windows Clean Access Agent 4.1.3.1, page 73 for details.
6. Auto-upgrade of the Mac OS X Agent is supported starting from version 4.1.3.0 and later. Release 4.1(1) and release 4.1(2)+ do not support auto-upgrade for the Mac OS X Agent. Users can upgrade client machines to the latest Mac OS X Agent by downloading the Agent via web login and running the Agent installation. For more information, see Mac OS X Clean Access Agent Enhancements, page 29.

Determining the Software Version

There are several ways to determine the version of software running on your Clean Access Manager (CAM), Clean Access Server (CAS), or Clean Access Agent, as described below.

- Clean Access Manager (CAM) Version, page 8
- Clean Access Server (CAS) Version, page 9
- Cisco NAC Appliance Agents Versioning, page 9
- Cisco Clean Access Updates Versioning, page 9

Clean Access Manager (CAM) Version

The top of the CAM web console displays the software version installed. After you add the CAM license, the top of the CAM web console displays the license type (Lite, Standard, Super). Additionally, the **Administration > CCA Manager > Licensing** page displays the types of licenses present after they are added.

The software version is also displayed as follows:

- From the CAM web console, go to **Administration > CCA Manager > System Upgrade | Current Version**
- SSH to the machine and type: `cat /perfigo/build`

CAM Lite, Standard, Super

The NAC Appliance Clean Access Manager (CAM) is licensed based on the number of NAC Appliance Clean Access Servers (CASes) it supports. You can view license details under **Administration > CCA Manager > Licensing**. The top of CAM web console identifies the type of CAM license installed:

- Cisco Clean Access Lite Manager supports 3 Clean Access Servers (or 3 HA-CAS pairs)
- Cisco Clean Access Standard Manager supports 20 Clean Access Servers (or 20 HA-CAS pairs)
- Cisco Clean Access Super Manager supports 40 Clean Access Servers (or 40 HA-CAS pairs)

Note the following:

- The Super CAM software runs **only** on the Cisco NAC-3390 MANAGER.
- Initial configuration is the same for the Standard CAM and Super CAM.
- Software upgrades of the Super CAM use the same upgrade file and procedure as the Standard CAM. You can use web upgrade or console/SSH instructions to upgrade a Super CAM to the latest release. However, a new CD installation of the Super CAM requires a separate .ISO file.

Clean Access Server (CAS) Version

You can determine the CCA software version running on the Clean Access Server (whether NAC-3300 appliances or Cisco NAC network modules) using the following methods:

- From the CAM web console, go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Misc > Update | Current Version**
- From CAS direct access console, go to **Administration > Software Update | Current Version** (CAS direct console is accessed via **https://<***CAS_eth0_IP_address***>/admin**)
- SSH or console to the machine (or network module) and type `cat /perfigo/build`

Note If configuring High Availability CAM or CAS pairs, see also Access Web Consoles for High Availability, page 106 for additional information.

Cisco NAC Appliance Agents Versioning

On the CAM web console, you can determine versioning for the Cisco NAC Appliance Agents from the following pages:

- **Monitoring > Summary** (Windows Setup/Patch, Mac OS X Agent, Web Agent)
- **Device Management > Clean Access > Clean Access Agent > Distribution** (persistent Agents only)
- **Device Management > Clean Access > Updates > Summary** (all Cisco Updates versioning and Agent Patch Version; see also Cisco Clean Access Updates Versioning, page 9)
- **Device Management > Clean Access > Clean Access Agent > Reports | View** (individual report shows username, operating system, Clean Access Agent version and type, System/User domain information, client AV/AS version)

From the Clean Access Agent itself on the client machine, you can view the following information from the Agent taskbar menu icon:

- Right-click **About** to view the Agent version.
- Right-click **Properties** to view AV/AS version information for any AV/AS software installed, and the Discovery Host (used for L3 deployments)

Cisco Clean Access Updates Versioning

To view the latest version of Updates downloaded to your CAM, including Cisco Checks & Rules, Cisco NAC Web Agent, Clean Access Agent Upgrade Patch, Supported AV/AS Product List, go to **Device Management > Clean Access > Update > Summary** on the CAM web console. See Clean Access Supported AV/AS Product List, page 32 and Clean Access Supported AV/AS Product List, page 32 for additional details.

New and Changed Information

This section describes enhancements added to the following releases of Cisco NAC Appliance for the Clean Access Manager and Clean Access Server.

- Enhancements in Release 4.1.3.2, page 10
- Enhancements in Release 4.1.3.1, page 10
- Enhancements in Release 4.1(3), page 10

See Cisco NAC Appliance Agents, page 25 for new features and enhancements to Cisco NAC Appliance Agents.

For additional details, see also:

- Hardware Supported, page 2
- Clean Access Supported AV/AS Product List, page 32
- Caveats, page 57
- Known Issues for Cisco NAC Appliance, page 86

Enhancements in Release 4.1.3.2

Windows Clean Access Agent Language Template Support Enhancement (Version 4.1.3.2)

Added Agent language template support for Russian, Turkish, and Serbian (Cyrillic) for Windows Agents. The Agent will display localized text for these languages if run from localized Windows operating system.

Note The Agent picks the correct language template based on the local computer Locale (under Control Panel > Regional and Language Options). Cisco recommends using the localized Agent in the localized version of Windows (e.g. French Agent in French Windows). Agent language template support only controls what the viewer sees after the Agent is installed; it does not include support for different client operating systems for the Agent Installer or for AV/AS products.

Note If the administrator includes non-English text in the CAM configuration (e.g. non-English characters in a requirement description or registry value check), it may not be displayed correctly or run correctly.

See Cisco NAC Appliance Agents, page 25 for enhancement details per Agent version.

Enhancements in Release 4.1.3.1

Release 4.1.3.1 is a general and important bug fix release for the Clean Access Manager and Clean Access Server that addresses the caveats described in Resolved Caveats - Release 4.1.3.1, page 71. No new features are added.

For upgrade instructions, please refer to Upgrading to 4.1(3), page 92.

Enhancements in Release 4.1(3)

This section details the enhancements delivered with Cisco NAC Appliance release 4.1(3) for the Clean Access Manager and Clean Access Server.

General Enhancements

- Cisco NAC Web Agent
- Support for Clients with Multiple Active NICs
- Clean Access Server HA Heartbeat Link Enhancement
- Clean Access Manager HA Configuration and Heartbeat Link Enhancements

- Guest User Login and Registration Enhancements
- LDAP Authentication Enhancement
- Clean Access Server and WSUS Interaction Enhancement
- Agent Restricted User Access Enhancement
- Device Filter List Display and Import/Export Enhancement
- Agent Report Information Display and Export Enhancement
- VPN SSO Login Enhancement
- VPN SSO Enhancement to Support Existing Clientless SSL VPN Users Launching the AnyConnect Client from a WebVPN Portal
- Syslog Configuration Enhancement
- Debug Log Download Enhancement
- cisco_api.jsp Enhancement
- CSRF Protection
- Proxy Support Enhancements
- ARP Broadcast Packet Handling Improvement
- Clean Access Server HA ARP Broadcast Enhancement
- Deprecated “Retag Trusted-side Egress Traffic with VLAN (In-Band)” Feature
- Previously-Deprecated Features Removed from CAM/CAS Web Console Pages
- Clean Access Agent Auto Remediation
- Delay Agent Logoff on CAM/CAS
- 64-bit Windows Operating System Agent Support
- Supported AV/AS Product List Enhancements (Version 67)

Out-of-Band Enhancements

- Access to Authentication VLAN Change Detection Enhancement
- SNMP Inform Notification Enhancement
- SNMP “MAC Move Notification” Switch Port Configuration Support

Cisco NAC Appliance Agent Enhancements

- Windows Clean Access Agent Language Template Support Enhancement (Version 4.1.3.0)

General Enhancements

Cisco NAC Web Agent

Warning **Cisco does not recommend using the Cisco NAC Web Agent on client machines connecting with link speeds slower than 56Kbits/s.**

Cisco NAC Appliance release 4.1(3) introduces a new temporal Agent for Windows client machines. Unlike the Clean Access Agent, the Cisco NAC Web Agent is not a "persistent" entity, thus it only exists on the client machine long enough to accommodate a single user session. Instead of downloading and installing an Agent application, once the user opens a browser window, logs in to the Cisco NAC Appliance web login page, and chooses to launch the Cisco NAC Web Agent, an ActiveX control or Java applet (you specify the preferred method using the **Web Client (Active X/Applet)** option in the **Administration > User Pages > Login Page** configuration page) initiates a self-extracting stub installer on the client machine to install Agent files in a client's temporary directory, perform posture assessment/scan the system to ensure security compliance, and report compliance status back to the Cisco NAC Appliance system. During this period, the user is granted access only to the Temporary Role and if the client machine is not compliant for one or more reasons, the user is informed of the issues preventing network access and may do one of the following:

- Users must manually remediate/update their client machine and try to test compliance again before the Temporary Role times out
- Accept "restricted" network access for the time being and try to ensure the client machine meets requirements for the next login session

Note The Cisco NAC Web Agent does not perform client remediation. Users must adhere to Cisco NAC Appliance requirement guidelines independent of the Web Agent session to ensure compliance before they can gain access to the internal network. If users are able to correct/update their client machine to be compliant before the Temporary Role time-out expires, they can choose to "Re-scan" the client machine and successfully log in to the network.

Once the user has provided appropriate login credentials and the Web Agent ensures the client machine meets the NAC Appliance security requirements, the browser session remains open and the user is logged in to the network until the user clicks the **Logout** button in the Web Agent browser window, shuts off their system, or the NAC Appliance administrator terminates the session from the CAM. After the session terminates, the Web Agent "removes" itself from the client machine and the temporary files used to install are deleted from the system.

Note Security restrictions for the "Guest" user profile in Windows Vista operating systems prevent ActiveX controls and Java applets from running properly. Therefore, you must log into the Windows Vista client machine as a known user (not a "Guest") in order to log into Cisco NAC Appliance via the Web Agent.

The Cisco NAC Web Agent enhancement affects the following page of the CAM web console:

- **Device Management > Clean Access > General Setup > Agent Login—new Require use of Cisco NAC Web Agent option to enable the Cisco NAC Web Agent for user login**

Note For system requirements and details on version updates, refer to Cisco NAC Web Agent Enhancements, page 30.

Support for Clients with Multiple Active NICs

Cisco NAC Appliance release 4.1(3) includes an enhancement to help stabilize connection problems from client machines with more than one active Network Interface Card (NIC). For example, a client machine may have an active LAN Ethernet connection and an active wireless NIC connection where each interface sends SWISS UDP discovery packets to initiate a connection to a network CAS. To address this potential situation, the CAS now examines the SWISS packets from the client machine to record the requesting NIC IP address and verifies all subsequent SWISS UDP packets for the NIC IP address to ensure the same client only logs in from one interface.

Without this enhancement, the following scenario can occur:

The client machine A sends out SWISS UDP discovery packets to the CAS and receives a response directing the user to enter their authentication credentials. During this process, another active NIC on client machine A sends SWISS UDP discovery plackets to the same CAS even though the first interface is already establishing a connection. After the first client session is established, the user sees a login screen again, despite having already successfully established connection. Until the secondary NIC is disabled or the client machine does something to halt SWISS UDP packet transmission, the user can continually see login screen after login screen.

For information regarding clients with multiple active NICs and how to configure them to interoperate with the Access to Authentication VLAN change detection feature, see Access to Authentication VLAN Change Detection Interoperability with Clients Featuring More Than One Active NIC, page 23.

For more information, see the "Supporting Multiple Active NICs on the Clean Access Agent Client Machine" section in the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(3)*.

Clean Access Server HA Heartbeat Link Enhancement

Clean Access Server HA heartbeat link capabilities have been enhanced in release 4.1(3). In addition to the existing serial interface and optional trusted (eth0 and eth2/eth3) interface heartbeat connections, you can now also configure the CAS to employ the (untrusted side) eth1 interface to provide redundant HA heartbeat monitoring.

This enhancement affects the following page of the CAS web console:

- **Administration > Failover > General | HA-Primary Mode and HA-Secondary Mode CAS mode configuration pages now allow for up to three optional Heartbeat UDP Interfaces: one dedicated on the (trusted side) eth0; one dedicated on the (untrusted side) eth1 interface; and a third on either of the eth2 or eth3 interfaces, if installed and enabled.**

Clean Access Manager HA Configuration and Heartbeat Link Enhancements

In release 4.1(3), the Clean Access Manager web console interface now features a new (separate) **Failover** tab as well as additional failover configuration settings to support up to three optional redundant Heartbeat UDP Interfaces. In addition to the existing optional serial interface and dedicated eth1 interface heartbeat connections, you can now also configure the CAM to employ the (trusted side) eth0 interface and an additional optional Ethernet link to provide redundant HA heartbeat monitoring.

This enhancement affects the following pages of the CAM web console:

- **Administration > CCA Manager > Network** (formerly **Network & Failover**) no longer features any CAM HA/failover configuration settings
- **Administration > CCA Manager | new Failover tab featuring HA-Primary Mode and HA-Secondary Mode CAM mode configuration pages that allow for up to three optional Heartbeat UDP Interfaces: one dedicated/preconfigured heartbeat link on eth1; one dedicated link on eth0; and a third on either of the eth2 or eth3 interfaces, if installed and enabled.**

Guest User Login and Registration Enhancements

Release 4.1(3) enhances the way the CAM handles Guest user login, registration, and access with a new Guest Registration feature. Rather than allow users to simply gain undifferentiated Guest access to the system, the administrator can now configure guest users to register their own local accounts on the CAM using a variety of fields, including email, phone number, or affiliation. The new feature provides a customizable level of guest authentication using a new Guest Auth Server Type, new Guest Registration configuration pages, and the default guest role.

The CAM can automatically time out guest accounts using token expiration, or flush out unused guest accounts from the local database after a configurable number of days. Administrators can view newly created guest accounts on a new Guest Users local users list, and on the Certified Device List and Online Users List by configured Guest Auth Provider and Guest role.

Note Guest Registration on the CAM in 4.1(3) is independent of the Cisco NAC Guest Server solution. For details on Cisco NAC Guest Server, refer to the *Release Notes for Cisco NAC Guest Server, Release 1.0.0*.

To update any existing Guest user access model on the CAM to take advantage of the enhancements in release 4.1(3), administrators can perform the following tasks:

1. Disable/remove previous Guest user account(s)—You can accomplish this by either removing all existing guest users from the CAM's user database or (if all existing guest registration information is accessible from the same authentication source, removing the authentication server from the CAM
2. Create a new Guest user role—You can create a new Guest user role just as you would any other login account with which users can access the NAC Appliance system
3. Configure the Guest authentication server—You can configure a Guest authentication server just as you would any other standard authorization server, with the addition of two "housekeeping" features designed for Guest user authentication: an account lifetime setting and an option that enables you to automatically remove invalid guest accounts once a specified period of inactivity has passed
4. Configure Guest login page(s)—This function allows you to require Guest registration and add existing Guest provider options to the login page
5. Customize the Guest page—You can also specify the content and type of information Guest users must provide during the registration process

This enhancement affects the following pages of the CAM web console:

- **User Management > Auth Servers > New** | new "Guest" **Authentication Type** and respective settings
- **User Management > Local Users**: now features a new **Guest Users** tab (formerly a subtab of existing **Local Users**) with which you can view Guest user information more exclusively
- **Administration > User Pages** | new **Guest Registration Page** tab with **Content** and **Guest Info** subtabs

LDAP Authentication Enhancement

Release 4.1(3) enhances the authentication settings available when authenticating user credentials against an LDAP server. Administrators can now specify either the "Simple" or Generic Security Services Application Programming Interface (**GSSAPI**) authentication mechanism to better provide secure credential authentication in the network.

This enhancement affects the following pages of the CAM web console:

- **User Management > Auth Servers > New/Edit | Authentication Type | LDAP and User Management > Auth Servers > Lookup Servers > New both feature the following new user interface settings/options:**
  - **New GSSAPI Authentication Mechanism option with associated KDC Timeout (in seconds)**, **KDC/Realm Mapping**, **Domain/Realm Mapping** settings. and **Description**
  - New **Default Realm** LDAP configuration setting

Clean Access Server and WSUS Interaction Enhancement

Release 4.1(3) improves message text for Windows Server Update Services (WSUS) requirements. When the Clean Access Agent encounters a WSUS requirement compliance issue, the Agent launches a secondary client remediation frame from which the user can download the required Windows Update during client posture assessment.

Note For non-admin users of client machines, use of the Stub Agent is mandatory for WSUS requirements.

Agent Restricted User Access Enhancement

Cisco NAC Appliance Agent login behavior has been enhanced in release 4.1(3) to allow users "restricted" network access if/when their client machine does not pass posture assessment as configured in the requirements associated with the user's login role. If this function is enabled by the administrator, a new button labeled "Limited" now appears in the Clean Access Agent login dialog and "Get Restricted Network Access" (or another configurable text string) in the Cisco NAC Web Agent dialog to give the user the option to gain access to a restricted set of network resources via the NAC Appliance system. The administrator has control over which resources are available to users with restricted network access, according to the configuration settings specified in an existing user role. For example, the administrator can create a new user role called "Restricted" in **User Management > User Roles** that allows users who choose to accept restricted network access to launch their Email program and gain access to the WWW, but nothing else.

This enhancement affects the following web console page:

- **Device Management > Clean Access > General Setup > Agent Login | Allow restricted network access in case user cannot use Clean Access Agent or Cisco NAC Web Agent**

Device Filter List Display and Import/Export Enhancement

Starting from release 4.1(3), Cisco NAC Appliance administrators can export device filter lists to CSV files that can be searched, viewed, and manipulated in Microsoft Excel spreadsheets whenever the administrator needs them to troubleshoot connection issues or compile statistical reports, and the administrator can import device filter list information to populate (or repopulate) the CAMs device filter database from existing CSV files. In addition, the layout and function of the device filter list display (**Device Management > Filters > Devices > List**) has been updated in release 4.1(3) to give the administrator more direct control over the specific device entries displayed.

This enhancement affects the following page of the CAM web console:

- **Device Management > Filters > Devices > List**—display page options have been reorganized and the page features two new **Import** and **Export** buttons

Agent Report Information Display and Export Enhancement

Starting from release 4.1(3), Cisco NAC Appliance administrators can export Agent report information to CSV files that can be searched, viewed, and manipulated in Microsoft Excel spreadsheets whenever the administrator needs them to troubleshoot connection issues or compile statistical reports. In addition, the layout and function of the Agent report display list (**Device Management > Clean Access > Clean Access Agent > Reports**) has been updated in release 4.1(3) to give the administrator more direct control over the specific Agent report entries displayed.

This enhancement affects the following page of the CAM web console:

- **Device Management > Clean Access > Clean Access Agent > Reports**—display page options have been reorganized and the page features two new **Export** and **Export (with text)** buttons

Note The **Export** option creates an Excel file containing the columns displayed in the report viewer (Status, User, Agent, IP, MAC, OS, etc.).

The **Export (with text)** option provides an extra column containing the raw HTML code of the full Agent report that you can open for each report by clicking on view in the viewer.

VPN SSO Login Enhancement

Release 4.1(3) features a VPN SSO enhancement to ensure that users logging in via VPN are not erroneously presented with the Agent login dialog when signing in. When the user initiates a login session, the CAS passes information alerting the Agent that the user is already part of the VPN login list, thus enabling the CAM to avoid presenting the Agent login screen on the client machine. In network topologies that employ VPN concentrators, this potential situation can be made even more complex if the VPN concentrator delays sending the appropriate VPN login list notification to the CAS. To address this problem, the CAS is now able to specify a delay in the SWISS packet that tells the Agent to wait a short time before presenting the login screen.

VPN SSO Enhancement to Support Existing Clientless SSL VPN Users Launching the AnyConnect Client from a WebVPN Portal

Release 4.1(3) adds accounting update functionality to support existing AnyConnect clients accessing the network via Cisco ASA 5500 Series Adaptive Security Appliances platforms. To support VPN SSO, you must be running Cisco NAC Appliance release 4.1(3) or later and the Cisco ASA 5500 Series device must be running release 8.0(3)7 or later and be configured to send interim accounting update packets.

For example, your Cisco ASA 5500 Series configuration should include:

```
aaa-server radius protocol radius
interim-accounting-update
```

For VPN/Wireless SSO support information, refer to VPN and Wireless Components Supported for Single Sign-On (SSO), page 4

Note For additional details on the Cisco ASA enhancement, refer to http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsi75507.

Syslog Configuration Enhancement

Release 4.1(3) features a **Syslog Settings** page configuration enhancement allowing you to specify the **Syslog Facility** setting for a designated Syslog server where you direct Syslog messages originating from the CAM. You can use the default "User-Level" facility type, or you can assign any of the "local use" Syslog facility types defined in the Syslog RFC ("Local use 0" to "Local use 7"). This feature gives you the ability to differentiate Cisco NAC Appliance Syslog messages from "User-Level" Syslog entries you may already generate and direct to your Syslog server from other network components.

This enhancement affects the following page of the CAM web console:

- **Monitoring > Event Logs > Syslog Settings** | new **Syslog Facility** dropdown menu and **CPU Utilization Interval** field

Debug Log Download Enhancement

With release 4.1(3), you can now specify the number of days of collected debug logs to download in order to aid troubleshooting efforts when working with Cisco technical support. The default setting is one week (7 days). Previously, debug logs included all recorded log entries in the CAM/CAS database.

This enhancement adds a new field, "Download technical support logs for the last [] days" to the following web console pages:

- CAM web console: **Administration > Clean Access Manager > Support Logs**
- CAS web console: **Monitoring > Support Logs**

cisco_api.jsp Enhancement

In Release 4.1(3), the Cisco NAC Appliance API (**https://<*CAM-IP-address or hostmame*>/admin/cisco_api.jsp**) adds the following new functions which provide support for Cisco NAC Profiler deployments:

- **bounceport**—bounces an OOB switch port according to the switch and/or port ID
- **bounceportbymac**—bounces an OOB switch port according to the associated client machine MAC address
- **addsubnet**—Adds a subnet to the Device Filters list
- **updatesubnet**—Updates a subnet entry in the Device Filters list
- **removesubnet**—Removes a subnet entry from the Device Filters list

The API also includes the following enhancements:

- **getversion**—(new function) returns the version of the CAM
- **getreports**—(modified function) userKey query parameter is removed; agentType (web/win/mac) query parameter is added

See also CSRF Protection, page 18. For further details on the Cisco NAC Appliance API, see Appendix B "API Support" in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(3)*.

CSRF Protection

Release 4.1(3) enhances protection from Cross-Site Request Forgery attacks, which maliciously exploit web browser sessions. Release 4.1(3) provides the following enhancements:

- Upon admin login to the CAM web console, each session receives a randomly-generated token (CCA_TOKEN) which is appended to the login URL and all static links. For example, a link such as https://<cam-ip>/admin/authlist.jsp can no longer be accessed directly without the session token. Note that direct link access displays an error message but does not log the user out of the admin console. The user can simply click the browser's "Back" button to go back to the original page.
- The CAS web console login now presents a form-based login page instead of a basic HTTP browser-based popup dialog to authenticate the admin user to the CAS (similar to current CAM web console login).
- The Cisco NAC Appliance API (cisco_api.jsp) is further protected against crossovers from sessions initiated via the CAM admin console.

Proxy Support Enhancements

Starting with release 4.1(3), proxy-related enhancements enable you to configure the Clean Access Server to allow proxy support for user login sessions using the Unauthenticated role:

- Client machines requiring a preconfigured Proxy PAC (Proxy Auto Config) file to access network resources can now get the file via the CAS, rather than directly from a dedicated Enterprise Proxy server. Previously, allowing user access through the CAS to an Enterprise Proxy server would have required allowing all traffic for the Unauthenticated role, which does not allow all traffic by design.

  Note A Proxy PAC file is only required when the URL has the same IP address and port assignment as the proxy server. Otherwise, Cisco recommends using the existing IP or Host Traffic Policy to specify the Proxy PAC URL.

- You can now configure CAS Host Policies to validate users assigned to the Unauthenticated role using a proxy server, where before you could not.
- You can now redirect traffic to a login web page for HTTPS requests via a proxy server (previously was HTTP requests only).
- Port 80 is supported as the proxy port.

Note You must "exempt" the CAS from proxy settings. That is, client machines should access the CAS directly without passing traffic through a proxy server.

These enhancements affect the following pages of the CAM web console:

- **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Proxy—**new **PAC (Proxy Auto Config) file URL** field
- **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts**—updated **Parse Proxy Traffic** option (no longer excludes Unauthenticated Role)

ARP Broadcast Packet Handling Improvement

Release 4.1(3) features an ARP broadcast enhancement that helps alleviate erroneous ARP broadcast "re-broadcasting." When an ARP broadcast packet arrives at the untrusted eth1 interface on the CAS, the CAS now checks to verify the nature of the broadcast packet. If the destination IP address is a known IP address or a valid IP address as part of a managed subnet, the CAS "re-broadcasts" the packet on to the appropriate managed subnet. If the packet in question is an ARP broadcast itself (a request for the owner of *x.y.z*.255, for example), then the CAS does not forward/rebroadcast the request because no host on the managed subnet will be able to respond appropriately.

Therefore, the NAC Appliance system now performs as follows when we receive a broadcast message (with a broadcast destination IP address) at the trusted side of the CAS:

1. If the broadcast destination IP address is 255.255.255.255, NAC Appliance rebroadcasts the packet to all subnets on the untrusted side
2. If the broadcast destination IP address is the untrusted (eth1) interface's main subnet broadcast IP address, NAC Appliance rebroadcasts the packet to that subnet on the untrusted side
3. If the broadcast destination IP address is the broadcast IP address of one of the managed subnets on the untrusted (eth1) interface's managed subnet, rebroadcast the packet to that subnet on the untrusted side

Clean Access Server HA ARP Broadcast Enhancement

Release 4.1(3) features an ARP broadcast enhancement to improve Clean Access Server HA capabilities. In the event of a CAS failover, the HA-Secondary CAS (which assumes the HA-Primary role) now sends ARP request broadcast messages to all managed subnets on the untrusted (eth1) interface instead of just the primary subnet. These gratuitous ARPs help ensure that all clients on the untrusted side of the NAC Appliance network have a chance to update their ARP tables with the IP and MAC address of the new active CAS instead of first experiencing a session time-out and having to re-establish connection to the new active CAS.

Deprecated "Retag Trusted-side Egress Traffic with VLAN (In-Band)" Feature

The "Retag Trusted-side Egress Traffic with VLAN (In-Band)" feature for User Roles is deprecated in Release 4.1(3) and will be removed completely in a future release.

This affects the following page of the CAM web console:

- **User Management > User Roles > New Role | Edit Role**

Previously-Deprecated Features Removed from CAM/CAS Web Console Pages

The "Roaming" and "IPSec/L2TP/PPTP/PPP" features that have been deprecated in previous Cisco NAC Appliance releases now no longer appear in the web console interface for release 4.1(3). This change affects many pages of the CAM and CAS web user interfaces, most notably:

- The CAM web console **Device Management** node no longer features the **Roaming** menu item
- The CAS **Status** module list (**Device Management > CCA Servers > Manage [CAS_IP] > Status**) no longer features the **IPSec Server** category
- The CAS **Network** tab (**Device Management > CCA Servers > Manage [CAS_IP] > Network**) no longer features the **IPSec**, **L2TP**, **PPTP**, or **PPP** subtab headings
- The CAM **User Roles** list (**User Management > User Roles > List of Roles**) no longer features the **IPSec** or **Roam** column headings
- The CAM **User Roles** configuration screen list (**User Management > User Roles > List of Roles > Edit**) no longer features the **VPN Policy** dropdown menu, **Roam Policy** configuration radio buttons, or the **IPSec info** or **PPP info** options for the **Show Logged-on Users** display settings

- The CAM **Online Users** display options configuration page (**Monitoring > Online Users > Display Settings**) no longer features the **IPSec Key**, **IPSec Type**, or **Foreign CCA Server** options

Clean Access Agent Auto Remediation

Release 4.1(3) introduces a new configurable **Remediation Type[Manual | Automatic]** option when configuring Clean Access Agent Requirements for the following requirement types:

- Link Distribution
- AV Definition Update
- AS Definition Update
- Windows Update
- Launch Programs
- Windows Server Update Services

Choosing the **Manual Remediation Type** preserves the previous Agent behavior. The user has to click through each of the requirements using the **Next** button.

Choosing the **Automatic Remediation Type** sets the Agent to perform Auto Remediation. When Auto Remediation is configured, the Clean Access Agent automatically performs updates or launches required programs on the client after the user logs in.

During **Auto Remediation**, the Agent dialog displays only two buttons: **Details** and **Manual**. Clicking Details shows additional progress messages for the auto remediation. Clicking **Manual** changes the Agent back to Manual mode, where the user has to click through each requirement.

The auto-remediation actions the Agent performs depend on the requirement type, such as:

- Auto launching of URL in default browser for Link Distribution
- Auto-update of AV/AS definition files
- Auto launching of Windows Auto Update(s) (in background)
- Auto launching of programs for Launch Programs
- Auto installation of WSUS client updates

This enhancement affects the following pages of the CAM web console:

- **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement** (adds new fields **Remediation Type: [Manual | Automatic]/ Interval[] Secs/Retry Count []** to all requirement types except File Distribution and Local Check)

Note

- The Remediation Type configuration option is available for all Enforcement Types (Mandatory, Optional, Audit)
- File Distribution and Local Check requirement types do not support the new **Automatic** Remediation Type, and for these requirement types, the new **Remediation Type: [Manual | Automatic]/ Interval[] Secs/Retry Count []** entry does not appear at all on the UI.

Note For Download/Next/Cancel buttons, if the requirement is Mandatory, the “Next” button is disabled until the requirement is met.

Delay Agent Logoff on CAM/CAS

User logoff behavior for the Windows Clean Access Agent in In-Band deployments has been enhanced in release 4.1(3) to ensure that all scripts necessary to log the user out of the NAC Appliance system have had a chance to complete before the CAS restricts user traffic. The drawback of users not having had a chance to successfully log out of the CAM/CAS before Windows shuts down is that the user session may remain "active" on the CAM (the user ID and session information still appear in the **Monitoring > Online Users > View Online Users** display) and the user suffers connection issues the next time they attempt to connect to the network from the same client machine. To address this situation, the administrator can now configure a period of time to delay Agent logout from the CAS/CAM to ensure enough time to complete the logout script(s).

This enhancement affects the following page CAM web console:

- **Device Management > Clean Access > General Setup > Agent Login | Logoff Clean Access Agent users from network on their machine logoff or shutdown after <*x*> secs (for Windows & In-Band setup) option now reflects the capability to specify a delay for Agent logout**

64-bit Windows Operating System Agent Support

In release 4.1(3), the Windows Clean Access Agent and Cisco NAC Web Agent perform authentication only on 64-bit Windows Vista and Windows XP client operating systems.

Note The 4.1.3.0 Clean Access Agent performs authentication only for 64-bit Windows Vista and Windows XP client operating systems. Once the user is authenticated, the Agent does not perform posture assessment or remediation. To support 64-bit operating system Agents, the CAM and CAS must also be running release 4.1.2.1 or later. Because Cisco NAC Appliance provides authentication-only support for 64-bit operating system Agents, Nessus scanning via the Clean Access Agent does not perform posture assessment/remediation on the client machine.

Supported AV/AS Product List Enhancements (Version 67)

- See Clean Access Supported AV/AS Product List, page 32 for the latest AV/AS product charts.
- See Supported AV/AS Product List Version Summary, page 53 for details on each update to the list.

Out-of-Band Enhancements

Access to Authentication VLAN Change Detection Enhancement

Cisco NAC Appliance release 4.1(3) further enhances VLAN change detection mechanisms for Clean Access Agent machines in Out-of-Band (OOB) deployments to allow the client port to change from the Access to the Authentication VLAN without having to bounce the port.

Caution The Access to Authentication VLAN Change Detection feature should only be used for OOB deployments that require client DHCP IP refresh/renew. DHCP refresh/renew is configured under **Administration > User Pages > Login Page > List > Edit > General | Use web client to release and renew IP address when necessary (OOB)**. If your OOB deployment makes use of port bouncing, this feature is not needed and should not be configured.

This feature applies to the Clean Access Agent only and does not apply to web login or to the Cisco NAC Web Agent. This feature is designed to enhance support for the following deployments:

- L3 OOB (Real-IP or Virtual Gateway)
- L2 OOB Real IP Gateway
- L2 OOB Virtual Gateway with user-role based VLAN assignment

In OOB, when the user is logged out and the client port changes from the Access VLAN to the Authentication VLAN, the IP address for the client machine typically needs to change to coincide with the Authentication VLAN. In OOB, when the user is in the Access VLAN, the Clean Access Agent no longer communicates with the CAM or CAS, so the Agent is not aware when the CAM changes the VLAN for the client port. Although the CAM can bounce the port to change the IP address on the client, this solution is not recommended for IP Phone environments, as it can disrupt voice services.

Versions earlier than 4.1.3.0 of the Windows Clean Access Agent could only learn of a change from the Access VLAN to the Authentication VLAN once the current DHCP lease had expired and the client was forced to re-establish connection. With release 4.1(3), the Agent detects that the client has the wrong IP address for the current VLAN and automatically triggers an IP address change (release/renew) to maintain connection. No additional configuration on the CAM is required to use this enhancement.

Note This feature requires the user to have administrative privileges to the client machine. If the user does not have administrative privileges, then the Agent must be installed via the Clean Access Agent Stub service to ensure the Agent can perform an IP release/renew on the client.

Version 4.1.3.2 of the Windows Clean Access Agent modifies the Access to Authentication VLAN Change Detection feature as follows:

- The feature is turned off by default (version 4.1.3.1 and later)
- The Agent mechanism for detection changes from ARP to ICMP (ping) by default, and is configurable: ICMP, or ARP, or ICMP then ARP.
- There is a new retry detection interval which is configurable. The Agent retries gateway detection a default of 5 times before performing IP refresh.
- SWISS VLAN detection checks are enhanced to take multi-NIC configurations into account.
- **net dhcp stop/start** is turned off by default and is configurable with the 4.1.3.2 Agent. Only HKLM settings are now read instead of both HKCU and HKLM settings, and the registry settings will take effect after an Agent login.

Note

- When using ICMP, the client's default gateway must also allow ICMP responses to client pings.
- If the default gateway cannot accommodate responses to Agent ICMP requests, the client machine and the default gateway must be configured to use ARP.
- When using ARP with Windows XP and Windows 2000 client machines, use of the Clean Access Agent Stub is required, because standard users typically do not have privileges to alter the ARP cache.
- Cisco does not recommend configuring your system to use ARP for client-to-gateway communications, as it can generate unnecessary ARP traffic on the network.

Agent users with non-admin privileges and no Clean Access Agent Stub service installed on the client can use ICMP to detect the VLAN and then enable DHCP services (**net dhcp stop/start**) to change the client IP address. In order to utilize the option, however, you must configure a Group Policy Object (GPO) granting domain users full control of the DHCP client. Once DHCP control is enabled, the Agent attempts to restart the DHCP client to get a new IP address after failing IP address release/renew. See Table 5 for more information.

Note Agent versions 4.1.3.1 and 4.1.3.2 disable DHCP services (**net dhcp stop/start**) by default. Enabling this option may result in unexpected behavior, because the Agent refreshes IP addresses on all NICs, not just the one requiring refresh. Therefore, Agent IP refresh/renew is the preferred method for changing the client IP address.

Note Due to a characteristic of Windows 2000, users logged in with standard user privileges can take up to 15 minutes to refresh their IP address. Installing the Clean Access Agent Stub service does not resolve this issue.

This feature may not be compatible with all Cisco NAC Appliance deployments (such as VPN deployments). Therefore, although you can still enable and configure this feature, versions 4.1.3.1 and 4.1.3.2 of the Clean Access Agent disable this feature by default. Refer to Windows Clean Access Agent Version 4.1.3.1, page 27 and Windows Clean Access Agent Version 4.1.3.2, page 26 for additional details.

Access to Authentication VLAN Change Detection Interoperability with Clients Featuring More Than One Active NIC

If you use the Access to Authentication VLAN change detection feature on a client machine with more than one active NIC, all active NICs on the client use the feature. By design, the NIC with the lowest metric always takes precedence for routing purposes, and you can determine the metric using the `route print` command from a command prompt. Client-to-CAS communication depends on the specific scenario:

- If both active NICs are can simultaneously contact two different CASs, then the Port Profiles configured for the two CASs should feature the same port bouncing and/or IP refresh behavior.

  If one of the CASs is in Layer 2 OOB Virtual Gateway mode, and the client somehow switches back to the authentication VLAN (if the client is deleted form the Certified Device List, for example), then the client can no longer ping its default gateway. This situation can result in the client performing unnecessary, repetitive IP refreshes even though that NIC is not the one the client is currently using for traffic.

  If this configuration is required, you must configure a traffic policy on the CAM to allow ICMP traffic to the default gateway for the Unauthenticated Role.

- If one of the NICs connects to an In-Band CAS and the other connects to an Out-of-Band CAS, then both NICs should function properly whether the Access to Authentication VLAN change detection feature is required or not.

Configuring Registry Keys on the Windows Client

In order to configure a client machine with multiple NICs to appropriately interact with the Cisco NAC Appliance Access to Authentication VLAN detect feature, you must define the appropriate registry keys on the client, as shown in Table 5. The following required DWORD registry keys are all located in the same **HKEY_LOCAL_MACHINE\Software\Cisco\Clean Access Agent** registry location.

Table 5 Required DWORD Registry Key Settings for Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs

Registry Key	Default Value (Decimal)	Valid Range	Behavior
RetryDetection	5	Any	If ICMP or ARP polling fails, this setting configures the Agent to retry <*x*> times before refreshing the client IP address.
PingArp	0	0-2	• If this value is set to **0**, poll using ICMP. • If this value is set to **1**, poll using ARP. • If this value is set to **2**, poll using ICMP first, then (if ICMP fails) use ARP.
PingMaxTimeout	1	1-10	Poll using ICMP and if no response in <*x*> seconds, then declare ICMP polling failure.
DHCPServiceStartStop	0	Any	• If this setting is 0, do not perform DHCP services (**net dhcp stop/start**) when IP refresh fails with API. • If any value other than 0, perform DHCP services.
VlanDetectInterval	0	0, 5-60	• If this setting is **0**, the Access to Authentication VLAN change feature is disabled. • If this setting is **1-5**, the Agent sends ICMP/ARP queries every 5 seconds. • If this setting is **6-60**, ICMP/ARP every <*x*> seconds. (Any value greater than 60 seconds automatically reverts to 60.)

For more information on multiple-NIC client support, see Support for Clients with Multiple Active NICs, page 13.

SNMP Inform Notification Enhancement

SNMP notification behavior has been enhanced in release 4.1(3) to feature SNMP "inform request" behavior. Because SNMP traps can be unreliable due to the fact that the SNMP receiver is not required to send an acknowledgment when it receives a trap, the sender cannot determine if the trap was received. In release 4.1(3), the CAM is able to transmit SNMP inform acknowledgements in response to switch SNMP inform requests to ensure reliable information delivery between the switch and the CAM. (The inherent SNMP "inform request/acknowledgement" retry mechanism helps increase the chances of successful information delivery from the managed switch to the CAM.)

SNMP "MAC Move Notification" Switch Port Configuration Support

With release 4.1(3), Cisco NAC Appliance now supports the "MAC Move Notification" switch port configuration and notification feature. When the managed switch sends out a notification trap announcing that a connected host has moved from one port to another within the same VLAN, the CAM responds to the notification by updating the discovered client information and, if necessary, changing the VLAN assignment for the host port to reflect the information in the switch trap notification.

Releases earlier than 4.1(3) depend on "MAC Changed Notification" to detect the client device when it connects to the switch. From the notification, the switch learns a new MAC address on the port, and the Clean Access Manager learns from the switch what device is connected to which port. Based on this learned information, the CAM changes the VLAN for that switch port.

However, when the MAC Move Notification Trap is configured on the switch, the switch sends out the trap when a connected device moves from one port to another on the same VLAN. With CCA versions earlier than 4.1(3), the MAC Move Notification is not supported, and the CAM does not update connected device information when a MAC Move event occurs. As a result, CAM can end up incorrectly setting the VLAN on the switch port from which the device has already disconnected.

With release 4.1(3) and later, OOB deployments now support:

- Linkup/linkdown
- MAC change notification—when the switch learns a new MAC address on a managed port
- MAC move notification—when a device/host moves from one managed port to another

Cisco NAC Appliance Agent Enhancements

Windows Clean Access Agent Language Template Support Enhancement (Version 4.1.3.0)

Added Agent language template support for Dutch, Hungarian, and Portuguese for Windows Agents. The Agent will display localized text for these languages if run from localized Windows operating system.

Note The Agent picks the correct language template based on the local computer Locale (under Control Panel > Regional and Language Options). Cisco recommends using the localized Agent in the localized version of Windows (e.g. French Agent in French Windows). Agent language template support only controls what the viewer sees after the Agent is installed; it does not include support for different client operating systems for the Agent Installer or for AV/AS products.

Note If the administrator includes non-English text in the CAM configuration (e.g. non-English characters in a requirement description or registry value check), it may not be displayed correctly or run correctly.

See Cisco NAC Appliance Agents, page 25 for enhancement details per Agent version.

Cisco NAC Appliance Agents

This section consolidates information for Clean Access Agent and Cisco NAC Web Agent client software versions, as follows:

- Windows Clean Access Agent Enhancements, page 26
- Mac OS X Clean Access Agent Enhancements, page 29
- Cisco NAC Web Agent Enhancements, page 30

Enhancements are cumulative and apply both to the version introducing the feature and to subsequent later versions, unless otherwise noted. For all Agents:

- See Release 4.1(3) Compatibility Matrix and Release 4.1(3) Clean Access Agent Upgrade Compatibility Matrix, page 7 for compatibility details.
- See Clean Access Supported AV/AS Product List, page 32 for details on related AV/AS support.

Note Cisco strongly recommends running version 4.1.3.0 of the Clean Access Agent with release 4.1(3) and later of the CAM/CAS. However, administrators can optionally configure the 4.1(3) CAM/CAS to allow login and posture assessment from 4.1.0.x Agents. Refer to the "Supported AV/AS Product List Version Summary" of the applicable *Release Notes* for complete details on 4.1.0.x Agent AV/AS support.

Note See the "Clean Access Agent Version Summary" section in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) Version 4.1(2)* for details on the 4.1.2.x Agent.
See the "Clean Access Agent Version Summary" section in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) Version 4.1(1)* for details on the 4.1.1.0 Agent.

For additional details refer to Known Issues for Cisco NAC Appliance, page 86 and Troubleshooting, page 109 for Agent-related information.

Windows Clean Access Agent Enhancements

This section contains the latest enhancements per version of the Windows Clean Access Agent.

- Windows Clean Access Agent Version 4.1.3.2
- Windows Clean Access Agent Version 4.1.3.1
- Windows Clean Access Agent Version 4.1.3.0

Enhancements are cumulative and apply both to the version introducing the feature and to subsequent later versions, unless otherwise noted.

Windows Clean Access Agent Version 4.1.3.2

Version 4.1.3.2 of the Windows Clean Access Agent resolves caveats CSCsl77778 CSCsl77801, CSCsm04923, CSCsm38529, CSCsm39238, CSCsm54763, CSCsm42572, CSCsm62326, CSCsm67052, and CSCso22399. Refer to Resolved Caveats - Windows Clean Access Agent 4.1.3.2, page 65 for additional details.

New features or enhancements for Windows Clean Access Agent version 4.1.3.2 (persistent):

- Version 4.1.3.2 of Windows the Clean Access Agent modifies the Access to Authentication VLAN Change Detection feature as follows:
  - The feature is turned off by default (version 4.1.3.1 and later)
  - The Agent mechanism for detection changes from ARP to ICMP (ping) by default, and is configurable: ICMP, or ARP, or ICMP and ARP.
  - There is a new retry detection interval which is configurable. The Agent retries CAS detection a default of 5 times before performing IP refresh.
  - SWISS VLAN detection checks are enhanced so that VLAN change detection is not performed for 0.0.0.0, IP address = default gateway (VPN), or auto-assigned IP address deployments.

- **net dhcp stop/start** is turned off by default and is configurable with the 4.1.3.2 Agent. HKLM settings are now used instead of HKCU settings, and the registry settings will take effect after an Agent login.

Note See Table 5 under Access to Authentication VLAN Change Detection Enhancement, page 21 for details on the registry settings required to configure the Windows client for Access to Authentication VLAN change detection.

- Enhancements to Support for Clients with Multiple Active NICs, page 13
- Enhancements to Access to Authentication VLAN Change Detection Enhancement, page 21 (including new "Access to Authentication VLAN Change Detection Interoperability with Clients Featuring More Than One Active NIC" section on page 23)
- Added language template support for Russian, Turkish, and Serbian (Cyrillic) for Windows Agents.

Supported AV/AS Product List Enhancements (Version 68)

- See Clean Access Supported AV/AS Product List, page 32 for the latest AV/AS product charts.
- See Supported AV/AS Product List Version Summary, page 53 for details on each update to the list.

Windows Clean Access Agent Version 4.1.3.1

Version 4.1.3.1 of the Windows Clean Access Agent resolves caveat CSCsm05207. Refer to Resolved Caveats - Windows Clean Access Agent 4.1.3.1, page 73 and Access to Authentication VLAN Change Detection Enhancement, page 21 for additional details.

Note **MSI Package Installation:**

- When using MSI package installation/upgrade for the Clean Access Agent, minor version (4th digit) upgrades are affected by caveat CSCsm20655, page 64. Refer to the workaround for details.
- Also refer Known Issues with MSI Agent Installer, page 89 before downloading the MSI installer for the full Agent from Cisco Secure Downloads.

Windows Clean Access Agent Version 4.1.3.0

New features or enhancements for Windows Agent version 4.1.3.0 (persistent):

- Agent behavior supports multiple active NICs on the client machine. See Support for Clients with Multiple Active NICs, page 13 for details.
- User logoff behavior via the Windows Clean Access Agent has been enhanced to ensure that all scripts necessary to log the user out of the Cisco NAC Appliance system have had a chance to complete before the CAS restricts user traffic. See Delay Agent Logoff on CAM/CAS, page 21 for details.
- In an OOB environment, the Agent can detect the VLAN change and switch from the Access to the Authentication VLAN automatically. See Access to Authentication VLAN Change Detection Enhancement, page 21 for details.
- You can configure the Agent to delay a specified period of time before performing VPN SSO. See VPN SSO Login Enhancement, page 16 for details.

- Windows Clean Access Agents support requirement types that the administrator configures to employ automatic remediation. See Clean Access Agent Auto Remediation, page 20 for details.
- Added language template support for Dutch, Hungarian, and Portuguese for Windows Agents.
- Support for Stub installer on Windows Vista operating system.

Note For checks/rules/requirements, the Agent can detect "N" (European) versions of the Windows Vista operating system, but the CAM/CAS treat "N" versions of Vista as their US counterpart.

Note When installing the 4.1.3.0 Clean Access Agent via stub installation on Windows Vista machines only, Cisco recommends **not** to use the **Full UI** Stub Installation Option. To avoid the appearance of 5-minute installation dialog delays caused by the Vista Interactive Service Detection Service, do not use the **No UI** or **Reduced UI** option when configuring Stub Installation Options for Windows Vista client machines.

Note When non-admin users install/uninstall the Agent through stub service on Windows Vista, they will see an "Interactive Services Dialog Detection" dialog. If the user is installing, no input is required in the dialog session—it will automatically disappear. If the client machine is fast, the user may not even see the dialog appear at all, so the resulting behavior is as if the Agent gets silently installed after a few seconds. When uninstalling, however, the uninstall process does not complete until the user responds to a prompt inside the dialog.

This is expected behavior because, unlike earlier Windows operating systems, Windows Vista services run in an isolated session (session 0) from user sessions, and thus do not have access to video drivers. As a workaround for interactive services like the Agent stub installer, Windows Vista uses an Interactive Service Detection Service to prompt users for user input for interactive services and enable access to dialogs created by interactive services. The "Interactive Service Detection Service" will automatically launch by default and, in most cases, users are not required to do anything. If the service is disabled for some reason, however, Agent installation by non-admin users will not function.

For more information on the stub installer and its behavior, see the "Configuring Agent Distribution/Installation" section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(3)*. See also Known Issues with MSI Agent Installer, page 89.

- Performs authentication on 64-bit Windows Vista and Windows XP client operating systems. See 64-bit Windows Operating System Agent Support, page 21 for details.

Note The 4.1.3.0 Agent performs authentication only for 64-bit Windows Vista and Windows XP client operating systems. Once the user is authenticated, the Agent does not perform posture assessment or remediation. To support 64-bit operating system Agents, the CAM and CAS must also be running release 4.1.2.1 or later. Because Cisco NAC Appliance provides authentication-only support for 64-bit operating system Agents, nessus scanning via the Clean Access Agent does not perform remediation on the client machine.

Mac OS X Clean Access Agent Enhancements

This section contains the latest enhancements per version of the Mac OS X Clean Access Agent:

- Mac OS X Clean Access Agent Version 4.1.3.1
- Mac OS X Clean Access Agent Version 4.1.3.0

Enhancements are cumulative and apply both to the version introducing the feature and to subsequent later versions, unless otherwise noted.

Note Cisco NAC Appliance supports basic web login on Macintosh operating systems—whether Mac OS X, iPhone, or iPod Touch—as long as clients use Safari or Firefox browsers. Refer to *Supported Hardware and System Requirements for Cisco NAC Appliance (Clean Access)* for additional details.

Mac OS X Clean Access Agent Version 4.1.3.1

Version 4.1.3.1 of the Clean Access Agent resolves caveats CSCsl83353, CSCsl88985, CSCsl98060, CSCsm10311, CSCsm20813, CSCsm26806, and CSCsm47276 for Mac OS X Agents. Refer to Resolved Caveats - Mac OS X Agent 4.1.3.1, page 68 for additional details.

Mac OS X Clean Access Agent Version 4.1.3.0

New features or enhancements in Macintosh OS X Clean Access Agent version 4.1.3.0:

- Mac Agent directory has been changed from **/Library/Application Support/Cisco Systems/** folder to **/Applications/** folder. See also Generate Mac OS X Agent Debug Log, page 114 for additional details.
- Mac Agent logo and status icons have been redesigned. For details, see the “Cisco NAC Appliance Agents” chapter in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(3)*.
- The Mac OS X Agent features auto-upgrade for version 4.1.3.0 and later. During user login, when the 4.1.3.0 Mac Agent is in the process of establishing a connection to the CAS (SWISS UDP packet exchange), the Agent currently installed on the Mac client machine determines whether or not a newer version of the Mac OS X Clean Access Agent is available and, if so, automatically begins downloading and installing the newer Agent version. Once installed and initiated, the set-up process requires only very little user interaction. Once completely installed, the newer version of the Agent launches automatically.
- Mac OS X Agent version 4.1.3.0 features login support for Macintosh users running Mac OS X version 10.5 and 10.5.1 (“Leopard”).

  Note You must install release 4.1(3) on your CAM and CAS to enable Mac OS X version 10.5 or 10.5.1 users to access the network via Cisco NAC Appliance. Mac OS X version 10.5 and 10.5.1 users cannot log into earlier releases of Cisco NAC Appliance due to a mismatch in NIC MAC address identification from the client machine.

- Agent behavior supports multiple active NICs on the client machine. See Support for Clients with Multiple Active NICs, page 13 for details.

- In an OOB environment, the Agent can detect the VLAN change from the Access to the Authentication VLAN automatically. See Access to Authentication VLAN Change Detection Enhancement, page 21.
- VLAN change can be configured so the Agent will display a count down progress bar for the login until the delay times out.
- You can configure the Agent to delay a specified period of time before performing VPN SSO. See VPN SSO Login Enhancement, page 16

Cisco NAC Web Agent Enhancements

This section contains the latest enhancements per version of the Cisco NAC Web Agent:

- Cisco NAC Web Agent Version 4.1.3.10
- Cisco NAC Web Agent Version 4.1.3.9

Enhancements are cumulative and apply both to the version introducing the feature and to subsequent later versions, unless otherwise noted.

See Release 4.1(3) Compatibility Matrix, page 6 for general compatibility details.

Cisco NAC Web Agent Version 4.1.3.10

For release 4.1(3) and later, new versions of the Cisco NAC Web Agent are available from the Clean Access Manager via the Updates mechanism (**Device Management > Clean Access > Updates > Update**). If use of the Cisco NAC Web Agent is required for the role, users will automatically download the latest version that is available on the CAM. If you do not want to distribute the latest version of the Web Agent, you can deselect the “Check for Cisco NAC Web Agent updates” checkbox on the **Updates** page.

New features or enhancements for Windows Agent version 4.1.3.10:

- Signed Certificate Requirements
- Resolves caveats CSCsm03961 and CSCsm17435. See Resolved Caveats - Cisco NAC Web Agent 4.1.3.10, page 72.
- For general Web Agent system requirements, refer to Cisco NAC Web Agent Version 4.1.3.9

Signed Certificate Requirements

For version 4.1.3.10, the ActiveX control and Java Applet are signed by a certificate (“Cisco Systems”) which is signed by “Thawte Server CA,” and should be included in the Trusted Root Certificate Authority store.

If the certificate is not included in the Trusted Root Certificate Authority store, users will see a security alert dialog whenever they launch the Cisco NAC Web Agent. The dialog indicates a secure connection is required, but the certificate issuer is untrusted or unknown. The user can accept the certificate for this session, or install this certificate in the certificate store.

To install the certificate:

Step 1 During the login session, users can select **View Certificate** from the **Security Alert** (or similar) dialog.

Step 2 Select the **Certificate Path** tab.

Step 3 Select the “www.perfigo.com” certificate entry and click **View Certificate**.

Step 4 In the configuration wizard, click **Install Certificate** to launch the certificate wizard.

Step 5 In the wizard introduction page, click **Next**.

Step 6 In the wizard "Certificate Store" page, choose the **Automatically select...** radio button, click **Next**, and then click **Finish**. (If you are prompted to confirm the import, click **Yes**.)

For additional information, see also Vista/IE 7 Certificate Revocation List, page 110.

Cisco NAC Web Agent Version 4.1.3.9

Release 4.1(3) introduces the new (temporal) Cisco NAC Web Agent version 4.1.3.9.

Refer to Cisco NAC Web Agent, page 12 for feature details.

Versions 4.1.3.9 and later of the Cisco NAC Web Agent have the following system requirements:

- Operating System Dependencies
- Browser Support
- ActiveX and Java Applet Requirements
- Microsoft Internet Explorer 7 in Windows Vista

Operating System Dependencies

You can install and launch the Cisco NAC Web Agent on the following operating systems:

- Windows 2000 (Service Packs 4 and 6)
- Windows XP Professional/Home (Service Packs 1 and 2)
- Windows Vista Home Premium/Ultimate (authentication only)

Note Security restrictions for the "Guest" user profile in Windows Vista operating systems prevent ActiveX controls and Java applets from running properly. Therefore, you must be logged into the Windows Vista client machine as a known user (not a "Guest") in order to log into Cisco NAC Appliance via the Web Agent.

Browser Support

You can install and launch the Cisco NAC Web Agent from the following web browsers:

- Microsoft Internet Explorer versions 6 or 7 (ActiveX or Java applet)
- Firefox versions 1.5 or 2.0 (Java applet only)

ActiveX and Java Applet Requirements

- If you plan to use the Java applet version to install the Web Agent files, the client must already have Java version 1.4.2 or higher installed.
- If you plan to install the Web Agent files via ActiveX, the client machine must be using Microsoft Internet Explorer. You cannot install via ActiveX on a Firefox web browser.
- The user must have permissions for ActiveX download or admin privileges on the client machine to enable installation of ActiveX controls.

Note The Web Agent Java applet might fail to launch when the CPU load on the client machine approaches 100%. (ActiveX runs successfully under these conditions.)

Microsoft Internet Explorer 7 in Windows Vista

By default, Windows Vista checks the server certificate revocation list and prevents the Web Agent from launching on the client machine.

To disable this functionality:

Step 1 In Internet Explorer 7, navigate to **Menu > Tools > Internet Options**.

Step 2 Click the **Advanced** tab.

Step 3 Under Security, uncheck (disable) the **Check for server certificate revocation** option.

Step 4 Click **OK**.

For additional information, see also Vista/IE 7 Certificate Revocation List, page 110.

Clean Access Supported AV/AS Product List

This section describes the Supported AV/AS Product List that is downloaded to the Clean Access Manager via **Device Management > Clean Access > Updates > Update** to provide the latest antivirus (AV) and anti-spyware (AS) product integration support for Cisco NAC Appliance Agents that support AV/AS posture assessment/remediation. The Supported AV/AS Product List is a versioned XML file distributed from a centralized update server that provides the most current matrix of supported AV/AS vendors and product versions used to configure AV/AS Rules and AV/AS Definition Update requirements.

The Supported AV/AS Product List contains information on which AV/AS products and versions are supported in each Windows Clean Access Agent release along with other relevant information. It is updated regularly to bring the relevant information up to date and to include newly added products for new releases. Cisco recommends keeping your list current, especially when you upload a new Agent Setup version or Agent Patch version to your CAM. Having the latest Supported AV/AS list ensures your AV/AS rule configuration pages list all the new products supported in the new Agent.

Note Cisco recommends keeping your Supported AV/AS Product List up-to-date on your CAM by configuring the **Update Settings** under **Device Management > Clean Access > Updates > Update** to **Automatically check for updates starting from** <*x*> **every** <*y*> **hours**.

The following charts list the AV and AS product/version support per client OS as of the latest Clean Access release:

- Clean Access AV Support Chart (Windows Vista/XP/2000), page 33
- Clean Access AV Support Chart (Windows ME/98), page 45
- Clean Access AS Support Chart (Windows Vista/XP/2000), page 47

The charts show which AV/AS product versions support virus or spyware definition checks and automatic update of client virus/spyware definition files via the user clicking the Update button on the Clean Access Agent.

For a summary of the product support that is added per version of the Supported AV/AS Product List or Clean Access Agent, see also:

- Cisco NAC Appliance Agents, page 25
- Supported AV/AS Product List Version Summary, page 53

You can access additional AV and AS product support information from the CAM web console under **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**.

Note Where possible, Cisco recommends using AV Rules mapped to AV Definition Update Requirements when checking antivirus software on clients, and AS Rules mapped to AS Definition Update Requirements when checking anti-spyware software on clients. In the case of non-supported AV or AS products, or if an AV/AS product/version is not available through AV Rules/AS Rules, administrators always have the option of creating their own custom checks, rules, and requirements for the AV/AS vendor (and/or using Cisco provided pc_ checks and pr_rules) through **Device Management > Clean Access > Clean Access Agent** (use New Check, New Rule, and New File/Link/Local Check Requirement). See the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(3)* for configuration details.

Note that Clean Access works in tandem with the installation schemes and mechanisms provided by supported AV/AS vendors. In the case of unforeseen changes to underlying mechanisms for AV/AS products by vendors, the Cisco NAC Appliance team will update the Supported AV/AS Product List and/or Clean Access Agent in the timeliest manner possible in order to support the new AV/AS product changes. In the meantime, administrators can always use the “custom” rule workaround for the AV/AS product (such as pc_checks/pr_ rules) and configure the requirement for “Any selected rule succeeds.”

Clean Access AV Support Chart (Windows Vista/XP/2000)

Table 6 lists Windows Vista/XP/2000 Supported AV Products as of the latest release of the Cisco NAC Appliance software. (See Table 7 for Windows ME/98).

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 1 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
AEC, spol. s r.o.				
TrustPort Antivirus	2.x	yes (4.0.6.0)	-	yes
AhnLab, Inc.				
AhnLab Security Pack	2.x	yes (3.5.10.1)	yes (3.5.10.1)	yes
AhnLab V3 Internet Security 2007	7.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
AhnLab V3 Internet Security 2007 Platinum	7.x	yes (3.6.5.0)	yes (3.6.5.0)	yes
AhnLab V3 Internet Security 2008 Platinum	7.x	yes (4.1.3.0)	yes (4.1.3.0)	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 2 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
AhnLab V3 Internet Security 7.0 Platinum Enterprise	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
V3Pro 2004	6.x	yes (3.5.10.1)	yes (3.5.12)	yes
V3 VirusBlock 2005	6.x	yes (4.1.2.0)	yes (4.1.2.0)	-
ALWIL Software				
avast! Antivirus	4.x	yes (3.5.10.1)	yes (3.5.10.1)	yes
avast! Antivirus (managed)	4.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
avast! Antivirus Professional	4.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
America Online, Inc.				
Active Virus Shield	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
AOL Safety and Security Center Virus Protection	102.x	yes (4.0.4.0)	yes (4.0.4.0)	-
AOL Safety and Security Center Virus Protection	1.x	yes (3.5.11.1)	yes (3.5.11.1)	-
AOL Safety and Security Center Virus Protection	210.x	yes (4.0.4.0)	yes (4.0.4.0)	-
AOL Safety and Security Center Virus Protection	2.x	yes (4.1.0.0)	yes (4.1.0.0)	-
Authentium, Inc.				
Command Anti-Virus Enterprise	4.x	yes (3.5.0)	yes (3.5.0)	yes
Command AntiVirus for Windows	4.x	yes (3.5.0)	yes (3.5.0)	yes
Command AntiVirus for Windows Enterprise	4.x	yes (3.5.2)	yes (3.5.2)	yes
Cox High Speed Internet Security Suite	3.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
AVG Technologies				
AVG 8.0 [AntiVirus]	8.x	yes (4.1.3.2)	-	yes
Avira GmbH				
Avira AntiVir PersonalEdition Classic	7.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Avira AntiVir PersonalEdition Premium	7.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Avira AntiVir Windows Workstation	7.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Avira Premium Security Suite	7.x	yes (3.6.5.0)	yes (3.6.5.0)	yes
Beijing Rising Technology Corp. Ltd.				
Rising Antivirus Software AV	17.x	yes (3.5.11.1)	yes (3.5.11.1)	yes
Rising Antivirus Software AV	18.x	yes (3.5.11.1)	yes (3.5.11.1)	yes
Rising Antivirus Software AV	19.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
Rising Antivirus Software AV	20.x	yes (4.1.3.0)	yes (4.1.3.0)	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 3 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
BellSouth				
BellSouth Internet Security Anti-Virus	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
BullGuard Ltd.				
BullGuard 7.0	7.x	yes (4.1.2.0)	yes (4.1.2.0)	-
BullGuard 8.0	8.x	yes (4.1.3.2)	yes (4.1.3.2)	-
Cat Computer Services Pvt. Ltd.				
Quick Heal AntiVirus Lite	9.5.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Quick Heal AntiVirus Plus	9.5.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Check Point, Inc				
ZoneAlarm Anti-virus	7.0.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
ZoneAlarm Anti-virus	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
ZoneAlarm (AntiVirus)	7.0.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
ZoneAlarm (AntiVirus)	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
ZoneAlarm Security Suite Antivirus	7.0.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
ZoneAlarm Security Suite Antivirus	7.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
ClamAV				
ClamAV	devel-x	yes (4.0.6.0)	yes (4.0.6.0)	yes
ClamWin				
ClamWin Antivirus	0.x	yes (3.5.2)	yes (3.5.2)	yes
ClamWin Free Antivirus	0.x	yes (3.5.4)	yes (3.5.4)	yes
Computer Associates International, Inc.				
CA Anti-Virus	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
CA Anti-Virus	9.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
CA eTrust Antivirus	7.x	yes (3.5.0)	yes (3.5.0)	yes
CA eTrust Internet Security Suite AntiVirus	7.x	yes (3.5.11)	yes (3.5.11)	yes
CA eTrustITM Agent	8.x	yes (3.5.12)	yes (3.5.12)	yes
eTrust Antivirus	6.0.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
eTrust EZ Antivirus	6.1.x	yes (3.5.3)	yes (3.5.8)	yes
eTrust EZ Antivirus	6.2.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Antivirus	6.4.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Antivirus	7.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Armor	6.1.x	yes (3.5.0)	yes (3.5.8)	yes
eTrust EZ Armor	6.2.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
eTrust EZ Armor	7.x	yes (3.5.0)	yes (3.5.0)	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 4 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Defender Pro LLC				
Defender Pro Anti-Virus	5.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
EarthLink, Inc.				
Aluria Security Center AntiVirus	1.x	yes (4.1.0.0)	yes (4.1.0.0)	-
EarthLink Protection Control Center AntiVirus	1.x	yes (3.5.10.1)	yes (3.5.10.1)	-
EarthLink Protection Control Center AntiVirus	2.x	yes (4.0.5.1)	yes (4.0.5.1)	-
EarthLink Protection Control Center AntiVirus	3.x	yes (4.1.3.0)	yes (4.1.3.0)	-
eEye Digital Security				
eEye Digital Security Blink Personal	3.x	yes (4.0.6.0)	yes (4.0.6.0)	yes
eEye Digital Security Blink Professional	3.x	yes (4.0.6.0)	yes (4.0.6.0)	-
Eset Software				
ESET NOD32 Antivirus	3.x	yes (4.1.3.2)	yes (4.1.3.2)	-
NOD32 antivirus system	2.x	yes (3.5.5)	yes (3.5.5)	yes
NOD32 antivirus system	x	yes (4.1.3.2)	yes (4.1.3.2)	yes
NOD32 antivirus System	x	yes (4.1.3.2)	yes (4.1.3.2)	yes
NOD32 Antivirus System	x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Fortinet Inc.				
FortiClient Consumer Edition	3.x	yes (4.0.6.0)	yes (4.0.6.0)	yes
Frisk Software International				
F-PROT Antivirus for Windows	6.0.x	yes (4.0.5.1)	yes (4.0.5.1)	-
F-Prot for Windows	3.14e	yes (3.5.0)	yes (3.5.0)	yes
F-Prot for Windows	3.15	yes (3.5.0)	yes (3.5.0)	yes
F-Prot for Windows	3.16c	yes (3.5.11)	yes (3.5.11)	yes
F-Prot for Windows	3.16d	yes (3.5.11)	yes (3.5.11)	yes
F-Prot for Windows	3.16x	yes (3.5.11.1)	yes (3.5.11.1)	yes
F-Secure Corp.				
F-Secure Anti-Virus	5.x	yes (3.5.0)	yes (3.5.0)	yes
F-Secure Anti-Virus	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
F-Secure Anti-Virus	7.x	yes (4.0.4.0)	yes (4.0.4.0)	-
F-Secure Anti-Virus 2005	5.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
F-Secure Anti-Virus Client Security	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
F-Secure Anti-Virus for Windows Servers	5.x	yes (4.1.3.2)	yes (4.1.3.2)	-

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 5 of 12)

		AV Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Virus Definition**	**Live Update** [2, 3]
F-Secure Internet Security	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
F-Secure Internet Security	7.x	yes (4.0.4.0)	yes (4.0.4.0)	-
F-Secure Internet Security 2005	5.x	yes (4.1.3.0)	yes (4.1.3.0)	-
F-Secure Internet Security 2006 Beta	6.x	yes (3.5.8)	yes (3.5.8)	yes
GData Software AG				
AntiVirusKit 2006	2006.x	yes (4.1.0.0)	yes (4.1.0.0)	-
G DATA AntiVirus 2008	18.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
G DATA AntiVirusKit	17.x	yes (4.1.3.0)	yes (4.1.3.0)	-
G DATA InternetSecurity [Antivirus]	17.x	yes (4.1.3.0)	yes (4.1.3.0)	-
G DATA InternetSecurity [Antivirus]	18.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
G DATA TotalCare [Antivirus]	18.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Grisoft, Inc.				
Antivirussystem AVG 6.0	6.x	yes (3.5.0)	yes (3.5.0)	-
AVG 6.0 Anti-Virus - FREE Edition	6.x	yes (3.5.0)	yes (3.5.0)	-
AVG 6.0 Anti-Virus System	6.x	yes (3.5.0)	yes (3.5.0)	-
AVG 7.5	7.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
AVG Antivirensystem 7.0	7.x	yes (3.5.0)	yes (3.5.0)	yes
AVG Anti-Virus 7.0	7.x	yes (3.5.0)	yes (3.5.0)	yes
AVG Anti-Virus 7.1	7.x	yes (3.6.3.0)	yes (3.6.3.0)	yes
AVG Free Edition	7.x	yes (3.5.0)	yes (3.5.0)	yes
HAURI, Inc.				
ViRobot Desktop	5.0.x	yes (4.0.5.1)	yes (4.0.5.1)	-
ViRobot Desktop	5.x	yes (4.1.3.0)	yes (4.1.3.0)	-
H+BEDV Datentechnik GmbH				
AntiVir PersonalEdition Classic Windows	7.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
AntiVir/XP	6.x	yes (3.5.0)	yes (3.5.0)	yes
IKARUS Software GmbH				
IKARUS Guard NT	2.x	yes (4.0.6.0)	yes (4.0.6.0)	-
IKARUS virus utilities	5.x	yes (4.0.6.0)	yes (4.0.6.0)	-
Internet Security Systems, Inc.				
Proventia Desktop	8.x	yes (4.0.6.0)	-	-
Proventia Desktop	9.x	yes (4.0.6.0)	yes (4.0.6.0)	-
Jiangmin, Inc.				
Jiangmin AntiVirus KV2007	10.x	yes (4.1.3.0)	-	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 6 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Kaspersky Labs				
Kaspersky Anti-Virus 2006 Beta	6.0.x	yes (3.5.8)	yes (3.5.8)	-
Kaspersky Anti-Virus 6.0	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Kaspersky Anti-Virus 6.0 Beta	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Kaspersky Anti-Virus 7.0	7.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Kaspersky Anti-Virus for Windows File Servers	5.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Kaspersky Anti-Virus for Windows File Servers	6.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Kaspersky Anti-Virus for Windows Servers	6.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Kaspersky Anti-Virus for Windows Workstations	5.0.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Kaspersky Anti-Virus for Windows Workstations	6.x	yes (4.0.6.0)	yes (4.0.6.0)	yes
Kaspersky Anti-Virus for Workstation	5.0.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Kaspersky Anti-Virus Personal	4.5.x	yes (3.5.0)	yes (3.5.0)	yes
Kaspersky Anti-Virus Personal	5.0.x	yes (3.5.0)	yes (3.5.0)	yes
Kaspersky Anti-Virus Personal Pro	5.0.x	yes (3.5.11)	yes (3.5.11)	yes
Kaspersky Internet Security	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Kaspersky Internet Security 7.0	7.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Kaspersky Internet Security 8.0	8.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Kaspersky(TM) Anti-Virus Personal 4.5	4.5.x	yes (3.5.0)	yes (3.5.0)	yes
Kaspersky(TM) Anti-Virus Personal Pro 4.5	4.5.x	yes (3.5.0)	yes (3.5.0)	yes
Kingsoft Corp.				
Kingsoft AntiVirus 2004	2004.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Kingsoft AntiVirus 2007 Free	2007.x	yes (4.1.3.2)	yes (4.1.3.2)	-
Kingsoft Internet Security	7.x	yes (3.6.5.0)	yes (3.6.5.0)	yes
Kingsoft Internet Security 2006 +	2006.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
McAfee, Inc.				
McAfee VirusScan Enterprise	8.x	yes (3.6.5.0)	yes (3.6.5.0)	yes
McAfee VirusScan Home Edition	7.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
McAfee VirusScan Professional	8.x	yes (3.5.1)	yes (3.5.1)	yes
McAfee VirusScan Professional	8xxx	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Professional	9.x	yes (3.5.1)	yes (3.5.1)	yes
McAfee VirusScan Professional Edition	7.x	yes (3.5.0)	yes (3.5.0)	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 7 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Total Protection for Small Business	4.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
McAfee Internet Security 6.0	8.x	yes (3.5.4)	yes (3.5.4)	yes
McAfee Managed VirusScan	3.x	yes (3.5.8)	yes (3.5.8)	yes
McAfee Managed VirusScan	4.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
McAfee VirusScan	10.x	yes (3.5.4)	yes (3.5.4)	yes
McAfee VirusScan	11.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
McAfee VirusScan	12.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
McAfee VirusScan	4.5.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan	8.x	yes (3.5.1)	yes (3.5.1)	yes
McAfee VirusScan	8xxx	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan	9.x	yes (3.5.1)	yes (3.5.1)	yes
McAfee VirusScan	9xxx	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Enterprise	7.0.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Enterprise	7.1.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Enterprise	7.5.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Enterprise	8.0.x	yes (3.5.0)	yes (3.5.0)	yes
Microsoft Corp.				
Microsoft Forefront Client Security	1.5.x	yes (4.0.5.0)	yes (4.0.5.0)	-
Windows Live OneCare	1.x	yes (4.1.0.0)	yes (4.1.0.0)	-
Windows Live OneCare	2.x	yes (4.1.3.2)	yes (4.1.3.2)	-
Windows OneCare Live	0.8.x	yes (3.5.11.1)	-	-
MicroWorld				
eScan Anti-Virus (AV) for Windows	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
eScan Corporate for Windows	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
eScan Internet Security for Windows	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
eScan Professional for Windows	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
eScan Virus Control (VC) for Windows	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Norman ASA				
Norman Virus Control	5.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Panda Software				
Panda Antivirus 2007	2.x	yes (4.0.4.0)	yes (4.0.4.0)	-
Panda Antivirus 2008	3.x	yes (4.0.6.1)	yes (4.0.6.1)	-
Panda Antivirus 6.0 Platinum	6	yes (3.5.0)	yes (3.5.0)	yes
Panda Antivirus + Firewall 2007	6.x	yes (4.0.4.0)	yes (4.0.4.0)	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 8 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Panda Antivirus + Firewall 2008	7.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Panda Antivirus Lite	1.x	yes (3.5.0)	yes (3.5.0)	-
Panda Antivirus Lite	3.x	yes (3.5.9)	yes (3.5.9)	-
Panda Antivirus Platinum	7.04.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Antivirus Platinum	7.05.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Antivirus Platinum	7.06.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Client Shield	4.x	yes (4.0.4.0)	yes (4.0.4.0)	-
Panda Internet Security 2007	11.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
Panda Internet Security 2008	12.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
Panda Platinum 2005 Internet Security	9.x	yes (3.5.3)	yes (3.5.3)	yes
Panda Platinum 2006 Internet Security	10.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
Panda Platinum Internet Security	8.03.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Titanium 2006 Antivirus + Antispyware	5.x	yes (3.5.10.1)	yes (3.5.10.1)	yes
Panda Titanium Antivirus 2004	3.00.00	yes (3.5.0)	yes (3.5.0)	yes
Panda Titanium Antivirus 2004	3.01.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Titanium Antivirus 2004	3.02.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Panda Titanium Antivirus 2005	4.x	yes (3.5.1)	yes (3.5.1)	yes
Panda TruPrevent Personal 2005	2.x	yes (3.5.3)	yes (3.5.3)	yes
Panda TruPrevent Personal 2006	3.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
WebAdmin Client Antivirus	3.x	yes (3.5.11)	yes (3.5.11)	-
PC Tools Software				
PC Tools AntiVirus 2.0	2.x	yes (4.1.3.0)	yes (4.1.3.0)	-
PC Tools AntiVirus 2007	3.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
PC Tools AntiVirus 2008	4.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
PC Tools Internet Security [Antivirus]	5.x	yes (4.1.3.0)	yes (4.1.3.0)	-
PC Tools Spyware Doctor [Antivirus]	5.x	yes (4.1.3.2)	-	-
Spyware Doctor [Antivirus]	5.x	yes (4.1.3.2)	yes (4.1.3.2)	-
ThreatFire 3.0	3.x	yes (4.1.3.0)	-	-
Radialpoint Inc.				
Radialpoint Security Services Virus Protection	6.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Radialpoint Virus Protection	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
Zero-Knowledge Systems Radialpoint Security Services Virus Protection	6.x	yes (4.0.5.1)	yes (4.0.5.1)	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 9 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
SalD Ltd.				
Dr.Web	4.32.x	yes (3.5.0)	yes (3.5.0)	yes
Dr.Web	4.33.x	yes (3.5.11.1)	yes (3.5.11.1)	yes
Dr.Web	4.44.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Sereniti, Inc.				
Sereniti Antivirus	1.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
The River Home Network Security Suite	1.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
SOFTWIN				
BitDefender 8 Free Edition	8.x	yes (3.5.8)	yes (3.5.8)	-
BitDefender 8 Professional Plus	8.x	yes (3.5.0)	yes (3.5.0)	-
BitDefender 8 Standard	8.x	yes (3.5.0)	yes (3.5.0)	-
BitDefender 9 Internet Security AntiVirus	9.x	yes (3.5.11.1)	yes (3.5.11.1)	-
BitDefender 9 Professional Plus	9.x	yes (3.5.8)	yes (3.5.8)	yes
BitDefender 9 Standard	9.x	yes (3.5.8)	yes (3.5.8)	yes
BitDefender Antivirus 2008	11.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
BitDefender Antivirus Plus v10	10.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
BitDefender Antivirus v10	10.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
BitDefender Client Professional Plus	8.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
BitDefender Free Edition	7.x	yes (3.5.0)	yes (3.5.0)	-
BitDefender Free Edition v10	10.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
BitDefender Internet Security 2008	11.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
BitDefender Internet Security v10	10.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
BitDefender Professional Edition	7.x	yes (3.5.0)	yes (3.5.0)	-
BitDefender Standard Edition	7.x	yes (3.5.0)	yes (3.5.0)	-
BitDefender Total Security 2008	11.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Sophos Plc.				
Sophos Anti-Virus	3.x	yes (3.5.3)	yes (3.5.3)	-
Sophos Anti-Virus	4.x	yes (3.6.3.0)	yes (3.6.3.0)	-
Sophos Anti-Virus	5.x	yes (3.5.3)	yes (3.5.3)	yes
Sophos Anti-Virus	6.x	yes (4.0.1.0)	yes (4.0.1.0)	yes
Sophos Anti-Virus	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Sophos Anti-Virus version 3.80	3.8	yes (3.5.0)	yes (3.5.0)	-
Symantec Corp.				
Norton 360 (Symantec Corporation)	1.x	yes (4.1.1.0)	yes (4.1.1.0)	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 10 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Norton 360 (Symantec Corporation)	2.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Norton AntiVirus	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus	14.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Norton AntiVirus	15.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
Norton AntiVirus 2002	8.00.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2002	8.x	yes (3.5.1)	yes (3.5.1)	yes
Norton AntiVirus 2002 Professional	8.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2002 Professional Edition	8.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2003	9.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2003 Professional	9.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2003 Professional Edition	9.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2004	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2004 Professional	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2004 Professional Edition	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2004 (Symantec Corporation)	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2005	11.0.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2006	12.0.x	yes (3.5.5)	yes (3.5.5)	yes
Norton AntiVirus 2006	12.x	yes (3.5.5)	yes (3.5.5)	yes
Norton AntiVirus Corporate Edition	7.x	yes (3.5.1)	yes (3.5.1)	yes
Norton Internet Security	7.x	yes (3.5.0)	yes (3.5.0)	yes
Norton Internet Security	8.0.x	yes (3.5.0)	yes (3.5.0)	yes
Norton Internet Security	8.2.x	yes (3.5.1)	yes (3.5.1)	yes
Norton Internet Security	8.x	yes (3.5.1)	yes (3.5.1)	yes
Norton Internet Security	9.x	yes (3.5.10.1)	yes (3.5.10.1)	yes
Norton Internet Security (Symantec Corporation)	10.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Norton Security Scan	1.x	yes (4.1.3.0)	yes (4.1.3.0)	-
Norton SystemWorks 2003	6.x	yes (3.5.3)	yes (3.5.3)	yes
Norton SystemWorks 2004 Professional	7.x	yes (3.5.4)	yes (3.5.4)	yes
Norton SystemWorks 2005	8.x	yes (3.5.3)	yes (3.5.3)	yes
Norton SystemWorks 2005 Premier	8.x	yes (3.5.3)	yes (3.5.3)	yes
Norton SystemWorks 2006 Premier	12.0.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Symantec AntiVirus	10.x	yes (3.5.3)	yes (3.5.3)	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 11 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Symantec AntiVirus	9.x	yes (3.5.0)	yes (3.5.0)	yes
Symantec AntiVirus Client	8.x	yes (3.5.0)	yes (3.5.0)	yes
Symantec AntiVirus Server	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Symantec AntiVirus Win64	10.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Symantec Client Security	10.x	yes (3.5.3)	yes (3.5.3)	yes
Symantec Client Security	9.x	yes (3.5.0)	yes (3.5.0)	yes
Symantec Endpoint Protection	11.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
Symantec Scan Engine	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
Trend Micro, Inc.				
PC-cillin 2002	9.x	yes (3.5.1)	yes (3.5.1)	-
PC-cillin 2003	10.x	yes (3.5.0)	yes (3.5.0)	-
ServerProtect	5.x	yes (4.1.0.0)	yes (3.6.5.0)	-
Trend Micro Antivirus	11.x	yes (3.5.0)	yes (3.5.0)	yes
Trend Micro AntiVirus	15.x	yes (3.6.5.0)	yes (3.6.5.0)	-
Trend Micro AntiVirus	16.x	yes (4.1.3.0)	yes (4.1.3.0)	-
Trend Micro Client/Server Security	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Trend Micro Client/Server Security Agent	7.x	yes (3.5.12)	yes (3.5.12)	yes
Trend Micro HouseCall	1.x	yes (4.0.1.0)	yes (4.0.1.0)	-
Trend Micro Internet Security	11.x	yes (3.5.0)	yes (3.5.0)	yes
Trend Micro Internet Security	12.x	yes (3.5.0)	yes (3.5.0)	-
Trend Micro Internet Security	16.x	yes (4.1.3.0)	yes (4.1.3.0)	-
Trend Micro OfficeScan Client	5.x	yes (3.5.1)	yes (3.5.1)	yes
Trend Micro OfficeScan Client	6.x	yes (3.5.1)	yes (3.5.1)	yes
Trend Micro OfficeScan Client	7.x	yes (3.5.3)	yes (3.5.3)	yes
Trend Micro OfficeScan Client	8.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
Trend Micro PC-cillin 2004	11.x	yes (3.5.0)	yes (3.5.0)	yes
Trend Micro PC-cillin Internet Security 12	12.x	yes (4.0.1.0)	yes (4.0.1.0)	-
Trend Micro PC-cillin Internet Security 14	14.x	yes (4.0.1.0)	yes (4.0.1.0)	yes
Trend Micro PC-cillin Internet Security 2005	12.x	yes (3.5.3)	yes (3.5.3)	yes
Trend Micro PC-cillin Internet Security 2006	14.x	yes (3.5.8)	yes (3.5.8)	yes
Trend Micro PC-cillin Internet Security 2007	15.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
VCOM				
Fix-It Utilities 7 Professional [AntiVirus]	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Fix-It Utilities 8 Professional [AntiVirus]	8.x	yes (4.1.3.2)	yes (4.1.3.2)	yes

Table 6 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 12 of 12)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
SystemSuite 7 Professional [AntiVirus]	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
SystemSuite 8 Professional [AntiVirus]	8.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
VCOM Fix-It Utilities Professional 6 [AntiVirus]	6.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
VCOM SystemSuite Professional 6 [AntiVirus]	6.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Verizon				
Verizon Internet Security Suite Anti-Virus	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
VirusBuster Ltd.				
VirusBuster for Windows Servers	5.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
VirusBuster Professional	5.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Webroot Software, Inc.				
Webroot Spy Sweeper Enterprise Client with AntiVirus	4.x	yes (4.1.3.2)	-	-
Webroot Spy Sweeper with AntiVirus	5.x	yes (4.1.3.0)	yes (4.1.3.0)	-
Yahoo!, Inc.				
AT&T Yahoo! Online Protection [AntiVirus]	7.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
SBC Yahoo! Anti-Virus	7.x	yes (3.5.10.1)	yes (3.5.10.1)	yes
Verizon Yahoo! Online Protection [AntiVirus]	7.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
Zone Labs LLC				
ZoneAlarm Anti-virus	6.x	yes (3.5.5)	yes (3.5.5)	-
ZoneAlarm Security Suite	5.x	yes (3.5.0)	yes (3.5.0)	-
ZoneAlarm Security Suite	6.x	yes (3.5.5)	yes (3.5.5)	-
ZoneAlarm with Antivirus	5.x	yes (3.5.0)	yes (3.5.0)	-

[1] "Yes" in the AV Checks Supported columns indicates the Agent supports the AV Rule check for the product starting from the version of the Agent listed in parentheses (CAM automatically determines whether to use Def Version or Def Date for the check).

[2] The Live Update column indicates whether the Agent supports live update for the product via the Agent **Update** button (configured by AV Definition Update requirement type). For products that support "Live Update," the Agent launches the update mechanism of the AV product when the Update button is clicked. For products that do not support this feature, the Agent displays a message popup. In this case, administrators can configure a different requirement type (such as "Local Check") to present alternate update instructions to the user.

[3] For Symantec Enterprise products, the Clean Access Agent can initiate AV Update when Symantec Antivirus is in unmanaged mode. If using Symantec AV in managed mode, the administrator must allow/deny managed clients to run LiveUpdate via the Symantec management console (right-click the primary server, go to All Tasks -> Symantec Antivirus, select Definition Manager, and configure the policy to allow clients to launch LiveUpdate for agents managed by that management server.) If managed clients are not allowed to run LiveUpdate, the update button will be disabled on the Symantec GUI on the client, and updates can only be pushed from the server.

Clean Access AV Support Chart (Windows ME/98)

Table 7 lists Windows ME/98 Supported AV Products as of the latest release of the Cisco NAC Appliance software. (See Table 6 for Windows Vista/XP/2000.)

Table 7 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 1 of 2)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2, 3]
		Installation	Virus Definition	
Beijing Rising Technology Corp. Ltd.				
Rising Antivirus Software AV	18.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
Computer Associates International, Inc.				
CA eTrust Antivirus	7.x	yes (3.5.3)	yes (3.5.3)	yes
eTrust EZ Antivirus	6.1.x	yes (3.5.0)	yes (3.5.8)	yes
eTrust EZ Antivirus	6.2.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Antivirus	6.4.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Antivirus	7.x	yes (3.5.3)	yes (3.5.3)	yes
eTrust EZ Armor	6.1.x	yes (3.5.3)	yes (3.5.8)	yes
McAfee, Inc.				
McAfee Managed VirusScan	3.x	yes (3.5.8)	yes (3.5.8)	yes
McAfee VirusScan	10.x	yes (3.5.4)	yes (3.5.4)	yes
McAfee VirusScan	4.5.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan	8.x	yes (3.5.3)	yes (3.5.3)	yes
McAfee VirusScan	9.x	yes (3.5.3)	yes (3.5.3)	yes
McAfee VirusScan Professional	8.x	yes (3.5.3)	yes (3.5.3)	yes
McAfee VirusScan Professional	8xxx	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Professional	9.x	yes (3.5.3)	yes (3.5.3)	yes
McAfee VirusScan Professional Edition	7.x	yes (3.5.0)	yes (3.5.0)	yes
SOFTWIN				
BitDefender 8 Free Edition	8.x	yes (3.5.8)	yes (3.5.8)	-
BitDefender 8 Professional Plus	8.x	yes (3.5.0)	yes (3.5.0)	-
BitDefender 8 Standard	8.x	yes (3.5.0)	yes (3.5.0)	-
BitDefender 9 Professional Plus	9.x	yes (3.5.8)	yes (3.5.8)	-
BitDefender 9 Standard	9.x	yes (3.5.8)	yes (3.5.8)	-
BitDefender Free Edition	7.x	yes (3.5.0)	yes (3.5.0)	-
BitDefender Professional Edition	7.x	yes (3.5.0)	yes (3.5.0)	-
BitDefender Standard Edition	7.x	yes (3.5.0)	yes (3.5.0)	-
Symantec Corp.				
Norton AntiVirus	10.x	yes (3.5.0)	yes (3.5.0)	yes

Table 7 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 2 of 2)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Norton AntiVirus 2002	8.00.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2002	8.x	yes (3.5.1)	yes (3.5.1)	yes
Norton AntiVirus 2003	9.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2003 Professional Edition	9.x	yes (3.5.3)	yes (3.5.3)	yes
Norton AntiVirus 2004	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2004 (Symantec Corporation)	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2005	11.0.x	yes (3.5.0)	yes (3.5.0)	yes
Norton Internet Security	8.0.x	yes (3.5.0)	yes (3.5.0)	yes
Norton Internet Security	8.x	yes (3.5.1)	yes (3.5.1)	yes
Symantec AntiVirus	10.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
Symantec AntiVirus	9.x	yes (3.5.8)	yes (3.5.3)	yes
Symantec AntiVirus Client	8.x	yes (3.5.9)	yes (3.5.9)	yes
Trend Micro, Inc.				
PC-cillin 2003	10.x	yes (3.5.0)	yes (3.5.0)	-
Trend Micro Internet Security	11.x	yes (3.5.0)	yes (3.5.0)	-
Trend Micro Internet Security	12.x	yes (3.5.0)	yes (3.5.0)	-
Trend Micro OfficeScan Client	7.x	yes (4.0.5.0)	yes (4.0.5.0)	-
Trend Micro PC-cillin 2004	11.x	yes (3.5.0)	yes (3.5.0)	-
Trend Micro PC-cillin Internet Security 2005	12.x	yes (3.5.3)	yes (3.5.3)	-

[1] "Yes" in the AV Checks Supported columns indicates the Agent supports the AV Rule check for the product starting from the version of the Agent listed in parentheses (CAM automatically determines whether to use Def Version or Def Date for the check).

[2] The Live Update column indicates whether the Agent supports live update for the product via the Agent **Update** button (configured by AV Definition Update requirement type). For products that support "Live Update," the Agent launches the update mechanism of the AV product when the Update button is clicked. For products that do not support this feature, the Agent displays a message popup. In this case, administrators can configure a different requirement type (such as "Local Check") to present alternate update instructions to the user.

[3] For Symantec Enterprise products, the Clean Access Agent can initiate AV Update when Symantec Antivirus is in unmanaged mode. If using Symantec AV in managed mode, the administrator must allow/deny managed clients to run LiveUpdate via the Symantec management console (right-click the primary server, go to All Tasks -> Symantec Antivirus, select Definition Manager, and configure the policy to allow clients to launch LiveUpdate for agents managed by that management server.) If managed clients are not allowed to run LiveUpdate, the update button will be disabled on the Symantec GUI on the client, and updates can only be pushed from the server.

Clean Access AS Support Chart (Windows Vista/XP/2000)

Table 8 lists Windows Vista/XP/2000 Supported Antispyware Products as of the latest release of the Cisco Clean Access software.

Table 8 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 1 of 6)

		AS Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Spyware Definition**	**Live Update[2]**
Agnitum Ltd.				
Outpost Firewall Pro 2008 [AntiSpyware]	6.x	yes (4.1.3.2)	yes (4.1.3.2)	-
AhnLab, Inc.				
AhnLab SpyZero 2.0	2.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
AhnLab SpyZero 2007	3.x	yes (3.6.5.0)	yes (3.6.5.0)	yes
AhnLab V3 Internet Security 2007 Platinum AntiSpyware	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
AhnLab V3 Internet Security 2008 Platinum AntiSpyware	7.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
AhnLab V3 Internet Security 7.0 Platinum Enterprise AntiSpyware	7.x	yes (4.1.2.0)	yes (4.1.2.0)	yes
America Online, Inc.				
AOL Safety and Security Center Spyware Protection	2.0.x	yes (4.1.0.0)	-	-
AOL Safety and Security Center Spyware Protection	2.1.x	yes (4.1.0.0)	yes (4.1.0.0)	-
AOL Safety and Security Center Spyware Protection	2.2.x	yes (4.1.0.0)	yes (4.1.0.0)	-
AOL Safety and Security Center Spyware Protection	2.3.x	yes (4.1.0.0)	yes (4.1.0.0)	-
AOL Safety and Security Center Spyware Protection	2.x	yes (3.6.1.0)	yes (3.6.1.0)	-
AOL Spyware Protection	1.x	yes (3.6.0.0)	yes (3.6.0.0)	-
AOL Spyware Protection	2.x	yes (3.6.0.0)	yes (4.1.3.0)	-
Anonymizer, Inc.				
Anonymizer Anti-Spyware	1.x	yes (4.1.0.0)	yes (4.1.0.0)	-
Anonymizer Anti-Spyware	3.x	yes (4.1.0.0)	yes (4.1.0.0)	-
Authentium, Inc.				
Cox High Speed Internet Security Suite	3.x	yes (4.0.4.0)	-	yes
AVG Technologies				
AVG 8.0 [AntiSpyware]	8.x	yes (4.1.3.2)	-	yes
BellSouth				
BellSouth Internet Security Anti-Spyware	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
Check Point, Inc				
ZoneAlarm (AntiSpyware)	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes

Table 8 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 2 of 6)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
ZoneAlarm Anti-Spyware	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
ZoneAlarm Pro Antispyware	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
ZoneAlarm Security Suite Antispyware	7.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
Computer Associates International, Inc.				
CA eTrust Internet Security Suite AntiSpyware	10.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
CA eTrust Internet Security Suite AntiSpyware	5.x	yes (3.6.1.0)	yes (3.6.1.0)	yes
CA eTrust Internet Security Suite AntiSpyware	8.x	yes (4.1.2.0)	yes (4.1.2.0)	yes
CA eTrust Internet Security Suite AntiSpyware	9.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
CA eTrust PestPatrol	5.x	yes (3.6.1.0)	yes (4.0.6.0)	yes
CA eTrust PestPatrol Anti-Spyware	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
CA eTrust PestPatrol Anti-Spyware Corporate Edition	5.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
PestPatrol Corporate Edition	4.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
PestPatrol Standard Edition (Evaluation)	4.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
EarthLink, Inc.				
Aluria Security Center AntiSpyware	1.x	yes (4.1.0.0)	yes (4.1.0.0)	-
EarthLink Protection Control Center AntiSpyware	1.x	yes (3.6.0.0)	yes (3.6.0.0)	-
EarthLink Protection Control Center AntiSpyware	2.x	yes (4.0.6.0)	-	-
EarthLink Protection Control Center AntiSpyware	3.x	yes (4.1.3.0)	-	-
Primary Response SafeConnect	2.x	yes (3.6.5.0)	-	-
FaceTime Communications, Inc.				
X-Cleaner Deluxe	4.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
F-Secure Corp.				
F-Secure (AntiSpyware)	7.x	yes (4.1.3.0)	yes (4.1.3.0)	-
F-Secure Internet Security (AntiSpyware)	7.x	yes (4.1.3.0)	yes (4.1.3.0)	-
Grisoft, Inc.				
AVG Anti-Malware [AntiSpyware]	7.x	yes (4.1.2.0)	-	-
AVG Anti-Spyware 7.5	7.x	yes (4.0.5.1)	yes (4.0.5.1)	-
iS3 Inc.				

Table 8 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 3 of 6)

		AS Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Spyware Definition**	**Live Update[2]**
STOPzilla	5.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Javacool Software LLC				
SpywareBlaster v3.1	3.1.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
SpywareBlaster v3.2	3.2.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
SpywareBlaster v3.3	3.3.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
SpywareBlaster v3.4	3.4.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
SpywareBlaster v3.5.1	3.5.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Kingsoft Corp.				
Kingsoft AntiSpyware 2007 Free	2007.x	yes (4.1.3.2)	yes (4.1.3.2)	-
Kingsoft Internet Security [AntiSpyware]	7.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
Lavasoft, Inc.				
Ad-Aware 2007	7.x	yes (4.1.3.0)	-	-
Ad-Aware 2007 Professional	7.x	yes (4.0.6.1)	-	yes
Ad-aware 6 Professional	6.x	yes (3.6.0.0)	yes (3.6.0.0)	-
Ad-Aware SE Personal	1.x	yes (3.6.0.0)	yes (3.6.0.0)	-
Ad-Aware SE Professional	1.x	yes (3.6.1.0)	yes (3.6.1.0)	yes
McAfee, Inc.				
McAfee AntiSpyware	1.5.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
McAfee AntiSpyware	1.x	yes (3.6.0.0)	yes (4.1.0.0)	yes
McAfee AntiSpyware	2.0.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
McAfee AntiSpyware	2.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
McAfee AntiSpyware Enterprise	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
McAfee Anti-Spyware Enterprise Module	8.0.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
McAfee AntiSpyware Enterprise Module	8.5.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
McAfee VirusScan AS	11.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
McAfee VirusScan AS	12.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
MicroSmarts LLC				
Spyware Begone	4.x	yes (3.6.0.0)	-	-
Spyware Begone	6.x	yes (4.1.0.0)	-	-
Spyware Begone	8.x	yes (4.1.0.0)	-	-
Spyware Begone Free Scan	7.x	yes (3.6.0.0)	-	-
Spyware Begone V7.30	7.30.x	yes (3.6.1.0)	-	-
Spyware Begone V7.40	7.40.x	yes (3.6.1.0)	-	-

Table 8 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 4 of 6)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
Spyware Begone V7.95	7.95.x	yes (4.1.0.0)	-	-
Spyware Begone V8.20	8.20.x	yes (4.1.0.0)	-	-
Spyware Begone V8.25	8.25.x	yes (4.1.0.0)	-	-
Spyware Begone! Version 9	9.x	yes (4.1.3.2)	-	-
Microsoft Corp.				
Microsoft AntiSpyware	1.x	yes (4.0.6.0)	-	yes
Windows Defender	1.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Windows Defender Vista	1.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
Omniquad				
Omniquad Total Security	2.0.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Panda Software				
Panda Titanium 2006 Antivirus + Antispyware [AntiSpyware]	5.x	yes (4.1.3.2)	yes (4.1.3.2)	-
PC Tools Software				
PC Tools Internet Security [Antispyware]	5.x	yes (4.1.3.0)	-	-
PC Tools Spyware Doctor	5.x	yes (4.1.3.2)	-	yes
Spyware Doctor	4.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Spyware Doctor	5.x	yes (4.0.6.0)	-	yes
Spyware Doctor 3.0	3.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
Spyware Doctor 3.1	3.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
Spyware Doctor 3.2	3.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
Spyware Doctor 3.5	3.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Spyware Doctor 3.8	3.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Spyware Doctor [AntiSpyware]	5.x	yes (4.1.3.2)	-	yes
Prevx Ltd.				
Prevx1	1.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Prevx1	2.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Prevx Home	2.x	yes (3.6.0.0)	yes (3.6.0.0)	-
Radialpoint Inc.				
Radialpoint Security Services Spyware Protection	6.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Radialpoint Spyware Protection	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
Zero-Knowledge Systems Radialpoint Security Services Spyware Protection	6.x	yes (4.0.6.0)	yes (4.0.6.0)	yes

Table 8 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 5 of 6)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
Safer Networking Ltd.				
Spybot - Search & Destroy 1.3	1.3	yes (3.6.0.0)	yes (3.6.0.0)	yes
Spybot - Search & Destroy 1.4	1.4	yes (3.6.0.0)	yes (3.6.0.0)	yes
Spybot - Search & Destroy 1.5	1.x	yes (4.0.6.1)	yes (4.0.6.1)	-
Sereniti, Inc.				
Sereniti Antispyware	1.x	yes (4.0.6.0)	-	yes
The River Home Network Security Suite Antispyware	1.x	yes (4.0.6.0)	-	yes
SOFTWIN				
BitDefender 9 Antispyware	9.x	yes (4.1.0.0)	yes (4.1.0.0)	-
BitDefender 9 Internet Security AS	9.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
BitDefender Antivirus Plus v10 AS	10.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
BitDefender Antivirus v10 AS	10.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
BitDefender Internet Security v10 AS	10.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Sunbelt Software				
CounterSpy Enterprise Agent	1.8.x	yes (4.0.6.0)	-	-
CounterSpy Enterprise Agent	2.0.x	yes (4.1.3.0)	-	-
Sunbelt CounterSpy	1.x	yes (3.6.0.0)	-	yes
Sunbelt CounterSpy	2.x	yes (4.0.6.0)	-	yes
Symantec Corp.				
Norton Internet Security AntiSpyware	15.x	yes (4.1.3.0)	-	-
Norton Spyware Scan	2.x	yes (4.1.0.0)	yes (4.1.0.0)	-
Trend Micro, Inc.				
Trend Micro Anti-Spyware	3.5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
Trend Micro Anti-Spyware	3.x	yes (3.6.0.0)	-	-
Trend Micro PC-cillin Internet Security 2007 AntiSpyware	15.x	yes (4.1.0.0)	yes (4.1.3.2)	yes
VCOM				
Fix-It Utilities 7 Professional [AntiSpyware]	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Fix-It Utilities 8 Professional [AntiSpyware]	8.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
SystemSuite 7 Professional [AntiSpyware]	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
SystemSuite 8 Professional [AntiSpyware]	8.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
VCOM Fix-It Utilities Professional 6 [AntiSpyware]	6.x	yes (4.0.6.1)	yes (4.0.6.1)	yes

Table 8 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 68, 4.1.3.2 Agent, CAM/CAS Release 4.1.3.1 (Sheet 6 of 6)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
VCOM SystemSuite Professional 6 [AntiSpyware]	6.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Verizon				
Verizon Internet Security Suite Anti-Spyware	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
Webroot Software, Inc.				
Spy Sweeper	3.x	yes (3.6.0.0)	-	-
Spy Sweeper	4.x	yes (3.6.0.0)	-	-
Spy Sweeper	5.0.x	yes (4.1.3.0)	-	-
Spy Sweeper	5.x	yes (4.1.0.0)	-	-
Webroot Spy Sweeper Enterprise Client	1.x	yes (3.6.0.0)	-	-
Webroot Spy Sweeper Enterprise Client	2.x	yes (3.6.1.0)	-	-
Webroot Spy Sweeper Enterprise Client	3.5.x	yes (4.1.3.2)	-	-
Webroot Spy Sweeper Enterprise Client	3.x	yes (4.0.5.1)	-	-
Yahoo!, Inc.				
AT&T Yahoo! Online Protection	2006.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
CA Yahoo! Anti-Spy	2.x	yes (4.1.3.2)	-	-
SBC Yahoo! Applications	2005.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
Verizon Yahoo! Online Protection	2005.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
Yahoo! Anti-Spy	1.x	yes (3.6.0.0)	yes (3.6.0.0)	-
Zone Labs LLC				
Integrity Agent	6.x	yes (4.1.2.0)	yes (4.1.2.0)	-

[1] "Yes" in the AS Checks Supported columns indicates the Agent supports the AS Rule check for the product starting from the version of the Agent listed in parentheses (CAM automatically determines whether to use Def Version or Def Date for the check).

[2] The Live Update column indicates whether the Agent supports live update for the product via the Agent **Update** button (configured by AS Definition Update requirement type). For products that support "Live Update," the Agent launches the update mechanism of the AS product when the Update button is clicked. For products that do not support this feature, the Agent displays a message popup. In this case, administrators can configure a different requirement type (such as "Local Check") to present alternate update instructions to the user.

Supported AV/AS Product List Version Summary

Table 9 details enhancements made per version of the Supported Antivirus/Antispyware Product List. See Clean Access Supported AV/AS Product List, page 32 for the latest Supported AV list as of the latest release. See New and Changed Information, page 9 for the release feature list.

Table 9 Supported AV/AS Product List Versions

Version	Enhancements
Release 4.1.3.1—4.1.3.2/4.1.3.1/4.1.3.0 Agents	
Version 68	**Added New AV Products (Windows Vista/XP/2000)**: • AVG 8.0 [AntiVirus], 8.x • BullGuard 8.0, 8.x • Quick Heal AntiVirus Lite, 9.5.x • Quick Heal AntiVirus Plus, 9.5.x • ZoneAlarm Anti-virus, 7.0.x • ZoneAlarm (AntiVirus), 7.0.x • ZoneAlarm Security Suite Antivirus, 7.0.x • NOD32 antivirus system, x • NOD32 Antivirus System, x • NOD32 antivirus System, x • ESET NOD32 Antivirus, 3.x • F-Secure Anti-Virus for Windows Servers, 5.x • Kaspersky Anti-Virus for Windows File Servers, 6.x • Kaspersky Anti-Virus for Windows Servers, 6.x • Kaspersky Internet Security 8.0, 8.x • Kingsoft AntiVirus 2007 Free, 2007.x • Windows Live OneCare, 2.x • PC Tools AntiVirus 2008, 4.x • PC Tools Spyware Doctor [Antivirus], 5.x • Spyware Doctor [Antivirus], 5.x • BitDefender Free Edition v10, 10.x • Norton 360 (Symantec Corporation), 2.x • Fix-It Utilities 8 Professional [AntiVirus], 8.x • SystemSuite 8 Professional [AntiVirus], 8.x • VirusBuster for Windows Servers, 5.x • VirusBuster Professional, 5.x • Webroot Spy Sweeper Enterprise Client with AntiVirus, 4.x

Table 9 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 68 (continued)	**Added New AS Products (Windows Vista/XP/2000)**: • Outpost Firewall Pro 2008 [AntiSpyware], 6.x • AVG 8.0 [AntiSpyware], 8.x • STOPzilla, 5.x • Kingsoft AntiSpyware 2007 Free, 2007.x • Spyware Begone! Version 9, 9.x • Panda Titanium 2006 Antivirus + Antispyware [AntiSpyware], 5.x • PC Tools Spyware Doctor, 5.x • Spyware Doctor [AntiSpyware], 5.x • BitDefender 9 Internet Security AS, 9.x • BitDefender Antivirus Plus v10 AS, 10.x • BitDefender Antivirus v10 AS, 10.x • BitDefender Internet Security v10 AS, 10.x • Fix-It Utilities 8 Professional [AntiSpyware], 8.x • SystemSuite 8 Professional [AntiSpyware], 8.x • Webroot Spy Sweeper Enterprise Client, 3.5.x • CA Yahoo! Anti-Spy, 2.x **Added Spyware definition check support:** • Trend Micro PC-cillin Internet Security 2007 AntiSpyware, 15.x
Release 4.1(3)—4.1.3.1/4.1.3.0 Windows Clean Access Agents	
Version 67	Added New AV Products (Windows Vista/XP/2000): • AhnLab V3 Internet Security 2007, 7.x • AhnLab V3 Internet Security 2008 Platinum, 7.x • Avira AntiVir PersonalEdition Classic, 7.x • Rising Antivirus Software AV, 20.x • CA Anti-Virus, 9.x • eTrust Antivirus, 6.0.x • EarthLink Protection Control Center AntiVirus, 3.x • F-Secure Internet Security 2005, 5.x • G DATA AntiVirus 2008, 18.x • G DATA AntiVirusKit, 17.x • G DATA InternetSecurity [Antivirus], 17.x • G DATA InternetSecurity [Antivirus], 18.x • G DATA TotalCare [Antivirus], 18.x

Table 9 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 67 (continued)	**New AV Products (continued)**: • ViRobot Desktop, 5.x • Jiangmin AntiVirus KV2007, 10.x • Kaspersky Anti-Virus 7.0, 7.x • Kaspersky Internet Security 7.0, 7.x • McAfee VirusScan, 12.x • Panda Antivirus + Firewall 2008, 7.x • PC Tools AntiVirus 2.0, 2.x • PC Tools AntiVirus 2007, 3.x • PC Tools Internet Security [Antivirus], 5.x • ThreatFire 3.0, 3.x • Radialpoint Security Services Virus Protection, 6.x • Dr.Web, 4.44.x • BitDefender Antivirus 2008, 11.x • BitDefender Client Professional Plus, 8.x • BitDefender Internet Security 2008, 11.x • BitDefender Total Security 2008, 11.x • Norton Security Scan, 1.x • Trend Micro AntiVirus, 16.x • Trend Micro Internet Security, 16.x • VCOM SystemSuite Professional 6 [AntiVirus], 6.x • Webroot Spy Sweeper with AntiVirus, 5.x

Table 9 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 67 (continued)	Added New AS Products (Windows Vista/XP/2000): • AhnLab V3 Internet Security 2008 Platinum AntiSpyware, 7.x • CA eTrust Internet Security Suite AntiSpyware, 10.x • EarthLink Protection Control Center AntiSpyware, 3.x • F-Secure (AntiSpyware), 7.x • F-Secure Internet Security (AntiSpyware), 7.x • Ad-Aware 2007, 7.x • McAfee AntiSpyware, 2.0.x • McAfee AntiSpyware Enterprise Module, 8.5.x • McAfee VirusScan AS, 12.x • Omniquad Total Security, 2.0.x • PC Tools Internet Security [Antispyware], 5.x • Radialpoint Security Services Spyware Protection, 6.x • CounterSpy Enterprise Agent, 2.0.x • Norton Internet Security AntiSpyware, 15.x • VCOM SystemSuite Professional 6 [AntiSpyware], 6.x • Spy Sweeper

Caveats

This section describes the following caveats:

- Open Caveats - Release 4.1(3), page 58
- Resolved Caveats - Windows Clean Access Agent 4.1.3.2, page 65
- Resolved Caveats - Mac OS X Agent 4.1.3.1, page 68
- Resolved Caveats - Release 4.1.3.1, page 71
- Resolved Caveats - Cisco NAC Web Agent 4.1.3.10, page 72
- Resolved Caveats - Windows Clean Access Agent 4.1.3.1, page 73
- Resolved Caveats - Release 4.1(3), page 75

Note If you are a registered cisco.com user, you can view Bug Toolkit on cisco.com at the following website:

http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl

To become a registered cisco.com user, go to the following website:

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

Open Caveats - Release 4.1(3)

Note Refer to the applicable version of the Release Notes for Cisco NAC Profiler for caveats related to Cisco NAC Profiler.

Table 10 List of Open Caveats (Sheet 1 of 8)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsd03509	No	The Time Servers setting is not updated in HA-Standby CAM web console After updating the "Time Servers" setting in HA-Primary CAM, the counterpart "Time Servers" setting for the HA-Standby CAM does not get updated in the web console even though the "Time Servers" setting is updated in the HA-Standby CAM database.
CSCsd90433	No	Apache does not start on HA-Standby CAM after heartbeat link is restored. Output from the fostate.sh command shows "My node is standby without web console, peer node is active."
CSCse86581	No	Agent does not correctly recognize def versions on the following Trend AV products: • PC-cillin Internet Security 2005 • PC-cillin Internet Security 2006 • OfficeScan Client Tested Clients: • PC-cillin Internet Security 2006 (English) on US-English Windows 2000 SP4 • OfficeScan Client (English) on US-English Windows 2000 SP4 • VirusBaster 2006 Internet Security (Japanese) on Japanese Windows XP SP2 • VirusBaster Corporate Edition (Japanese) on Japanese Windows XP SP2

Table 10 List of Open Caveats (Sheet 2 of 8)

DDTS Number	Software Release 4.1(3)	
	Corrected	**Caveat**
CSCsg07369	No	Incorrect "IP lease total" displayed on editing manually created subnets Steps to reproduce: 1. Add a Managed Subnet having at least 2500+ IP addresses (for example 10.101.0.1/255.255.240.0) using CAM web page **Device Management > Clean Access Servers > Manage [IP Address] > Advanced > Managed Subnet**. 2. Create a DHCP subnet with 2500+ hosts using CAM web page **Device Management > Clean Access Servers > Manage [IP Address] > Network > DHCP > Subnet List > New**. 3. Edit the newly created subnet using CAM web page **Device Management > Clean Access Servers > Manage [IP Address] > Network > DHCP > Subnet List > Edit**. 4. Click **Update**. The CAM displays a warning informing the administrator that the current IP Range brings IP lease total up to a number that is incorrect. The CAM counts the IP address in the subnet twice, creating the incorrect count. The issue is judged to be cosmetic and does not affect DHCP functionality.
CSCsg66511	No	Configuring HA-failover synchronization settings on Secondary CAS takes an extremely long time Once you have configured the Secondary CAS HA attributes and click **Update**, it can take around 3 minutes for the browser to get the response from the server. (Configuring HA-failover synchronization on the Primary CAS is nearly instantaneous.)
CSCsh77730	No	Clean Access Agent locks up when greyed out **OK** button is pressed The Clean Access Agent locks up when the client machine refreshes its IP address. This only occurs when doing an IP release/renew, so the CAS must be in an OOB setup. If the **Automatically close login success screen after** <*x*> **secs** option is enabled and the duration set to 0 (instantaneous) in the **Clean Access > General Setup > Agent Login** page and the user clicks on the greyed out **OK** button while the IP address is refreshing, the Clean Access Agent locks up after refreshing the IP address. The IP address is refreshed and everything else on the client machine works, but the user cannot close the Clean Access Agent without exiting via the system tray icon, thus "killing" the Agent process. **Workaround**: Either uncheck the box or set that timer to a non-zero value. If it is set to anything else, and the user hits the greyed out OK button while the IP is refreshing, then the Agent window closes successfully.

Table 10 List of Open Caveats (Sheet 3 of 8)

DDTS Number	Software Release 4.1(3)	
	Corrected	Caveat
CSCsi07595	No	DST fix will not take effect if generic MST, EST, HST, etc. options are specified Due to a Java runtime implementation, the DST 2007 fix does not take effect for Cisco NAC Appliances that are using generic time zone options such as "EST," "HST," or "MST" on the CAM/CAS UI time settings. **Workaround** If your CAM/CAS machine time zone setting is currently specified via the UI using a generic option such as "EST," "HST," or "MST." change this to a location/city combination, such as "America/Denver." **Note** CAM/CAS machines using time zone settings specified by the "service perfigo config" script or specified as location/city combinations in the UI, such as "America/Denver" are not affected by this issue.
CSCsk55292	No	Agent not added to system tray during boot up When the Agent is installed on a Windows client, the Start menu is updated and Windows tries to contact AD (in some cases where the AD credentials are expired) to refresh the Start menu. Due to the fact that the client machine is still in the Unauthenticated role, AD cannot be contacted and an approximately 60 second timeout ensues, during which the Windows taskbar elements (Start menu, System Tray, and Task Bar) are locked. As a result, the Agent displays a "Failed to add Clean Access Agent icon to taskbar status area" error message. **Workaround** • Allow AD traffic through the CAS for clients in the Unauthenticated role. • Try to start the Agent manually after the install and auto load process fails.
CSCsk58244	No	Clean Access Report for WSUS shows failed This situation applies to Windows XP and Windows Vista client machines. The Agent report on the CAM does not show any on the updates required for the client.
CSCsl00736	No	Download of the Cisco NAC Web Agent fails if the link speed is below 50Kbits/s **Note** Cisco does not recommend using the Cisco NAC Web Agent on client machines connecting with link speeds slower than 56Kbits/s.

Table 10 List of Open Caveats (Sheet 4 of 8)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsl13782	No	Microsoft Internet Explorer 7.0 browser pop-ups on Windows Vista launched from the Summary Report appear behind the Summary Report window This is also seen when you click on the Policy link in the Policy window. This issue appears on Vista Ultimate and Vista Home, but is not seen with Firefox or on Internet Explorer versions running in Windows 2000 or Windows XP. **Note** This problem only happens when a Google tool bar is installed and enabled in Internet Explorer.
CSCsl71585	No	DHCP status does not display non-restricted scope with Relay IP restriction When a DHCP range with no restrictions and a DHCP range with a Relay-IP restriction are created using the Clean Access Manager (CAM) GUI, the DHCP range with no restrictions does not display. Steps to reproduce: 1. Create a DHCP scope with no restriction, either VLAN ID or Relay-IP on the CAS using the CAM GUI. 2. Add a static route on the CAS using the CAM GUI. 3. Create another DHCP scope with a relay-IP restriction. 4. Go to the DHCP Status web page. The web page only displays the IPs for the relay-IP restriction and does not display the non-restricted IP scope. Workaround: Avoid creating DHCP scopes having both no restrictions and Relay-IP restrictions. **Note** The issue is known to be cosmetic and does not affect functionality.
CSCsl17379	No	Multiple Clean Access Agent pop-ups with Multi NIC in L2 VGW OOB role-based VLAN The user sees multiple Clean Access Agent login dialogs with two or more active NICs on the same client machine pointing to the Unauthenticated network access point (eth1 IP address). After the first Clean Access Agent pops up and the user logs in, a second Agent login dialog pops up. If the user logs in to this additional Agent instantiation there are now two entries for the same system with both MAC addresses in the CAM's Certified Device List and Online Users List. **Workaround** The user can manually Disable Agent login pop-up after authentication.
CSCsl22653	No	Mac OS X Agent running on 10.2 does not display green colored icons in places like the "About Us" dialog in the Finder.

Table 10 List of Open Caveats (Sheet 5 of 8)

DDTS Number	Software Release 4.1(3)	
	Corrected	**Caveat**
CSCsl22774	No	Incorrect download filename perfigo_dm_enforce.jsp for the 10.2 version of the Mac OS X Agent The filename for the agent download file should be "CCAAgent_MacOSX.tar," similar to that in versions 10.3, 10.4, and 10.5.
CSCsl40626	No	Cisco NAC Web Agent should handle certificate revocation dialogs similar to Clean Access Agent Upon logging in via the Cisco NAC Web Agent (with certificate revocation turned on or with Norton 360 installed), the user is presented with a "Revocation information for the security certificate for this site is not available. Do you want to proceed?" dialog box several times (approximately 40 to 50 times). If the user clicks **Yes** to proceed enough times, the Web Agent fails to login and reports "You will not be allowed to access the network due to internal error. Please contact your administrator." back to the user.
CSCsl40812	No	**The Refresh Windows domain group policy after login** option is not functioning for Cisco NAC Web Agent (It is working fine with the Clean Access Agent.) This scenario was tested configuring a GPO policy for a Microsoft Internet Explorer browser title. The browser was not refreshed as expected after login in using the Web Agent.
CSCsl75403	No	MAC filter does not work for Macintosh client machines connected to the network in VPN environment Steps to reproduce: 1. Setup a VPN environment. 2. Get the MAC address of the en0 interface of Macintosh client machine. 3. Put the MAC address in the CAM device filter list with "Deny" access type. 4. Connect the Macintosh client machine to the VPN concentrator. 5. Agent will be allowed to perform VPN SSO [or present login page if no VPN SSO is configured]. 6. Traffic originating from the client machine on the untrusted network is allowed to go to the trusted network even though the MAC address of the client machine is denied in the device filter list.

Table 10 List of Open Caveats (Sheet 6 of 8)

DDTS Number	Software Release 4.1(3)	
	Corrected	**Caveat**
CSCsl77701	No	Network Error dialog appears during CAS HA failover When a user is logged in as ADSSO user on CAS HA system and the CAS experiences a failover event, the user sees is a pop-up message reading, "Network Error! Detail: The network cannot be accessed because your machine cannot connect to the default gateway. Please release/renew IP address manually." This is not an error message and the user is still logged in to the system. The user simply needs to click on the **Close** button to continue normal operation.
CSCsl88429	No	User sees Invalid session after pressing [F5] following Temporary role time-out When a user presses [F5] or [Refresh] to refresh the web page after the Agent Temporary role access timer has expired, the user sees an "Invalid" session message. If the user then attempts to navigate to the originally requested web address, they are prompted with the web login page again and are able to log in.
CSCsl88627	No	Description of **removesubnet** has "updatesubnet" in op field The **removesubnet** API function description has "updatesubnet" listed in its operations field. The description should read "removesubnet."
CSCsm20254	No	CAS duplicates HSRP packets with Cisco NAC Profiler Collector Modules enabled. **Symptom** HSRP duplicate frames are sent by CAS in Real-IP Gateway with Collector modules enabled. This causes HSRP issues and the default gateway to go down. **Conditions** Real-IP Gateway and Collector modules enabled on a CAS with ETH0 and or ETH1 configured for NetWatch. **Workaround** Do not configure the CAS' ETH0 trusted interface or ETH1 untrusted interface in the NetWatch configuration settings for the CAS Collector. It is not a supported configuration.

Table 10 List of Open Caveats (Sheet 7 of 8)

DDTS Number	Software Release 4.1(3)	
	Corrected	**Caveat**
CSCsm20655	No	Can not do a minor upgrade for Clean Access Agent from MSI package. When CCAAgent.msi is used and the Clean Access Agent is upgraded to a minor version (e.g. 4.1.2.1 to 4.1.2.2) the following error message will be displayed: “Another version of this product is already installed. Installation of this version cannot continue. To configure or remove the existing version of this product, use Add/Remove Programs on the Control Panel.” **Reason**: Windows Installer uses only the first three fields of the product version. When a fourth field is included in the product version, the installer ignores the fourth field. For details refer to http://msdn2.microsoft.com/en-us/library/aa370859(VS.85).aspx **Workaround** Uninstall the program from Add/Remove Programs before installing it.
CSCsm25788	No	Avast 4.7 showing as not up to date with Cisco NAC Appliance Release 4.1(3) User is told that Avast needs to be updated, but shows as up to date. This occurs when user is running Avast 4.7 and the Agent version is 4.1.3.0 or 4.1.3.1 **Workaround** Create a custom check for Avast that allows the users on without verifying the definition version.
CSCsm53743	No	File ownership of Mac OS X Agent directory and related files should be corrected File ownership of Mac OS X Agent and related files should be “root:admin.” Currently, the file ownership is with UID 505 and GID 505. Anyone able to assume this UID could potentially modify the Agent application files and introduce a security threat.

Table 10 List of Open Caveats (Sheet 8 of 8)

DDTS Number	Software Release 4.1(3)	
	Corrected	**Caveat**
CSCsm76779	No	CSRF tag is added to CAS specific MAC Device Filter description field upon edit Steps to reproduce: 1. Go to CAS-specific device filters in the CAM web console (**Device Management > Clean Access Servers > Manage [IP_Address] > Filter > Devices**). 2. Edit a device filter with the description field like "<a href='http://www.cisco.com'>Cisco</a>" 3. Click **Save**. A CSRF tag is appended to (and is visible in) the hypertext entry in the device filter description field. Subsequent entry updates also append the same CSRF tag each time the administrator edits the description. After editing the description 3 times, however, the entry can no longer be edited and the CAS returns an "Updating device MAC failed" error message. **Note** This issue only addresses CAS-specific device filters and not *global* device filters addressed with caveat CSCsm55679.
CSCsm79088	No	Mac OS X Agent reports "Unknown user" when sending the second logout request The Mac OS X Agent specifies an "Unknown user" when it sends a second logout request before receiving a response from the first logout request. Steps to reproduce: 1. Log into the network using the Mac OS X Agent. 2. Right-click on Agent icon and choose **Logout**. 3. Repeat step 2 before receiving a response for the first logout request. The Mac Agent displays a "Cisco Clean Access Agent is having a difficulty with the server. Unknown user." error message, resulting in a situation where the client machine no longer appears in the CAM's Online Users list even though the Agent indicates that the user is logged in. In this situation, the Mac Agent essentially "freezes" as the user is no longer able to log out, ether.

Resolved Caveats - Windows Clean Access Agent 4.1.3.2

Refer to Windows Clean Access Agent Version 4.1.3.2, page 26 for additional information.

Table 11 List of Closed Caveats (Sheet 1 of 3)

	Windows Clean Access Agent 4.1.3.2	
DDTS Number	**Corrected**	**Caveat**
CSCsl77778	Yes	Russian Language is not translated accurately in 4.1.3.0 Agent Clean Access Agent version 4.1.3.0 displays English language in native Russian Windows operating systems and displays garbled Russian characters. For best results, Cisco recommends using the Russian version of the Clean Access Agent on a native Russian version of the Windows operating system. **Note** This also pertains to the 4.1.1.0 Clean Access Agent.
CSCsl77801	Yes	Turkish language partially translated in 4.1.3.0 Clean Access Agent Not all of the 4.1.3.0 Clean Access Agent dialogs related to new release 4.1(3) features (Auto-Remediation, new WSUS messages) are properly translated. Some read “Unknown String.”
CSCsm04923	Yes	Windows 2000 clients are asked to log in when using a MAC address filter This issue arises when the client machine is running the Nortel VPN software and Windows Clean Access Agent version 4.1.2.1.
CSCsm38529	Yes	A client with two active NICs faces repeated IP refresh events **Practical Scenario** **1.** Connect cable for the first NIC. The client is authenticated by the CAS. **2.** Enable 2nd NIC. Authentication for the second NIC does not start, because the default gateway is still valid on the first active NIC. **3.** The multiple NIC support feature blocks unneeded authentication. **4.** Disconnect cable for the first NIC. The default gateway changes to the second NIC. However, the Agent does *not* send an ARP packet to the default gateway, and the client machine starts to repeatedly refresh the IP address. The problem is not solved until the user exits and restarts the Agent or reboots the PC. **Workaround** **1.** Reload the Agent or PC. **2.** Disable the Access to Authentication VLAN Change Detection feature.

Table 11 List of Closed Caveats (Sheet 2 of 3)

	Windows Clean Access Agent 4.1.3.2	
DDTS Number	**Corrected**	**Caveat**
CSCsm39238	Yes	In 4.1.3.0 and 4.1.3.1 Windows Agents, clients that fail requirements may get hung at the Login Screen with "Validating Requirements...Please Wait" showing on the Agent This occurs when the session timer for the Agent Temporary Role is set to "Disabled," and when the user fails a requirement. Navigate to **User Management > User Roles > Schedule > Session Timer** in the CAM web console and set the Session Timeout value for the Temporary Role equal to a positive integer value. The Agent allows that amount of time for the user to remediate. In prior Agent versions, the Agent interpreted "Disabled" to mean unlimited time. However in 4.1.3.x, the Agent seems to interpret this as "0" and when the user fails a requirement, the user gets stuck because they have 0 seconds to remediate. (The remediation screen never appears and the user is stuck on the login screen.) **Note** Users that pass all requirements are fine.
CSCsm54763	Yes	Symantec endpoint protection definition updates require administrator permissions. This issue is resolved in Windows Clean Access Agent version 4.1.3.2. **Workaround** **Users can manually update their endpoint protection from the Symantec software user interface.**
CSCsm42572	Yes	NOD 32 antivirus fails an AV definition check even though it is up to date This occurs when running version 4.1.3.0 of the Windows Clean Access Agent. Currently, the only workaround is to create a custom check to "allow" NOD 32 users without checking for the definition version.
CSCsm62326	Yes	The 4.1.3.0 Windows Clean Access Agent installation process returns message: "Error 1324. The path My Pictures contains an invalid character" This occurs if the My Documents folder is mapped to a remote server to which the user does not have access in the unauthenticated role, for example: **\\servername\userid\My Documents**. **Workarounds** • Enable off-line file access. • Allow access to the server in the unauthenticated role.

Table 11 List of Closed Caveats (Sheet 3 of 3)

	Windows Clean Access Agent 4.1.3.2	
DDTS Number	**Corrected**	**Caveat**

CSCsm67052	Yes	When using Clean Access Agent posture assessment with Webroot AntiSpyware Corporate Edition, the Agent incorrectly detects the AS product as an unknown AV product and does not display the correct definition information. The administrator sees the following in the user Agent report:
		`Client AV Info`
		`Product ID: WmiAV`
		`Product Name: Webroot Software Inc. unknown product`
		`Product Version: 3.5`
		`Virus Definition File Version:`
		`Virus Definition File Date:`
		This occurs with Windows Agent versions 4.1.2.x and 4.1.3.x when used in conjunction with Webroot AntiSpyware Corporate Edition 3.5.
		Workaround
		Create a custom check using the following value: **HKLM\\Software\\Webroot\\Enterprise\\CommAgent\\sdfv**.

CSCso22399	Yes	On Windows 2000 SP4, the Clean Access Agent takes about 15 minutes to perform an IP refresh After switching back to the Authentication VLAN when the Access to Authentication VLAN change detection feature is enabled, and the VlanDetectInterval value is set to 5 per the appropriate registry key setting, the Windows Agent can take up to 15 minutes before the client machine recognizes the VLAN change from Access back to Auth and completes the client IP refresh. **Note** This issue only occurs on Windows 2000 SP4 client machines where the user does not have administrator privileges. **Workarounds** • Grant users administrator access to their client machines. • Do not enable the Access to Authentication VLAN change detection feature. Instead, use port bouncing to refresh client IP addresses. • Decrease the interval or the number of times the Agent attempts to retry connection. (Cisco does not recommend this option if there are other operating systems on the network, as this may result in unwarranted IP refreshes on other client machines.)

Resolved Caveats - Mac OS X Agent 4.1.3.1

Refer to Mac OS X Clean Access Agent Version 4.1.3.1, page 29 for additional information.

Table 12 List of Closed Caveats (Sheet 1 of 3)

DDTS Number	Mac OS X Agent 4.1.3.1	
	Corrected	**Caveat**
CSCsl83353	Yes	Mac OS X Agent does not refresh icon status after disconnecting interface The Mac OS X Agent does not refresh the tray icon status when you physically disconnect the network interface cable. Steps to reproduce: **1.** Log in to Cisco NAC Appliance using the Mac OS X Agent. **2.** Disconnect the network cable from the active network interface. The Mac Agent status does not change from “Logged-in.” **Note** The issue is cosmetic and does not affect Agent functionality.
CSCsl88985	Yes	Mac Agent logs out user after every login once operating system mismatch is detected The Mac OS X Clean Access Agent logs the user out after every login once the Agent detects an operating system mismatch and prompts the user with a new login dialog requesting credentials. When the user logs in again, the Agent again detects the operating system mismatch and repeats the process. **Workaround** Exit and re-launch the Clean Access Agent on Macintosh client machine.
CSCsl98060	Yes	Mac OS X Agent CPU usage spikes every few seconds The CPU usage rises to 85-99% every few seconds, recedes, and then spikes again.
CSCsm10311	Yes	Mac OS X Agent changes Applications folder permissions to “unknown” Installing the 4.1.3.0 Agent on a Mac client machine changes the Applications folder permissions to “Owner:unknown” with read/write access and the Application Group to “Unknown” with read only and Others to read permissions. This issue impacts other applications already installed and can keep them from updating themselves and could even affect the stability of the Finder system application. **Note** Any new additions to the Applications folder require non-root users to login as root in order to make changes.

Table 12 List of Closed Caveats (Sheet 2 of 3)

	Mac OS X Agent 4.1.3.1	
DDTS Number	**Corrected**	**Caveat**
CSCsm20813	Yes	Mac OS X Agent difficult to exit when discovery host FQDN cannot be resolved For users attempting to log in via the Mac Agent 4.1.3.0 where the discovery host cannot be resolved, it is difficult to close/exit the Agent (or use any other menu items). In addition, a “System failed to resolve the host name!” message appears repeatedly. **Workaround** You must add an entry to **/etc/hosts** to resolve the host name of the CAS server correctly: • When the user first clicks on the menu, the error message appears. • If the user clicks the **OK** button or anywhere else on the screen (after getting the error message), the user sees the error message again. • If the user clicks on the menu without clicking anywhere else on the screen, the menu comes up (instead of the error) and the user can then quit/exit the Mac Agent. Therefore, if you only use the mouse (and do not clear the error message by pressing enter to trigger the **OK** button), quitting or accessing anything else in the Mac Agent is difficult. **Note** This error message makes it difficult to clear the Mac Agent from the screen and the verbiage may baffle many Mac users who do not know what “*nix” is.

Table 12 List of Closed Caveats (Sheet 3 of 3)

DDTS Number	Mac OS X Agent 4.1.3.1	
	Corrected	Caveat
CSCsm26806	Yes	The Mac OS X Agent fails to work with device filters in L3 deployment In some deployment scenarios, the Mac Agent does not work correctly with device filters based on the ROLE or CHECK settings. Layer 3 (L3) Real-IP-mode topologies do not appear to properly obtain the MAC address of the Mac Agent and apply filter policies. A discrepancy exists in an environment with the following topology: `Client---AP---Routing Devices---CAS (Real IP)---Inside Network` where the client machine entry appears as a device filter (specifying both MAC and IP address) set to “Check” the user role, resulting in the following behavior: **Windows Agent** After connecting via wireless, the Windows Agent pops up stating that authentication is being performed via a device filter and the login session completes successfully. Once this is done, the user has full access granted by the assigned role and is not redirected (desired behavior). **Mac OS X Agent** After connecting via wireless, the Mac Agent icon turns orange, stating that the session is “Not Supported,” and the user continues to receive redirects to the authentication page (user does not have the full access specified in the assigned user role). **Note** If the filter is changed from “Check” to “Assign a role,” the Mac Agent turns green rather than orange, but the end-user still receives redirects to the CAS authentication page for all web requests. This issue does *not* occur if the Mac Agent is used in an L2 setup.
CSCsm47276	Yes	Mac OS X Agent memory usage goes up with time To reproduce the issue, let the Mac Agent run for several hours or a day and watch the memory usage going up using the “top” system command.

Resolved Caveats - Release 4.1.3.1

Refer to Enhancements in Release 4.1.3.1, page 10 for additional information.

Table 13 List of Closed Caveats

	Software Release 4.1.3.1	
DDTS Number	**Corrected**	**Caveat**
CSCsm13673	Yes	CAM 4.1(3) upgrade from release 4.0(x) and 3.6(x) takes too long with too many Agent reports Clean Access Manager (CAM) 4.1(3) upgrade from Cisco NAC Appliance release 4.0(x) and 3.6(x) should not take too long with too many Clean Access Agent reports. The upgrade can take over 90 minutes on a Cisco NAC-3310 appliance with 30,000 Agent reports in the CAM database before the upgrade.
CSCsm27731	Yes	CAM should not send Auth VLAN set request when receiving MAC move notification Normally, when the CAM receives a MAC move notification, the CAM consults the client database to deduce the original managed port from which the MAC address first became known on the system, and set the port VLAN to Authentication VLAN. This operation can cause problems in certain situations. If, for example, the port over which the client first authenticated and the port to which the client is moving (per the MAC move notification SNMP trap) are same, the CAM assigns the Authentication VLAN to the port even though the client MAC address has already been certified. Although the period of time that the port remains assigned to the Authentication VLAN is very short: • If a SWISS discovery packet is sent from the client during this period, an erroneous user login popup can appear, prompting the user to enter their login credentials. • If a DHCP packet is sent from the client during this period, the client's IP may be reassigned to the Authentication VLAN.
CSCsm55679	Yes	CSRF tag is added to a global MAC device filter's description when edited If the description of a global MAC filter contains a single quote (') and you edit the description entry in the CAM web console, a CSRF tag is appended to the description when you save the changes. (The same CSRF tag is appended every time you edit and save the filter from the CAM web console.) **Note** This issue directly impacts Cisco NAC Profiler users as Profiler also includes a link in Filter List descriptions and, whenever you edit them, the same additional CSRF "token" is appended to the URL.

Resolved Caveats - Cisco NAC Web Agent 4.1.3.10

Refer to Cisco NAC Web Agent Version 4.1.3.10, page 30 for additional information.

Table 14 List of Closed Caveats

	Cisco NAC Web Agent 4.1.3.10	
DDTS Number	**Corrected**	**Caveat**
CSCsm03961	Yes	A certificate warning dialog appears even when the root certificate is trusted A warning message stating there is a mismatch between the website name and the certificate presented is displayed to end users when they launch the Web Agent in an environment which uses FQDN within certificates. This condition arises because the Web Agent tries to access the CAS via IP address and the certificate CN value has a Hostname/FQDN instead of an IP address. This causes the mismatch between the URL requested and the actual Certificate presented. **Note** If the URL called by the Web Agent is the CAS FQDN, the message does not appear. **Workaround** 1. The warning message can be ignored and the Web Agent will still function. 2. Generate certificates with an IP address for the CN instead of FQDN/Hostname.
CSCsm17435	Yes	Audit requirements should not be visible in Web Agent reports When an audit requirement is included in the requirement list, the result of the audit requirement should still be sent to the CAM/CAS, but should not be displayed on the Web Agent report. In addition, the audit check status should not affect the overall posture status.

Resolved Caveats - Windows Clean Access Agent 4.1.3.1

Refer to Windows Clean Access Agent Version 4.1.3.1, page 27 for additional information.

Table 15 List of Closed Caveats

	Clean Access Agent 4.1.3.1	
DDTS Number	**Corrected**	**Caveat**

CSCsm05207	Yes	Windows Clean Access Agent drops network connection after delayed or no ARP reply
		The Clean Access Agent transmits ARP requests for the default gateway, and if it does not receive a reply, the client automatically performs an IP address release/renew. In customer environments where the default gateway does not return an ARP reply, the 4.1.3.0 Agent can cause link-flapping.
		With version 4.1.3.1 of the Windows Clean Access Agent, the new Access to Authentication VLAN switching feature is disabled by default from regkey settings from the installer (4.1.3.1).
		Workaround
		For Windows, there is a registry key that can be set to “not check” for the ARP replies. The same is true for Mac OS X clients.
		Create one of the following registry keys:
		1. Global registry key:
		`HKEY_LOCAL_MACHINE/SOFTWARE/Cisco/Clean Access Agent/`
		`DWORD Value Name: VlanDetectInterval`
		`DWORD Value Data: 0`
		2. User-specific registry key:
		`HKEY_CURRENT_USER/SOFTWARE/Cisco/Clean Access Agent/`
		`DWORD Value Name: VlanDetectInterval`
		`DWORD Value Data: 0`
		Both of these disable the Access to Authentication VLAN switching and the Agent will no longer send ARP queries.
		The registry keys can be set from GPO or by manual registry edit. Restarting the Agent is not required. The Agent should automatically pick this new value before the next retry and turn the feature off.
		To re-enable the feature, users must restart the Agent by setting the VlanDetectInterval setting to a positive integer value or deleting the registry entry (which returns the VlanDetectInterval value to 5 seconds).
		Non-GPO Approach
		Alternatively, the administrator can create a **stopvlandetect.reg** file with a new registry key and set up a File Distribution requirement for the correct registry value. Users will fail the posture check and be required to download the file and double click it to setup the registry.

Resolved Caveats - Release 4.1(3)

Note Refer to the applicable version of the Release Notes for Cisco NAC Profiler for caveats related to Cisco NAC Profiler.

Table 16 List of Closed Caveats (Sheet 1 of 12)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCpe00141	Yes	Agent does not support multiple NICs to Cisco NAC Appliance If a client machine is connected to the wired network and a wireless card pointing to the same CAS eth1 address is also enabled, the Agent login dialog keeps popping up, even though you have logged on the wired network. And if you logged on again on the wireless, then it will still continue to popup endlessly until you disable the second NIC.
CSCse63299	Yes	DHCP slp-directory-agent option not recognized This issue is specific to Cisco NAC Appliance release 4.0(x) where the administrator tries to enable the "slp-directory-agent" on a CAS deployed in Real-IP mode is also set up to be the DHCP server. Regardless of which string the administrator enters for the option, it is not enabled and the "Option type boolean-ip-address not known" error message is displayed.

CSCse91057	Yes	Non-existent serial ports should not be displayed in HA-Failover setting
		Selecting non-existent serial ports for heartbeat communication while configuring high-availability causes the Cisco Clean Access (CCA) machine, either Clean Access Manager (CAM) or Clean Access Server (CAS), not to boot up completely. HA needs to be configured with heartbeat configured on a non-existent serial port and CCA machine should be rebooted for this issue to be observed. If a non-existent serial port is selected for heartbeat serial interface, the CCA machine cannot boot up completely since service perfigo does not start and will wait indefinitely to open the serial port for heartbeat communication on the serial port.
		Workaround:
		1. SSH to CAM and move the files configured for HA to a different location using the following commands
		`mv /etc/ha.d/perfigo.conf /tmp`
		`mv /etc/ha.d/ha.cf /tmp`
		2. Reboot the box:
		`reboot`
		3. Re-configure HA.

Table 16 List of Closed Caveats (Sheet 2 of 12)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsf19976	Yes	Changing hostname causes HA not come up On a working HA config if you change the hostname of one of the HA pairs and then reboot the box. The change in the hostname is not automatically propagated to the ha.cf file. So, even if you change the hostname on the peer to the correct value and reboot the peer, HA does not come up. Primary (where name was changed) remains in stand alone mode. The logs on primary say that ha.cf does not have the correct hostname. **Workaround** Go to the HA name on the device (where the name was changed) and just click Update (even though settings are not changed). Then reboot and HA comes up.
CSCsf98683	Yes	CAM does not send Class attribute in RADIUS accounting The CAM does not include the Class attribute when transmitting user login account information to a RADIUS server.
CSCsg32944	Yes	Active Directory SSO Service does not start when you reboot a CAS in HA mode This issue is only seen in HA. CAS-HA mechanism does not initialize the AD service completely on failover. So the SSO service remains as what its previous state was when perfigo service is started. Sometimes on rebooting the CAS, the Active Directory SSO service does not get started automatically. You have to go to **CCA Servers > Manage > Authentication > Windows Auth > Active Directory SSO** and manually click the update button to start the service. The problem is random in nature and is only seen sometimes. It appears to be a timing issue on some boxes where the KRB-Request packet from CAS does not leave the box because some network resource is not available in a timely fashion.

Table 16 List of Closed Caveats (Sheet 3 of 12)

DDTS Number	Software Release 4.1(3)	
	Corrected	Caveat
CSCsg38702	Yes	Agent does not recognize Japanese Trend AV installation. Agent properties shows “Product Name” garbled. Client OS affected: • Japanese Windows XP Professional SP2 • Japanese Windows 2000 Professional SP4 AV product affected: • Japanese VirusBaster Corporate Edition 7.3 (US Product Name: Trend Micro OfficeScan Client) To reproduce, create a new AV rule with the following attributes: • Antivirus Vendor: Trend Micro, Inc. • Type: Installation • Operating System: Windows XP/2K • Checks for Selected Operating Systems: Trend Micro OfficeScan Client, version 7.x

CSCsg98960	Yes	The Cisco NAC Appliance Release 4.1(1) installer does not recognize certain SCSI drives
		When you install release 4.1(1) code (either CAM or CAS) on certain hardware with SCSI drives, the installation process fails and displays the following message:
		“An error has occurred - no valid devices were found on which to create new filesystems. Please check your hardware for the cause of the problem”
		Workaround
		At the boot prompt that appears during installation, enter “DL140” and then press <Enter>.
		`Cisco Clean Access Installer (C) 2006 Cisco Systems, Inc.`
		`Welcome to the Cisco Clean Access Installer!`
		`- To install a Cisco Clean Access device, press the <ENTER> key.`
		`- To install a Cisco Clean Access device over a serial console, enter serial at the boot prompt and press the <ENTER> key.`
		`boot: `**`DL140`**
		Note Upgrades to release 4.1(1) from previous versions are not affected by this bug.

Table 16 List of Closed Caveats (Sheet 4 of 12)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsh84260	Yes	User gets redirected to CAS after successful web login using a Safari browser in Mac OS X When functioning normally, a Mac OS X client browser opens another window that displays the original URL requested at login following successful authentication. The issue in this case, however, is that the Safari 2.0.3 browser on the client opens another window displaying the CAS web login form over again.
CSCsi33630	Yes	CAM/CAS should not pull all old data when getting support logs When the option to download the support logs from the Clean Access Manager and/or Clean Access Server is used download a .tar archive of the logs, the entire history of that CAM or CAS is downloaded resulting in massive log files with very little relevant content which are downloaded by the customer and sent to Cisco TAC to troubleshoot the Clean Access system.
CSCsi44112	Yes	'service perfigo config' wipes secondary dns servers and host name 'service perfigo config' does not preserve search domain and secondary DNS servers in file /etc/resolv.conf. If a host domain and more than one DNS server has been entered in the CAM Web Console, these entries are wiped even if the DNS server entry is not modified. At this point, service perfigo config does not prompt for a host domain value and deletes the entry without verification.
CSCsi47547	Yes	AD SSO does not work if the CAS Account Password contains “()” When CAS account password contains parentheses “()”, the AD SSO service does not start after entering the “Service perfigo restart” command.
CSCsi62063	Yes	SSLVPN Single Sign On with ISR is unsuccessful The user can log onto the SSLVPN gateway, but is then asked for logon credentials again when trying to access the trusted network.
CSCsi75692	Yes	HTTP 500 error when attempting to upload a file to CAS When the administrator tries to upload a file to the CAS via the CAM web console, the CAM returns an HTTP 500 error message. This error appears when the admin chooses Authentication > Login Page and clicks File Upload when managing the CAS from the CAM web console. **Note** In addition to the HTTP 500 error message, the actual file upload function fails, as well.
CSCsi78024	Yes	Guest Access option fails if the provider option is not Local DB Under Web Login page, the Guest Access option does not work if the Provider is anything other than the local database. To enable the Guest option, change the Provider to “Local DB” and click the Guest Access button.

Table 16 List of Closed Caveats (Sheet 5 of 12)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsi79315	Yes	Nessus Scanner: unable to update "SMB domain (optional)" value Administrators cannot update or remove the preference value for the SMB domain specified under **Device Management > Clean Access > Network Scanner > Options > "Login Configurations" Category > Preference Name SMB**.
CSCsi83381	Yes	Clean Access presents an erroneous popup window when case-insensitive is enabled When the Case-Insensitive option under a user role is enabled, the Clean Access system returns a popup window for users after they log in through the web interface.
CSCsi90893	Yes	No message goes to perfigo-log when user cannot add CAS to CAM When a user exceeds the maximum number of CAS licenses or there is no CAS license present, the Clean Access system logs an entry in the event log, but not in the perfigo-log. For consistency and ease of troubleshooting, both logs should feature the event as most other CAS/CAM issues are already logged in both places.
CSCsi94224	Yes	When setting up mapping rules for AD SSO where multiple VLANs are also added to the rule, the Clean Access system returns an Internal Server Error.
CSCsi97216	Yes	CAM does not change port to Authentication VLAN when Certified Devices List is cleared using a port bounce When the CDL is cleared, the CAM does one of the following, depending on the **Remove out-of-band online user without bouncing the port** profile setting: • If the port setting is enabled (checked), the CAM changes the port to Authentication VLAN, but does not bounce the port. • If the above setting is disabled (unchecked), the CAM bounces the port, but does not change it to Authentication VLAN. The CAM must change the port to the Authentication VLAN every time the CDL is cleared (i.e., when user is removed from the Online Users list) regardless of whether the port is bounced or not.

Table 16 List of Closed Caveats (Sheet 6 of 12)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsj00939	Yes	Non-URL right frame content not displayed to end users When using a Frame-based design for the login page, the content on the right frame is not displayed to the end user when the content is HTML or text entered in the CAM web console page. Although the preview displays correctly (as preview is from the CAM), the end user does not see the content on the right frame when it is presented from the CAS. **Workaround options** **1.** Use a URL on the right frame instead of HTML or text content. **Note** You will need to open access to URL in the Unauthenticated role as documented. **2.** Use a frameless approach.
CSCsj05227	Yes	OOB VGW controlling native VLAN can cause intermittent connectivity An OOB virtual gateway CAS managing client access via changing a “dot1x” trunk VLAN (rather than the much more common practice of changing the client access VLAN) can introduce connectivity issues due to a potential ARP request loop condition. The Cisco NAC Appliance system introduces a condition where the ARP request is looped back to the switch from which the request originated. If this repeat packet reaches the client machine before the ARP reply, the client may never receive the ARP reply. One potential solution is to block broadcasts from the trusted to the untrusted interface originating from the specified client IP or MAC addresses that are already associated with the Access VLAN. This scenario, however, could potentially deny traffic (including DHCP) when users log in from another physical location.
CSCsj05741	Yes	Spaces in Distinguished Name (DN) cause LDAP authentication failure When attempting an auth test with an LDAP provider, if the DN contains a space, the auth fails and returns a “LDAP: error code 49” message. The space can be anywhere in the DN, and is represented with the %20 escape character found in the perfigo-log. **Note** There could also be a “,” or other special character in the DN. For example, “CN= Doe, Jane”.
CSCsj08474	Yes	Release 4.0(x) does not allow same default gateway for multiple subnets A check was added in release 4.0(x) to prevent administrators from specifying the same default gateway for more than one IP subnet range in the DHCP subnet list. This check can prove problematic for customers upgrading to 4.0(x) from 3.5.7 out of necessity to support Windows Vista because they must modify the setup to have a separate default gateway/VLAN for every /24 network, which can place additional routing burden on CAS.

Table 16 List of Closed Caveats (Sheet 7 of 12)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsj08522	Yes	HA-CAM should check the database schema before sync to prevent corruption When an administrator upgrades between various 4.x.x releases of CCA and leaves the secondary CAM up during upgrade, the database can become corrupted.
CSCsj13933	Yes	New AV Rules does not work for Japanese Trend Micro AV When a New AV Rule is created for Japanese Trend Micro under Clean Access > Clean Access Agent > Rules > New AV Rule > Antivirus Vendor: Trend Micro, Inc., Type: “Installation” & “Virus Definition”, the created rule does not work (always fails) for AV product Japanese Trend Micro AV.
CSCsj15078	Yes	VLAN profile should accept wildcard specified in port profile Administrators can enter port profile VLAN names using wildcards, but Cisco NAC Appliance only uses the wildcard on the switch, not the local VLAN profile.
CSCsj18239	Yes	Requirement Description field does not allow double-quotes When adding a description to a requirement if double quotes are used any text after the first double quote will be removed after a save. Also the text will not be included in the agent report. Single quotes are acceptable.
CSCsj29701	Yes	Agent may pop up again after login in OOB deployment In an OOB deployment, the Agent login screen may pop up again after login when it gets a SWISS response between successful login and the CAMs authorization-to-access VLAN change. During this period, SWISS thinks Agent is not authenticated and continues sending UDP discovery packets while the CAM is about to set the access VLAN for the Agent.
CSCsj33552	Yes	fostate.sh shows incorrect UI status The fostate.sh command displays a result of “My node is standby without web console, peer node is active” when the web console is unavailable. This occurs after the standby CAM recovers from an active-active CAM HA status. Steps to reproduce 1. Unplug the heartbeat interface of the CAM HA pair. 2. Both CAMs become active. 3. Reconnect the heartbeat interface. 4. The new standby CAM will show “My node is standby without web console, peer node is active”, but actually the web console is unavailable. **Workaround** Reboot the standby CAM to start the web console and correct the status.

Table 16 List of Closed Caveats (Sheet 8 of 12)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsj36082	Yes	Device Filter assigns incorrect user role With Device Filters configured for MAC addresses in the network, the Clean Access system assigns incorrect roles to user profiles.
CSCsj36576	Yes	VLAN Passthrough should be disabled in Real-IP Gateway mode Pass through VLAN ID to trusted network is not a valid setting for Real-IP Gateway mode and should be either greyed out or hidden when the CAS is configured as a Real-IP Gateway. **Note** NAT and 1-1 NAT should also be disabled in non-NAT gateway.
CSCsj49408	Yes	Clean Access Agent lists Microsoft Forefront as an "Unknown" Microsoft Product Clean Access Agent 4.0.5.1 and 4.1.1.0 do not properly detect the Microsoft Forefront Client even though it is listed as a supported product for these platforms.
CSCsj50387	Yes	AD SSO service may stop on the CAS if the DC has dynamic IP When the "Domain" option is selected for Windows Authentication, the CAS does not query DNS for the domain once the TGT is expired. If the DC IP address changes during this time, the ADSSO service fails because the CAS tries to connect using the old IP address.
CSCsj54337	Yes	No guest access for PocketPC devices Customer has a wireless PocketPC devices connected for guest access. Cisco NAC Appliance displays the web login page that the administrator has configured, but the guest access button i only appears as text. (There is no button to click to continue the authentication process.)
CSCsj62927	Yes	ADSSO service stops on the CAS if the CAS Admin password is changed
CSCsj76706	Yes	Clicking refresh on the switch management screen can reset all parameters to factory default settings Clicking the **Refresh** button repeatedly on the browser while editing an OOB switch in a Virtual Gateway environment eventually results in an "Unable to control this switch" error message and the switch is reset to default values.

Table 16 List of Closed Caveats (Sheet 9 of 12)

DDTS Number	Software Release 4.1(3)	
	Corrected	**Caveat**

CSCsj84398	Yes	"hda" error appears with specific Seagate hard drive model on Cisco NAC-3310
		An "hda" error message shows up on Cisco NAC-3310s with a specific Seagate hard drive model. (A known test issue was discovered and recorded with the Seagate hard drive model ST380815AS featuring "HPFO" firmware.)
		As a result, the following error message appears on the user console and is logged in the /var/log/messages file:
		`hda: status timeout: status=0xd0 { Busy }`
		
		`ide: failed opcode was: unknown`
		`hda: no DRQ after issuing MULTWRITE_EXT`
		`ide0: reset: success`

CSCsk05330	Yes	Clean Access Agent does not work in 64-bit Windows operating systems
CSCsk07841	Yes	AD/LDAP Auth test does not display all attributes used for mapping
CSCsk08870	Yes	Web proxy settings are erroneously cached The proxy password update fails when the proxy password expires and is changed in a Cisco NAC Appliance system using basic authentication. **Note** If the admin restarts the "perfigo services" after changing the password, the proxy uses the new password.
CSCsk09542	Yes	Subnet filter allows a space at the end of the network address Under **Device Management > Filters > Subnets**, the user interface allows you to add subnet address with a space at the end. When CAM publishes the configuration, you should see the following error in write handler "'publish_add' for 'Filter_table::Linear IP Filter2' argument 2 takes IP addresses"
CSCsk11463	Yes	4.1.2.0 Mac OS X Agent does not start on login
CSCsk15081	Yes	Apple iPhone should not be categorized as Mac OS X Apple iPhone users are categorized as Mac OS X users (in the online user list, for example). Because the Mac Agent does not support iPhone, we should not categorize iPhone users as Mac OS X.
CSCsk18401	Yes	Clean Access Agent incorrectly categorizes the Windows Vista "32-bit" operating system as "64-bit" An installed 32-bit Windows Vista Agents appears to be a "64-bit" Agent in the debug log. The operating system also appears incorrectly in the CAM Online User list, Agent report file, and Agent debug logs.

Table 16 List of Closed Caveats (Sheet 10 of 12)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsk20213	Yes	The Windows Vista Clean Access Agent fails Windows Update check in the Korean time zone The Clean Access Agent for clients running the Windows Vista operating system fail the Windows Update check because the Agent and operating system use different delimiters for date formats. (The Windows Vista operating system uses a (yyyy-mm-dd) date format while the Clean Access Agent uses (yyyy/mm/dd).
CSCsk31476	Yes	Windows Server Update Services Requirement "Show UI" option not working on Windows XP client machines When you configure the Windows Server Update Services (WSUS) Requirement to show the update interface session to users with the "Show UI" Installation Wizard Interface Setting, Windows XP client machines install the latest windows update software (currently wuaueng.dll version 7.0.6000.381), but the Clean Access Agent only displays a grey window instead of the expected "Download and Install Updates" window. **Workaround** To avoid this issue, be sure to specify "No UI" for the Installation Wizard Interface Setting on your CAM's Windows Server Update Services Requirement configuration page (**Device Management > Clean Access > Clean Access Agent > Requirements > New/Edit**).
CSCsk35149	Yes	Cisco NAC Appliance needs an error check to see if the server is reachable This situation applies to the Clean Access Agent as well as CAM and CAS, where the report on the CAM either indicates a failure with no accompanying information, or indicates a failure with the messages "Failed to find Windows Updates" and "Missing Windows updates: 0."
CSCsk46439	Yes	Clean Access Server does not replicate all CAM settings Not all parameters are properly replicated to the secondary CAS when configuring an HA pair.
CSCsk46672	Yes	CAS stops listening on 8910 after threads in CLOSE_WAIT state The Agent cannot perform AD SSO when the CAS is no longer listening on port 8910 due to a large number of threads in CLOSE_WAIT state. **Workaround** Under **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth**, click **Update** on the SSO service to flush the CLOSE_WAIT states. **Note** Starting from release 4.1(3), L3 OOB Real-IP Gateway deployments using AD SSO require the CAS SSL certificate to be generated using the untrusted IP address of the CAS. Refer to Settings That May Change With Upgrade, page 93 for details.

Table 16 List of Closed Caveats (Sheet 11 of 12)

DDTS Number	Software Release 4.1(3)	
	Corrected	Caveat
CSCsk53735	Yes	Trend Micro Client/Server Security Agent 7.6 not detected The Cisco NAC Appliance release 4.1(2) Agent does not correctly detect version 7.6 of the Trend Micro Client Security Agent.
CSCsk58244	Yes	Clean Access Report for WSUS shows failed This situation applies to Windows XP and Windows Vista client machines. The Agent report on the CAM does not show any on the updates required for the client.
CSCsk66548	Yes	Ports revert to default profile values if the CAM fails to appropriately retrieve the port list from the switch.
CSCsk83429	Yes	Vista client machines are not able to renew their IP address if UAC is enabled When using the 4.12.1 Clean Access Agent on a Vista client in an OOB setup, the client machine should receive a new IP address when it moves to a different VLAN, but the client is unable to refresh the IP address if UAC (Vista User Account Control) is enabled. Once UAC is disabled, the client is able to successfully retrieve the new IP address.
CSCsk88803	Yes	Cannot enter quotations when configuring Launch Program requirement If you configure a Launch Programs requirement type to start a service on a client and use the "net start" command, you need to use quotations if the Service Name is more than one word. However, if you enter quotes, as soon as you save the requirement, everything after the first quotation mark disappears.
CSCsk91135	Yes	SNMP walk takes too much CPU The "snmpwalk" function used by HP Openview (and other SNMP-based management platforms) results in very high CPU utilization on the Clean Access Manager.
CSCsk96328	Yes	Configuration update initializes **/etc/hosts** file Clicking **Update** in CAS HA configuration causes /etc/hosts file initialization without any alerts. **Note** The **/etc/hosts** file may also be initialized from `service perfigo config`, updating the Network page, or updating the DNS page.
CSCsk98601	Yes	iPod Touch recognized as Mac OS X The new iPod Touch is recognized as Mac OS X instead of Mac_All. This is similar to CSCsk15081.
CSCsl04222	Yes	Clean Access fails to check a file modification date against the CAM date If a check is created to check a file modification date and it is selected to compare the date to be +/- days from the current date on the CAM, then the check fails even if the file is up to date.

Table 16 List of Closed Caveats (Sheet 12 of 12)

	Software Release 4.1(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsl06922	Yes	Cannot add a more specific static route when managed subnet exists in Virtual Gateway mode If you define a managed subnet for a subnet range, but want one host (DC, etc.) on the trusted side, you can define a static route. However, once you reboot the CAS, the managed subnet entry gets deleted from the real_routing_table and leaves the /32 route in the table. **Note** Both routes exist in the table after you reboot the CAS in Real-IP mode.
CSCsl10185	Yes	CAM is unable to get port list from switch After a period of time, memory use climbs and the CAM becomes unable to control a switch until it can be restarted.
CSCsl52603	Yes	Clean Access failover does not work with HA CAS pair behind a NAT device CAS failover does not work when the CASes are deployed behind a NAT device and the CAM only knows of the translated IP address. Whenever a Secondary CAS takes over a service IP in an HA pair environment, it automatically tries to connect to the CAM and send a key and the service IP address it is taking over (via https). The CAM then attempts to verify this IP address against the known service IP address found in its **/etc/hosts** file. Since the CAS has pushed out the untranslated service IP to the CAM, and the CAM does not know that address (because it has been NATed), communication between the CAM and CAS fails.
CSCsl76977	Yes	Direct upgrade from 3.5(11) to 4.1(3) is not supported "In-place" upgrade from version 3.5(11) to 4.1(3) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(3) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(3) via the instructions in Upgrading to 4.1(3), page 92. Refer to the "In-Place Upgrade from 3.5(7)+ to 4.0(x)" instructions for Standalone Machines or HA-pairs in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.0(6)* for details. You can download the upgrade from 3.5(11) to 4.0(6) at: http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-4.0.6
CSCsl80459	Yes	Auto updates for Cisco Checks and Rules fail on Clean Access Manager

Known Issues for Cisco NAC Appliance

This section describes known issues when integrating Cisco NAC Appliance:

- Known Issues with HP ProLiant DL140 G3 Servers

- Known Issue with NAC-3310 CD Installation
- Known Issues with NAC-3300 Series Appliances and Serial HA (Failover) Connection
- Known Issues with Cisco NAC Profiler Release 2.1.7
- Known Issues with Switches
- Known Issue with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs)
- Known Issues with Broadcom NIC 5702/5703/5704 Chipsets
- Known Issues for Windows Vista and Agent Stub, page 89
- Known Issues with MSI Agent Installer
- Known Issue with Windows 2000 Clean Access Agent/Local DB Authentication
- Known Issue with Windows 98/ME/2000 and Windows Script 5.6

Note For additional information, see also Troubleshooting, page 109.

Known Issues with HP ProLiant DL140 G3 Servers

The NAC-3310 appliance is based on the HP ProLiant DL140 G3 server and is subject to any BIOS/firmware upgrades required for the DL140 G3. Refer to *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for detailed instructions.

Known Issue with NAC-3310 CD Installation

The NAC-3310 appliance (MANAGER and SERVER) requires you to enter the **DL140** or **serial_DL140** installation directive at the "boot:" prompt when you install new system software from a CD-ROM.

When following the CD-ROM system software installation procedures outlined in Chapter 2: "Installing the Clean Access Manager" of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(3)* and Chapter 4: "Installing the Clean Access Server NAC Appliance" of the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(3)*, users installing release 4.1(3) on a NAC-3310 appliance (both MANAGER and SERVER) from a CD-ROM are presented with the following prompt during the installation process:

```
Cisco Clean Access Installer (C) 2007 Cisco Systems, Inc.
Welcome to the Cisco Clean Access Installer!
- To install a Cisco Clean Access device, press the <ENTER> key.
- To install a Cisco Clean Access device over a serial console, enter serial at the boot
prompt and press the <ENTER> key.
boot:
```

The standard procedure asks you to press "Enter" or, if installing via serial console connection, enter **serial** at the "boot:" prompt, For release 4.1(3) and later, however, NAC-3310 customers are required enter one of the following, instead:

- **`DL140`**—if you are directly connected (monitor, keyboard, and mouse) to the NAC-3310
- **`serial_DL140`**—if you are installing the software via serial console connection

After you enter either of these commands, the Package Group Selection screen appears where you can then specify whether you are setting up a Clean Access Manager or Clean Access Server and install the system software following the standard installation process.

Known Issues with NAC-3300 Series Appliances and Serial HA (Failover) Connection

When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances and any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.

Known Issues with Cisco NAC Profiler Release 2.1.7

Cisco NAC Appliance Release 4.1(3) does not support Cisco NAC Profiler Release 2.1.7. If you are currently running Cisco NAC Appliance Release 4.1(2) and Cisco NAC Profiler Release 2.1.7 on your network, it is recommended to upgrade your Cisco NAC Profiler system to a compatible release first (such as upcoming release 2.1.8) before upgrading your Cisco NAC Appliance machines to release 4.1(3).

Note You will need to upgrade the Collector component on the 4.1(3) and later CAS for compatibility with the Cisco NAC Profiler Server.

Note Cisco NAC Profiler Release 2.1.7 does not support Out-of-Band deployments or Layer 3 In-Band deployments.

Refer to the *Release Notes for Cisco NAC Profiler* for updated product information.

Known Issues with Switches

For complete details, see *Switch Support for Cisco NAC Appliance*.

Known Issue with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs)

Due to changes in DHCP server operation with Cisco NAC Appliance release 4.0(2) and later, networks with Cisco 2200/4400 Wireless LAN Controllers (also known as Airespace WLCs) which relay requests to the Clean Access Server (operating as a DHCP server) may have issues. Client machines may be unable to obtain DHCP addresses. Refer to the “Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs) and DHCP” section of *Switch Support for Cisco NAC Appliance* for detailed instructions.

Note For further details on configuring DHCP options, see the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(3)*.

Known Issues with Broadcom NIC 5702/5703/5704 Chipsets

Customers running Cisco NAC Appliance release 4.1(3) and later on servers with 5702/5703/5704 Broadcom NIC cards may be impacted by caveat CSCsd74376. Server models with Broadcom 5702/5703/5704 NIC cards may include: Dell PowerEdge 850, CCA-3140-H1, HP ProLiant DL140 G2/DL360/DL380. This issue involves the repeated resetting of the Broadcom NIC cards. The NIC cards do not recover from some of the resets causing the machine to become unreachable via the network.

For details, see the *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*.

Known Issues for Windows Vista and Agent Stub

Use "No UI" or "Reduced UI" Installation Option

When installing the 4.1.3.0 Clean Access Agent via stub installation on Windows Vista machines only, Cisco recommends **not** to use the **Full UI** Stub Installation Option. To avoid the appearance of 5-minute installation dialog delays caused by the Vista Interactive Service Detection Service, Cisco recommends using the **No UI** or **Reduced UI** option when configuring Stub Installation Options for Windows Vista client machines.

"Interactive Services Dialog Detection" and Uninstall

When non-admin users install/uninstall the Clean Access Agent through the Agent Stub service on Windows Vista, they will see an "Interactive Services Dialog Detection" dialog. If the user is installing, no input is required in the dialog session—it will automatically disappear. If the client machine is fast, the user may not even see the dialog appear at all, so the resulting behavior is as if the Agent gets silently installed after a few seconds. When uninstalling, however, the uninstall process does not complete until the user responds to a prompt inside the dialog.

This is expected behavior because, unlike earlier Windows operating systems, Windows Vista services run in an isolated session (session 0) from user sessions, and thus do not have access to video drivers. As a workaround for interactive services like the Agent Stub installer, Windows Vista uses an Interactive Service Detection Service to prompt users for user input for interactive services and enable access to dialogs created by interactive services. The "Interactive Service Detection Service" will automatically launch by default and, in most cases, users are not required to do anything. However, if the service is disabled for some reason, Agent installation by non-admin users will not function.

Known Issues with MSI Agent Installer

MSI File Name

The MSI installation package for each version of the full Windows Clean Access Agent (CCAAgent-<version>.msi) is available for download from the Cisco Software Download site at http://www.cisco.com/pcgi-bin/tablebuild.pl/cca-agent

When downloading the Clean Access Agent MSI file from the Cisco Software Download site, you MUST rename the "CCAAgent-<version>.msi" file to "**CCAAgent.msi**" before installing it.

Renaming the file to "CCAAgent.msi" ensures that the install package can remove the previous version then install the latest version when upgrading the Agent on clients.

Minor Version Updates

You cannot upgrade minor version (4th digit) updates of the Clean Access Agent from the MSI package directly. You must uninstall the program from Add/Remove programs first before installing the new version. Refer to CSCsm20655, page 64 for details.

See also Troubleshooting, page 109 for additional Agent- related information.

Known Issue with Windows 2000 Clean Access Agent/Local DB Authentication

When a user logs in via the Clean Access Agent on a Windows 2000 machine with a username/password linked to the "Local DB" provider and must validate a requirement (in a test environment, for example), the Agent returns a "The application experienced an internal error loading the SSL libraries (12157)" error message. Following the error message, the Agent remains in the login state even though it is not actually logged in and the user must either stop the process or restart the client machine for the Agent login dialog to re-appear. (Requirements are not validated and the CAM does not create an Agent report for the Windows 2000 session, so it can be difficult to determine which requirement fails.)

Known Issue with Windows 98/ME/2000 and Windows Script 5.6

Windows Script 5.6 is required for proper functioning of the Clean Access Agent in release 3.6(x) and later. Most Windows 2000 and older operating systems come with Windows Script 5.1 components. Microsoft automatically installs the new 5.6 component on performing Windows updates. Windows installer components 2.0 and 3.0 also require Windows Script 5.6. However, PC machines with a fresh install of Windows 98, ME, or 2000 that have never performed Windows updates will not have the Windows Script 5.6 component. Cisco Clean Access cannot redistribute this component as it is not provided by Microsoft as a merge module/redistributable.

In this case, administrators will have to access the MSDN website to get this component and upgrade to Windows Script 5.6. For convenience, links to the component from MSDN are listed below:

Win 98, ME, NT 4.0:

Filename: scr56en.exe

URL:
http://www.microsoft.com/downloads/details.aspx?familyid=0A8A18F6-249C-4A72-BFCF-FC6AF26DC390&displaylang=en

Win 2000, XP:

Filename: scripten.exe

URL:
http://www.microsoft.com/downloads/details.aspx?familyid=C717D943-7E4B-4622-86EB-95A22B832CAA&displaylang=en

Tip If these links change on MSDN, try a search for the file names provided above or search for the phrase "Windows Script 5.6."

New Installation of Release 4.1(3)

If you are performing a new CD software installation of Cisco NAC Appliance (Cisco Clean Access) on the Cisco NAC Appliance 3300 Series server hardware platform, use the steps described below.

If re-imaging a Cisco NAC Network Module, refer to the instructions in the *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*.

If performing upgrade on an existing NAC Appliance or NAC Network Module, refer to the instructions in Upgrading to 4.1(3), page 92.

For New Installation:

1. If you are going to perform a new installation but are running a previous version of Cisco Clean Access, back up your current Clean Access Manager installation and save the snapshot on your local computer, as described in General Preparation for Upgrade, page 94.
2. Follow the instructions on your welcome letter to obtain a license file for your installation. See Cisco NAC Appliance Service Contract/Licensing Support, page 2 for details. (If you are evaluating Cisco Clean Access, visit http://www.cisco.com/go/license/public to obtain an evaluation license.)
3. Install the latest version of 4.1(3) on each Clean Access Server and Clean Access Manager, as follows:
   - Log in to Cisco Secure Software and download the latest 4.1.3.x .ISO image from http://www.cisco.com/public/sw-center/ciscosecure/cleanaccess.shtml and burn it as a bootable disk to a CD-R.
   - Insert the CD into the CD-ROM drive of each installation server, and follow the instructions in the auto-run installer.
4. After software installation, access the Clean Access Manager web admin console by opening a web browser and typing the IP address of the CAM as the URL. The Clean Access Manager License Form will appear the first time you do this to prompt you to install your FlexLM license files.
5. Install a valid FlexLM license file for the Clean Access Manager (either evaluation, starter kit, or individual license). You should have already acquired license files as described in Cisco NAC Appliance Service Contract/Licensing Support, page 2.
6. At the admin login prompt, login with the default user name and password **`admin/cisco123`** or with the web console username and password you configured when you installed the Clean Access Manager.
7. In the web console, navigate to **Administration > CCA Manager > Licensing** if you need to install any additional FlexLM license files for your Clean Access Servers.
8. For detailed software installation steps and further steps for adding the Clean Access Server(s) to the Clean Access Manager and performing basic configuration, refer to the following guides:
   - *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(3)*
   - *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(3)*

Note Clean Access Manager 4.1(3) is bundled with Clean Access Agent 4.1.3.0.

Upgrading to 4.1(3)

This section provides instructions for how to upgrade your existing Cisco Clean Access system to release 4.1(3).

Refer to the following general information prior to upgrade:

- Notes on 4.1(3) Upgrade
- Settings That May Change With Upgrade
- General Preparation for Upgrade

Refer to one of the following sets of upgrade instructions for the upgrade you need to perform:

- Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—Standalone Machines
- Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—HA Pairs

If you need to perform a fresh installation of the software, refer instead to New Installation of Release 4.1(3), page 91.

If you need to upgrade from a much older version of Cisco Clean Access, you may need to perform an interim upgrade to a version that is supported for upgrade to 4.1(3). In this case, refer to the applicable *Release Notes* for upgrade instructions for the interim release. Cisco recommends always testing new releases on a different system first before upgrading your production system.

Notes on 4.1(3) Upgrade

If planning to upgrade to Cisco NAC Appliance (Cisco Clean Access) 4.1(3) ED and later, note the following:

Warning **The standard period of time required to upgrade is approximately 10 to 20 minutes. If you are upgrading from release 3.6(x) or 4.0(x) to release 4.1(3) and later, depending on the size of your existing Agent Report log, the upgrade process may take longer than usual. For example, if your Agent Report log is relatively large (~30,000 entries) the upgrade process from 3.6(x) to Release 4.1.3.1 could take around 40 minutes.**

To help avoid longer upgrade times, delete Agent Report entries (under Device Management > Clean Access > Clean Access Agent > Reports) before upgrading from release 3.6(x) or 4.0(x) to release 4.1(3) and later. Alternatively, you can upgrade from release 3.6(x) or 4.0(x) to release 4.1.2.1 and *then* upgrade to release 4.1(3) and later.

- Only releases 4.1(3)+, 4.1(2)+, and 4.1(1)+ can be installed on Cisco NAC Appliance 3300 Series platforms.
- You can upgrade your Cisco NAC Network Module(s) from release 4.1(2) to release 4.1(3) or later via web upgrade, just like any other Clean Access Server. If upgrading to release 4.1(3) or later, you must also upgrade all other CAM/CAS appliances on your network.

Note Cisco NAC Network Module is supported starting from release 4.1(2) and later only.

- While upgrading to release 4.1(3) or later is not required to support Cisco NAC network modules, if you are supporting 64-bit Windows Vista client systems, you must upgrade to release 4.1.2.1 or later.

- Windows Vista is supported starting from release 4.1(1) and version 4.1.1.0 of the Agent, with the exception of the 4.1.2.1, 4.1.2.0, and 4.1.1.0 Agent Stub installers, which are not supported on Windows Vista.
- Cisco NAC Appliance (Cisco Clean Access) release 4.1(3) ED is a major software release with Early Deployment status.

Caution "In-place" upgrade from version 3.5(11) to 4.1(3) and later is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(3) and later must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(3) and later via the instructions in Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—Standalone Machines, page 95 or Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—HA Pairs, page 104. (See CSCsl76977.)

Refer to the "In-Place Upgrade from 3.5(7)+ to 4.0(x)" instructions for Standalone Machines or HA-pairs in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.0(6)* for details.

- Cisco recommends using the console/SSH upgrade procedure to upgrade appliance hardware from release 3.6(x), 4.0(x), or 4.1(0)+, or 4.1.(2)+ to release 4.1(3) and later. See Console/SSH Upgrade—Standalone Machines, page 101.
- When upgrading from 3.6(x)/4.0(x) to the latest 4.1(x) release:
  - You can only perform web console upgrade on standalone non-HA CAM machines if they have already been patched for caveat CSCsg24153.
  - If the system has not already been patched, upgrade all your machines via console/SSH.
  - Standalone CAS machines must still be upgraded using the console/SSH upgrade procedure.

  For further details on Patch-CSCsg24153, refer to the README-CSCsg24153 file under http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches and the associated Resolved Caveats table entry in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(0)*.

Warning **Web upgrade is NOT supported for software upgrade of HA-CAM pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs, page 107.**

- If you have existing users, test the ED release in your lab environment first and complete a pilot phase prior to production deployment.

Note Your production license will reference the MAC address of your production CAM. When testing on a different machine before upgrading your production Cisco NAC Appliance environment, you will need to get a trial license for your test servers. For details, refer to *Cisco NAC Appliance Service Contract/Licensing Support*.

Settings That May Change With Upgrade

- **AD SSO and L3 OOB Real-IP Gateway Deployments**: Starting from release 4.1(3), L3 OOB Real-IP Gateway deployments using AD SSO require the CAS SSL certificate to be generated using the untrusted IP address. If the certificate is generated with the CAS trusted IP address, AD SSO will fail after upgrade to 4.1(3) and later. You will need to regenerate the certificate. If using

FQDN-based certificates, simply change the DNS entry to point to the CAS untrusted interface. This allows the Agent to send traffic to port 8910 on the untrusted interface. See caveat CSCsk46672, page 84 for additional details.

- **5702/5703/5704 Broadcom NIC chipsets:** If your system uses 5702/5703/5704 Broadcom NIC chipsets, and you are upgrading from 4.1(2)+, 4.1(1)+, 4.1(0)+, 4.0(x), or 3.6(x), or 3.5(x), you will need to perform a firmware upgrade from HP. See Known Issues with Broadcom NIC 5702/5703/5704 Chipsets, page 89 for details.
- **Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs)**: If using the CAS as a DHCP server in conjunction with Airespace WLCs, you may need to configure DHCP options as described in Known Issue with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs), page 88.
- **OOB Deployments:** Because Cisco NAC Appliance can control switch trunk ports for OOB (starting from release 3.6(1) +), please ensure the uplink ports for controlled switches are configured as “uncontrolled” ports either before or after upgrade.

Note For additional OOB troubleshooting, see *Switch Support for Cisco NAC Appliance*.

- **DHCP Options:** When upgrading from 3.5/3.6 to 4.1(3) and later, any existing DHCP options on the CAS are not retained. Administrators must re-enter any previously configured DHCP options using the newly-enhanced **Global Options** page.
- **SNMP Settings:** When upgrading from 3.5 to 4.1(3) and later, any existing SNMP traps configured on the CAM are not retained. Administrators must re-enter any previously configured SNMP settings using the **SNMP** page.

General Preparation for Upgrade

Caution Please review this section carefully before commencing any Cisco NAC Appliance upgrade.

- **Homogenous Clean Access Server Software Support**

  You must upgrade your Clean Access Manager and all your Clean Access Servers (including NAC Network Modules) concurrently. The Cisco NAC Appliance architecture is not designed for heterogeneous support (i.e., some Clean Access Servers running 4.1(3) and later software and some running 4.1(2), 4.1(1), 4.1(0), or 4.0(x) software).
- **Upgrade Downtime Window**

  Depending on the number of Clean Access Servers you have, the upgrade process should be scheduled as downtime. For minor release upgrades (e.g. 4.1(3) to 4.1.3.x), our estimates suggest that it takes approximately 10 to 20 minutes for the Clean Access Manager upgrade and 10 minutes for each Clean Access Server upgrade. Use this approximation to estimate your downtime window.

Warning **The standard period of time required to upgrade is approximately 10 to 20 minutes. If you are upgrading from release 3.6(x) or 4.0(x) to release 4.1(3) and later, depending on the size of your existing Agent Report log, the upgrade process may take longer than usual. For example, if your Agent Report log is relatively large (~30,000 entries) the upgrade process from 3.6(x) to Release 4.1.3.1 could take around 40 minutes.**

To help avoid longer upgrade times, delete Agent Report entries (under Device Management > Clean

Access > Clean Access Agent > Reports) before upgrading from release 3.6(x) or 4.0(x) to release 4.1(3) and later. Alternatively, you can upgrade from release 3.6(x) or 4.0(x) to release 4.1.2.1 and *then* upgrade to release 4.1(3) and later.

- **Clean Access Server Effect During Clean Access Manager Downtime**

  While the Clean Access Manager upgrade is being conducted, the Clean Access Server (which has not yet been upgraded, and which loses connectivity to the Clean Access Manager during Clean Access Manager restart or reboot) continues to pass authenticated user traffic.

Caution New users will not be able to logon or be authenticated until the Clean Access Server reestablishes connectivity with the Clean Access Manager.

- **High Availability (Failover) Via Serial Cable Connection**

  When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances, and for any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.

- **Database Backup (Before and After Upgrade)**

  For additional safekeeping, Cisco recommends manually backing up your current Clean Access Manager installation (using **Administration > Backup**) both before and after the upgrade and to save the snapshot on your local computer. Backing up prior to upgrade enables you to revert to your previous release database should you encounter problems during upgrade. Backing up immediately following upgrade preserves your upgraded tables and provides a baseline of your 4.1(3) database. After the migration is completed, go to the database backup page (**Administration > Backup**) in the CAM web console. Download and then delete all earlier snapshots from there as they are no longer compatible. See Create CAM DB Backup Snapshot, page 96 for details.

Warning **You cannot restore a CAM database from a snapshot created using a different release. For example, you cannot restore a 4.1(2) or earlier database snapshot to a 4.1(3) CAM.**

- **Software Downgrade**

  Once you have upgraded your software to 4.1(3) or later, if you wish to revert to your previous version of CCA software, you will need to reinstall the previous CCA version from the CD and recover your configuration based on the backup you performed prior to upgrading to 4.1(3) or later.

- **Passwords**

  For upgrade via console/SSH, you will need your CAM and CAS `root` user password (default CAM root password is `cisco123`). For web console upgrade, you will need your CAM web console `admin` user password (and, if applicable, CAS direct access console `admin` user password).

Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—Standalone Machines

This section describes the upgrade procedure for upgrading your standalone CAM/CAS machine from release 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ to the latest 4.1(3) release. You can upgrade 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ standalone machines to the latest 4.1(3) release using one of the following two methods:

- Web Console Upgrade—Standalone Machines, page 98

- Console/SSH Upgrade—Standalone Machines, page 101

Warning **The standard period of time required to upgrade is approximately 10 to 20 minutes. If you are upgrading from release 3.6(x) or 4.0(x) to release 4.1(3) and later, depending on the size of your existing Agent Report log, the upgrade process may take longer than usual. For example, if your Agent Report log is relatively large (~30,000 entries) the upgrade process from 3.6(x) to Release 4.1.3.1 could take around 40 minutes.**

To help avoid longer upgrade times, delete Agent Report entries (under Device Management > Clean Access > Clean Access Agent > Reports) before upgrading from release 3.6(x) or 4.0(x) to release 4.1(3) and later. Alternatively, you can upgrade from release 3.6(x) or 4.0(x) to release 4.1.2.1 and *then* upgrade to release 4.1(3) and later.

Note

- If upgrading high-availability (HA) pairs of CAM or CAS servers running 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+, refer instead to Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—HA Pairs, page 104.
- "In-place" upgrade from version 3.5(11) to 4.1(3) and later is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(3) and later must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(3) and later. (See CSCsl76977.)

Note Review the following sections before proceeding with the upgrade instructions:

- Upgrading to 4.1(3), page 92
- Settings That May Change With Upgrade, page 93
- General Preparation for Upgrade, page 94

Summary of Steps for 3.6/4.0/4.1(0)+/4.1(1)+/4.1(2)+ Upgrade

The sequence of steps for standalone 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ system upgrade is as follows:

1. Create CAM DB Backup Snapshot, page 96
2. Download the Upgrade File, page 97
3. Web Console Upgrade—Standalone Machines or Console/SSH Upgrade—Standalone Machines, page 101

Create CAM DB Backup Snapshot

Cisco recommends creating a manual backup snapshot of your CAM database. Backing up prior to upgrade enables you to revert to your previous database should you encounter problems during upgrade. Backing up immediately following upgrade preserves your upgraded tables and provides a baseline of your database. Make sure to download the snapshots to another machine for safekeeping.

Note that Cisco NAC Appliance automatically creates daily snapshots of the CAM database and preserves the most recent from the last 30 days (starting from release 3.5(3)). It also automatically creates snapshots before and after software upgrades and failover events. For upgrades and failovers, only the last 5 backup snapshots are kept. (For further details, see "Database Recovery Tool" in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(3)*.

Note Only the CAM snapshot needs to be backed up. The snapshot contains all CAM database configuration and CAS configuration for all the Clean Access Servers added to the CAM's domain. The snapshot is a standard postgres data dump.

To create a manual backup snapshot:

Step 1 From the CAM web console, go to the **Administration > Backup** page.

Step 2 The **Snapshot Tag Name** field automatically populates with a name incorporating the current time and date (e.g. 04_15_07-14-58_snapshot). You can also either accept the default name or type another.

Step 3 Click **Create Snapshot**. The CAM generates a snapshot file and adds it to the snapshot list at the bottom of the page. The file physically resides on the CAM machine for archiving purposes. The Version field and the filename display the software version of the snapshot for convenience (e.g. 04_15_07-14-58_snapshot_**VER_4.1.3.0.**gz).

Step 4 For backup, download the snapshot to another computer by clicking the **Tag Name** or the **Download** button for the snapshot to be downloaded.

Step 5 In the file download dialog, select the **Save File to Disk** option to save the file to your local computer.

Download the Upgrade File

For Cisco NAC Appliance upgrades from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+, a single **.tar.gz** upgrade file is downloaded to each Clean Access Manager (CAM) and Clean Access Server (CAS) machine to be upgraded. The upgrade script automatically determines whether the machine is a CAM or CAS. For Cisco NAC Appliance minor release or patch upgrades, the upgrade file can be for the CAM only, CAS only, or for both CAM/CAS, depending on the patch upgrade required.

Step 1 Navigate to “Cisco Download Security Software” (http://www.cisco.com/public/sw-center/sw-ciscosecure.shtml) and log in. Navigate to the “Network Admission Control” section of the page, and click **Cisco NAC Appliance Software**.

Step 2 On the Cisco Secure Software page for Cisco Clean Access, click the link for the appropriate release.

Step 3 Download the upgrade file (e.g. **cca_upgrade-<***version***>.tar.gz)** to the local computer from which you are accessing the CAM web console.

Note Upgrade files use the following format.

- cca_upgrade-4.1.3.x.tar.gz (CAM/CAS release upgrade file)
- cam-upgrade-4.1.3.x.tar.gz (CAM-only patch upgrade file)
- cas-upgrade-4.1.3.x.tar.gz (CAS-only patch upgrade file)

For patch upgrades, replace the .x in the file name with the minor release version numbers to which you are upgrading, for example, **cca-upgrade-4.1.3.1.tar.gz**.

Web Console Upgrade—Standalone Machines

Note Cisco recommends using console/SSH to upgrade your machines from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ to 4.1(3) and later. See Console/SSH Upgrade—Standalone Machines, page 101.

When upgrading from 3.6(x)/4.0(x) to the latest 4.1(x) release:

- You can only perform web console upgrade on standalone non-HA CAM machines if they have already been patched for caveat CSCsg24153.
- If the system has not already been patched, upgrade all your machines via console/SSH.
- Standalone CAS machines must still be upgraded using the console/SSH upgrade procedure.

For further details on Patch-CSCsg24153, refer to the README-CSCsg24153 file under http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches and the associated Resolved Caveats table entry in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(0)*.

Warning **Web upgrade is NOT supported for software upgrade of HA-CAM pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs, page 107.**

With web upgrade, administrators can perform software upgrade on standalone CAS and CAM machines using the following web console interfaces:

- To upgrade the CAM, go to: **Administration > Clean Access Manager > System Upgrade**
- To upgrade the CAS go to either:
  - **Device Management > CCA Servers > Manage [CAS_IP] > Misc** (CAS management pages)
  - **https://**<*CAS_eth0_IP_address*>**/admin** (CAS direct web console)

For web console upgrade, you will need your CAM web console **`admin`** user password.

If using the CAS direct access web console, you will need your CAS direct access console **`admin`** user password.

Note

- For web upgrade, upgrade each CAS first, then the CAM.
- Release 3.6(0)/4.0(0)/4.1(0)/4.1(1)/4.1(2) or later must be installed and running on your CAM/CAS(es) before you can upgrade to release 4.1(3) and later via web console.
- Alternatively, you can always upgrade using the instructions in Console/SSH Upgrade—Standalone Machines, page 101.
- If upgrading failover pairs, refer to Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—HA Pairs, page 104.

With web upgrade, the CAM and CAS automatically perform all the upgrade tasks that are done manually for console/SSH upgrade (for example, untar file, cd to /store, run upgrade script). The CAM also automatically creates snapshots before and after upgrade. When upgrading via web console only, the machine automatically reboots after the upgrade completes. The steps for web upgrade are as follows:

1. Upgrade CAS from CAS Management Pages, **or**
2. Upgrade CAS from CAS Direct Access Web Console, **and**
3. Upgrade CAM from CAM Web Console

Upgrade CAS from CAS Management Pages

You can upgrade your CAS from release 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ to release 4.1(3) and later using web upgrade via the CAS management pages as described below or, if preferred, using the instructions for Upgrade CAS from CAS Direct Access Web Console, page 100.

Step 1 Create CAM DB Backup Snapshot, page 96.

Step 2 Download the Upgrade File, page 97.

Step 3 From the CAM web console, access the CAS management pages as follows:

a. Go to **Device Management > CCA Servers > List of Servers.**

b. Click the **Manage** button for the CAS to upgrade. The CAS management pages appear.

c. Click the **Misc** tab. The **Update** form appears by default.

Step 4 Click **Browse** to locate the upgrade **.tar.gz** file you just downloaded from Cisco Downloads.

Step 5 Click the **Upload** button. This loads the upgrade file into the CAM's upgrade directory for this CAS and all CASes in the **List of Servers**. (Note that at this stage the upgrade file is not yet physically on the CAS.) The list of upgrade files on the page will display the newly-uploaded upgrade file with its date and time of upload, file name, and notes (if applicable).

Step 6 Click the **Apply** icon for the upgrade file, and click **OK** in the confirmation dialog that appears. This will start the CAS upgrade. The CAS will show a status of "Not connected" in the List of Servers during the upgrade. After the upgrade is complete, the CAS automatically reboots.

Note For web console upgrades only, the machine automatically reboots after upgrade.

Step 7 Wait 2-5 minutes for the upgrade and reboot to complete. The CAS management pages will become unavailable during the reboot, and the CAS will show a Status of "Disconnected" in the **List of Servers**.

Step 8 Access the CAS management pages again and click the **Misc** tab. The new software version and date will be listed in the **Current Version** field. (See also Determining the Software Version, page 8.)

Step 9 Repeat steps 3, 6, 7 and 8 for each CAS managed by the CAM.

Note The format of the Upgrade Details log is: state before upgrade, upgrade process details, state after upgrade. It is normal for the "state before upgrade" to contain several warning/error messages (e.g. "INCORRECT"). The "state after upgrade" should be free of any warning or error messages.

Upgrade CAS from CAS Direct Access Web Console

You can upgrade the CAS from the CAS direct access web console using the following instructions. To upgrade the CASes from the CAM web console, see Upgrade CAS from CAS Management Pages, page 99.

Step 1 Create CAM DB Backup Snapshot, page 96.

Step 2 Download the Upgrade File, page 97.

Step 3 To access the Clean Access Server's direct access web admin console:

a. Open a web browser and type the IP address of the CAS's trusted (eth0) interface in the URL/address field, as follows: **https://<*CAS_eth0_IP_address*>/admin** (for example, **`https://172.16.1.2/admin`**).

b. Accept the temporary certificate and log in as user **`admin`** and enter the CAS web console password (default CAS web console password is **`cisco123`**).

Step 4 In the CAS web console, go to **Administration > Software Update**.

Step 5 Click **Browse** to locate the upgrade **.tar.gz** file you just downloaded from Cisco Downloads.

Step 6 Click the **Upload** button. This loads the upgrade file to the CAS and displays it in the upgrade file list with date and time of upload, file name, and notes (if applicable).

Step 7 Click the **Apply** icon for the upgrade file, and click **OK** in the confirmation dialog that appears. This will start the CAS upgrade. The CAS will show a status of "Not connected" in the **List of Servers** during the upgrade. After the upgrade is complete, the CAS will automatically reboot.

Note For web console upgrades only, the machine automatically reboots after upgrade.

Step 8 Wait 2-5 minutes for the upgrade and reboot to complete. The CAS web console will become unavailable during the reboot.

Step 9 Access the CAS web console again and go to **Administration > Software Update**. The new software version and date will be listed in the **Current Version** field. (See also Determining the Software Version, page 8)

Step 10 Repeat steps 3 through 9 for each CAS managed by the CAM.

Note The format of the Upgrade Details log is: state before upgrade, upgrade process details, state after upgrade. It is normal for the "state before upgrade" to contain several warning/error messages (e.g. "INCORRECT"). The "state after upgrade" should be free of any warning or error messages.

Upgrade CAM from CAM Web Console

Upgrade your standalone CAM from the CAM web console using the following instructions.

Warning **Web upgrade is *not* supported for software upgrade of HA-CAM pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs, page 107.**

Step 1 Create CAM DB Backup Snapshot, page 96.

Step 2 Download the Upgrade File, page 97.

Step 3 Log into the web console of your Clean Access Manager as user `admin` (default password is `cisco123`), and go to **Administration > CCA Manager > System Upgrade**.

Step 4 Click **Browse to** locate the upgrade **.tar.gz** file you just downloaded from Cisco Downloads.

Step 5 Click the **Upload** button. This loads the upgrade file to the CAM and displays it in the upgrade file list with date and time of upload, file name, and notes (if applicable).

Step 6 Click the **Apply** icon for the upgrade file, and click **OK** in the confirmation dialog that appears. This will start the CAM upgrade. After the upgrade is complete, the CAM will automatically reboot.

Note For web console upgrades only, the machine automatically reboots after upgrade.

Step 7 Wait 2-5 minutes for the upgrade and reboot to complete. The CAM web console will become unavailable during the reboot.

Step 8 Access the CAM web console again. After login, you will see the new software version at the top right corner of the web console. (See also Determining the Software Version, page 8.)

Note The format of the Upgrade Details log is: state before upgrade, upgrade process details, state after upgrade. It is normal for the “state before upgrade” to contain several warning/error messages (e.g. “INCORRECT”). The “state after upgrade” should be free of any warning or error messages.

Console/SSH Upgrade—Standalone Machines

This section describes the standard console/SSH upgrade procedure when upgrading your standalone CAM/CAS from release 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ to the latest 4.1(3) release. For this procedure, you need to access the command line of the CAM or CAS machine using one of the following methods:

- SSH connection
- Direct console connection using KVM or keyboard/monitor connected directly to the machine
- Serial console connection (e.g. HyperTerminal or SecureCRT) from an external workstation connected to the machine via serial cable

Warning **Do not use SSH connection to upgrade Virtual Gateway CASes. Use direct console connection (keyboard/monitor/KVM) if upgrading Virtual Gateway Clean Access Servers. You can use serial console connection for standalone CASes only.**

Note

- If upgrading high-availability (HA) pairs of CAM or CAS servers running 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+, refer instead to Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—HA Pairs, page 104.
- "In-place" upgrade from version 3.5(11) to 4.1(3) and later is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(3) and later must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(3) and later. (See CSCsl76977.)

For upgrade via console/SSH, you will need your CAM and CAS `root` user password.

Note The default username/password for console/SSH login on the CAM/CAS is `root / cisco123`.

A single upgrade **.tar.gz** file is downloaded to each installation machine. The upgrade script automatically determines whether the machine is a Clean Access Manager (CAM) or Clean Access Server (CAS), and executes if the current system is running release 3.6(0) or later.

For patch upgrades, the upgrade file can be for the CAM only, CAS only, or for both CAM/CAS, depending on the patch upgrade required.

Note Review the following before proceeding with the 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ to 4.1(3) and later console/SSH upgrade instructions:

- Upgrading to 4.1(3), page 92
- Settings That May Change With Upgrade, page 93
- General Preparation for Upgrade, page 94

Summary of Steps for Console/SSH Upgrade from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+

Steps are as follows:

1. Download the Upgrade File and Copy to CAM/CAS
2. Perform Console/SSH Upgrade on the CAM
3. Perform Console/SSH Upgrade on the CAS

Download the Upgrade File and Copy to CAM/CAS

Step 1 Create CAM DB Backup Snapshot, page 96.

Step 2 Download the Upgrade File, page 97.

Step 3 Copy the upgrade file to the Clean Access Manager and Clean Access Server(s) respectively using WinSCP, SSH File Transfer or PSCP as described below

If using WinSCP or SSH File Transfer:

a. Copy **cca_upgrade-4.1.3.tar.gz** to the /store directory on the Clean Access Manager.

b. Copy **cca_upgrade-4.1.3.tar.gz** to the /store directory on *each* Clean Access Server.

If using PSCP:

a. Open a command prompt on your Windows computer.

b. Cd to the path where your PSCP resides (e.g, C:\Documents and Settings\desktop).

c. Enter the following command to copy the file to the CAM:

```
pscp cca_upgrade-4.1.3.tar.gz root@ipaddress_manager:/store
```

d. Enter the following command to copy the file to the CAS (copy to each CAS):

```
pscp cca_upgrade-4.1.3.tar.gz root@ipaddress_server:/store
```

Perform Console/SSH Upgrade on the CAM

Step 4 Connect to the Clean Access Manager to upgrade using console connection, or Putty or SSH.

a. Connect to the Clean Access Manager.

b. Login as user **root** with root password (default password is **cisco123**).

c. Change directory to /store:

```
cd /store
```

d. Uncompress the downloaded file:

```
tar xzvf cca_upgrade-4.1.3.tar.gz
```

4. Execute the upgrade process:

```
cd cca_upgrade-4.1.3
./UPGRADE.sh
```

Note If you are upgrading from release 4.0.0-4.0.3.2 or 3.6.0-3.6.4.2 and have not previously applied Patch-CSCsg24153 to the CAM, the upgrade script prompts you to enter and verify the shared secret. (Only the first eight characters of the shared secret are used.)

For more information on the nature and workaround for Patch-CSCsg24153, see the associated Resolved Caveats table entry in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(0)*.

e. If necessary, enter and verify the shared secret configured on the CAM.

Note For CAM upgrade, the 4.1(3) upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.3.0.

f. When the upgrade is complete, reboot the machine:

```
reboot
```

Perform Console/SSH Upgrade on the CAS

Warning **Do not use SSH connection to upgrade Virtual Gateway CASes. Use console connection (keyboard/monitor/KVM) if upgrading Virtual Gateway Clean Access Servers. You can use serial console connection for standalone CASes only.**

Step 5 Connect to the Clean Access Server to upgrade using connection, or Putty or SSH:

a. Connect to the Clean Access Server.

b. Login as user **`root`** and enter the root password.

c. Change directory to /store:

```
cd /store
```

d. Uncompress the downloaded file:

```
tar xzvf cca_upgrade-4.1.3.tar.gz
```

5. Execute the upgrade process:

```
cd cca_upgrade-4.1.3
./UPGRADE.sh
```

Note If you are upgrading from release 4.0.0-4.0.3.2 or 3.6.0-3.6.4.2 and have not previously applied Patch-CSCsg24153 to the CAS, the upgrade script prompts you to enter and verify both the shared secret and web console administrator password. (Only the first eight characters of the shared secret are used.)

For more information on the nature and workaround for Patch-CSCsg24153, see the associated Resolved Caveats table entry in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(0)*.

e. If necessary, enter and verify the shared secret and web console administrator password configured on the CAS.

f. When the upgrade is complete, reboot the machine:

```
reboot
```

g. Repeat steps a-f for each CAS managed by the CAM.

Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—HA Pairs

This section describes the upgrade procedure for upgrading high-availability (HA) pairs of CAM or CAS servers from release 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ to the latest 4.1(3) release.

Warning **The standard period of time required to upgrade is approximately 10 to 20 minutes. If you are upgrading from release 3.6(x) or 4.0(x) to release 4.1(3) and later, depending on the size of your existing Agent Report log, the upgrade process may take longer than usual. For example, if your Agent Report log is relatively large (~30,000 entries) the upgrade process from 3.6(x) to Release 4.1.3.1 could take around 40 minutes.**

To help avoid longer upgrade times, delete Agent Report entries (under Device Management > Clean Access > Clean Access Agent > Reports) before upgrading from release 3.6(x) or 4.0(x) to release 4.1(3) and later. Alternatively, you can upgrade from release 3.6(x) or 4.0(x) to release 4.1.2.1 and *then* upgrade to release 4.1(3) and later.

If you have standalone CAM/CAS servers, refer instead to Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—Standalone Machines, page 95.

Note Your system must be on 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ to use the upgrade procedure described in this section.

"In-place" upgrade from version 3.5(11) to 4.1(3) and later is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(3) and later must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(3) and later. (See CSCsl76977.)

Warning **Do not use SSH connection to upgrade Virtual Gateway CASes. Use direct console connection (keyboard/monitor/KVM) if upgrading Virtual Gateway Clean Access Servers. You can use serial console connection for standalone CASes only.**

If you are using serial connection for HA, do not attempt to connect serially to the CAS during the upgrade procedure. When serial connection is used for HA, serial console/login will be disabled and serial connection cannot be used for installation/upgrade.

If you are using serial connection for HA, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances, and for any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.

Warning **Web upgrade is NOT supported for software upgrade of HA-CAM pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs, page 107.**

Note Review the following before proceeding with the 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ to 4.1(3) and later HA upgrade instructions:

- Upgrading to 4.1(3), page 92
- Settings That May Change With Upgrade, page 93
- General Preparation for Upgrade, page 94

Steps for HA 3.6/4.0/4.1(0)+/4.1(1)+/4.1(2)+ Upgrade

The steps to upgrade HA 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+ systems are described in the following sections:

- Access Web Consoles for High Availability
- Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs

Note For additional details on CAS HA requirements, see also *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*.

Access Web Consoles for High Availability

Determining Active and Standby CAM

Access the web console for each CAM in the HA pair by typing the IP address of each individual CAM (not the Service IP) in the URL/Address field of a web browser. You should have two browsers open. The web console for the Standby (inactive) CAM will only display the **Administration** module menu.

Note The CAM configured as HA-Primary may not be the currently Active CAM.

Determining Primary and Secondary CAM

In each CAM web console, go to **Administration > CCA Manager > Network & Failover | High Availability Mode.**

- The Primary CAM is the CAM you configured as the **HA-Primary** when you initially set up HA.
- The Secondary CAM is the CAM you configured as the **HA-Secondary** when you initially set up HA.

Note For releases prior to 4.0(0), the Secondary CAM is labeled as **HA-Standby** (CAM) for the initial HA configuration.

Determining Active and Standby CAS

From the CAM web console, go to **Device Management > CCA Servers > List of Servers** to view your HA-CAS pairs. The List of Servers page displays the **Service IP** of the CAS pair first, followed by the IP address of the Active CAS in brackets. When a secondary CAS takes over, its IP address will be listed in the brackets as the Active server.

Note The CAS configured in HA-Primary-Mode may not be the currently Active CAS.

Determining Primary and Secondary CAS

Open the direct access console for each CAS in the pair by typing the following in the URL/Address field of a web browser (you should have two browsers open):

- For the Primary CAS, type: **https://**<*primary_CAS_eth0_IP_address*>**/admin**. For example, `https://172.16.1.2/admin`.
- For the Secondary CAS, type: **https://**<*secondary_CAS_eth0_IP_address*>**/admin**. For example, `https://172.16.1.3/admin`.

In each CAS web console, go to **Administration > Network Settings > Failover | Clean Access Server Mode**.

- The Primary CAS is the CAS you configured in **HA-Primary-Mode** when you initially set up HA**.**
- The Secondary CAS is the CAS you configured in **HA-Secondary-Mode** when you initially set up HA.

Note For releases prior to 4.0(0), the Secondary CAS is labelled as **HA-Standby Mode** (CAS) for the initial HA configuration.

Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs

The following steps show the recommended way to upgrade an existing high-availability (failover) pair of Clean Access Managers or Clean Access Servers.

Warning **Make sure to carefully execute the following procedure to prevent the database from getting out of sync.**

Step 1 From either a console connection (keyboard/monitor/KVM) or via SSH, connect into each machine in the failover pair. Login as the **root** user with the root password (default is **cisco123**)

Warning **Do not use SSH connection to upgrade Virtual Gateway CASes. Use direct console connection (keyboard/monitor/KVM) if upgrading Virtual Gateway Clean Access Servers. You can use serial console connection for standalone CASes only.**

If you are using serial connection for HA, do not attempt to connect serially to the CAS during the upgrade procedure. When serial connection is used for HA, serial console/login will be disabled and serial connection cannot be used for installation/upgrade.

If you are using serial connection for HA, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances, and for any other server hardware platform that supports the BIOS redirection to serial port functionality. See *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for more information.

Step 2 Verify that the upgrade package is present in the /store directory on each machine. (Refer to Download the Upgrade File and Copy to CAM/CAS, page 102 for instructions.)

Step 3 Determine which box is active, and which is in standby mode, and that both are operating normally, as follows:

a. Untar the upgrade package in the /store directory of each machine:

```
tar xzvf cca_upgrade-4.1.3.tar.gz
```

b. CD into the created "cca_upgrade-4.1.3" directory on each machine.

c. Run the following command on each machine:

```
./fostate.sh
```

The results should be either "My node is active, peer node is standby" or "My node is standby, peer node is active". No nodes should be dead. This should be done on both boxes, and the results should be that one box considers itself active and the other box considers itself in standby mode. Future references in these instructions that specify "active" or "standby" refer to the results of this test as performed at this time.

Note The `fostate.sh` command is part of the upgrade script (starting from 3.5(3)+). You can also determine which box is active or standby as follows:

- Access the web console as described in Access Web Consoles for High Availability, page 106, or
- SSH to the Service IP of the CAM/CAS pair, and type **`ifconfig eth0`**. The Service IP will always access the active CAM or CAS, with the other pair member acting as standby.

Step 4 Bring the box acting as the standby down by entering the following command via the console/SSH terminal:

```
shutdown -h now
```

Step 5 Wait until the standby box is completely shut down.

Step 6 CD into the created "cca_upgrade-4.1.3" directory on the active box.

```
cd cca_upgrade-4.1.3
```

Step 7 Run the following command on the active box:

```
./fostate.sh
```

Make sure this returns "My node is active, peer node is dead" before continuing.

Step 8 Perform the upgrade on the active box, as follows:

a. Make sure the upgrade package is untarred in the /store directory on the active box.

b. From the untarred upgrade directory created on the active box (for example "cca_upgrade-4.1.3"), run the upgrade script on the active box:

```
./UPGRADE.sh
```

Note If you are upgrading from release 4.0.0-4.0.3.2 or 3.6.0-3.6.4.2 and have not previously applied Patch-CSCsg24153 to the CAM, the upgrade script prompts you to enter and verify the shared secret. (Only the first eight characters of the shared secret are used.)

If you are performing this upgrade on the CAS, the upgrade script prompts you to enter the web console administrator password in addition to the shared secret. (As with the CAM, only the first eight characters of the shared secret are used.)

For more information on the nature and workaround for Patch-CSCsg24153, see the associated Resolved Caveats table entry in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(0)*.

c. If necessary, enter and verify the shared secret configured on the CAM, or enter and verify the shared secret and web console administrator password configured on the CAS.

Note For CAM upgrade, the 4.1(3) upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.3.0.

Step 9 After the upgrade is completed, shut down the active box by entering the following command via the console/SSH terminal:

```
shutdown -h now
```

Step 10 Wait until the active box is done shutting down.

Step 11 Boot up the standby box by powering it on.

Step 12 Perform the upgrade to the standby box:

a. Make sure the upgrade package is untarred in the /store directory on the standby box.

b. CD into the untarred upgrade directory created on the standby box:

```
cd cca_upgrade-4.1.3
```

c. Run the upgrade script on the standby box:

```
./UPGRADE.sh
```

Step 13 Shut down the standby box by entering the following command via the console/SSH terminal:

```
shutdown -h now
```

Step 14 Power up the active box. Wait until it is running normally and connection to the web console is possible

Step 15 Power up the standby box.

Note There will be approximately 2-5 minutes of downtime while the servers are rebooting.

Troubleshooting

This section provides troubleshooting information for the following topics:

- Windows Vista Agent Stub Installer Error
- Vista/IE 7 Certificate Revocation List
- Agent Stub Upgrade and Uninstall Error
- Clean Access Agent AV/AS Rule Troubleshooting
- Generating Windows Installer Log Files for Agent Stub
- Debug Logging for Cisco NAC Appliance Agents
- Vista/IE 7 Certificate Revocation List
- Creating CAM/CAS Support Logs
- Recovering Root Password for CAM/CAS (Release 4.1.x/4.0.x/3.6.x)
- No Web Login Redirect / CAS Cannot Establish Secure Connection to CAM
- Troubleshooting Switch Support Issues
- Troubleshooting Network Card Driver Support Issues
- Other Troubleshooting Information

Note For additional troubleshooting information, see also Known Issues for Cisco NAC Appliance, page 86.

Vista/IE 7 Certificate Revocation List

Note In IE 7, the "Check for server certificate revocation (requires restart)" checkbox is enabled **by default** under IE's Tools > Internet Options > Advanced | Security settings

The "Network error: SSL certificate rev failed 12057" error can occur and prevent login for Clean Access Agent or Cisco NAC Web Agent users in either of the following cases:

1. The client system is using Microsoft Internet Explorer 7 and/or Windows Vista operating system, and the certificate issued for the CAS is not properly configured with a CRL (Certificate Revocation List).
2. A temporary SSL certificate is being used for the CAS (i.e. issued by www.perfigo.com) AND
   - The user has not imported this certificate to the trusted root store.
   - The user has not disabled the "Check for server certificate revocation (requires restart)" checkbox in IE.

To resolve the error, perform the following actions:

Step 1 (**Preferred**) When using a CA-signed CAS SSL certificate, check the "CRL Distribution Points" field of the certificate (including intermediate or root CA), and add the URL hosts to the allowed Host Policy of the Unauthenticated/Temporary/Quarantine Roles. This will allow the Agent to fetch the CRLs when logging in.

Step 2 Or, if continuing to use temporary certificates for the CAS (i.e. issued by www.perfigo.com), the user will need to perform ONE of the following actions:

a. Import the certificate to the client system's trusted root store.

b. Disable the "Check for server certificate revocation (requires restart)" checkbox under IE's Tools > Internet Options > Advanced | Security settings.

Windows Vista Agent Stub Installer Error

When initiating the Agent stub installer on the Windows Vista operating system, the user may encounter the following error message:

> "Error 1722: There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor."

The possible cause is that there are remnants of a partial previous Agent stub installation present on the client machine stub. The user must take steps to remove the previous partial installation before attempting to run the Agent stub installer again.

To solve the problem:

Step 1 Disable the Windows Vista UAC and restart the computer.

Step 2 In a Command Prompt window, run `C:\windows\system32\CCAAgentStub.exe install`.

Step 3 Launch the Agent stub installer again and choose **Remove**.

Step 4 Enable the Windows Vista UAC and restart the computer.

Step 5 Run the stub installer again and it should install the Windows Vista Agent successfully.

Agent Stub Upgrade and Uninstall Error

To resolve the situation where a user receives an "Internal error 2753:ccaagentstub.exe" message during stub installation:

Step 1 Run `C:\windows\system32\CCAAgentStub.exe` install from a Command Prompt window.

Step 2 Launch the Clean Access Agent stub installer again and choose **Remove**.

Step 3 Manually delete "%systemroot%\system32\ccaagentstub.exe."

Note Installing a previous version of stub is not recommended after uninstalling the later version.

Clean Access Agent AV/AS Rule Troubleshooting

When troubleshooting AV/AS Rules:

- View administrator reports for the Clean Access Agent from **Device Management > Clean Access > Clean Access Agent > Reports** (see Cisco NAC Appliance Agents Versioning, page 9)
- Or, to view information from the client, right-click the Agent taskbar icon and select **Properties**.

When troubleshooting AV/AS Rules, please provide the following information:

1. Version of CAS, CAM, and Clean Access Agent (see Determining the Software Version, page 8).
2. Version of client OS (e.g. Windows XP SP2).
3. Version of Cisco Updates ruleset (see Cisco Clean Access Updates Versioning, page 9.
4. Product name and version of AV/AS software from the Add/Remove Program dialog box.
5. What is failing—AV/AS installation check or AV/AS update checks? What is the error message?
6. What is the current value of the AV/AS def date/version on the failing client machine?
7. What is the corresponding value of the AV/AS def date/version being checked for on the CAM? (See **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**.)
8. If necessary, provide Agent debug logs as described in Debug Logging for Cisco NAC Appliance Agents, page 112.
9. If necessary, provide CAM support logs as described in Creating CAM/CAS Support Logs, page 115.

Generating Windows Installer Log Files for Agent Stub

Users can compile the Windows Installer logs generated by the InstallShield application when the Windows Agent is installed on a client machine using the MSI or EXE installer packages.

MSI Installer

To compile the logs generated by a Windows Agent MSI installer session as the installation takes place, enter the following at a command prompt:

ccaagent.msi /log C:\ccainst.log

This function creates an installer session log file called "ccainst.txt" in the client machine's C:\ drive when the MSI Installer installs the Agent files on the client.

EXE Installer

You can use the Windows Installer **/v** CLI option to pass arguments to the **msiexec** installer within **CCAAgent_Setup.exe** by entering the following at a command prompt:

CCAAgent_Setup.exe /v"/L*v \"C:\ccainst.log\""

This command saves an installation session log file called "ccainst.log" in the client machine's C:\ drive when the embedded **msiexec** command installs the Agent files on the client.

For more information, refer to the Windows Installer CLI reference page.

Debug Logging for Cisco NAC Appliance Agents

This section describes how to view and/or enable debug logging for Cisco NAC Appliance Agents. Refer to the following sections for steps for each Agent type:

- Cisco NAC Web Agent Logs
- Generate Windows Agent Debug Log
- Generate Mac OS X Agent Debug Log

Copy these event logs to include them in a customer support case.

Cisco NAC Web Agent Logs

The Cisco NAC Web Agent version 4.1.3.9 and later can generate logs when downloaded and executed. By default, the Cisco NAC Web Agent writes the log file upon startup with debugging turned on. The Cisco NAC Web Agent (see Cisco NAC Web Agent, page 12) generates the following log files for troubleshooting purposes: **webagent.log** and **webagentsetup.log**. These files should be included in any TAC support case for the Web Agent. Typically, these files are located in the user's temp directory, in the form:

C:\Document and Settings\<*user*>\Local Settings\Temp\webagent.log

C:\Document and Settings\<*user*>\Local Settings\Temp\webagentsetup.log

If these files are not visible, check the TEMP environment variable setting. From a command-prompt, type "echo %TEMP%" or "cd %TEMP%".

When the client uses Microsoft Internet Explorer, the Cisco NAC Web Agent is downloaded to the **C:\Documents and Settings\<*user*>\Local Settings\Temporary internet files** directory.

Generate Windows Agent Debug Log

For 4.1.x.x versions of the persistent Clean Access Agent (and 4.0.x.x/3.6.1.0+), you can enable debug logging on the Agent by adding a LogLevel registry value on the client with value "debug." For Windows Agents (see Cisco NAC Appliance Agents, page 25), the event log is created in the directory **%APPDATA%\CiscoCAA**, where %APPDATA% is the Windows environment variable.

Note For most Windows operating systems, the Agent event log is found in **<user home directory>\Application Data\CiscoCAA\**.

To view and/or change the Agent LogLevel setting:

Step 1 Exit the Clean Access Agent on the client by right-clicking the taskbar icon and selecting **Exit**.

Step 2 Edit the registry of the client by going to Start > Run and typing `regedit` in the **Open:** field of the Run dialog. The Registry Editor opens.

Step 3 In the Registry Editor, navigate to HKEY_CURRENT_USER\Software\Cisco\Clean Access Agent\

Note For 3.6.0.0/3.6.0.1 and 3.5.10 and earlier, this is HKEY_LOCAL_MACHINE\Software\Cisco\Clean Access Agent\

Step 4 If "LogLevel" is not already present in the directory, go to Edit > New > String Value and add a String to the Clean Access Agent Key called `LogLevel`.

Step 5 Right-click **LogLevel** and select Modify. The **Edit String** dialog appears.

Step 6 Type `debug` in the **Value data** field and click **OK** (this sets the value of the LogLevel string to "debug").

Step 7 Restart the Clean Access Agent by double-clicking the desktop shortcut.

Step 8 Re-login to the Clean Access Agent.

Step 9 When a requirement fails, click the **Cancel** button in the Clean Access Agent.

Step 10 Take the resulting "event.log" file from the home directory of the current user (e.g. C:\Documents and Settings\<username>\Application Data\CiscoCAA\event.log) and send it to TAC customer support, for example:

a. Open **Start > Run**.

b. In the **Open:** field, enter `%APPDATA%/CiscoCAA`. The "event.log" file should already be there to view.

Step 11 **When done, make sure to remove** the newly added "LogLevel" string from the client registry by opening the Registry Editor, navigating to HKEY_CURRENT_USER\Software\Cisco\Clean Access Agent\, right-clicking **LogLevel**, and selecting **Delete**.

Note

- For 3.6.0.0/3.6.0.1 and 3.5.10 and earlier, the event.log file is located in the Agent installation directory (e.g. C:\Program Files\Cisco Systems\Clean Access Agent\).
- For 3.5.0 and earlier, the Agent installation directory is C:\Program Files\Cisco\Clean Access\.

Generate Mac OS X Agent Debug Log

For Mac OS X Agents (see Mac OS X Clean Access Agent Version 4.1.3.0, page 29), the Agent **event.log** file and **preference.plist** user preferences file are available under <*username*> **> Library > Application Support > Cisco Systems > CCAAgent.app**. To change or specify the LogLevel setting, however, you must access the global **setting.plist** file (which is *different* from the user-level **preference.plist** file).

Because Cisco does not recommend allowing individual users to change the LogLevel value on the client machine, you must be a superuser or root user to alter the global **setting.plist** system preferences file and specify a different Agent LogLevel.

Note For releases prior to 4.1.3.0, debug logging for the Mac OS X Agent is enabled under <*local drive ID*> **> Library > Application Support > Cisco Systems | CCAAgent.app > Show Package Contents > setting.plist**.

To view and/or change the Agent LogLevel:

Step 1 Open the navigator pane and navigate to <*local drive ID*> **> Applications**.

Step 2 Highlight and right-click the **CCAAgent.app** icon to bring up the selection menu.

Step 3 Choose **Show Package Contents > Resources.**

Step 4 Choose **setting.plist**.

Step 5 If you want to change the current LogLevel setting using Mac **Property Editor** (for Mac OS 10.4 and later) or any standard text editor (for Mac OS X releases earlier than 10.4), find the current LogLevel Key and replace the exiting value with one of the following:

- **Info**—Include only informational messages in the event log
- **Warn**—Include informational and warning messages in the event log
- **Error**—Include informational, warning, and error messages in the event log
- **Debug**—Include all Agent messages (including informational, warning, and error) in the event log

Note The **Info** and **Warn** entry types only feature a few messages pertaining to very specific Agent events. Therefore, you will probably only need either the **Error** or **Debug** Agent event log level when troubleshooting Agent connection issues.

Note Because Apple, Inc. introduced a binary-format .plist implementation in Mac OS 10.4, the .plist file may not be editable by using a common text editor such as vi. If the .plist file is not editable (displayed as binary characters), you either need to use the Mac **Property List Editor** utility from the Mac OS X CD-ROM or acquire another similar tool to edit the **setting.plist** file.

Property List Editor is an application included in the Apple Developer Tools for editing .plist files. You can find it at <*CD-ROM*>/Developer/Applications/Utilities/Property List Editor.app.

If the **setting.plist** file *is* editable, you can use a standard text editor like vi to edit the LogLevel value in the file.

You must be the root user to edit the file.

Creating CAM DB Snapshot

See the instructions in Create CAM DB Backup Snapshot, page 96 for details.

Creating CAM/CAS Support Logs

The **Support Logs** web console pages for the CAM and CAS allow administrators to combine a variety of system logs (such as information on open files, open handles, and packages) into one tarball that can be sent to TAC to be included in the support case. Administrators should **Download** the CAM and CAS support logs from the CAM and CAS web consoles respectively and include them with their customer support request, as follows:

- CAM web console: **Administration > CCA Manager > Support Logs**
- CAS direct access console (https://<*CAS_eth0_IP_address*>/admin): **Monitoring > Support Logs**

Note

- CAS-specific support logs are obtained from the CAS direct console only.
- For releases 3.6(0)/3.6(1) and 3.5(3)+, the support logs for the CAS are accessed from: **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Support Logs**
- For releases prior to 3.5(3), contact TAC for assistance on manually creating the support logs.

Recovering Root Password for CAM/CAS (Release 4.1.x/4.0.x/3.6.x)

Use the following procedure to recover the root password for a 4.1/4.0/3.6 CAM or CAS machine. The following password recovery instructions assume that you are connected to the CAM/CAS via a keyboard and monitor (i.e. console or KVM console, NOT a serial console)

1. Power up the machine.
2. When you see the boot loader screen with the "`Press any key to enter the menu…`" message, press any key.
3. You will be at the GRUB menu with one item in the list "`Cisco Clean Access (2.6.11-perfigo)`." Press **`e`** to edit.
4. You will see multiple choices as follows:

```
root (hd0,0)
kernel /vmlinuz-2.6.11-perfigo ro root=LABEL=/ console=tty0 console=ttyS0,9600n8
Initrd /initrd-2.6.11-perfigo.img
```

5. Scroll to the second entry (line starting with "`kernel…`") and press **`e`** to edit the line.
6. Delete the line `console=ttyS0,9600n8`, add the word **`single`** to the end of the line, then press **`Enter`**. The line should appear as follows:

```
kernel /vmlinuz-2.6.11-perfigo ro root=LABEL=/ console=tty0 single
```

7. Next, press **b** to boot the machine in single user mode. You should be presented with a root shell prompt after boot-up (note that you will not be prompted for password).
8. At the prompt, type **passwd**, press **Enter** and follow the instructions.
9. After the password is changed, type **reboot** to reboot the box.

No Web Login Redirect / CAS Cannot Establish Secure Connection to CAM

- Clean Access Server is not properly configured, please report to your administrator
- Clean Access Server could not establish a secure connection to the Clean Access Manager at <IP/domain>

Clean Access Server is not properly configured, please report to your administrator

A login page must be added and present in the system in order for both web login and Clean Access Agent users to authenticate. If a default login page is not present, Clean Access Agent users will see the following error dialog when attempting login:

```
Clean Access Server is not properly configured, please report to your administrator
```

To resolve this issue, add a default login page on the CAM under **Administration > User Pages > Login Page > Add**.

Clean Access Server could not establish a secure connection to the Clean Access Manager at <IP/domain>

The following client connection errors can occur if the CAS does not trust the certificate of the CAM, or vice-versa:

- No redirect after web login—users continue to see the login page after entering user credentials.
- Agent users attempting login get the following error:

  ```
  Clean Access Server could not establish a secure connection to the Clean Access
  Manager at <IPaddress or domain>
  ```

These errors typically indicate one of the following certificate-related issues:

- The time difference between the CAM and CAS is greater than 5 minutes
- Invalid IP address
- Invalid domain name
- CAM is unreachable

To identify common issues:

1. Check the CAM's certificate and verify it has not been generated with the IP address of the CAS (under **Administration > CCA Manager > SSL Certificate > Export CSR/Private Key/Certificate | Currently Installed Certificate | Details**).
2. Check the time set on the CAM and CAS (under **Administration > CCA Manager > System Time**, and **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Time**). The time set on the CAM and the CAS must be 5 minutes apart or less.

To resolve these issues:

1. Set the time on the CAM and CAS correctly first.

2. Regenerate the certificate on the CAS using the correct IP address or domain.
3. Reboot the CAS.
4. Regenerate the certificate on the CAM using the correct IP address or domain.
5. Reboot the CAM.

Troubleshooting Switch Support Issues

To troubleshoot switch issues, see *Switch Support for Cisco NAC Appliance*.

Troubleshooting Network Card Driver Support Issues

For network card driver troubleshooting, see *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*.

Other Troubleshooting Information

For general troubleshooting tips, see the following Technical Support webpage:

http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html

Documentation Updates

Table 17 Updates to Release Notes for Cisco NAC Appliance, Release 4.1(3)

Date	Description
6/24/08	• Updted caveat CSCsk55292 in Open Caveats - Release 4.1(3), page 58 • Updated Support for Clients with Multiple Active NICs, page 13 • Updated Access to Authentication VLAN Change Detection Enhancement, page 21
6/6/08	• Updated Table 1 on page 5 and VPN SSO Enhancement to Support Existing Clientless SSL VPN Users Launching the AnyConnect Client from a WebVPN Portal, page 16 from ASA 8.0.3.1 to ASA 8.0(3)7. • Updated template/boilerplat
6/5/08	• Updated Table 5 on page 24 to specify decimal default values • Updated Cisco NAC Web Agent Logs, page 112
5/9/08	• Added Generating Windows Installer Log Files for Agent Stub, page 111 to Troubleshooting section. • Enhanced description of Agent localization to clarify support level.

Table 17 Updates to Release Notes for Cisco NAC Appliance, Release 4.1(3)

Date	Description
5/2/08	• Added Macintosh OS note to Mac OS X Clean Access Agent Enhancements, page 29 • Added references to Table 5 in Windows Clean Access Agent Version 4.1.3.2, page 26 • Replaced all old references to **Device Management > Clean Access > Clean Access Agent > Updates**
4/8/08	• Updated Support for Clients with Multiple Active NICs, page 13 • Updated Access to Authentication VLAN Change Detection Enhancement, page 21 • Updated trademarks (version 0408R)
4/7/08	Updates for Windows Agent version 4.1.3.2: • Cisco NAC Appliance Releases, page 2 (updated) • Release 4.1(3) Compatibility Matrix, page 6 (updated) • Release 4.1(3) Clean Access Agent Upgrade Compatibility Matrix, page 7 (updated) • Support for Clients with Multiple Active NICs, page 13 (updated) • Access to Authentication VLAN Change Detection Enhancement, page 21 (updated) • Windows Clean Access Agent Version 4.1.3.2, page 26 (new) • Clean Access Supported AV/AS Product List, page 32 (updated) • Resolved Caveats - Windows Clean Access Agent 4.1.3.2, page 65 (new) General: • Updated hypertext links throughout
2/26/08	Added CSCsm20254, page 63 to Open Caveats - Release 4.1(3), page 58.
2/21/08	Updates for Mac OS X Agent version 4.1.3.1: • Cisco NAC Appliance Releases, page 2 (updated) • Release 4.1(3) Compatibility Matrix, page 6 (updated) • Release 4.1(3) Clean Access Agent Upgrade Compatibility Matrix, page 7 (updated) • Mac OS X Clean Access Agent Version 4.1.3.1, page 29 (new) • Open Caveats - Release 4.1(3), page 58 (added CSCsm53743 and CSCsm79088) • Resolved Caveats - Mac OS X Agent 4.1.3.1, page 68 (new)
2/18/08	Updates for Release 4.1.3.1: • Cisco NAC Appliance Releases, page 2 (updated) • Release 4.1(3) Compatibility Matrix, page 6 (updated) • Release 4.1(3) CAM/CAS Upgrade Compatibility Matrix, page 6 (updated) • Release 4.1(3) Clean Access Agent Upgrade Compatibility Matrix, page 7 (updated) • Enhancements in Release 4.1.3.1, page 10 (new) • Resolved Caveats - Release 4.1.3.1, page 71 (new) • Upgrading to 4.1(3), page 92 (updated)

Table 17 Updates to Release Notes for Cisco NAC Appliance, Release 4.1(3)

Date	Description
1/30/08	• Moved caveat CSCsk18401 to Resolved Caveats - Release 4.1(3), page 75 • Applied new template and updated trademark information
1/25/08	Added AD SSO note to Settings That May Change With Upgrade, page 93 and updated caveat CSCsk46672 in Resolved Caveats - Release 4.1(3), page 75.
1/24/08	Updates for Cisco NAC Web Agent version 4.1.3.10: • Cisco NAC Appliance Releases, page 2 (updated) • Release 4.1(3) Compatibility Matrix, page 6 (updated) • Release 4.1(3) Clean Access Agent Upgrade Compatibility Matrix, page 7 (updated) • Cisco NAC Web Agent Enhancements, page 30 (new) • Resolved Caveats - Cisco NAC Web Agent 4.1.3.10, page 72(new) • New Cisco NAC Appliance Agents, page 25 section replaces “Agent Enhancements” and “Agent Support Table”. • Added Cisco NAC Web Agent Logs, page 112 • Updates to Vista/IE 7 Certificate Revocation List, page 110 Other updates: • Updates to 64-bit Windows Operating System Agent Support, page 21 • Updates to Mac OS X Clean Access Agent Version 4.1.3.0, page 29. • Added Known Issues for Windows Vista and Agent Stub, page 89
1/22/08	Added caveat CSCse91057 to Resolved Caveats - Release 4.1(3), page 75.
1/18/08	Additional updates to: Cisco NAC Appliance Releases, page 2 Known Issues with Cisco NAC Profiler Release 2.1.7, page 88 Release 4.1(3) Compatibility Matrix, page 6 Release 4.1(3) Clean Access Agent Upgrade Compatibility Matrix, page 7 Windows Clean Access Agent Version 4.1.3.1, page 27 Known Issues with MSI Agent Installer, page 89
1/17/08	Updates to Access to Authentication VLAN Change Detection Enhancement, page 21 Added caveat CSCsm25788 to Open Caveats - Release 4.1(3), page 58 Added caveats CSCsg38702 and CSCsj13933 to Resolved Caveats - Release 4.1(3), page 75

Table 17 Updates to Release Notes for Cisco NAC Appliance, Release 4.1(3)

Date	Description
1/15/08	Updates for Windows Agent version 4.1.3.1: • Cisco NAC Appliance Releases, page 2 (updated) • Release 4.1(3) Compatibility Matrix, page 6 (updated) • Release 4.1(3) Clean Access Agent Upgrade Compatibility Matrix, page 7 (updated) • Windows Clean Access Agent Version 4.1.3.1, page 27 (new) • Open Caveats - Release 4.1(3), page 58 (added CSCsm20655) • Resolved Caveats - Windows Clean Access Agent 4.1.3.1, page 73 (new) Other updates: • Moved information from Agent Summary to Known Issue with Windows 2000 Clean Access Agent/Local DB Authentication, page 90. • Minor updates/corrections to various descriptions under Enhancements in Release 4.1(3), page 10.
1/11/08	Added caveat CSCsk05330 to Resolved Caveats - Release 4.1(3), page 75
1/10/08	Added caveat CSCsh77730 to Open Caveats - Release 4.1(3), page 58
1/9/08	• Added caveat CSCsm05207 to Open Caveats - Release 4.1(3), page 58 • Added link to CSCsi75507 to footnote in VPN and Wireless Components Supported for Single Sign-On (SSO), page 4 and VPN SSO Enhancement to Support Existing Clientless SSL VPN Users Launching the AnyConnect Client from a WebVPN Portal, page 16
1/7/08	• Updated Cisco NAC Web Agent, page 12 to clarify requirement that Windows Vista users cannot be signed in to the client machine as a “Guest” before launching the Cisco NAC Web Agent • Added CSCsl71585 to Table 10: List of Open Caveats
1/2/08	Added VPN SSO Enhancement to Support Existing Clientless SSL VPN Users Launching the AnyConnect Client from a WebVPN Portal, page 16 Updated VPN and Wireless Components Supported for Single Sign-On (SSO), page 4
1/1/08	Added warning recommending administrators delete Agent Report entries prior to upgrade from release 3.6(x) and 4.0(x) under Notes on 4.1(3) Upgrade, page 92
12/20/07	Release 4.1(3)

Related Documentation

For the latest updates to Cisco NAC Appliance (Cisco Clean Access) documentation on Cisco.com see:

http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html

or simply http://www.cisco.com/go/cca

- *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(3)*
- *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(3)*
- *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*
- *Connecting Cisco Network Admission Control Network Modules*

- Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)
- Switch Support for Cisco NAC Appliance
- *Cisco NAC Appliance Service Contract / Licensing Support*

Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.