Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(6)

Revised: November 30, 2010, OL-16660-01

Contents

These release notes provide late-breaking and release information for Cisco® NAC Appliance, formerly known as Cisco Clean Access (CCA), release 4.1(6). 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
4.1.7.0 Cisco Clean Access Agent	September 30, 2008
4.1(6) ED	July 31, 2008

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
- Cisco NAC-3300 Series Appliances
- Important Installation Information for NAC-3310
- Additional Hardware Support Information

Cisco NAC Network Module

Release 4.1(6) 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 Cisco 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(6) 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.

Cisco NAC-3300 Series Appliances

Release 4.1(6) 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(6) using a single upgrade file, **cca_upgrade-4.1.6.tar.gz**.

CD installation of release 4.1(6) is also supported:

- For NAC-3310 and NAC-3350, the **cca-4.1_6-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_6-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(6) and Cisco NAC Profiler

Release 4.1(6) includes version 2.1.8-37 of 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 61.

Important Installation Information for NAC-3310

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 details.

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 60.

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 84 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(6)	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 62.
2. Release 4.1(6) 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 the *Release Notes for Cisco NAC Appliance, Version 4.1(3)*, 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(6)* and the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(6)*.

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 15
- Clean Access Supported AV/AS Product List, page 18

Software Compatibility Matrixes

This section describes the following:

- Release 4.1(6) Compatibility Matrix
- Release 4.1(6) CAM/CAS Upgrade Compatibility Matrix
- Release 4.1(6) Clean Access Agent Upgrade Compatibility Matrix

Release 4.1(6) 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(6) 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(6) Compatibility Matrix

Clean Access Manager [1]	Clean Access Server [1]	Cisco NAC Appliance Agents [2]		
		Windows [3]	Mac OS X [4]	Web Agent
4.1(6) [5]	4.1(6) [5]	4.1.7.0 4.1.6.0 4.1.3.x 4.1.2.x 4.1.1.0 4.1.0.x [6]	4.1.3.x 4.1.2.x 4.1.1.0 4.1.0.x [6]	4.1.6.0 4.1.3.x

1. Make sure that both CAM and CAS are of same version.
2. See Cisco NAC Appliance Agents, page 15 for details on version updates for each Windows/Mac OS X/Web Agent.
3. Version 4.1.6.0 of the Windows Clean Access Agent is compatible with the 4.1(6) CAM and CAS releases. See Cisco NAC Appliance Agents, page 15 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.
5. Cisco NAC Appliance Release 4.1(6) is a general and important bug fix release that resolves issues as described in Enhancements in Release 4.1(6), page 10.
6. Cisco strongly recommends running the latest 4.1.6.x version of the Clean Access Agent with release 4.1(6) of the CAM/CAS. If necessary, release 4.1(6) allows administrators to optionally configure the 4.1(6) 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(6) Cisco NAC Appliance system. However, an Agent upgraded to 4.1.6.0 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(6) CAM/CAS Upgrade Compatibility Matrix

Table 3 shows 4.1(6) 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(6) CAM/CAS Upgrade Compatibility Matrix

Clean Access Manager		Clean Access Server	
Upgrade From:	**To:**	**Upgrade From:**	**To:**
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(6) [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(6) [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(6) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(6) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(6).
3. Cisco NAC Appliance Release 4.1(6) is a general and important bug fix release that resolves issues as described in Enhancements in Release 4.1(6), page 10.

Release 4.1(6) Clean Access Agent Upgrade Compatibility Matrix

Table 4 shows Clean Access Agent upgrade compatibility when upgrading existing versions of the Agent after 4.1(6) CAM/CAS upgrade. You can auto-upgrade any 3.5.1+ Windows Agent directly to the latest 4.1.6.0 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(6) 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(6)	4.1(6)	4.1.3.x [4] 4.1.2.x 4.1.1.0 4.1.0.x [5]	4.1.7.0	4.1.3.1
		4.0.x.x 3.6.x.x 3.5.1 and later	4.1.7.0	—

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 4.1.6.0 Agent.

2. See Cisco NAC Appliance Agents, page 15 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. 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 17.
5. Cisco strongly recommends running the latest 4.1.6.x version of the Clean Access Agent with release 4.1(6) of the CAM/CAS. If necessary, release 4.1(6) allows administrators to optionally configure the 4.1(6) 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(6) Cisco NAC Appliance system. However, an Agent upgraded to 4.1.6.0 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.

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

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 80 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 18 and Clean Access Supported AV/AS Product List, page 18 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.

See Cisco NAC Appliance Agents, page 15 for new features and enhancements to Cisco NAC Appliance Agents.

For additional details, see also:

Enhancements in Release 4.1(6)

This section details the enhancements delivered with Cisco NAC Appliance release 4.1(6) for the Clean Access Manager and Clean Access Server.

General Enhancements

Cisco NAC Appliance Agent Enhancements

- See Cisco NAC Appliance Agents, page 15 for enhancement details per Agent version.

Trusted Certificate Authority Enhancement for Production Environments

Cisco NAC Appliance release 4.1(6) addresses a known security issue that can allow outside unauthenticated entities access to the Cisco NAC Appliance network via the same end entity certificate used to initially configure and provide access to newly installed Clean Access Managers and Clean Access Servers.

When you first access your CAM/CAS web console, security warning messages prompt you to address this situation before deploying your CAM/CAS in a production environment. The "EMAILADDRESS=info@perfigo.com, CN=www.perfigo.com, OU=Product, O="Perfigo, Inc.", L=San Francisco, ST=California, C=US" Certificate Authority is required during initial configuration so that you can produce local Temporary Certificates on the CAM and CAS. After initial configuration, however, Cisco strongly recommends removing the "www.perfigo.com" Certificate Authority before deploying your CAM/CAS in a production environment. After you have imported a third-party

CA-signed certificate, use the search function on the new **Administration > CCA Manager > SSL > Trusted Certificate Authorities** CAM web console page and **Administration > SSL > Trusted Certificate Authorities** CAS administrator web console page to isolate and delete the "www.perfigo.com" Certificate Authority.

Note Starting from release 4.1(6), Cisco strongly recommends obtaining dual-purpose CA-signed certificates for your production CAMs/CASs to enable them to act as both SSL clients and SSL servers.

The primary elements of this enhancement include the following topics:

- Enhanced CAM/CAS Web Console Features Certificate Warning Messages, page 11
- Ability to View and Remove Certificate Authorities from CAM/CAS Without Rebooting, page 12
- Enhanced Security with Server Identity Based Authorization, page 12

Note When upgrading to release 4.1(6) from a prior Cisco NAC Appliance release, Cisco strongly recommends that you remove any certificates issued by the "www.perfigo.com" Certificate Authority from all client machines in your production deployment after you have imported CA-signed certificates. There is a potential risk for any web browser client where the user has accepted a certificate issued by the "www.perfigo.com" Certificate Authority on their machine.

Enhanced CAM/CAS Web Console Features Certificate Warning Messages

Release 4.1(6) provides three new types of warning messages to administrators, two of which are designed to address the presence of a potentially harmful Trusted CA in the CAM and/or CAS trusted store.

The "EMAILADDRESS=info@perfigo.com, CN=www.perfigo.com, OU=Product, O="Perfigo, Inc.", L=San Francisco, ST=California, C=US" Certificate Authority is required during initial configuration so that you can produce local Temporary Certificates on the CAM and CAS. However, this same CA can also introduce a security risk for the CAM/CAS and client production networks. Based on this potential security issue, the CAM/CAS web console now displays two types of certificate warning messages that appear after you install and/or upgrade to release 4.1(6):

- A warning that the current certificate on your CAM/CAS should be used for testing only and that you need to import a trusted third-party certificate before deploying in a production environment
- A warning informing you that a potentially non-secure certificate authority is currently part of your CAM/CAS trust store and should be removed to prevent security threats in a production environment

In addition, the CAM/CAS web console provides a third type of warning message informing you that your trusted certificate is either expired or going to expire within 30 days.

Note Starting from release 4.1(6), Cisco strongly recommends obtaining dual-purpose CA-signed certificates for your production CAMs/CASs to enable them to act as both SSL clients and SSL servers.

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

- **Administrator > Summary**

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

- **Network Settings > IP**

Note Starting with Cisco NAC Appliance release 4.1(6), the CAM and CAS require encrypted communication. Therefore, the CAM must contain the Trusted Certificate Authorities from which the certificates on all of its managed CASs originate, and all CASs must all contain the same Trusted Certificate Authority from which the CAM certificate originates before deploying Cisco NAC Appliance in a production environment.

Ability to View and Remove Certificate Authorities from CAM/CAS Without Rebooting

Cisco NAC Appliance Release 4.1(6) enables administrators to view and delete Trusted Certificate Authorities from both the CAM and CAS trust stores. Using the CAM or CAS web console, you can now access the local Trusted CA database, filter the list of current Trusted CAs, and select one or more CAs to remove. Once you have refined the list to only the CAs you want to keep in the trust store, you can now also restart CA services on the CAM or CAS without rebooting the system.

Note Starting from release 4.1(6), Cisco strongly recommends obtaining dual-purpose CA-signed certificates for your production CAMs/CASs to enable them to act as both SSL clients and SSL servers.

Note Admins should expect a few minutes of downtime when updating trusted CAs on the CAS, as updating certificate information restarts services. This is due to the fact that, starting from release 4.1(6), the CAM/CAS use mutual authentication to communicate back and forth and although you are no longer required to reboot the CAS when you change the certificate or import new Trusted CAs, the CAM-to-CAS connections are still "reset" to ensure network security. Therefore, Cisco recommends performing this type of action during periods of very low Cisco NAC Appliance network traffic.

The new View/Remove CA feature is intended to allow administrators to remove Trusted CAs that may introduce a potential security threat within the Cisco NAC Appliance system. For more information, see Enhanced CAM/CAS Web Console Features Certificate Warning Messages.

Note When upgrading to release 4.1(6) from a prior Cisco NAC Appliance release, Cisco strongly recommends that you remove any certificates issued by the "www.perfigo.com" Certificate Authority from all client machines in your production deployment after you have imported CA-signed certificates. There is a potential risk for any web browser client where the user has accepted a certificate issued by the "www.perfigo.com" Certificate Authority on their machine.

This feature adds the following page to the CAM web console:

- **Administration > CCA Manager > SSL > Trusted Certificate Authorities**

This feature adds the following page to the CAS web console:

- **Administration > SSL > Trusted Certificate Authorities**

Enhanced Security with Server Identity Based Authorization

In Cisco NAC Appliance release 4.1(6), administrators can now enforce explicit Authorization between the CAM and CAS in the network. If you enable this feature on the CAM, you must enter the Distinguished Names (DNs) of all of the CASs managed by the CAM on the Authorization page, and enable the same function on all of the CASs managed by the CAM in the CAS Authorization page.

Note Distinguished names require exact syntax. Therefore, Cisco recommends copying the CAM DN and CAS DN from the bottom portion of the respective **Administration > CCA MAnager > SSL > X509 Certificate** CAM web console page or **Administration > SSL > X509 Certificate** CAS web console page and pasting them into the corresponding Authorization page to ensure you specify the exact name for the CAM on the CAS and the CAS on the CAM.

If you have deployed your CAMs/CASs in an HA environment, you can enable authorization for both the HA-Primary and HA-Secondary machines in the HA pair by specifying the DN of only the HA-Primary appliance. For example, if the CAM manages a CAS HA pair, you only need to list the HA-Primary CAS on the CAM's Authorization page. Likewise, if you are enabling this feature on a CAS managed by a CAM HA-pair, you only need to list the HA-Primary CAM on the CAS's Authorization page.)

This feature is optional, but Cisco recommends enabling Authorization for your CAM/CASs to enhance secure communication within the Cisco NAC Appliance system.

This feature adds the following page to the CAM web console:

- **Device Management > CCA Servers > Authorization**

This feature adds the following page to the CAS web console:

- **Administration > Authorization**

JMX Over SSL Secured with Mutual Authentication

Starting from release 4.1(6), the CAM now authenticates with the CAS using Java Management Extensions (JMX) over the Secure Sockets Layer (SSL). In prior releases of Cisco NAC Appliance, communications between the CAM and CAS only utilized HTTPS, making it possible (however unlikely) that an outside party could "act" as the CAM in the network and gain unauthorized access. By ensuring that encrypted JMX communications now require the CAM and CAS to use SSL for two-way authentication, Cisco NAC Appliance transmissions from the CAM to the CAS are secure from outside entities.

Note Starting with Cisco NAC Appliance release 4.1(6), the CAM and CAS require encrypted communication. Therefore, the CAM must contain the Trusted Certificate Authorities from which the certificates on all of its managed CASs originate, and all CASs must all contain the same Trusted Certificate Authority from which the CAM certificate originates before deploying Cisco NAC Appliance in a production environment.

HTTPS Connections Enhanced with Mutual Authentication

HTTPS communications from the CAS to the CAM have been improved to require mutual authentication from both appliances via SSL before allowing two-way access:

- Cisco NAC Appliance only allows trusted certificates for mutual authentication
- To help support mutual authentication, administrators can also choose to enable CAM/CAS Authorization using Cisco NAC Appliance distinguished names (DNs) (see Enhanced Security with Server Identity Based Authorization)

Note Starting with Cisco NAC Appliance release 4.1(6), the CAM and CAS require encrypted communication. Therefore, the CAM must contain the Trusted Certificate Authorities from which the certificates on all of its managed CASs originate, and all CASs must all contain the same Trusted Certificate Authority from which the CAM certificate originates before deploying Cisco NAC Appliance in a production environment.

Features Optimized/Removed

The following functions have been optimized or removed in Cisco NAC Appliance Release 4.1(6):

- Administrators no longer have to reboot the CAS when importing new Trusted CAs or generating a new certificate. Instead, you simply need to update certificate information which then automatically restarts services on the CAM/CAS.
- The CAM/CAS now only feature one Trusted CA store. The administrator is not required to import a CA for Java in the CAM and CAS web console. (In previous releases of Cisco NAC Appliance, the CAM/CAS maintained separate Trusted CA databases for regular and LDAP CAs.)
- The *** Trust Non-Standard CA** option has been removed from the **Administration > CCA Manager > SSL > X509 Certificate | Import Certificate** CAM page
- The Cisco NAC Appliance system no longer manages certificates using JMX.
- The **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs** CAM web console page has been removed in favor of the **Administration > SSL > X509 Certificate** and **Administration > SSL > Trusted Certificate Authority** CAS web console pages.

Supported AV/AS Product List Enhancements (Version 69)

- See Clean Access Supported AV/AS Product List, page 18 for the latest AV/AS product charts.
- See Supported AV/AS Product List Version Summary, page 40 for details on each update to the list.

Cisco NAC Appliance Agent Enhancements

See Cisco NAC Appliance Agents, page 15 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 15
- Mac OS X Clean Access Agent Enhancements, page 17
- Cisco NAC Web Agent Enhancements, page 17

Refer to Resolved Caveats - Agent Version 4.1.6.0, page 56 for additional information.

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(6) Compatibility Matrix and Release 4.1(6) Clean Access Agent Upgrade Compatibility Matrix, page 7 for compatibility details.
- See Clean Access Supported AV/AS Product List, page 18 for details on related AV/AS support.

Note

- Cisco strongly recommends running version 4.1.6.0 of the Clean Access Agent with release 4.1(6) of the CAM/CAS. However, administrators can optionally configure the 4.1(6) 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 Cisco NAC Appliance (Cisco Clean Access), Version 4.1(0)* for complete details on 4.1.0.x Agent AV/AS support.
- For information on other prior release Agent versions, refer to the following:
  - See the "Cisco NAC Appliance Agents" section in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) Version 4.1(3)* for details on the 4.1.3.x Agent
  - 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 60 and Troubleshooting, page 84 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 4.1.7.0
- Windows Clean Access Agent Version 4.1.6.0

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 4.1.7.0

This section summarizes the latest enhancements for version 4.1.7.0 of the Windows Clean Access Agent. Refer to the following links for additional information:

- Supported AV/AS Product List Version Summary, page 40
- Resolved Caveats - Agent Version 4.1.7.0, page 54
- Open Caveats - Release 4.1(6), page 44 (added CSCsr50995)

Windows Clean Access Agent Version 4.1.6.0

This section contains the latest enhancements for the Windows Clean Access Agent. Refer to Resolved Caveats - Agent Version 4.1.6.0, page 56 for additional information.

- Added Clean Access Agent language template support for French Canadian language
- Version 4.1.6.0 of the Clean Access Agent introduces three registry key settings to configure Windows Clean Access Agent behavior on the client machine:
  - **HKLM/Software/Cisco/Clean Access Agent/KeepWSUSOnTop** (DWORD)—Addresses a potential situation where users are not able to remediate and authenticate when in the Agent Temporary Role because the Windows Server Update Service (WSUS) update/install dialog remains hidden behind the Clean Access Agent login dialog. Eventually, the remediation process times out and users are able to begin the log in process again, but still cannot pass the WSUS requirement and are not able to authenticate with the Cisco NAC Appliance system. A value of 1 enables this feature and forces the WSUS update/installation dialog to stay on top of the client machine's desktop so users are able to complete authentication. The default value is 0 (disabled). For more information, see CSCso87910, page 57.
  - **HKLM/Software/Cisco/Clean Access Agent/SwissTimeout** (DWORD)—This registry setting is designed to overcome potential latency issues in remote client networks. When the Clean Access Agent sends SWISS discovery packets to the network looking for a CAS through which the user can authenticate, the default 1 second timeout value for SWISS response may not be long enough to allow the response packet from the CAS in networks that include inherent packet latency. To address this issue, Cisco NAC Appliance administrators can provide an increased value for the SwissTimeout registry setting. Specifying a value greater than 1 enables and increases the SWISS timeout delay on Clean Access Agent client machines. (If you choose to enable this feature, Cisco recommends specifying a 3 second delay.) For more information, see CSCso55025, page 56.

    Note The potential side effect of enabling this feature is that authentication methods involving VPN and/or SSO may take significantly longer than normal to complete.

  - **HKLM/Software/Cisco/Clean Access Agent/ExceptionMACList** (String)—This registry setting enables you to create a list of client-side adapter MAC addresses that the Clean Access Agent should *not* send to the CAS during authentication. To use this setting, you must specify a comma-separated series of MAC addresses (using colons ":" to delineate the MAC address value) so that the Clean Access Agent knows to leave those MAC addresses out of the transmission the Agent advertises to the CAS. For example:

    ```
    AA:BB:CC:DD:EE:FF,11:22:33:44:55:66
    ```

    For more information, see CSCsm87761, page 56.

Mac OS X Clean Access Agent Enhancements

There are no new features or enhancements in the Mac OS X Agent for Release 4.1(6).

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.

Cisco NAC Web Agent Enhancements

There are no new features or enhancements in the Cisco NAC Web Agent for Release 4.1(6). Refer to Resolved Caveats - Agent Version 4.1.6.0, page 56 for additional information.

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

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 19
- Clean Access AV Support Chart (Windows ME/98), page 32
- Clean Access AS Support Chart (Windows Vista/XP/2000), page 34

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 15
- Supported AV/AS Product List Version Summary, page 40

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(6)* 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 5 lists Windows Vista/XP/2000 Supported AV Products as of the latest release of the Cisco NAC Appliance software. (See Table 6 for Windows ME/98).

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 1 of 13)

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
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
AVG Technologies				
AVG 8.0 [AntiVirus]	8.x	yes (4.1.3.2)	yes (4.1.7.0)	yes
AVG Anti-Virus Free	8.x	yes (4.1.6.0)	yes (4.1.7.0)	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
AhnLab V3 Internet Security 7.0 Platinum Enterprise	7.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
V3 VirusBlock 2005	6.x	yes (4.1.2.0)	yes (4.1.2.0)	-
V3Pro 2004	6.x	yes (3.5.10.1)	yes (3.5.12)	yes
America Online, Inc.				
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	102.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)	-
AOL Safety and Security Center Virus Protection	210.x	yes (4.0.4.0)	yes (4.0.4.0)	-

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 2 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Active Virus Shield	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
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
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 Premium	8.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
Avira AntiVir Professional	8.x	yes (4.1.6.0)	yes (4.1.6.0)	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
Avira Premium Security Suite	8.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
Beijing Rising Technology Corp. Ltd.				
Rising Antivirus Network Edition	20.x	yes (4.1.7.0)	yes (4.1.7.0)	-
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
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)	yes
BullGuard Gamers Edition	8.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
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 (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 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

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 3 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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
ZoneAlarm Security Suite Antivirus	8.x	yes (4.1.7.0)	yes (4.1.7.0)	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
Comodo Group				
Comodo BOClean Anti-Malware	4.25.x	yes (4.1.6.0)	-	yes
Computer Associates International, Inc.				
CA Anti-Virus	10.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
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
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)	-

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 4 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Eset Software				
ESET NOD32 Antivirus	3.x	yes (4.1.3.2)	yes (4.1.3.2)	-
ESET Smart Security	3.x	yes (4.1.6.0)	yes (4.1.6.0)	-
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	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
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)	-
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	8.x	yes (4.1.6.0)	yes (4.1.6.0)	-
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
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
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

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 5 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
G DATA TotalCare [Antivirus]	18.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Grisoft, Inc.				
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 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 Antivirensystem 7.0	7.x	yes (3.5.0)	yes (3.5.0)	yes
AVG Free Edition	7.x	yes (3.5.0)	yes (3.5.0)	yes
Antivirussystem AVG 6.0	6.x	yes (3.5.0)	yes (3.5.0)	-
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
HAURI, Inc.				
ViRobot Desktop	5.0.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
ViRobot Desktop	5.x	yes (4.1.3.0)	yes (4.1.3.0)	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	10.x	yes (4.1.6.0)	yes (4.1.6.0)	-
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
Jiangmin AntiVirus KV2008	11.x	yes (4.1.7.0)	-	yes
K7 Computing Pvt. Ltd.				
K7 Total Security	9.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
K7AntiVirus 7.0	7.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
Kaspersky Labs				
Kaspersky Anti-Virus 2006 Beta	6.0.x	yes (3.5.8)	yes (3.5.8)	-
Kaspersky Anti-Virus 2009	8.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
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

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 6 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Kaspersky Anti-Virus 7.0	7.x	yes (4.1.3.0)	yes (4.1.3.0)	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 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 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
Kingsoft Internet Security 9	2008.x	yes (4.1.7.0)	yes (4.1.7.0)	-
Lavasoft, Inc.				
Lavasoft Ad-Aware 2008 Professional [Antivirus]	7.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
McAfee, Inc.				
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

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 7 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
McAfee VirusScan	13.x	yes (4.1.7.0)	yes (4.1.7.0)	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
McAfee VirusScan Enterprise	8.7.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
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
Total Protection for Small Business	4.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
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
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)	-	-
New Technology Wave Inc.				
Virus Chaser	5.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
Norman ASA				
Norman Virus Control	5.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Norman Virus Control	7.x	yes (4.1.6.0)	yes (4.1.6.0)	yes

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 8 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
Omniquad				
Omniquad Total Security AV	9.x	yes (4.1.7.0)	yes (4.1.7.0)	-
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 AntiVirus 2008	5.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
PC Tools Internet Security [Antivirus]	5.x	yes (4.1.3.0)	yes (4.1.3.0)	-
PC Tools Internet Security [Antivirus]	6.x	yes (4.1.7.0)	yes (4.1.7.0)	-
PC Tools Spyware Doctor [Antivirus]	5.x	yes (4.1.3.2)	-	-
PC Tools Spyware Doctor [Antivirus]	6.x	yes (4.1.7.0)	-	-
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)	-	-
ThreatFire 3.5	3.5.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
Panda Software				
Panda Antivirus + Firewall 2007	6.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
Panda Antivirus + Firewall 2008	7.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
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 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 Antivirus Pro 2009	8.x	yes (4.1.7.0)	yes (4.1.7.0)	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 Internet Security 2009	14.x	yes (4.1.7.0)	yes (4.1.7.0)	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

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 9 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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)	-
Radialpoint Inc.				
Radialpoint Security Services Virus Protection	6.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Radialpoint Security Services Virus Protection	7.x	yes (4.1.7.0)	yes (4.1.7.0)	-
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
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

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 10 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
BitDefender Total Security 2009	12.x	yes (4.1.7.0)	yes (4.1.7.0)	-
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
SecurityCoverage, Inc.				
SecureIT [Antivirus]	1.x	yes (4.1.7.0)	yes (4.1.7.0)	-
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
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
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	16.x	yes (4.1.7.0)	yes (4.1.7.0)	-
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 (Symantec Corporation)	10.x	yes (3.5.0)	yes (3.5.0)	yes

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 11 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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 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	16.x	yes (4.1.7.0)	yes (4.1.7.0)	-
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
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 Anti-Virus	17.x	yes (4.1.7.0)	yes (4.1.7.0)	-

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 12 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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 Antivirus	11.x	yes (3.5.0)	yes (3.5.0)	yes
Trend Micro Client/Server Security	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Trend Micro Client/Server Security Agent	15.x	yes (4.1.6.0)	yes (4.1.6.0)	-
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 Internet Security	17.x	yes (4.1.6.0)	yes (4.1.6.0)	-
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
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)	-
VirusBlokAda Ltd.				
Vba32 Personal	3.x	yes (4.1.6.0)	yes (4.1.6.0)	-

Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 13 of 13)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
VirusBuster Ltd.				
VirusBuster Professional	5.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
VirusBuster for Windows Servers	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)	-
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 Personal	4.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
eEye Digital Security Blink Professional	3.x	yes (4.0.6.0)	yes (4.0.6.0)	yes
eEye Digital Security Blink Professional	4.x	yes (4.1.7.0)	yes (4.1.7.0)	yes

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 6 lists Windows ME/98 Supported AV Products as of the latest release of the Cisco NAC Appliance software. (See Table 5 for Windows Vista/XP/2000.)

Table 6 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 72, 4.1.6.0 Agent, CAM/CAS Release 4.1(6) (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 6 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 72, 4.1.6.0 Agent, CAM/CAS Release 4.1(6) (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 7 lists Windows Vista/XP/2000 Supported Antispyware Products as of the latest release of the Cisco Clean Access software.

Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 1 of 7)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
AVG Technologies				
AVG 8.0 [AntiSpyware]	8.x	yes (4.1.3.2)	-	yes
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
BellSouth				

Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 2 of 7)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
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
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 Pro Antispyware	8.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
ZoneAlarm Security Suite Antispyware	7.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
ZoneAlarm Security Suite Antispyware	8.x	yes (4.1.7.0)	yes (4.1.7.0)	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	11.x	yes (4.1.7.0)	yes (4.1.7.0)	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
CA eTrustITM Agent (AntiSpyware)	8.x	yes (4.1.6.0)	yes (4.1.6.0)	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)	-	-
F-Secure Corp.				

Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 3 of 7)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
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)	-
F-Secure Internet Security (AntiSpyware)	8.x	yes (4.1.7.0)	yes (4.1.7.0)	-
FaceTime Communications, Inc.				
X-Cleaner Deluxe	4.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
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)	-
Javacool Software LLC				
Javacool SpywareBlaster	4.x	yes (4.1.6.0)	yes (4.1.6.0)	-
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 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
Ad-aware 6 Professional	6.x	yes (3.6.0.0)	yes (3.6.0.0)	-
Lavasoft Ad-Aware 2008	7.x	yes (4.1.6.0)	-	-
Lavasoft Ad-Aware 2008 Professional	7.x	yes (4.1.6.0)	-	yes
McAfee, Inc.				
McAfee Anti-Spyware Enterprise Module	8.0.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
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

Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 4 of 7)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
McAfee AntiSpyware Enterprise Module	8.5.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
McAfee AntiSpyware Enterprise Module	8.7.x	yes (4.1.6.0)	yes (4.1.6.0)	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
McAfee VirusScan AS	13.x	yes (4.1.7.0)	yes (4.1.7.0)	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)	-	-
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
NETGATE Technologies s.r.o				
Spy Emergency 2008	5.x	yes (4.1.7.0)	-	-
Omniquad				
Omniquad Total Security	2.0.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Omniquad Total Security	3.0.x	yes (4.1.7.0)	yes (4.1.7.0)	-
PC Tools Software				
PC Tools Internet Security [Antispyware]	5.x	yes (4.1.3.0)	-	-
PC Tools Internet Security [Antispyware]	6.x	yes (4.1.7.0)	-	-
PC Tools Spyware Doctor	5.x	yes (4.1.3.2)	-	yes
PC Tools Spyware Doctor	6.x	yes (4.1.7.0)	-	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

Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 5 of 7)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
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
Panda Software				
Panda Titanium 2006 Antivirus + Antispyware [AntiSpyware]	5.x	yes (4.1.3.2)	yes (4.1.3.2)	-
Prevx Ltd.				
Prevx Home	2.x	yes (3.6.0.0)	yes (3.6.0.0)	-
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
Radialpoint Inc.				
Radialpoint Security Services Spyware Protection	6.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Radialpoint Security Services Spyware Protection	7.x	yes (4.1.7.0)	yes (4.1.7.0)	-
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
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
SUPERAntiSpyware.com				
SUPERAntiSpyware Free Edition	4.x	yes (4.1.7.0)	yes (4.1.7.0)	-
SUPERAntiSpyware Professional	4.x	yes (4.1.7.0)	yes (4.1.7.0)	-
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)	-
Spybot - Search & Destroy 1.6	1.6.x	yes (4.1.7.0)	yes (4.1.7.0)	yes

Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 6 of 7)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
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
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 AntiVirus [AntiSpyware]	16.x	yes (4.1.7.0)	-	-
Norton Internet Security AntiSpyware	15.x	yes (4.1.3.0)	-	-
Norton Internet Security [AntiSpyware]	16.x	yes (4.1.7.0)	-	-
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
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)	-	-

Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 72, 4.1.7.0 Agent, CAM/CAS Release 4.1(6) (Sheet 7 of 7)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
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)	yes (4.1.7.0)	yes
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)	-
ZoneAlarm Pro (AntiSpyware)	6.x	yes (4.1.6.0)	yes (4.1.6.0)	-
iS3 Inc.				
STOPzilla	5.x	yes (4.1.3.2)	yes (4.1.3.2)	yes

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 8 details enhancements made per version of the Supported Antivirus/Antispyware Product List. See Clean Access Supported AV/AS Product List, page 18 for the latest Supported AV list as of the latest release. See New and Changed Information, page 10 for the release feature list.

Table 8 Supported AV/AS Product List Versions

Version	Enhancements
Release 4.1(6)—4.1.7.0 Agent	
Version 72	Minor internally used data change.

Table 8 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 71	Minor internally used data change.
Version 70	**Added AV def date support for:** • AVG 8.0 [AntiVirus], 8.x • AVG Anti-Virus Free, 8.x **Added AV Live Update for:** • ViRobot Desktop, 5.0.x • ViRobot Desktop, 5.x **New AV products (Windows Vista/XP/2000):** • Rising Antivirus Network Edition, 20.x • BullGuard Gamers Edition, 8.x • ZoneAlarm Security Suite Antivirus, 8.x • CA Anti-Virus, 10.x • Jiangmin AntiVirus KV2008, 11.x • K7 Total Security, 9.x • K7AntiVirus 7.0, 7.x • Kaspersky Anti-Virus 2009, 8.x • Kingsoft Internet Security 9, 2008.x • McAfee VirusScan, 13.x • Virus Chaser, 5.x • Omniquad Total Security AV, 9.x • PC Tools AntiVirus 2008, 5.x • PC Tools Internet Security [Antivirus], 6.x • PC Tools Spyware Doctor [Antivirus], 6.x • Panda Antivirus Pro 2009, 8.x • Panda Internet Security 2009, 14.x • Radialpoint Security Services Virus Protection, 7.x • BitDefender Total Security 2009, 12.x • SecureIT [Antivirus], 1.x • Norton AntiVirus, 16.x • Norton Internet Security, 16.x • Trend Micro Anti-Virus, 17.x • eEye Digital Security Blink Personal, 4.x • eEye Digital Security Blink Professional, 4.x

Table 8 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 70 (continued)	**Added AS def date support for:** • CA Yahoo! Anti-Spy, 2.x **New AS Products (Windows Vista/XP/2000):** • ZoneAlarm Pro Antispyware, 8.x • ZoneAlarm Security Suite Antispyware, 8.x • CA eTrust Internet Security Suite AntiSpyware, 11.x • F-Secure Internet Security (AntiSpyware), 8.x • McAfee VirusScan AS, 13.x • Spy Emergency 2008, 5.x • Omniquad Total Security, 3.0.x • PC Tools Internet Security [Antispyware], 6.x • PC Tools Spyware Doctor, 6.x • Radialpoint Security Services Spyware Protection, 7.x • SUPERAntiSpyware Free Edition, 4.x • SUPERAntiSpyware Professional, 4.x • Spybot - Search & Destroy 1.6, 1.6.x • Norton AntiVirus [AntiSpyware], 16.x • Norton Internet Security [AntiSpyware], 16.x
Release 4.1(6)—4.1.6.0 Agent	

Table 8 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 69	**Added AV def date check:** • eEye Digital Security Blink Professional, 3.x **Added AV def version check:** • VirusBuster for Windows Servers, 5.x • VirusBuster Professional, 5.x **Added New AV Products (Windows Vista/XP/2000):** • AVG Anti-Virus Free, 8.x • Avira AntiVir Premium, 8.x • Avira AntiVir Professional, 8.x • Avira Premium Security Suite, 8.x • Comodo BOClean Anti-Malware, 4.25.x • ESET Smart Security, 3.x • F-Secure Internet Security, 8.x • Proventia Desktop, 10.x • Lavasoft Ad-Aware 2008 Professional [Antivirus], 7.x • McAfee VirusScan Enterprise, 8.7.x • Norman Virus Control, 7.x • ThreatFire 3.5, 3.5.x • Trend Micro Client/Server Security Agent, 15.x • Trend Micro Internet Security, 17.x • Vba32 Personal, 3.x **Added New AS Products (Windows Vista/XP/2000):** • CA eTrustITM Agent (AntiSpyware), 8.x • Javacool SpywareBlaster, 4.x • Lavasoft Ad-Aware 2008, 7.x • Lavasoft Ad-Aware 2008 Professional, 7.x • McAfee AntiSpyware Enterprise Module, 8.7.x • ZoneAlarm Pro (AntiSpyware), 6.x

Caveats

This section describes the following caveats:

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(6)

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

Table 9 List of Open Caveats (Sheet 1 of 10)

	Software Release 4.1(6)	
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.”

Table 9 List of Open Caveats (Sheet 2 of 10)

	Software Release 4.1(6)	
DDTS Number	**Corrected**	**Caveat**
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
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.)

Table 9 List of Open Caveats (Sheet 3 of 10)

	Software Release 4.1(6)	
DDTS Number	**Corrected**	**Caveat**
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.
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.

Table 9 List of Open Caveats (Sheet 4 of 10)

	Software Release 4.1(6)	
DDTS Number	**Corrected**	**Caveat**
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.
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.

Table 9 List of Open Caveats (Sheet 5 of 10)

DDTS Number	Software Release 4.1(6) Corrected	Caveat
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.
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 9 List of Open Caveats (Sheet 6 of 10)

	Software Release 4.1(6)	
DDTS Number	**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 9 List of Open Caveats (Sheet 7 of 10)

	Software Release 4.1(6)	
DDTS Number	**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 9 List of Open Caveats (Sheet 8 of 10)

	Software Release 4.1(6)	
DDTS Number	**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 "Cisco" 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.
CSCso41549	No	Administrator cannot delete the OUL manually if the In-Band CAS is not available to the CAM If an In-Band CAS fails for some reason (if the CAS suffers a hardware failure, for example), users stay in the Online Users List. **Workaround** Manually delete the entry from the "user_info" table in the CAM database.

Table 9 List of Open Caveats (Sheet 9 of 10)

	Software Release 4.1(6)	
DDTS Number	**Corrected**	**Caveat**
CSCso49473	No	SEVERE: javax.naming.CommunicationException causes no provider list Configuration: ADSSO with LDAP Lookup If the LDAP connection to AD drops because the lookup takes a long time or the route is lost suddenly, the Agent does not receive the list of auth providers so the user is presented with a blank provider list. Symptom: The dropdown list of authentication providers is blank. Conditions: LDAP server fails to respond due to network connectivity failure or a long directory search. The failure must occur after communication to the LDAP server has begun. Workaround: None **Note** CSCso61317 is a duplicate of this bug.
CSCsr52953	No	RMI error messages periodically appears for deleted and/or unauthorized CASs in CAM event logs Clean Access Servers connected to a CAM can periodically appear as “deleted” or “unauthorized” in the CAM event logs even though the CAS is functioning properly and has not experienced any connection issues with the Clean Access Manager. Error message examples are: • “SSL Communication 2008-07-23 00:31:29 SSLManager:authorizing server failed CN=10.201.217.201, OU=Perfigo, O=Cisco Systems, L=San Jose, ST=California, C=US” • “SSL Communication 2008-07-23 00:31:29 RMISocketFactory:Creating RMI socket failed to host 10.201.217.201:java.security.cert.CertificateException: Unauthorized server CN=10.201.217.201, OU=Perfigo, O=Cisco Systems, L=San Jose, ST=California, C=US” **Workaround** • Reboot the CAS and wait for the CAM to re-establish connection. • Reboot the CAM after deleting and removing the CAS from the Authorized CCA Server list using the CAM **Device Management > CCA Servers > Authorization** admin web console page.

Table 9 List of Open Caveats (Sheet 10 of 10)

	Software Release 4.1(6)	
DDTS Number	**Corrected**	**Caveat**
CSCsr50995	No	Agent doesn't detect Zone Alarm Security definitions correctly Symptom: User fails posture assessment when checking for AV definitions for Zone Alarm Security Suite 7.0. Conditions: This occurs using either the Any AV check or the Checkpoint Any check. **Workaround** Create a custom check for Zone Alarm Security Suite definition.
CSCsu02167	No	SSL fails when Netscape Cert Type field does not contain "SSL Client" As a result, the CAS and CAM disconnect from one another and users cannot authenticate. Report log entries show: "SEVERE: SSLManager: client's certificate chain verification failed CN=CAS, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US:Netscape cert type does not permit use for SSL client" If certificates contain a Netscape Cert Type field and are used in release 4.1(6), that field has to contain both "SSL Server" and "SSL Client." If the field does not contain "SSL Client," communication between the CAS and CAM fails. If the Netscape Cert Type field does not exist, then SSL succeeds. If the Netscape Cert Type field does exist, but does not contain both "SSL Server" and "SSL Client," authentication fails. **Note** This issue has been observed with Entrust certificates and another educational CA. **Workaround** • Get certificate reissued by CA with no Netscape Cert Type field, or ensure the field contains both "SSL Server" and "SSL Client." • Use temporary certs (**not recommended**).

Resolved Caveats - Agent Version 4.1.7.0

Refer to Windows Clean Access Agent Version 4.1.7.0, page 16 and Enhancements in Release 4.1(6), page 10 for additional information.

Table 10 List of Resolved Caveats (Sheet 1 of 2)

	Agent Version 4.1.7.0	
DDTS Number	**Corrected**	**Caveat**
CSCsr75771	Yes	Symantec AntiVirus 10.x not fully compatible with CCA Agent Symptom: CCA Agent failed to properly update Symantec AntiVirus Version 10.1.5.500. The Agent detected that the definition needed to be updated, but the Agent would never allow the next button to become active. Launching the update via the Symantec software allowed for a successful update. Conditions: Symantec Antivirus version 10.1.5.500 and CCA Agent configured to manually or automatically remediate does not successfully update the client. **Workaround** Manually launch the update from Symantec systray, or upgrade to 4.1.7.0 or later. The Symantec AntiVirus rule definition must be configured for Symantec Client Security in order for the check to pass with version 4.1.7.0.
CSCsr87134	Yes	Vista Agent does not detect MAC Address of Wireless NIC Symptom: The CCA Agent on Windows Vista does not detect the MAC address of the wireless NIC. It detects the MAC address of the wired NIC twice (so when sending the maciplist it sends the wired_mac:wired_ip combo and the wired_mac:wireless_ip combo). This in itself would not cause a problem but it breaks other features such as the “Enable L2 Strict mode to block L3 devices with Clean Access Agent” because the CAS has one MAC address in its intern_arpq table, and gets a different one from the Agent. When these addresses do not match, the CAS blocks the user with the message “Access blocked by Administrator.” In addition, a Vista client with only the wireless NIC active will not be able to connect. Conditions: The invalid detection of MAC addresses happens on any Vista client running 4.1.6.0. The blocking of users happens if L2 Strict mode is enabled on the CAS to which the user is logging in. **Workaround** The options are as follows: 1. Stop pushing out the 4.1.6.0 Agent and return to 4.1.3.x or prior. 2. Disable the “Enable L2 Strict Mode” option. 3. Upgrade the Agent to 4.1.7.0

Table 10 List of Resolved Caveats (Sheet 2 of 2)

	Agent Version 4.1.7.0	
DDTS Number	**Corrected**	**Caveat**
CSCsr97355	Yes	AVG Anti-Virus Free 8.x support for Virus Definition check Symptom: CCA 4.1.6 checks for AVG Anti-Virus Free 8.x installation but does not check for 8.x definition update. Conditions: When AVG Anti-virus free 8.x is installed on the client machine. **Workaround** Create custom checks and rules to detect virus definition update, or upgrade Agent to 4.1.7.0 or later.

Resolved Caveats - Agent Version 4.1.6.0

Refer to Cisco NAC Appliance Agents, page 15 and Enhancements in Release 4.1(6), page 10 for additional information.

Table 11 List of Resolved Caveats (Sheet 1 of 2)

	Agent Version 4.1.6.0	
DDTS Number	**Corrected**	**Caveat**
CSCsl59656	Yes	Java version of Web Agent does not run with Vista/Firefox combo The Cisco NAC Web Agent Java applet installer does not load when the user attempts to launch it from the browser and the Java applet returns an "Error when running Java applet for Cisco NAC web agent (status = -1)" error message. This is only seen in Windows Vista under the following conditions: • The user is a local administrator • UAC is enabled • User logging in via Firefox web browser **Workaround** 1. Use Microsoft Internet Explorer to connect to the network. 2. Disable UAC.
CSCsm04923	Yes	Clean Access Agent detects incorrect MAC address when using Nortel VPN Client Windows 2000 machines are asked to login when using a MAC filter. This scenario typically occurs if the client is running the Nortel VPN software and the user logs in using Clean Access Agent version 4.1.2.1.
CSCsm87761	Yes	Agent detects irrelevant MAC addresses The clean access agent will detect irrelevant MAC addresses such as a PPP adapter on the client side of the network. This can result in different users having the same MAC address in clean access.
CSCso26102	Yes	Need Agent support for French Canadian language If the user specifies the Windows locale to be "French (Canada)," the Clean Access Agent dialogs come up in English.
CSCso55025	Yes	Clean Access Agent fails over slow links Due to a slow network link, delayed responses from the CAS can cause the client machine to keep sending SWISS discovery packets in an effort to contact the CAS.
CSCso73630	Yes	Russian Agent text is incorrectly formatted This has been observed using Clean Access Agent version 4.1.3.2, the first version to support Russian language.

Table 11 List of Resolved Caveats (Sheet 2 of 2)

	Agent Version 4.1.6.0	
DDTS Number	**Corrected**	**Caveat**
CSCso76507	Yes	Clean Access Agent only detects one version of Symantec Antivirus if more than one is installed The Clean Access Agent can only detect one Symantec Antivirus application installed on a client. Since we do not support definition checking with NSS, clients will fail AV definition checks even though their full AV installation may be up to date. **Note** The Agent detects other Antivirus vendors' products accurately. **Workaround** Uninstall all but the main Antivirus on the client so the agent will recognize the one we want it to.
CSCso87910	Yes	Clean Access Agent dialog covers the Windows installer dialog when performing WSUS installation using "Show UI" option The dialog for Windows Update can remain hidden behind the Agent if the "Show UI" option is enabled. The Agent does not continue remediation until Windows Updates dialog is closed. As a result, the Agent remediation session might never complete if the user does not realize the Windows Updates dialog is hidden behind the Agent dialog. **Workaround** Users can move the Agent dialog off to the side, revealing the button users must click to complete the Windows Update.
CSCsq31451	Yes	Auto Remediation Updating screen for McAfee AV keeps appearing When logging into Cisco NAC Appliance with an old McAfee definition file (McAfee VirusScan Enterprise 8.0.0), the Agent automatically performs an AV Definition Update. However, the "Updating Virus Definition..." message keeps appearing even after McAfee has been updated. The result is that temporary user access to the network expires. **Workaround** The user must click the **Manual** button then click the **Next** button in the Agent dialogs successfully log into the network.
CSCsq76860	Yes	Cisco NAC Web Agent fails to parse file date stamp A user can have a custom rule to check to confirm a file is not than 30 days from the current date. This custom requirement works on version 4.1.3.2 of the Windows Clean Access Agent client but fails for version 4.1.3.10 of the Web Agent. The **webagent.log** file lists the following error message: "- Date check failed due to strptime conversion error" **Workaround** To address this issue, Cisco recommends using the Clean Access Agent for user login instead of the Cisco NAC Web Agent.

Resolved Caveats - Release 4.1(6)

Refer to Enhancements in Release 4.1(6), page 10 for additional information.

Table 12 List of Resolved Caveats (Sheet 1 of 2)

	Software Release 4.1(6)	
DDTS Number	**Corrected**	**Caveat**
CSCsm96148	Yes	VPN SSO log out feature does not work The VPN SSO logo ut feature does not log users out of Cisco NAC Appliance when the VPN session has already closed.

CSCsm82486	Yes	CAM Web Console slow and java process taking 99% CPU
		The "Device List" and "Profile" from the web console Administration menu on a release 4.1(3) CAM hosting approximately 1000 users are opening very slowly. Investigation reveals that the CAM is utilizing 99.9% of the CPU for the JAVA process.
		Workaround
		Turn off the CSRF Filter on the CAM in /perfigo/control/tomcat/normal-webapps/admin/WEB-INF/web.xml:
		`+ <!--`
		`  <filter-mapping>`
		`  <filter-name>CSRFFilter</filter-name>`
		`  <url-pattern>/*</url-pattern>`
		`  </filter-mapping>`
		`+ -->`

CSCso16240	Yes	Web Redirect, Cisco NAC Web Agent, and Clean Access Agent do not work in VGW mode with dissimilar IP addresses An HA-CAS pair configured in VGW mode with dissimilar IP addresses does not support web redirect, Web Agent, or Clean Access Agent in Cisco NAC Appliance Release 4.1.3.1. **Workaround** Install the CASs in a more "common" configuration, with both the eth0 and eth1 interfaces on the CASs in the same network with the same IP address. **Note** This resolves the issue, but disables link-based failover for the eth1 interfaces.
CSCso38182	Yes	Deleting a static route on one CAS deletes the same static route on all managed servers If you create the same static route on two or more CASs and then delete the route on one server, all servers managed by the same CAM delete the route. This behavior has been observed in Cisco NAC Appliance Release 4.1.2.1. **Workaround** Recreate the deleted static routes.

Table 12 List of Resolved Caveats (Sheet 2 of 2)

	Software Release 4.1(6)	
DDTS Number	**Corrected**	**Caveat**
CSCso46353	Yes	Users already in the Certified Device List (CDL) are prompted to enter credentials again When a user connects to a CAS other than the one to which they were first connected (and they are already in the CDL), the user may be repeatedly prompted for their credentials. This issue can occurs when there are multiple CASs in a campus network and a user moves from one CAS to another. **Workaround** Ensure that the user has been removed from the CDL.
CSCso68182	Yes	OpenSSH signal handling issue The OpenSSH version (4.4) on Cisco NAC Appliance releases older than 4.1(6) introduce a potential signal handler race condition that can allow remote attackers to initiate a denial of service (DoS) attack and crash the system. This issue becomes a potential threat when GSSAPI authentication is enabled, thus allowing for unspecified vectors leading to a "double-free." For more information, go to http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-5051 There is no known workaround for this issue.
CSCso72123	Yes	AD SSO listen/accept thread exited on exception and fails to restart AD SSO thread fails to automatically restart if the thread is abnormally exited. **Workaround** Manually restart the SSO service.

Known Issues for Cisco NAC Appliance

This section describes known issues when integrating Cisco NAC Appliance:

Note For additional information, see also Troubleshooting, page 84.

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(6)* 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(6)*, users installing release 4.1(6) 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) 2008 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(6), 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(6) does not support Cisco NAC Profiler Release 2.1.7. If you are planning to upgrade, and 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(6).

Note You will need to upgrade the Collector component on the 4.1(6) 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, refer to the applicable version of the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide*.

Known Issues with Broadcom NIC 5702/5703/5704 Chipsets

Customers running Cisco NAC Appliance release 4.1(6) 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 or later 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 50 for details.

See also Troubleshooting, page 84 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(6)

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(6), page 66.

Warning **New installations of Cisco NAC Appliance release 4.1(6) no longer contain any default third-party Trusted Certificate Authorities. Therefore, after a new installation of release 4.1(6) you must obtain and import Trusted Certificate Authorities before deploying Cisco NAC Appliance in a production environment.**

For New Installation:

1. If you are going to perform a new installation but are running a previous version of Cisco Clean Access and want to preserve existing settings and/or database information, back up your current Clean Access Manager installation and save the snapshot on your local computer, as described in General Preparation for Upgrade, page 69.
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(6) on each Clean Access Server and Clean Access Manager, as follows:
   a. Log in to Cisco Secure Software and download the latest 4.1(6) .ISO image from http://www.cisco.com/pcgi-bin/apps/tblbld/tablebuild.pl?topic=279515766, or click the "Download Software" link from the Cisco NAC Appliance support page here.
   b. Burn the .ISO image as a bootable disk to a CD-R.
   c. 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.

Note If you plan to import database information from a backup snapshot after installing your new Clean Access Manager, Cisco recommends you add any new licenses to your system *before* creating and saving a system snapshot. If you install new licenses and then import a previously saved snapshot, any new licenses you have installed are overwritten by the license information contained in the system snapshot.

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(6)*
   - *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(6)*

Note Clean Access Manager 4.1(6) is bundled with Windows Clean Access Agent version 4.1.6.0 and Mac OS X Clean Access Agent version 4.1.3.1.

Upgrading to 4.1(6)

This section provides instructions for how to upgrade your existing Cisco Clean Access system to release 4.1(6).

Refer to the following general information prior to upgrade:

- Notes on 4.1(6) 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 to Release 4.1(6)—Standalone Machines
- Upgrading to 4.1(6)—HA Pairs

If you need to perform a fresh installation of the software, refer instead to New Installation of Release 4.1(6), page 65.

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(6). 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(6) Upgrade

If planning to upgrade to Cisco NAC Appliance (Cisco Clean Access) 4.1(6) ED, note the following:

- New installations of Cisco NAC Appliance release 4.1(6) no longer contain any default third-party Trusted Certificate Authorities. However, with upgrades to release 4.1(6), Cisco NAC Appliance preserves the CAM/CAS trusted certificate store to ensure all existing trusted end-entity certificates remain on that CAM/CAS after upgrade.
- Starting from release 4.1(6), Cisco strongly recommends obtaining dual-purpose CA-signed certificates for your production CAMs/CASs to enable them to act as both SSL clients and SSL servers.

- When upgrading to release 4.1(6) from a prior Cisco NAC Appliance release, Cisco strongly recommends that you remove any certificates issued by the "www.perfigo.com" Certificate Authority from all client machines in your production deployment after you have imported CA-signed certificates. There is a potential risk for any web browser client where the user has accepted a certificate issued by the "www.perfigo.com" Certificate Authority on their machine.

Warning **If your previous deployment uses a chain of SSL certificates that is incomplete, incorrect, or out of order, CAM/CAS communication may fail after upgrade to release 4.1(6). You must correct your certificate chain to successfully upgrade to release 4.1(6). For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.1(6), refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade to 4.1(6)* Troubleshooting Tech Note.**

Certificate chains can only be 10 certificates long (including intermediate and root certificates) in Cisco NAC Appliance Release 4.1(6).

Warning **Release 4.1(6) may not support SSL server certificates that contain Netscape extensions (Netscape Cert Type field). Refer to caveat CSCsu02167, page 53 for details.**

- Due to Java version dependencies in the system software, Cisco Clean Access only supports 1024- and 2048-bit RSA key lengths for SSL certificates.
- If you are upgrading the CAS to release 4.1(6) via the CAM web console where the CAM's available memory is less than 1GB, you may see an HTTP status 500 error message reading "java.lang.OutofMemoryError."

Note This potential issue is only a problem in non-Cisco hardware platforms with less than 1GB of memory installed (i.e. Dell 750, 850, or 860 platforms).

- Clean Access Servers connected to a CAM can periodically appear as "deleted" or "unauthorized" in the CAM event logs even though the CAS is functioning properly and has not experienced any connection issues with the Clean Access Manager. See caveat CSCsr52953, page 52 for more details.
- Only releases 4.1(6), 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) and later to release 4.1(6) via web upgrade, just like any other Clean Access Server. If upgrading to release 4.1(6), 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.

- Cisco NAC Appliance release 4.1(6) ED is a major software release with Early Deployment status.
- Cisco recommends using the console/SSH upgrade procedure to upgrade appliance hardware from release 3.6(x), 4.0(x), or 4.1(0)+, 4.1(2)+, or 4.1(3)+ to release 4.1(6). See Console/SSH Upgrade—Standalone Machines, page 76.
- 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 81.**

- 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*.

Caution "In-place" upgrade from version 3.5(11) to 4.1(6) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(6) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to release 4.1(6) via the instructions in Upgrading to Release 4.1(6)—Standalone Machines, page 70 or Upgrading to 4.1(6)—HA Pairs, page 79. Refer to the "In-Place Upgrade from 3.5(7)+ to 4.0(x)—Standalone Machines" or "In-Place Upgrade from 3.5(7)+ to 4.0(x)—HA-Pairs" in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.0(6)* for details.

Settings That May Change With Upgrade

Refer to Notes on 4.1(6) Upgrade, page 66 for additional information.

- **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(6). 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.
- **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 62 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 62.
- **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(6), 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(6), 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(6) software and some running 4.1(3), 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(6) to 4.1.6.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.

- **Upgrade Clean Access Servers Before Clean Access Manager**

  Starting with Cisco NAC Appliance release 4.1(6), the Clean Access Manager and Clean Access Server require encrypted communication. Therefore, you must upgrade CASs *before* the CAM that manages them to ensure the CASs have the same (upgraded) release when the CAM comes back online and attempts to reconnect to the managed CASs.

  If you upgrade the Clean Access Manager by itself, the Clean Access Server (which loses connectivity to the CAM during Clean Access Manager restart or reboot) continues to pass authenticated user traffic only if the CAS Fallback Policy specifies that Cisco NAC Appliance should “ignore” traffic from client machines.

Caution New users will not be able to log in or authenticate with Cisco NAC Appliance 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(6) 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 71 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(3) or earlier database snapshot to a 4.1(6) CAM.**

- **Software Downgrade**

  Once you have upgraded your software to 4.1(6), 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(6).

- **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 to Release 4.1(6)—Standalone Machines

Note "In-place" upgrade from version 3.5(x) to 4.1(6) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(6) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(6). Refer to the "In-Place Upgrade from 3.5(7)+ to 4.0(x)—Standalone Machines" in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.0(6)* for details.

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)+/4.1(3)+ to the latest 4.1(6) release. You can upgrade 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+/4.1(3)+ standalone machines to the latest 4.1(6) release using one of the following two methods:

- Web Console Upgrade—Standalone Machines, page 72
- Console/SSH Upgrade—Standalone Machines, page 76

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 to 4.1(6)—HA Pairs, page 79.

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

- Upgrading to 4.1(6), page 66
- Settings That May Change With Upgrade, page 68

- General Preparation for Upgrade, page 69

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 71
2. Download the Upgrade File, page 72
3. Web Console Upgrade—Standalone Machines or Console/SSH Upgrade—Standalone Machines, page 76

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(6)*.

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. 06_20_08-09-36_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. 06_20_08-09-36_snapshot_**VER_4_1_6.**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-4.1.6.*x*.tar.gz (CAM/CAS release upgrade file)
- cam-upgrade-4.1.6.*x*.tar.gz (CAM-only patch upgrade file)
- cas-upgrade-4.1.6.*x*.tar.gz (CAS-only patch upgrade file)

Major release upgrade file names do not feature the fourth (.*x*) digit. A major release file name example would be **cca-upgrade-4.1.6.tar.gz**. For patch upgrades, however, replace the .*x* in the file name with the minor release version number to which you are upgrading, for example, **cca-upgrade-4.1.6.1.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)+/4.1(3)+ to 4.1(6). See Console/SSH Upgrade—Standalone Machines, page 76.

If you are upgrading the CAS to release 4.1(6) via the CAM web console where the CAM's available memory is less than 1GB, you may see an HTTP status 500 error message reading "java.lang.OutofMemoryError."

Note This potential issue is only a problem in non-Cisco hardware platforms with less than 1GB of memory installed (i.e. Dell 750, 850, or 860 platforms).

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 81.**

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)/4.1(3) or later must be installed and running on your CAM/CAS(es) before you can upgrade to release 4.1(6) via web console.
- Alternatively, you can always upgrade using the instructions in Console/SSH Upgrade—Standalone Machines, page 76.
- If upgrading failover pairs, refer to Upgrading to 4.1(6)—HA Pairs, page 79.

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)+/4.1(3)+ to release 4.1(6) 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 74.

Step 1 Create CAM DB Backup Snapshot, page 71.

Step 2 Download the Upgrade File, page 72.

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 73.

Step 1 Create CAM DB Backup Snapshot, page 71.

Step 2 Download the Upgrade File, page 72.

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 81.**

Step 1 Create CAM DB Backup Snapshot, page 71.

Step 2 Download the Upgrade File, page 72.

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)+/4.1(3)+ to the latest 4.1(6) 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

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 to 4.1(6)—HA Pairs, page 79.
- "In-place" upgrade from version 3.5(x) to 4.1(6) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(6) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(6). Refer to the "In-Place Upgrade from 3.5(7)+ to 4.0(x)—Standalone Machines" in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.0(6)* for details.

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)+/4.1(3)+ to 4.1(6) console/SSH upgrade instructions:

- Upgrading to 4.1(6), page 66
- Settings That May Change With Upgrade, page 68

- General Preparation for Upgrade, page 69

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 71.

Step 2 Download the Upgrade File, page 72.

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-4.1.6.tar.gz** to the /store directory on the Clean Access Manager.

b. Copy **cca_upgrade-4.1.6.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-4.1.6.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-4.1.6.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-4.1.6.tar.gz
```

4. Execute the upgrade process:

```
cd cca_upgrade-4.1.6
./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(6) upgrade script automatically upgrades the Clean Access Agent files inside the CAM to Windows version 4.1.6.0 and Mac OS X version 4.1.3.1.

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

```
reboot
```

Perform Console/SSH Upgrade on the CAS

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-4.1.6.tar.gz
```

5. Execute the upgrade process:

```
cd cca_upgrade-4.1.6
./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 to 4.1(6)—HA Pairs

Note "In-place" upgrade from version 3.5(x) to 4.1(6) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(6) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(6). Refer to the "In-Place Upgrade from 3.5(7)+ to 4.0(x)—HA-Pairs" in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.0(6)* for details.

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)+/4.1(3)+ to the latest 4.1(6) release.

If you have standalone CAM/CAS servers, refer instead to Upgrading to Release 4.1(6)—Standalone Machines, page 70.

Note Your system must be on 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+/4.1(3)+ to use the upgrade procedure described in this section.

Warning **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 81.**

Note Review the following before proceeding with the 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+/4.1(3)+ to 4.1(6) HA upgrade instructions:

- Upgrading to 4.1(6), page 66
- Settings That May Change With Upgrade, page 68
- General Preparation for Upgrade, page 69

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

If you are upgrading the CAS to release 4.1(6) via the CAM web console where the CAM's available memory is less than 1GB, you may see an HTTP status 500 error message reading "java.lang.OutofMemoryError."

Note This potential issue is only a problem in non-Cisco hardware platforms with less than 1GB of memory installed (i.e. Dell 750, 850, or 860 platforms).

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 to the individual IP address of each machine in the failover pair.

Note Do not connect to the Service IP of the pair, as you will lose connection during the upgrade.

Step 2 Login as the **`root`** user with the root password (default is **`cisco123`**)

Warning **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 3 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 77 for instructions.)

Step 4 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-4.1.6.tar.gz
```

b. CD into the created “cca_upgrade-4.1.6” 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 80, 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 5 Bring the box acting as the standby down by entering the following command via the console/SSH terminal:

```
shutdown -h now
```

Step 6 Wait until the standby box is completely shut down.

Step 7 CD into the created "cca_upgrade-4.1.6" directory on the active box.

```
cd cca_upgrade-4.1.6
```

Step 8 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 9 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-4.1.6"), 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(6) upgrade script automatically upgrades the Clean Access Agent files inside the CAM to Windows version 4.1.6.0 and Mac OS X version 4.1.3.1.

Step 10 After the upgrade is completed, shut down the active box by entering the following command via the console/SSH terminal:

```
shutdown -h now
```

Step 11 Wait until the active box is done shutting down.

Step 12 Boot up the standby box by powering it on.

Step 13 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-4.1.6
```

c. Run the upgrade script on the standby box:

```
./UPGRADE.sh
```

Step 14 Shut down the standby box by entering the following command via the console/SSH terminal:

```
shutdown -h now
```

Step 15 Power up the active box. Wait until it is running normally and connection to the web console is possible

Step 16 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:

Note For additional troubleshooting information, see also Known Issues for Cisco NAC Appliance, page 60.

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 87.
9. If necessary, provide CAM support logs as described in Creating CAM/CAS Support Logs, page 89.

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 Enhancements, page 17) 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 15), 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 Enhancements, page 17), 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 versions 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 71 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 13 Updates to Release Notes for Cisco NAC Appliance, Release 4.1(6)

Date	Description
10/20/08	Minor update to NAC-3310 Required BIOS/Firmware Upgrade, page 4
9/29/08	Updates for Version 4.1.7.0 of the Cisco Clean Access Agent: • Cisco NAC Appliance Releases, page 2 • Release 4.1(6) Compatibility Matrix, page 6 • Release 4.1(6) Clean Access Agent Upgrade Compatibility Matrix, page 7 • Windows Clean Access Agent Version 4.1.7.0, page 16 • Clean Access AV Support Chart (Windows Vista/XP/2000), page 19 • Clean Access AS Support Chart (Windows Vista/XP/2000), page 34 • Supported AV/AS Product List Version Summary, page 40 • Open Caveats - Release 4.1(6), page 44 (added CSCsr50995) • Resolved Caveats - Agent Version 4.1.7.0, page 54 Also: • Removed the following Note from all upgrade-via-console instructions (no longer applies): "Do not use SSH connection to upgrade Virtual Gateway CASs. Use direct console connection (keyboard/monitor/KVM) if upgrading Virtual Gateway Clean Access Servers. You can use serial console connection for standalone CASs only." (CSCsu70542)
9/22/08	• Updated first steps of Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs, page 81 to specify connecting to the individual IP and not Service IP address of each machine in the HA pair (CSCsu70542). • Removed CSCso61317 (duplicate) and added CSCso49473 to Open Caveats - Release 4.1(6), page 44.
9/12/08	• Updated SSL certificate notes under Trusted Certificate Authority Enhancement for Production Environments, page 10, Enhanced CAM/CAS Web Console Features Certificate Warning Messages, page 11, Ability to View and Remove Certificate Authorities from CAM/CAS Without Rebooting, page 12 • Updated Notes on 4.1(6) Upgrade, page 66 • Added caveat CSCsu02167 to Open Caveats - Release 4.1(6), page 44
8/8/08	• Added caveat CSCsq31451 to Resolved Caveats - Agent Version 4.1.6.0, page 56
8/6/08	• Added caveat CSCso68182 to Resolved Caveats - Release 4.1(6), page 58
8/1/08	• Added caveat CSCso41549 to Open Caveats - Release 4.1(6), page 44 • Clarified shared Trusted CA requirements for CAM/CAS in New and Changed Information, page 10 and Upgrading to 4.1(6), page 66
7/31/08	Release 4.1(6)

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(6)*
- *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(6)*
- *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.