



Release Notes for Cisco NAC Appliance, Version 4.1(8)

Revised: June 7, 2011, OL-18651-01

Contents

These release notes provide late-breaking and release information for Cisco® NAC Appliance, release 4.1(8). 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.

- [Cisco NAC Appliance Releases, page 2](#)
- [Cisco NAC Appliance Service Contract/Licensing Support, page 2](#)
- [System and Hardware Requirements, page 2](#)
- [Software Compatibility, page 6](#)
- [New and Changed Information, page 10](#)
- [Cisco NAC Appliance Agents, page 12](#)
- [Clean Access Supported AV/AS Product List, page 15](#)
- [Caveats, page 47](#)
- [Known Issues for Cisco NAC Appliance, page 73](#)
- [New Installation of Release 4.1\(8\), page 78](#)
- [Upgrading to 4.1\(8\), page 79](#)
- [Troubleshooting, page 98](#)
- [Documentation Updates, page 106](#)
- [Obtaining Documentation and Submitting a Service Request, page 106](#)



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

Cisco NAC Appliance Releases

Cisco NAC Appliance Version	Availability
4.1.10.0 Cisco Clean Access Agent	May 26, 2009
4.1(8) ED	January 29, 2009


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(8) 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 Cisco 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, all CAM/CAS appliances and Cisco NAC network modules must run the same release for compatibility (release 4.1.2.1 or later). Cisco NAC Appliances and Cisco NAC network modules must be upgraded to the same release.

Cisco NAC-3300 Series Appliances

Release 4.1(8) 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(8) using a single upgrade file, **cca_upgrade-4.1.8.tar.gz**.

CD installation of release 4.1(8) is also supported:

- For NAC-3310 and NAC-3350, the **cca-4.1_8-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_8-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(8) and Cisco NAC Profiler

Release 4.1(8) includes version 2.1.8-37 of the Cisco NAC Profiler Collector component that resides on Clean Access Server installations. You will need to upgrade the Collector component on the 4.1(8) CAS for compatibility with the latest release of the Cisco NAC Profiler software. Refer to the latest version of the [Release Notes for Cisco NAC Profiler](#) for details.

**Note**

Cisco NAC Appliance Release 4.1(8) 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, Cisco recommends upgrading your Cisco NAC Profiler system components to the latest compatible release (e.g. 2.1.8) at the same time.

Important Installation Information for NAC-3310

- [NAC-3310 Required BIOS/Firmware Upgrade, page 4](#)
- [NAC-3310 Required DL140 or serial_DL140 CD Installation Directive, page 4](#)

NAC-3310 Required BIOS/Firmware Upgrade

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

NAC-3310 Required DL140 or serial_DL140 CD Installation Directive

With Cisco NAC Appliance 4.1(x) releases, 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 to [Known Issue with NAC-3310 CD Installation, page 74](#).

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 98](#) 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(8)	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	<ul style="list-style-type: none"> • 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 75.
2. Release 4.1(8) 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\(8\)](#) and the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(8\)](#).

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 12](#)
- [Clean Access Supported AV/AS Product List, page 15](#)

Software Compatibility Matrixes

This section describes the following:

- [Release 4.1\(8\) Compatibility Matrix](#)
- [Release 4.1\(8\) CAM/CAS Upgrade Compatibility Matrix](#)
- [Release 4.1\(8\) Agent Upgrade Compatibility Matrix](#)

Release 4.1(8) Compatibility Matrix

Table 2 shows Clean Access Manager and Clean Access Server compatibility and the Agent version supported with each Cisco NAC Appliance 4.1(8) release (if applicable). CAM/CAS/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(8) 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(8) ⁵	4.1(8) ⁵	4.1.10.0	4.1.3.x	4.1.10.0
		4.1.8.0	4.1.2.x	4.1.8.2
		4.1.7.0	4.1.1.0	4.1.6.0
		4.1.6.0	4.1.0.x ⁶	4.1.3.x
		4.1.3.x		
		4.1.2.x		
		4.1.1.0		
		4.1.0.x ⁶		

1. Make sure that both CAM and CAS are of same version.
2. See [Cisco NAC Appliance Agents, page 12](#) for details on version updates for each Windows/Mac OS X/Web Agent.
3. Version 4.1.10.0 of the Windows Clean Access Agent is compatible with the 4.1(8) CAM and CAS releases. See [Cisco NAC Appliance Agents, page 12](#) 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(8) is a general and important enhancement and bug fix release as described in [Enhancements in Release 4.1\(8\), page 10](#).

6. Cisco strongly recommends running the latest 4.1.10.x version of the Clean Access Agent with release 4.1(8) of the CAM/CAS. If necessary, release 4.1(8) allows administrators to optionally configure the 4.1(8) 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(8) Cisco NAC Appliance system. However, an Agent upgraded to 4.1.10.0 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(8) CAM/CAS Upgrade Compatibility Matrix

[Table 3](#) shows 4.1(8) 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(8) CAM/CAS Upgrade Compatibility Matrix

Clean Access Manager		Clean Access Server	
Upgrade From:	To:	Upgrade From:	To:
4.1(6)	4.1(8) ³	4.1(6)	4.1(8) ³
4.1(3)+		4.1(3)+	
4.1(2)+		4.1(2)+	
4.1(1)		4.1(1)	
4.1(0)+ ¹		4.1(0)+ ¹	
4.0(x)		4.0(x)	
3.6(x)		3.6(x)	
3.5(7)+ ²		3.5(7)+ ²	

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(7)+ to 4.1(8) is not supported. Customers wishing to upgrade a system from 3.5(7)+ to 4.1(8) must use the supported in-place upgrade procedure to upgrade from 3.5(7)+ to 4.0(6), and then upgrade to 4.1(8).
3. Cisco NAC Appliance Release 4.1(8) is a general and important enhancement and bug fix release as described in [Enhancements in Release 4.1\(8\)](#), page 10.

Release 4.1(8) Agent Upgrade Compatibility Matrix

[Table 4](#) shows Clean Access Agent upgrade compatibility when upgrading existing versions of the Agent after 4.1(8) CAM/CAS upgrade. You can auto-upgrade any 3.5.1+ Windows Agent directly to the latest 4.1.10.0 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(8) 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(8)	4.1(8)	4.1.7.0 4.1.6.0 4.1.3.x ⁴ 4.1.2.x 4.1.1.0 4.1.0.x ⁵	4.1.10.0 4.1.8.0	4.1.3.1
		4.0.x.x 3.6.x.x 3.5.1.0 and later	4.1.10.0 4.1.8.0	—

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 4.1.10.0 Agent.
2. See [Cisco NAC Appliance Agents, page 12](#) 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 uninstalling the existing Mac OS X Agent, downloading the new Agent via web login, and running the Agent installation. For more information, see [Mac OS X Clean Access Agent Enhancements, page 13](#).
5. Cisco strongly recommends running the latest 4.1.10.x version of the Clean Access Agent with release 4.1(8) of the CAM/CAS. If necessary, release 4.1(8) allows administrators to optionally configure the 4.1(8) 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(8) Cisco NAC Appliance system. However, an Agent upgraded to 4.1.10.0 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, page 8](#)
- [Clean Access Server \(CAS\) Version, page 9](#)
- [Cisco NAC Appliance Agents Versioning, page 9](#)
- [Cisco Clean Access Updates Versioning, page 10](#)

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 CAS HA pairs)
- Cisco Clean Access Standard Manager supports 20 Clean Access Servers (or 20 CAS HA pairs)
- Cisco Clean Access Super Manager supports 40 Clean Access Servers (or 40 CAS HA 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 94](#) 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 10](#))
- **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 15](#) and [Clean Access Supported AV/AS Product List, page 15](#) for additional details.

New and Changed Information

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

- [Enhancements in Release 4.1\(8\), page 10](#)

See [Cisco NAC Appliance Agents, page 12](#) for new features and enhancements to Cisco NAC Appliance Agents.

For additional details, see also:

- [Hardware Supported, page 2](#)
- [Clean Access Supported AV/AS Product List, page 15](#)
- [Caveats, page 47](#)
- [Known Issues for Cisco NAC Appliance, page 73](#)

Enhancements in Release 4.1(8)

This section details the enhancements delivered with Cisco NAC Appliance release 4.1(8) for the Clean Access Manager and Clean Access Server.

General Enhancements

- [CAS Fallback Behavior Enhancement, page 11](#)
- [CAS HA Pair Link-Detect Configuration Enhancement, page 11](#)
- [DHCP Failover Behavior Enhancement, page 12](#)

Cisco NAC Appliance Agent Enhancements

- See [Cisco NAC Appliance Agents, page 12](#) for enhancement details per Agent version.

General Enhancements

CAS Fallback Behavior Enhancement

In Cisco NAC Appliance Release 4.1(8), the CAS Fallback function has been enhanced to more appropriately handle CAS Fallback behavior when the CAM becomes unreachable on the network. In previous releases of Cisco NAC Appliance, the CAS determined that the CAM was unreachable after failing to successfully poll the CAM over a specified **Detect Timeout** period and would automatically initiate a Fallback event. Once the CAS was able to successfully contact the CAM one time following a Fallback event, the CAS would assume the CAM was “alive” again and resume normal operation (exit Fallback mode). Unfortunately, depending on the Fallback settings for the CAS, this behavior could lead to the CAS continually flapping between Fallback mode and normal operation when the network experienced even minor intermittent connectivity issues, and leave large segments of the user pool unable to log in.

With Cisco NAC Appliance Release 4.1(8), in addition to setting both the **Detect Interval** and **Detect Timeout** values in the CAS Fallback page, administrators can also specify the CAM detection **Fail Percentage** threshold value that helps better tune the CAS Fallback behavior to the network. When the administrator specifies a value for the **Fail Percentage** setting, the CAS also automatically sets the subsequent **Resume Percentage** success threshold value that determines when the CAS returns to normal operation following a CAS Fallback event.

For new installations of Cisco NAC Appliance Release 4.1(8), this enhancement also introduces new default value of 20 seconds for the **Detect Interval** setting and requires the **Detect Timeout** value to be at least 15 times the specified **Detect Interval**. If you are upgrading to release 4.1(8) and already employ CAS Fallback behavior in your system, your existing values for these settings are preserved, and you may need to reconfigure your settings to maintain expected CAS Fallback behavior in your network.



Note

Although the **Detect Timeout** must be at least 15 times the **Detect Interval**, Cisco recommends making the **Detect Timeout** 30 times the **Detect Interval** value.

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

- **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Fallback**—new **Fail Percentage** and **Restore Percentage** settings and new default value of 20 seconds for the **Detect Interval** setting (the **Detect Interval** default value was 60 seconds in previous releases)

CAS HA Pair Link-Detect Configuration Enhancement

Cisco NAC Appliance Release 4.1(8) enables administrators to create and/or edit a configuration file residing on the CAS to specify link-detect interfaces to monitor on the CAS. This enhancement is designed to provide a solution for Cisco NAC Appliance networks where, due to network topology or configuration issues, CAS high-availability (HA) pairs may be unable to verify connectivity with the trusted (eth0) and/or untrusted (eth1) external interfaces specified in the CAS web console (**Administration > Network Settings > Failover**).

To enable this enhancement, the administrator must add or update the **linkdetect.conf** file residing in the **/etc/ha.d/** directory on the CAS, specifying the interface(s) on which to enable Link-detect functionality. After adding/updating the file, you must stop and then restart services on the CAS using the **service perfigo stop** and **service perfigo start** commands.

For more information, see [CSCsv74447](#), page 70.

DHCP Failover Behavior Enhancement

Cisco NAC Appliance Release 4.1(8) enhances the CAS failover behavior for DHCP when a standby CAS assumes the role of the active CAS. In the event an active HA CAS performing DHCP address assignment is in Fallback (Fail Open) state before the failover event, the standby CAS is now able to assume DHCP address management functions in addition to user login.

This enhancement addresses an issue where client machines are unable to get IP addresses or even renew address leases when the DHCP service is configured to run on an active HA CAS and the CAS goes into Fallback (Fail Open) mode when the CAM becomes unreachable for an extended period of time. This enhancement also improves Cisco NAC Appliance availability and operation when the active CAS reboots or the CAS fails over when the CAM is unreachable on the network.

For more information, see [CSCsv71328](#), page 70.

Supported AV/AS Product List Enhancements (Version 73)

- See [Clean Access Supported AV/AS Product List](#), page 15 for the latest AV/AS product charts.
- See [Supported AV/AS Product List Version Summary](#), page 42 for details on each update to the list.

Cisco NAC Appliance Agent Enhancements

See [Cisco NAC Appliance Agents](#), page 12 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 13
- [Mac OS X Clean Access Agent Enhancements](#), page 13
- [Cisco NAC Web Agent Enhancements](#), page 14

Refer to [Resolved Caveats - Agent Version 4.1.8.0](#), page 61 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\(8\) Compatibility Matrix](#) and [Release 4.1\(8\) Agent Upgrade Compatibility Matrix](#), page 7 for compatibility details.
- See [Clean Access Supported AV/AS Product List](#), page 15 for details on related AV/AS support.



Note

- Cisco strongly recommends running version 4.1.10.0 of the Clean Access Agent with release 4.1(8) of the CAM/CAS. However, administrators can optionally configure the 4.1(8) 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\(6\)](#) for details on the 4.1.6.0 and 4.1.7.0 Agent.

- 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 73](#) and [Troubleshooting, page 98](#) for Agent-related information.

Windows Clean Access Agent Enhancements

This section contains the latest enhancements of the Windows Clean Access Agent. Enhancements are cumulative and apply both to the version introducing the feature and to subsequent later versions, unless otherwise noted.



Note

To upgrade to the latest version of the Clean Access Agent, navigate to **Cisco Download Security Software** (<http://www.cisco.com/cisco/web/download/index.html>) > **Network Admission Control (NAC) Software** > **Cisco Network Admission Control** > **Cisco NAC Appliance (Clean Access)** > **Cisco NAC Appliance 4.1**, and click **Network Admission Control (NAC) Agent Software** and download the upgrade file (e.g. **CCAAgentUpgrade-<version>.tar.gz**) to the local computer from which you are accessing the CAM web console.

Windows Clean Access Agent Version 4.1.10.0

This section summarizes the latest enhancements for version 4.1.10.0 of the Windows Clean Access Agent. Refer to the following links for additional information:

- [Supported AV/AS Product List Version Summary, page 42](#)
- [Resolved Caveats - Agent Version 4.1.10.0, page 59](#)
- [Open Caveats - Release 4.1\(8\), page 47](#)

Windows Clean Access Agent Version 4.1.8.0

This section summarizes the latest enhancements for version 4.1.8.0 of the Windows Clean Access Agent. Refer to the following links for additional information:

- [Supported AV/AS Product List Version Summary, page 42](#)
- [Resolved Caveats - Agent Version 4.1.8.0, page 61](#)
- [Open Caveats - Release 4.1\(8\), page 47](#)

Mac OS X Clean Access Agent Enhancements

There are no new features or enhancements in the Mac OS X Agent version 4.1.3.1 for release 4.1(8).

**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(8). Refer to [Resolved Caveats - Agent Version 4.1.10.0, page 59](#) for additional information.

See [Release 4.1\(8\) 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 16](#)
- [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 12](#)
- [Supported AV/AS Product List Version Summary, page 42](#)

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\(8\)](#) 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 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 1 of 15)*

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
avast! Server Edition	4.x	yes (4.1.8.0)	yes (4.1.8.0)	yes
AT&T				
AT&T Internet Security Suite AT&T Anti-Virus	6.x	yes (4.1.10.0)	-	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
AhnLab V3 VirusBlock Internet Security 2007	7.x	yes (4.1.8.0)	yes (4.1.8.0)	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
Aliant				
Aliant Business Security Suite Anti-Virus	6.x	yes (4.5.1.0)	-	yes

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 2 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
Aliant Business Security Suite Anti-Virus	7.x	yes (4.1.10.0)	-	-
Aliant Security Services Anti-Virus	7.x	yes (4.1.10.0)	-	-
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)	-
Active Virus Shield	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Authentium, Inc.				
Command Anti-Malware	5.x	yes (4.1.10.0)	yes (4.1.10.0)	yes
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 Personal - Free Antivirus	9.x	yes (4.1.10.0)	yes (4.1.10.0)	yes
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 Premium	9.x	yes (4.1.10.0)	yes (4.1.10.0)	yes
Avira AntiVir Professional	8.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
Avira AntiVir Professional	9.x	yes (4.1.10.0)	yes (4.1.10.0)	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
Avira Premium Security Suite	9.x	yes (4.1.10.0)	yes (4.1.10.0)	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

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 3 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
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
Rising Antivirus Software AV	21.x	yes (4.1.10.0)	yes (4.1.10.0)	-
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
Bullguard Internet Security Suite	8.x	yes (4.1.8.0)	yes (4.1.8.0)	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	10.x	yes (4.5.1.0)	yes (4.5.1.0)	yes
Quick Heal AntiVirus Plus	9.5.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Quick Heal Total Security	10.x	yes (4.5.1.0)	yes (4.5.1.0)	yes
Quick Heal Total Security	9.5.x	yes (4.1.8.0)	yes (4.1.8.0)	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
ZoneAlarm Anti-virus	8.x	yes (4.5.1.0)	yes (4.5.1.0)	yes
ZoneAlarm Security Suite Antivirus	7.0.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
ZoneAlarm Security Suite Antivirus	7.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
ZoneAlarm Security Suite Antivirus	8.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
Cisco Systems, Inc.				
Cisco Security Agent	6.x	yes (4.5.1.0)	yes (4.1.10.0)	-
ClamAV				
ClamAV	0.x	yes (4.1.8.0)	yes (4.1.8.0)	yes
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

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 4 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
Comodo Group				
COMODO Internet Security	3.5.x	yes (4.1.8.0)	-	-
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)	-
Eset Software				
ESET NOD32 Antivirus	3.x	yes (4.1.3.2)	yes (4.1.3.2)	-
ESET NOD32 Antivirus	4.x	yes (4.1.10.0)	yes (4.1.10.0)	-
ESET Smart Security	3.x	yes (4.1.6.0)	yes (4.1.6.0)	-
ESET Smart Security	4.x	yes (4.1.10.0)	yes (4.1.10.0)	-
NOD32 Antivirus System	x	yes (4.1.3.2)	yes (4.1.3.2)	yes

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 5 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
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	8.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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
FairPoint				
FairPoint Security Suite Virus Protection	7.x	yes (4.1.10.0)	yes (4.1.10.0)	-
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)	-
F-Prot for Windows	3.15	yes (3.5.0)	yes (3.5.0)	-
F-Prot for Windows	3.16c	yes (3.5.11)	yes (3.5.11)	-
F-Prot for Windows	3.16d	yes (3.5.11)	yes (3.5.11)	-
F-Prot for Windows	3.16x	yes (3.5.11.1)	yes (3.5.11.1)	-
GData Software AG				
AntiVirusKit 2006	2006.x	yes (4.1.0.0)	yes (4.1.0.0)	-
G DATA AntiVirenKit Client	8.x	yes (4.1.10.0)	yes (4.1.10.0)	-
G DATA AntiVirus 2008	18.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
G DATA AntiVirus 2009	19.x	yes (4.5.1.0)	yes (4.5.1.0)	yes
G DATA AntiVirusKit	17.x	yes (4.1.3.0)	yes (4.1.3.0)	-

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 6 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
G DATA InternetSecurity [Antivirus]	17.x	yes (4.1.3.0)	yes (4.1.3.0)	-
G DATA InternetSecurity [Antivirus]	18.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
G DATA InternetSecurity [Antivirus]	19.x	yes (4.5.1.0)	yes (4.5.1.0)	yes
G DATA TotalCare [Antivirus]	18.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
G DATA TotalCare [Antivirus]	19.x	yes (4.5.1.0)	yes (4.5.1.0)	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
ViRobot Expert Ver 4.0	2006.x	yes (4.1.10.0)	yes (4.1.10.0)	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

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 7 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
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
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

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 8 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
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
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	4.7.x	yes (4.1.8.0)	yes (4.1.8.0)	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
eScan Virus Control (VC) for Windows	9.x	yes (4.1.8.0)	yes (4.1.8.0)	yes

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 9 of 15)*

		AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
Product Name	Product Version	Installation	Virus Definition	
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.				
Client Internet Security	5.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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	6.x	yes (4.1.10.0)	yes (4.1.10.0)	yes
Norman Virus Control	7.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
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
ThreatFire 4.0	4.x	yes (4.1.8.0)	yes (4.1.8.0)	-
ThreatFire 4.1	4.x	yes (4.1.10.0)	-	-
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)	-

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 10 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
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 Endpoint Protection	5.x	yes (4.1.10.0)	yes (4.1.10.0)	-
Panda Global Protection 2009	2.x	yes (4.1.8.0)	yes (4.1.8.0)	yes
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
Panda Security for Desktops	4.x	yes (4.1.8.0)	yes (4.5.1.0)	-
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)	-
Parallels, Inc.				
Parallels Internet Security	7.x	yes (4.5.1.0)	yes (4.1.10.0)	yes
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)	-

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 11 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
Radialpoint Security Services Virus Protection	8.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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 2009	12.x	yes (4.1.8.0)	yes (4.1.8.0)	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 Business Client	11.x	yes (4.1.10.0)	yes (4.1.10.0)	-
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 2009	12.x	yes (4.1.8.0)	yes (4.1.8.0)	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
BitDefender Total Security 2009	12.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
SaID 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
Dr.Web	5.x	yes (4.1.10.0)	yes (4.1.10.0)	yes
SecurityCoverage, Inc.				
SecureIT [Antivirus]	1.x	yes (4.1.7.0)	yes (4.1.7.0)	-

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 12 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
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)	-
Sunbelt Software				
Sunbelt VIPRE Enterprise Agent	3.x	yes (4.1.10.0)	yes (4.1.10.0)	-
VIPRE Antivirus	3.x	yes (4.1.10.0)	yes (4.1.10.0)	yes
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 360 (Symantec Corporation)	3.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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
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

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 13 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
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)	-
TELUS				
TELUS security services Anti-Virus	7.x	yes (4.1.10.0)	-	-
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)	-

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 14 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
Trend Micro Anti-Virus	17.x	yes (4.1.7.0)	yes (4.1.7.0)	yes
Trend Micro AntiVirus	15.x	yes (3.6.5.0)	yes (3.6.5.0)	-
Trend Micro AntiVirus	16.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
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)	yes
Trend Micro Internet Security	17.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
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
TrustPort, a.s.				
TrustPort Antivirus	2.8.x	yes (4.1.10.0)	-	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
SystemSuite 9 Professional	9.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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

Table 5 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 15 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed) ¹		Live Update ^{2, 3}
		Installation	Virus Definition	
Verizon				
Verizon Internet Security Suite Anti-Virus	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
Verizon Internet Security Suite Anti-Virus	7.x	yes (4.5.1.0)	yes (4.5.1.0)	-
Verizon Internet Security Suite Anti-Virus	8.x	yes (4.1.10.0)	yes (4.1.10.0)	-
VirusBlokAda Ltd.				
Vba32 Personal	3.x	yes (4.1.6.0)	yes (4.1.6.0)	-
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 AntiVirus	6.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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
iolo technologies, LLC				
iolo AntiVirus	1.x	yes (4.1.8.0)	yes (4.1.8.0)	-

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

2. The Live Update column indicates whether the Agent supports live update for the product via the Agent **Update** button (configured by AV Definition Update requirement type). For products that support “Live Update,” the Agent launches the update mechanism of the AV product when the Update button is clicked. For products that do not support this feature, the Agent displays a message popup. In this case, administrators can configure a different requirement type (such as “Local Check”) to present alternate update instructions to the user.
3. For Symantec Enterprise products, the Clean Access Agent can initiate AV Update when Symantec Antivirus is in unmanaged mode. If using Symantec AV in managed mode, the administrator must allow/deny managed clients to run LiveUpdate via the Symantec management console (right-click the primary server, go to All Tasks -> Symantec Antivirus, select Definition Manager, and configure the policy to allow clients to launch LiveUpdate for agents managed by that management server.) If managed clients are not allowed to run LiveUpdate, the update button will be disabled on the Symantec GUI on the client, and updates can only be pushed from the server.

Clean Access AV Support Chart (Windows ME/98)

Table 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 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (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 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (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 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 1 of 8)*

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed) ¹		Live Update ²
		Installation	Spyware Definition	
AT&T				
AT&T Internet Security Suite AT&T Anti-Spyware	6.x	yes (4.1.10.0)	yes (4.1.10.0)	yes
AVG Technologies				
AVG 8.0 [AntiSpyware]	8.x	yes (4.1.3.2)	yes (4.1.8.0)	yes
AVG Anti-Virus Free [AntiSpyware]	8.x	yes (4.1.8.0)	yes (4.1.8.0)	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
Aliant				
Aliant Business Security Suite Anti-Spyware	6.x	yes (4.5.1.0)	yes (4.5.1.0)	yes
Aliant Business Security Suite Anti-Spyware	7.x	yes (4.1.10.0)	yes (4.1.10.0)	-
Aliant Security Services Anti-Spyware	7.x	yes (4.1.10.0)	yes (4.1.10.0)	-
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)	-

Table 7 *Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 2 of 8)*

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed) ¹		Live Update ²
		Installation	Spyware Definition	
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				
BellSouth Internet Security Anti-Spyware	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-
BigFix, Inc.				
BigFix AntiPest	2.x	yes (4.1.10.0)	-	-
Cat Computer Services Pvt. Ltd.				
Quick Heal AntiVirus Plus [AntiSpyware]	10.x	yes (4.1.10.0)	yes (4.1.10.0)	yes
Quick Heal Total Security [AntiSpyware]	10.x	yes (4.1.10.0)	yes (4.1.10.0)	yes
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

Table 7 *Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 3 of 8)*

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed) ¹		Live Update ²
		Installation	Spyware Definition	
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.				
F-Secure (AntiSpyware)	7.x	yes (4.1.3.0)	yes (4.1.3.0)	-
F-Secure Anti-Virus (AntiSpyware)	8.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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
FairPoint				
FairPoint Security Suite Spyware Protection	7.x	yes (4.1.10.0)	yes (4.1.10.0)	-
Grisoft, Inc.				
AVG Anti-Malware [AntiSpyware]	7.x	yes (4.1.2.0)	-	-
AVG Anti-Spyware 7.5	7.x	yes (4.0.5.1)	yes (4.0.5.1)	-
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

Table 7 *Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 4 of 8)*

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed) ¹		Live Update ²
		Installation	Spyware Definition	
Kephyr				
Bazooka Scanner	1.x	yes (4.1.8.0)	-	-
Kingsoft Corp.				
Kingsoft AntiSpyware 2007 Free	2007.x	yes (4.1.3.2)	yes (4.1.3.2)	-
Kingsoft Internet Security 9 [AntiSpyware]	2008.x	yes (4.1.10.0)	-	-
Kingsoft Internet Security [AntiSpyware]	7.x	yes (4.0.6.1)	yes (4.0.6.1)	yes
Lavasoftware, Inc.				
Ad-Aware	8.x	yes (4.1.10.0)	-	yes
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)	-
Lavasoftware Ad-Aware 2008	7.x	yes (4.1.6.0)	-	-
Lavasoftware Ad-Aware 2008 Professional	7.x	yes (4.1.6.0)	-	yes
Malwarebytes Corporation				
Malwarebytes Anti-Malware	1.x	yes (4.1.8.0)	-	yes
Maxion Software				
Spy Killer	5.x	yes (4.1.8.0)	yes (4.1.10.0)	-
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
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)	-	-

Table 7 *Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 5 of 8)*

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed) ¹		Live Update ²
		Installation	Spyware Definition	
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
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)	-

Table 7 *Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 6 of 8)*

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed) ¹		Live Update ²
		Installation	Spyware Definition	
Prevx Ltd.				
Prevx 2.0 Agent	1.x	yes (4.1.8.0)	yes (4.1.8.0)	yes
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 Security Services Spyware Protection	8.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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
SecurityCoverage, Inc.				
SecureIT [AntiSpyware]	1.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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

Table 7 *Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 7 of 8)*

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed) ¹		Live Update ²
		Installation	Spyware Definition	
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 360 [AntiSpyware]	3.x	yes (4.1.8.0)	yes (4.1.8.0)	-
Norton AntiVirus [AntiSpyware]	15.x	yes (4.1.10.0)	yes (4.1.10.0)	-
Norton AntiVirus [AntiSpyware]	16.x	yes (4.1.7.0)	yes (4.1.10.0)	-
Norton Internet Security AntiSpyware	15.x	yes (4.1.3.0)	yes (4.1.10.0)	-
Norton Internet Security [AntiSpyware]	16.x	yes (4.1.7.0)	yes (4.1.10.0)	-
Norton Spyware Scan	2.x	yes (4.1.0.0)	yes (4.1.0.0)	-
TELUS				
TELUS security services Anti-Spyware	7.x	yes (4.1.10.0)	yes (4.1.10.0)	-
Tenebril Inc.				
SpyCatcher Express	4.x	yes (4.1.8.0)	yes (4.1.8.0)	-
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 OfficeScan Client (AntiSpyware)	8.x	yes (4.1.8.0)	yes (4.1.8.0)	yes
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)	-

Table 7 *Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000)
Version 77, 4.1.10.0 Agent, CAM/CAS Release 4.1(8) (Sheet 8 of 8)*

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed) ¹		Live Update ²
		Installation	Spyware Definition	
Verizon Internet Security Suite Anti-Spyware	7.x	yes (4.5.1.0)	yes (4.5.1.0)	-
Verizon Internet Security Suite Anti-Spyware	8.x	yes (4.1.10.0)	yes (4.1.10.0)	-
Webroot Software, Inc.				
Spy Sweeper	3.x	yes (3.6.0.0)	-	-
Spy Sweeper	4.x	yes (3.6.0.0)	-	-
Spy Sweeper	5.0.x	yes (4.1.3.0)	-	-
Spy Sweeper	5.x	yes (4.1.0.0)	-	-
Spy Sweeper	6.x	yes (4.1.8.0)	-	-
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 15](#) 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(8)—4.1.10.0 Agent	
Version 77	Minor internally used data change
Version 76	<p>Added feature support for the following AV products:</p> <ul style="list-style-type: none"> • Panda Security for Desktops, 4.x: added def date, version and live update support • Malwarebytes Anti-Malware, 1.x: added live update support • Cisco Security Agent, 6.x: added def date and version support • Parallels Internet Security, 7.x: added def date and version support <p>Added new AV products:</p> <ul style="list-style-type: none"> • Aliant Business Security Suite Anti-Virus, 6.x • Quick Heal AntiVirus Plus, 10.x • Quick Heal Total Security, 10.x • ZoneAlarm Anti-virus, 8.x • Cisco Security Agent, 6.x • G DATA AntiVirus 2009, 19.x • G DATA InternetSecurity [Antivirus], 19.x • G DATA TotalCare [Antivirus], 19.x • Parallels Internet Security, 7.x • Verizon Internet Security Suite Anti-Virus, 7.x • AT&T Internet Security Suite AT&T Anti-Virus, 6.x • Aliant Business Security Suite Anti-Virus, 7.x • Aliant Security Services Anti-Virus, 7.x • Command Anti-Malware, 5.x • Avira AntiVir Personal - Free Antivirus, 9.x • Avira AntiVir Premium, 9.x

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

Version	Enhancements
Version 76 (continued)	<ul style="list-style-type: none"> • Avira AntiVir Professional, 9.x • Avira Premium Security Suite, 9.x • Rising Antivirus Software AV, 21.x • G DATA AntiVirenKit Client, 8.x • ViRobot Expert Ver 4.0, 2006.x • Norman Virus Control, 6.x • Panda Endpoint Protection, 5.x • BitDefender Business Client, 11.x • Dr.Web, 5.x • TELUS security services Anti-Virus, 7.x • Sunbelt VIPRE Enterprise Agent, 3.x • VIPRE Antivirus, 3.x • ESET NOD32 Antivirus, 4.x • ESET Smart Security, 4.x • FairPoint Security Suite Virus Protection, 7.x • ThreatFire 4.1, 4.x • TrustPort Antivirus, 2.8.x • Verizon Internet Security Suite Anti-Virus, 8.x <p>Added feature support for the following AS products:</p> <ul style="list-style-type: none"> • Norton Internet Security AntiSpyware, 15.x: added def date support • Norton AntiVirus [AntiSpyware], 16.x: added def date support • Norton Internet Security [AntiSpyware], 16.x: added def date support • Malwarebytes Anti-Malware, 1.x: added def date support • Spy Killer, 5.x: added def date support

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

Version	Enhancements
Version 76 (continued)	Added new AS products: <ul style="list-style-type: none"> • Aliant Business Security Suite Anti-Spyware, 6.x • Verizon Internet Security Suite Anti-Spyware, 7.x • AT&T Internet Security Suite AT&T Anti-Spyware, 6.x • Aliant Business Security Suite Anti-Spyware, 7.x • Aliant Security Services Anti-Spyware, 7.x • Quick Heal AntiVirus Plus [AntiSpyware], 10.x • Quick Heal Total Security [AntiSpyware], 10.x • Ad-Aware, 8.x • TELUS security services Anti-Spyware, 7.x • BigFix AntiPest, 2.x • FairPoint Security Suite Spyware Protection, 7.x • Kingsoft Internet Security 9 [AntiSpyware], 2008.x • Norton AntiVirus [AntiSpyware], 15.x • Verizon Internet Security Suite Anti-Spyware"), 8.x
Version 74, 75	Minor internally used data change

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

Version	Enhancements
Release 4.1(8)—4.1.8.0 Agent	
Version 73	<p>Added AV def version support:</p> <ul style="list-style-type: none"> • Sophos Anti-Virus, 4.x <p>Added AV def date support:</p> <ul style="list-style-type: none"> • Microsoft Forefront Client Security, 1.5.x <p>Added AV live update support:</p> <ul style="list-style-type: none"> • Trend Micro AntiVirus, 16.x • Trend Micro Internet Security, 16.x • Trend Micro Internet Security, 17.x • BitDefender Total Security 2009, 12.x • Trend Micro Anti-Virus, 17.x <p>Added new AV products:</p> <ul style="list-style-type: none"> • avast! Server Edition, 4.x • AhnLab V3 VirusBlock Internet Security 2007, 7.x • Bullguard Internet Security Suite, 8.x • Quick Heal Total Security, 9.5.x • ClamAV, 0.x • F-Secure Anti-Virus, 8.x • Total Protection for Small Business, 4.7.x • eScan Virus Control (VC) for Windows, 9.x • ThreatFire 4.0, 4.x • Panda Global Protection 2009, 2.x • Panda Security for Desktops, 4.x • BitDefender Antivirus 2009, 12.x • BitDefender Internet Security 2009, 12.x

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

Version	Enhancements
Version 73 (continued)	<ul style="list-style-type: none"> • Norton 360 (Symantec Corporation), 3.x • iolo AntiVirus, 1.x • COMODO Internet Security, 3.5.x • Client Internet Security, 5.x • Radialpoint Security Services Virus Protection, 8.x • SystemSuite 9 Professional, 9.x • Webroot AntiVirus, 6.x <p>Added AS def date:</p> <ul style="list-style-type: none"> • AVG 8.0 [AntiSpyware], 8.x <p>Added new AS products:</p> <ul style="list-style-type: none"> • AVG Anti-Virus Free [AntiSpyware], 8.x • F-Secure Anti-Virus (AntiSpyware), 8.x • Bazooka Scanner, 1.x • Malwarebytes Anti-Malware, 1.x • Spy Killer, 5.x • Prevx 2.0 Agent, 1.x • SecureIT [AntiSpyware], 1.x • SpyCatcher Express, 4.x • Trend Micro OfficeScan Client (AntiSpyware), 8.x • Radialpoint Security Services Spyware Protection, 8.x • Norton 360 [AntiSpyware], 3.x • Spy Sweeper, 6.x

Caveats

This section describes the following caveats:

- [Open Caveats - Release 4.1\(8\), page 47](#)
- [Resolved Caveats - Agent Version 4.1.10.0, page 59](#)
- [Resolved Caveats - Agent Version 4.1.8.0, page 61](#)
- [Resolved Caveats - Release 4.1\(8\), page 65](#)



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(8)



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 12)*

DDTS Number	Software Release 4.1(8)	
	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 12)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCse86581	No	<p>Agent does not correctly recognize def versions on the following Trend AV products:</p> <ul style="list-style-type: none"> • PC-cillin Internet Security 2005 • PC-cillin Internet Security 2006 • OfficeScan Client <p>Tested Clients:</p> <ul style="list-style-type: none"> • 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	<p>Incorrect “IP lease total” displayed on editing manually created subnets</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> 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. <p>The issue is judged to be cosmetic and does not affect DHCP functionality.</p>
CSCsg66511	No	<p>Configuring HA-failover synchronization settings on Secondary CAS takes an extremely long time</p> <p>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.)</p>

Table 9 List of Open Caveats (Sheet 3 of 12)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsh77730	No	<p>Clean Access Agent locks up when greyed out OK button is pressed</p> <p>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.</p> <p>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.</p> <p>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.</p>
CSCsi07595	No	<p>DST fix will not take effect if generic MST, EST, HST, etc. options are specified</p> <p>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.</p> <p>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.”</p> <p>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.</p>

Table 9 List of Open Caveats (Sheet 4 of 12)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsj16366	No	<p>Time sync on CAS</p> <p>The CAS network module (NME-NAC-K9) appears as “not connected” in CAM web console after a router/rack power outage.</p> <p>This issue has been observed on a NME-NAC-K9 running Cisco NAC Appliance release 4.5(1) installed in a Cisco 2821 ISR in Out-of-Band Real-IP Gateway mode. In addition, the CAM returns the following event log message:</p> <p>“AutoConnectManager failed relinking CAM with CAS-i.p.add.rs.”</p> <p>Note The time on the CAS module goes back to some time in 2006.</p> <p>Workaround The administrator should manually reset the system time in the CAS web console.</p>
CSCsk55292	No	<p>Agent not added to system tray during boot up</p> <p>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.</p> <p>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.</p> <p>Workaround There are two methods to work around this issue:</p> <ul style="list-style-type: none"> • 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	<p>Microsoft Internet Explorer 7.0 browser pop-ups on Windows Vista launched from the Summary Report appear behind the Summary Report window</p> <p>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.</p> <p>Note This problem only happens when a Google tool bar is installed and enabled in Internet Explorer.</p>

Table 9 List of Open Caveats (Sheet 5 of 12)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsl71585	No	<p>DHCP status does not display non-restricted scope with Relay IP restriction</p> <p>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.</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> 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. <p>The web page only displays the IPs for the relay-IP restriction and does not display the non-restricted IP scope.</p> <p>Workaround Avoid creating DHCP scopes having both no restrictions and Relay-IP restrictions.</p> <p>Note The issue is known to be cosmetic and does not affect functionality.</p>
CSCsl17379	No	<p>Multiple Clean Access Agent pop-ups with Multi NIC in L2 VGW OOB role-based VLAN</p> <p>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).</p> <p>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.</p> <p>Workaround The user can manually Disable Agent login pop-up after authentication.</p>
CSCsl40626	No	<p>Cisco NAC Web Agent should handle certificate revocation dialogs similar to Clean Access Agent</p> <p>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.</p>

Table 9 **List of Open Caveats (Sheet 6 of 12)**

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsl40812	No	<p>The Refresh Windows domain group policy after login option is not functioning for Cisco NAC Web Agent</p> <p>(It is working fine with the Clean Access Agent.)</p> <p>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.</p>
CSCsl75403	No	<p>MAC filter does not work for Macintosh client machines connected to the network in VPN environment</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> 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.
CSCsl77701	No	<p>Network Error dialog appears during CAS HA failover</p> <p>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.”</p> <p>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.</p>
CSCsl88429	No	<p>User sees Invalid session after pressing [F5] following Temporary role time-out</p> <p>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.</p>
CSCsl88627	No	<p>Description of removesubnet has “updatesubnet” in op field</p> <p>The removesubnet API function description has “updatesubnet” listed in its operations field. The description should read “removesubnet.”</p>

Table 9 **List of Open Caveats (Sheet 7 of 12)**

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsm20254	No	<p>CAS duplicates HSRP packets with Cisco NAC Profiler Collector Modules enabled.</p> <p>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.</p> <p>Conditions Real-IP Gateway and Collector modules enabled on a CAS with ETH0 and or ETH1 configured for NetWatch.</p> <p>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.</p>
CSCsm20655	No	<p>Can not do a minor upgrade for Clean Access Agent from MSI package.</p> <p>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:</p> <p>“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.”</p> <p>This issue occurs because the 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</p> <p>Workaround Uninstall the program from Add/Remove Programs before installing it.</p>
CSCsm25788	No	<p>Avast 4.7 showing as not up to date with Cisco NAC Appliance Release 4.1(3)</p> <p>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</p> <p>Workaround Create a custom check for Avast that allows the users on without verifying the definition version.</p>

Table 9 **List of Open Caveats (Sheet 8 of 12)**

Software Release 4.1(8)		
DDTS Number	Corrected	Caveat
CSCsm53743	No	<p>File ownership of Mac OS X Agent directory and related files should be corrected</p> <p>File ownership of Mac OS X Agent and related files should be “root:admin.”</p> <p>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.</p>
CSCsm61077	No	<p>ActiveX fails to perform IP refresh on Windows Vista with User Account Control (UAC) turned on.</p> <p>When logged in as a machine admin on Vista and using web login with IP refresh configured, IP address refresh/renew via ActiveX or Java will fail due to the fact that IE does not run as an elevated application and Vista requires elevated privileges to release and renew an IP address.</p> <p>Workaround In order to use the IP refresh feature, you will need to:</p> <ol style="list-style-type: none"> 1. Log into the Windows Vista client as an administrator. 2. Create a shortcut for IE on your desktop. 3. Launch it by right-clicking the shortcut and running it as administrator. This will allow the application to complete the IP Refresh/Renew. Otherwise, the user will need to do it manually via Command Prompt running as administrator. <p>This is a limitation of the Windows Vista OS.</p> <p>Alternatively, the Cisco NAC Web Agent can be used with no posture requirements enabled.</p> <p>See also Known Issue for Windows Vista and IP Refresh/Renew, page 75.</p>

Table 9 List of Open Caveats (Sheet 9 of 12)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsm76779	No	<p>CSRF tag is added to CAS specific MAC Device Filter description field upon edit</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> 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. <p>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.</p> <p>Note This issue only addresses CAS-specific device filters and not <i>global</i> device filters addressed with caveat CSCsm55679.</p>
CSCsm79088	No	<p>Mac OS X Agent reports “Unknown user” when sending the second logout request</p> <p>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.</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> 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. <p>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.</p>
CSCso41549	No	<p>Administrator cannot delete the OUL manually if the In-Band CAS is not available to the CAM</p> <p>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.</p> <p>Workaround Manually delete the entry from the “user_info” table in the CAM database.</p>

Table 9 List of Open Caveats (Sheet 10 of 12)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCso49473	No	<p>SEVERE: javax.naming.CommunicationException causes no provider list</p> <p>Configuration: ADSSO with LDAP Lookup</p> <p>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.</p> <p>Symptom: The dropdown list of authentication providers is blank.</p> <p>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.</p> <p>Workaround: None</p> <p>Note CSCso61317 is a duplicate of this bug.</p>
CSCsr52953	No	<p>RMI error messages periodically appears for deleted and/or unauthorized CASs in CAM event logs</p> <p>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:</p> <ul style="list-style-type: none"> “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” <p>Workaround</p> <ul style="list-style-type: none"> 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 11 of 12)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsr90712	No	<p>Symantec Antivirus delays Clean Access Agent startup</p> <p>The Agent takes a long time to pop up on a client machine with real-time antivirus scanning enabled and operating.</p> <p>Workaround</p> <p>Exclude the Clean Access Agent AV411 directory from Symantec Antivirus scanning. See http://service1.symantec.com/support/ent-security.nsf/docid/2002092413394848.</p> <p>Note The step to configure Extensions can be omitted.</p> <p>For Vista, refer to http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008111414031848.</p>
CSCsx05054	No	<p>DHCP does not work with IGNORE fallback policy and CAS Failover</p> <p>If CAS Fallback policy is set to IGNORE and the CAM becomes unreachable from CAS, the CAS blocks all traffic and CAS DHCP stops working.</p> <p>Workaround Setting the CAS Fallback policy to “Allow All” or “Block All” solves the issue. Also, if you can ensure that the active CAS does not fail over when CAM is unreachable, this situation should not happen.</p>
CSCsx05141	No	<p>Clients cannot get IP addresses from CAS DHCP relay agent in CAS fail-open with CAS fallback scenario</p> <p>Steps to reproduce this issue:</p> <ol style="list-style-type: none"> 1. Log into the CAM web console and set CAS Fallback policy as “Allow All.” 2. Configure DHCP relay on CAS and configure IP address of external DHCP server. All clients should be able to get the IP at this point. 3. Make the CAM unreachable from CAS. 4. Active CAS fails-open within 5 minutes. Clients can still get IP address assignments from the DHCP server (all traffic is allowed). 5. Fail-over the CAS by executing “service perfigo stop” or rebooting the appliance. The HA-Secondary CAS now becomes Active and dhcrelay starts on the CAS if you enter netstat. <p>Even though the administrator can see dhcrelay functioning, clients are now unable to get IP addresses through new Active CAS.</p>

Table 9 List of Open Caveats (Sheet 12 of 12)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsx25557	No	<p>NOD32 3.x does not pass remediation and the Def date is not recognized by the Clean Access Agent</p> <p>Cisco NAC Appliance cannot remediate client machines where NOD32 3.x is installed and the Def date string is not recognized.</p> <p>Note There is no known workaround for this issue.</p>
CSCsx35438	No	<p>Clean Access Manager read timeout reached when deleting many DHCP IPs at once</p> <p>After upgrading to or installing release 4.1(8) and deleting hundreds of DHCP IPs at once, the Clean Access Server becomes unmanageable. This issue affects Clean Access Servers configured as a DHCP server on which the administrator tries to delete more than 800 DHCP IPs at once.</p> <p>Workaround Please see Known Issue with Mass DHCP Address Deletion, page 73.</p>
CSCsz67981	No	<p>MSI-based upgrade from Agent version 4.1.3.x to 4.1.8.0 requires uninstall</p> <p>Attempts to upgrade MSI-based Clean Access Agents (provided either manually or via policy-based installation rather than downloaded from the CAS, directly) fails. The Cisco NAC Appliance system also returns the following error message:</p> <p>“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.”</p> <p>This occurs even if the installation file is correctly renamed to CCAAgent.msi prior to installation.</p> <p>Note This issue does not affect Agent upgrade when the Agent is downloaded directly from the CAS.</p> <p>Workaround Manually uninstall the previous Agent prior to upgrading to version 4.1.8.0.</p>

Resolved Caveats - Agent Version 4.1.10.0

Refer to [Cisco NAC Appliance Agents, page 12](#) and [Enhancements in Release 4.1\(8\), page 10](#) for additional information.

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

DDTS Number	Agent Version 4.1.10.0	
	Corrected	Caveat
CSCsr50995	Yes	<p>Agent does not detect Zone Alarm Security definitions correctly</p> <p>Symptom: User fails posture assessment when checking for AV definitions for Zone Alarm Security Suite 7.0.</p> <p>Conditions: This occurs using either the Any AV check or the Checkpoint Any check.</p> <p>Workaround Create a custom check for Zone Alarm Security Suite definition.</p>
CSCsr87134	Yes	<p>Vista Agent does not detect MAC address of Wireless NICs</p> <p>The 4.1.6.0 Vista Agent detects the MAC address of the wired NIC twice and sends both the wired_mac:wired_ip and wired_mac:wireless_ip combinations.</p> <p>This issue affects Cisco NAC Appliance features like 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 receives a different address from the Agent. When there is a mismatch, the CAS blocks user traffic and returns a “Access blocked by Administrator” message.</p> <p>Note A Vista client on which the only active NIC is wireless is also not able to connect.</p> <p>Workaround You can address this issue in the following ways:</p> <ul style="list-style-type: none"> • Return to Agent version 4.1.3.x or earlier. • Upgrade to Agent version 4.1.7.0 or later. • Disable the Enable L2 Strict Mode option on the CAS.
CSCsu30467	Yes	<p>NIC must be present when using VPN over EVDO</p> <p>The Clean Access Agent does not work if the machine has the wireless and/or wired adapter disabled and the user is using an EVDO-only connection. (Evolution Data Only/Evolution Data Optimized is a 3G wireless broadband standard.) This is because the Agent considers the MAC address for PPP and VPN connections “irrelevant” so the Agent cannot find a unique MAC with which to associate.</p> <p>Workaround Enable the wireless or wired adapter.</p>
CSCsx44947	Yes	<p>Add support for Panda Managed Office Protection</p> <p>Clean Access Agent does not support Panda Managed Office Protection.</p>

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

DDTS Number	Agent Version 4.1.10.0	
	Corrected	Caveat
CSCsx45087	Yes	TrendMicro 16.x auto remediation happens but reports as “fail” Workaround Clicking OK in the failed remediation dialog screen triggers another auto-remediation which causes TrendMicro 16.x to pass remediation.
CSCsx50715	Yes	Clean Access Agent does not support for BitDefender Business Client 11.0.17
CSCsy21096	Yes	Clean Access Agent does not detect AVG version 8.5 Workaround The only option is to use the previous AVG Free edition (version 8.0).
SCSsy24791	Yes	Clean Access Agent does not detect Kaspersky Anti-Virus (Russian version)
CSCsy63500	Yes	Clean Access Agent does not detect Norton Internet Security AV 16.5
CSCsy78308	Yes	Clean Access Agent does not detect Norton 360 Premier version 3.x
CSCsz19205	Yes	Clean Access Agent does not detect Norton Internet Security AV 15.0

Resolved Caveats - Agent Version 4.1.8.0

Refer to [Cisco NAC Appliance Agents, page 12](#) and [Enhancements in Release 4.1\(8\), page 10](#) for additional information.

Table 11 *List of Resolved Caveats (Sheet 1 of 4)*

DDTS Number	Agent Version 4.1.8.0	
	Corrected	Caveat
CSCsq70524	Yes	<p>Winsock Error on agent after login is complete</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> 1. Ensure Cisco NAC Appliance is a Layer 2 Out-of-Band VGW setup. 2. In CAM web console, go to Device Management > Clean Access > General Setup > Agent Login and enable the Show Network Policy to Clean Access Agent and Cisco NAC Web Agent users option, enter a link in the text box, and click Update. 3. Log in to Cisco NAC Appliance from an Agent machine and enter user credentials. The Agent displays a screen prompting the user to read and accept the policy. 4. Accept the policy. 5. After that, the Agent login is complete and the Winsock error appears on the client machine. <p>Note This does issue does not occur in a Layer 3 In-Band RIP setup.</p>
CSCsr20126	Yes	<p>Clean Access Agent does not notify user of need to reboot after WSUS remediation</p> <p>When using the clean access agent with a WSUS server and the Clean Access Agent WSUS requirement is OPTIONAL and AUTOMATIC, you can not get to the temporary role because as soon as you click Next, the “Your system does not meet Windows Update requirements” message appears.</p> <p>This problem has been observed when the WSUS updates require a reboot. The fact that the updates require a reboot can be seen in the windowsupdate.log file and when you click on the DETAILS button in the Clean Access Agent after installing the updates.</p> <p>Workaround The only workaround is to educate users to use the details button in the agent and to restart after updating the operating system.</p>
CSCsr63531	Yes	<p>Cisco NAC Web Agent does not fully recognize Norton Corporate 10.1</p> <p>Cisco NAC Web Agent fails posture assessment when using an up-to-date version of Norton Corporate 10.1, but the Cisco Clean Access Agent successfully authenticates the client.</p> <p>Workaround Ensure users with Norton Corporate installed on the client machine use the persistent Clean Access Agent instead of the Cisco NAC Web Agent.</p>

Table 11 **List of Resolved Caveats (Sheet 2 of 4)**

DDTS Number	Agent Version 4.1.8.0	
	Corrected	Caveat
CSCsr75771	Yes	<p>Symantec AntiVirus 10.x not fully compatible with Clean Access Agent</p> <p>The Clean Access Agent can fail to properly update Symantec AntiVirus Version 10.1.5.500 when the requirement type is configured to automatically remediate. The Agent detects that the definition needs to be updated, but the Agent does not display the Next button to the user.</p> <p>Note Launching the update via the Symantec software successfully updates and the client machine, which then passes posture assessment.</p> <p>Workaround Manually launch the update using the Symantec System Tray icon. (The Symantec AntiVirus rule definition must be configured for Symantec Client Security in order for the check to pass using Agent version 4.1.7.0.)</p>
CSCsr97355	Yes	<p>AVG Anti-Virus Free 8.x support for Virus Definition check</p> <p>Clean Access Agent version 4.1.6.0 checks for AVG Anti-Virus Free 8.x installation but does not check for 8.x definition update when AVG Anti-virus free 8.x is installed on the client machine.</p> <p>Workaround Create custom checks and rules to detect virus definition update.</p>

Table 11 List of Resolved Caveats (Sheet 3 of 4)

DDTS Number	Agent Version 4.1.8.0	
	Corrected	Caveat
CSCsu54170	Yes	<p>Clean Access Agent does not properly detect McAfee? Total Protection Service 4.7</p> <p>The Clean Access Agent does not detect McAfee Total Protection 4.7:</p> <pre> 1. Product Type : AntiVirus (WmiAV) Product Name : McAfee unknown product Product Ver. : 4.7.0.566 Def Ver. : Def Date : </pre> <p>This issue causes clients to fail the AV definition check even though they are up to date. This has been observed with Agent/CAM/CAS 4.1.6.0, and McAfee Total Protection version 4.7.0.538 Patch 003, with definition date 5382.0000.</p> <p>Workaround Create a custom check to check with the following attributes:</p> <ul style="list-style-type: none"> • Registry Check • Registry Value • Registry Key: HKLM\SOFTWARE\McAfee\AVEngine • Value Name: AVDatDate • Value DataType: Date • Operator: later than • Value Data: CAM date (midnight) - X days • OS: Windows 2000, XP (All), Vista (All)
CSCsu69956	Yes	<p>Clean Access Agent version 4.1.6.0 fails checks in Vista for Symantec Endpoint Protection</p> <p>The Clean Access Agent version 4.1.6.0 fails to detect the definition version, definition signature, and definition time for Symantec Endpoint Protection. The Agent detects the installation of the software, but fails any version checks defined for clients that fall into the conditions detailed below as it will be unable to parse the version or date:</p> <ul style="list-style-type: none"> • Version of Symantec Endpoint Protection is 11.x • It is installed on Vista and not all components are installed (i.e., only Antivirus and Anti-Spyware Protection). <p>Workaround Install all Symantec Endpoint Protection components (including Proactive Threat Protection and Network Threat Protection).</p>
CSCsv49290	Yes	<p>BitDefender Total Security 2009 not detected in Cisco NAC Appliance release 4.1(6)</p>

Table 11 List of Resolved Caveats (Sheet 4 of 4)

DDTS Number	Agent Version 4.1.8.0	
	Corrected	Caveat
CSCsw22000	Yes	<p>Intermediate issues detecting the AVG virus definition in Clean Access Agent 4.1.7.0</p> <p>Clean Access Agent version 4.1.7.0 for Windows XP and Vista has intermediate issues detecting the virus definition version from AVG Free 8.0.</p> <p>Note There is no known workaround for this issue.</p>
CSCsw32990	Yes	<p>Cisco NAC Web Agent version 4.1.6 not checking AVG 8.0</p> <p>When the Cisco NAC Web Agent is performing posture assessment verifying whether or not AVG 8 is installed on the client machine, the Web Agent does not correctly recognize AVG 8.</p> <p>Note There is no known workaround for this issue.</p>
CSCsw52528	Yes	<p>Disable Exit button in System Tray</p> <p>The Exit button can be disabled if the user adds the following DWORD registry key to the client machine:</p> <p>DisableExit = 1 at HKLM\SOFTWARE\Cisco\Clean Access Agent\</p>

Resolved Caveats - Release 4.1(8)

Refer to [Enhancements in Release 4.1\(8\)](#), page 10 for additional information.

Table 12 *List of Resolved Caveats (Sheet 1 of 8)*

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsl94153	Yes	Add date-based checks to Cisco NAC Appliance for Microsoft Forefront Cisco NAC Appliance checks for installation of Microsoft Forefront and can perform a version check, but the current version check does not support the “check by date” option.
CSCsm32684	Yes	Double-quote in message body corrupts HTML presentation The web page presented to the user to download the Cisco Clean Access Agent features the “Require use of Clean Access Agent” message body twice. This issue occurs when a double-quote is added to the configuration in Device-Management > Clean Access > General Setup > Agent Login > [user role] > Require use of Clean Access Agent and the associated check box is checked. Workaround Remove the double-quotes or use a single quote.
CSCsm41462	Yes	Heartbeat timer expires repeatedly after HA failover Once an In-band CAS HA failover event takes place, all clients authenticated by original active CAS repeatedly receive “heartbeat timer expired” messages within short time (30 seconds to 1 minute) whether the client is sending packets or not. Workaround Reboot the active or standby CAS.
CSCsm81853	Yes	Blank space characters on Program Parameters are corrupted If program parameters is configured a blank space character, the parameter is corrupted. For example, when “arg1 arg2” is configured on Program Parameters, it is corrupted like “arg1+arg2,” “arg1%2Barg2.”
CSCsm82486	Yes	CAM web console slow and Java process taking 99% CPU While trying to access the “Device list” and “Profile” from the CAM web console Administration menu, the user interface opens very slowly and, after further investigation, it is observed that the CAM is utilizing 99.9% of the CPU for the Java process. Workaround Turn off the CSRF filter on CAM in /perfigo/control/tomcat/normal-webapps/admin/WEB-INF/web.xml: <pre> + <!-- + <filter-mapping> + <filter-name>CSRFFilter</filter-name> + <url-pattern>/*</url-pattern> + </filter-mapping> + --> </pre>

Table 12 List of Resolved Caveats (Sheet 2 of 8)

	Software Release 4.1(8)																													
DDTS Number	Corrected	Caveat																												
CSCso32106	Yes	<p>Port list on CAM should be sortable by description instead of index</p> <p>In the ports list on the CAM, ports are sorted by their index instead of by their slot/port number in IOS. The ports all show up in the correct order:</p> <table><tr><td>GigabitEthernet1/2</td><td>unassigned</td><td>YES</td><td>unset</td><td>down</td><td>down</td></tr><tr><td>GigabitEthernet2/1</td><td>unassigned</td><td>YES</td><td>unset</td><td>down</td><td>down</td></tr><tr><td>GigabitEthernet2/2</td><td>unassigned</td><td>YES</td><td>unset</td><td>down</td><td>down</td></tr><tr><td>GigabitEthernet3/1</td><td>unassigned</td><td>YES</td><td>unset</td><td>up</td><td>up</td></tr></table> <p>But these ports are sorted by their index on the CAS, so GigabitEthernet 2/1 appears after GigabitEthernet 3/48 on the CAM. This issue has been observed with certain switch configurations, including on the Catalyst 4507R with two SupII+ modules.</p> <p>Workaround None. All the ports show up in the CAM, they are just not in the expected order.</p>					GigabitEthernet1/2	unassigned	YES	unset	down	down	GigabitEthernet2/1	unassigned	YES	unset	down	down	GigabitEthernet2/2	unassigned	YES	unset	down	down	GigabitEthernet3/1	unassigned	YES	unset	up	up
GigabitEthernet1/2	unassigned	YES	unset	down	down																									
GigabitEthernet2/1	unassigned	YES	unset	down	down																									
GigabitEthernet2/2	unassigned	YES	unset	down	down																									
GigabitEthernet3/1	unassigned	YES	unset	up	up																									
CSCso44904	Yes	<p>CAM does not manage CAS via the Manage icon in web console</p> <p>When clicking the Manage icon in the CAM GUI, the CAM occasionally locks up and does not open the CAS web console, rendering all associated CASs unmanageable.</p> <p>Note Although the CAS web console is unreachable, operations continue normally and users are able to authenticate via the Cisco NAC Appliance.</p> <p>Workaround Restarting services on the CAM can resolve this issue.</p>																												
CSCso57843	Yes	<p>Standby CAS sends improper ARP request after bootup</p> <p>This issue occurs in an HA pair environment using DHCP Synchronization.</p> <p>Standby CAS sends improper ARP request from untrusted interface after bootup. The ARP request incorrectly updates ARP table on neighbor devices, then the Link Detect response on the untrusted interface is no longer able to reach the active CAS. As the result, HA is triggered.</p> <p>The ARP packet contains the MAC address of the standby CAS as “Sender MAC” and the IP address of the active CAS as the “Sender IP.”</p> <ol style="list-style-type: none">1. Sender MAC: Untrust MAC of Standby CAS—Correct Info2. Sender IP: Untrust IP of Active CAS— Wrong Info3. Target MAC: 0000.0000.0000—Correct Info4. Target IP: Link Detect IP for Untrusted—Correct Info <p>Note There is no known workaround for this issue.</p>																												

Table 12 List of Resolved Caveats (Sheet 3 of 8)

Software Release 4.1(8)		
DDTS Number	Corrected	Caveat
CSCsq27411	Yes	<p>Standby CAS responds to ARP with the wrong MAC address</p> <p>The CAS responds to ARPs on the untrusted interface with the MAC address of the trusted interface, thus causing the CAS to remain unreachable on the untrusted network.</p> <p>This occurs if the CAS is set up in Virtual Gateway mode with both interfaces set to the same IP address and it only occurs on the standby CAS in an HA pair. Failing over causes the symptom to move to the other CAS. This issue mainly causes a problem when you are doing link detect on the untrusted side.</p> <p>Note There is no known workaround for this issue.</p>
CSCsq59801	Yes	<p>Nessus plug-ins greater than 10 MB size limitation</p> <p>When uploading a NESSUS plug-in .tar file that is greater than 10MB, the CAM returns the following error:</p> <p>“Result: Error: Failed to upload file Content Length Error (18113815 > 10485760)”</p> <p>When the upload file is greater than 10MB, the upload fails.</p> <p>Workaround Make the .tar file smaller than 10MB. Split the original .tar file into several smaller files by extracting the .tar file and re-compressing smaller portions of the file collection so that the resulting .tar files are smaller.</p>
CSCsr75123	Yes	<p>Better handling for certificate chain in chain.crt file</p> <p>Logs show SSL certificate chain errors even though the chain is present in the CAM and CAS. The issue is that the CA elements in the chain.crt file in the /root/.perfigo directory are out of sequence. The result is that the CAM is not able to manage the CAS, even though the certificate chain is present on both appliances.</p> <p>Workaround Edit the chain.crt file to correct the sequence of elements in the chain.</p>

Table 12 List of Resolved Caveats (Sheet 4 of 8)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsr95218	Yes	<p>CAM Filters page does not display properly with limited Admin privileges</p> <p>When bringing up the CAM web console Filters page, the administrator receives the following error:</p> <p>“The link you requested is not present on this clean access system. If you reached this page by following a link from the user interface of the clean access manager or server then please report this as a bug.”</p> <p>Note When limiting permissions for Cisco NAC Appliance administrators, if the filters page is set for read-only, but the CDL Page is set to Hidden, then administrators get the failure message when attempting to access the Filters page.</p> <p>Workaround Set the Certified Devices page to read only under the Admin Group permissions setup (Administration > Admin Users > Admin Groups > Edit).</p>
CSCsu02167	Yes	<p>SSL fails when Netscape Cert Type field does not contain “SSL Client”</p> <p>As a result, the CAS and CAM disconnect from one another and users cannot authenticate. Report log entries show:</p> <p>“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”</p> <p>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.</p> <p>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.</p> <p>Note This issue has been observed with Entrust certificates and another educational CA.</p> <p>Workaround There are two methods to work around this issue:</p> <ul style="list-style-type: none"> • Get certificate reissued by CA with no Netscape Cert Type field, or ensure the field contains both “SSL Server” and “SSL Client.” • Use temporary certificates (not recommended).
CSCsu46733	Yes	<p>CAM/CAS does not handle blank spaces in certificate</p> <p>CAM/CAS certificates containing blank spaces do not work when uploaded. You can verify whether or not your certificate contains blank spaces by viewing the certificate in a text editor application like Wordpad or Notepad.</p> <p>Workaround Ensure you remove all blank spaces from the certificate.</p>

Table 12 **List of Resolved Caveats (Sheet 5 of 8)**

Software Release 4.1(8)		
DDTS Number	Corrected	Caveat
CSCsv10336	Yes	<p>CAS does not accommodate RADIUS accounting packets greater than 8192 bytes</p> <p>Cisco Clean Access Servers appear to have a 8192 byte limitation in the size of accounting packets they can successfully reassemble when performing VPN SSO. Packets exceeding 8192 bytes result in an “INFO: Accounting Packet - Stated packet length [10696] is less than physical packet length [8192]” error message.</p> <p>This limitation means that VPN SSO users with a large amount of groups or other information specified within the RADIUS accounting packet are unable to use SSO and “fall back” to a different authentication mechanism.</p> <p>Workaround Set a local authentication fallback.</p>
CSCsv49225	Yes	<p>Unable to create a VLAN Profile when the VLAN name contains a hyphen</p> <p>This problem only applies to creating a VLAN profile and not when using the name for VLAN mapping.</p> <p>Note There is no known workaround for this issue.</p>
CSCsv61373	Yes	<p>DHCP Option 78 (slp-directory-agent) is not offered to clients, even though it is a scope option on the server</p> <p>The behavior has been observed in 4.1.3.1 Real-IP CASs.</p> <p>Workaround Configure the CAS as DHCP Passthrough device.</p>
CSCsv64925	Yes	<p>SSL communication error with LDAP server while using non-standard CA</p> <p>When upgrading from a previous release of Cisco NAC Appliance, LDAP lookup on the CAM may stop working. This situation can occur if the administrator uses LDAP instead of the correct component included in Cisco NAC Appliance to enable SSL.</p>

Table 12 **List of Resolved Caveats (Sheet 6 of 8)**

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsv71328	Yes	<p>Start the DHCP server when CAM is not reachable</p> <p>Clients cannot get IP addresses or even renew the leases when the DHCP service is configured to run on an active CAS (in HA) and the CAS is in Fail Open (FailOpen) due to CAM not reachable for an extended period of time.</p> <p>Under the following condition the issue will show up:</p> <ul style="list-style-type: none"> • HA CAS in RIP mode • DHCP is configured to run in the CAS. • CAM is not reachable to the CAS pair. • CAS has to Fail Open the traffic. • Clients on the untrusted side depend on the DHCP service running on the CAS. <p>Note DHCP lease/configuration information between the CAS HA pair appliance is assumed to be in sync.</p> <p>See DHCP Failover Behavior Enhancement, page 12 for more information.</p>
CSCsv74447	Yes	<p>CAS Link-detect to check interface health</p> <p>For some customers, network topology restricts them from configuring external pingable IP address to handle CAS HA link detection. (When active CAS detects network interface failure, failover will be triggered.)</p> <p>Workaround We provide an alternative for the Link-detect function in the CAS web console. Cisco NAC Appliance administrators must add the <code>/etc/ha.d/linkdetect.conf</code> file specifying CAS interface eth0, eth1, or both to be monitored locally for link healthiness. See CAS HA Pair Link-Detect Configuration Enhancement, page 11 for more information.</p>
CSCsw20607	Yes	<p>CAS/CAM Disconnect</p> <p>In previous releases of Cisco NAC Appliance, the AutoConnectManager could get stuck publishing to one CAS. Bad network connectivity can make the AutoConnectManager hang for very long time.</p> <p>Cisco has addressed this issue by introducing socket timeouts that have been tested in LAN and WAN environments.</p>
CSCsw22557	Yes	<p>OS Fingerprint Update required for Blackberry Bold</p> <p>Cisco NAC Appliance is reading the Blackberry Bold OS identifier as a Windows OS.</p> <p>Note There is no known workaround for this issue.</p>

Table 12 List of Resolved Caveats (Sheet 7 of 8)

Software Release 4.1(8)		
DDTS Number	Corrected	Caveat
CSCsw33455	Yes	<p>Improve CAM/CAS communication resiliency during network link failures</p> <p>Bad WANs can make AutoConnectManager hang and not service cases that should connect.</p> <p>Cisco has addressed this issue by adding socket timeouts and large file chunking so that the AutoConnectManager can escape certain cases where really bad network connectivity exists.</p>
CSCsw35162	Yes	<p>UI Forefront date-based checks support does not work</p> <p>Client machine posture assessment fails for up-to-date Microsoft Forefront 1.5.x or when dates are within the selected range and the For AV Virus Definition rules, allow definition file to be <x> days older than option is being used.</p> <p>Note Date-based checks are not supported at this time.</p> <p>Workaround Turn off the For AV Virus Definition rules, allow definition file to be <x> days older than option under Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules.</p>
CSCsw86694	Yes	<p>CAS/CAM references wrong network configuration file</p> <p>Netstat -an shows wrong local IP address for a socket.</p> <p>Workaround Delete ifcfg-eth0/eth1.bak files from the “networkscripts” directory on the appliance.</p>
CSCsw97200	Yes	<p>Upgrade does not preserve DB snapshot create date/time reported by CAM</p> <p>The CAM does not preserve the date/time for DB snapshot files in the /perfigo/control/tomcat/webapps/download/WEB-INF/ directory for release 4.0(x)/4.0(x), nor does the CAM preserve the date/time in the /perfigo/control/data/download/ directory for release 4.5.</p> <p>Note There is no known workaround for this issue.</p>
CSCsx02849	Yes	<p>ADSSO can run into trouble if exception is thrown</p> <p>If the network environment is such that an ADSSO server can enter a state where the only way to fix the problem is to fix the environment and restart the CAS.</p> <p>Workaround Reboot the CAS.</p>

Table 12 List of Resolved Caveats (Sheet 8 of 8)

DDTS Number	Software Release 4.1(8)	
	Corrected	Caveat
CSCsx10139	Yes	<p>Upgrade should modify CAS Fallback old default settings to the new one</p> <p>If you upgrade the CAS to release 4.1(8) and are using CAS Fallback with the old default settings, the upgrade script modifies those Detect Interval and Detect Timeout settings to the new default values, notifies the administrator of the change, and inserts an entry in the upgrade logs. If the administrator specified new (non-default) values for the CAS Fallback feature settings, then the upgrade script recommends that the admin user modify the CAS Fallback settings manually to maintain expected behavior.</p> <p>Workaround Modify the CAS Fallback settings by going to the Device Management > CCA Servers > Manage [CAS_IP] > Filter > Fallback web console page on the CAM.</p> <p>Note The CAS Fallback default settings for Cisco NAC Appliance releases prior to 4.1(8) are:</p> <ul style="list-style-type: none"> – Fallback Policy: Ignore – Detect Interval: 60 seconds – Detect Timeout: 300 seconds <p>The new CAS Fallback default settings with 4.1(8) are:</p> <ul style="list-style-type: none"> – Fallback Policy: Ignore – Detect Interval: 20 seconds – Detect Timeout: 300 seconds – Fail Percentage: 30%

Known Issues for Cisco NAC Appliance

This section describes known issues when integrating Cisco NAC Appliance:

- [Known Issue with Mass DHCP Address Deletion](#)
- [Known Issues with HP ProLiant DL140 G3 Servers](#)
- [Known Issue with NAC-3310 CD Installation](#)
- [Known Issues with NAC-3300 Series Appliances and Serial HA \(Failover\) Connection](#)
- [Known Issues with Switches](#)
- [Known Issue with Cisco 2200/4400 Wireless LAN Controllers \(Airespace WLCs\)](#)
- [Known Issues with Broadcom NIC 5702/5703/5704 Chipsets](#)
- [Known Issue for Windows Vista and IP Refresh/Renew](#)
- [Known Issues for Windows Vista and Agent Stub, page 76](#)
- [Known Issues with MSI Agent Installer](#)
- [Known Issue with Windows 2000 Clean Access Agent/Local DB Authentication](#)
- [Known Issue with Windows 98/ME/2000 and Windows Script 5.6](#)



Note

For additional information, see also [Troubleshooting, page 98](#).

Known Issue with Mass DHCP Address Deletion

An issue exists in release 4.1(8) where a Clean Access Server configured to be a DHCP server can become unmanageable if the administrator attempts to delete more than 800 DHCP addresses from the appliance using the Clean Access Manager web console. If you have more than 800 DHCP addresses, Cisco recommends deleting addresses in smaller blocks of no more than 800 addresses at a time.

In addition to ensuring you do not delete more than 800 DHCP addresses at a time, there are two methods to work around this potential issue.

Workaround 1

The DHCP IP delete can be done manually by connecting to the CLI and executing the following commands:

```
service perfigo stop
rm -f /var/state/dhcp/dhcpd.leases
touch /var/state/dhcp/dhcpd.leases
service perfigo start
```

If on an HA system, Cisco strongly recommends taking the CASs offline and performing the commands on both machines simultaneously, taking particular care to issue the **service perfigo start** on the two appliances at roughly the same time.

Workaround 2

If you experience this problem more than once, Cisco recommends changing the Clean Access Manager timeout value by editing the `/perfigo/control/bin/starttomcat` file and adding “-DRMI_READ_TIME_OUT=<new value>” to the end of the CATALINA_OPTS options string. (The current default value is 60 seconds, and Cisco does not recommend increasing the timeout value to any

more than 300 seconds.) Please note that increasing the read time out value can likely lower the resiliency of WAN deployments, thus reversing the CAM/CAS connectivity improvements introduced when Cisco addressed caveat [CSCsw20607](#), page 70.

**Note**

In release 4.1(8), the CAM only allows 60 seconds for a response on remote calls to the CAS. This impacts deleting hundreds of DHCP IPs at once, particularly on slower CAS hardware platforms. Cisco recommends that you do not delete any more than 3 class C address segments at once.

For more information, see [CSCsx35438](#), page 58.

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\(8\)](#) 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\(8\)](#), users installing release 4.1(8) 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(8), 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 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(8) 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 Issue for Windows Vista and IP Refresh/Renew

When logged in as a machine admin on Windows Vista and using web login with IP refresh configured, IP address refresh/renew via ActiveX or Java will fail due to the fact that Internet Explorer does not run as an elevated application and Vista requires elevated privileges to release and renew an IP address.

Workaround

In order to use the IP refresh feature, you will need to:

1. Log into the Windows Vista client as an administrator.
2. Create a shortcut for IE on your desktop.

3. Launch it by right-clicking the shortcut and running it as administrator. This will allow the application to complete the IP Refresh/Renew. Otherwise, the user will need to do it manually via Command Prompt running as administrator. This is a limitation of the Windows Vista OS.

See also [CSCsm61077](#), page 54.

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/cgi-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 53 for details.

See also [Troubleshooting, page 98](#) 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(8)

If you are performing a new CD software installation of Cisco NAC Appliance 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\(8\)](#), page 79.



Warning

New installations of Cisco NAC Appliance release 4.1(8) no longer contain any default third-party Trusted Certificate Authorities. Therefore, after a new installation of release 4.1(8) 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 82.
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(8) on each Clean Access Server and Clean Access Manager, as follows:
 - a. Log in to the [Cisco NAC Appliance Software Download Site](#). You will likely be required to provide your CCO credentials.
 - b. Navigate to the Cisco NAC Appliance 4.1.8 subdirectory, download the latest 4.1(8) .ISO image, and burn the 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\(8\)](#)
 - [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(8\)](#)

**Note**

Clean Access Manager 4.1(8) is bundled with Windows Clean Access Agent version 4.1.8.0 and Mac OS X Clean Access Agent version 4.1.3.1.

Upgrading to 4.1(8)

This section provides instructions for how to upgrade your existing Cisco NAC Appliance system to release 4.1(8).

Refer to the following general information prior to upgrade:

- [Notes on 4.1\(8\) 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\(8\)—Standalone Machines](#)
- [Upgrading to 4.1\(8\)—HA Pairs](#)

If you need to perform a fresh installation of the software, refer instead to [New Installation of Release 4.1\(8\)](#), page 78.

If you need to upgrade from a much older version of Cisco NAC Appliance, you may need to perform an interim upgrade to a version that is supported for upgrade to 4.1(8). 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(8) Upgrade

If planning to upgrade to Cisco NAC Appliance release 4.1(8) ED, note the following:

- For new installations of Cisco NAC Appliance Release 4.1(8), the CAS Fallback behavior enhancement introduces new default values for the **Detect Interval** and **Detect Timeout** settings (10 and 300 seconds, respectively) and requires that the **Detect Timeout** value be at least 20 times the specified **Detect Interval**. If you are upgrading to release 4.1(8), however, your existing values for these settings are preserved and you must specify new values for these settings to take advantage of the enhanced CAS Fallback capabilities available in release 4.1(8). For more information, see [CAS Fallback Behavior Enhancement](#), page 11.

- New installations of Cisco NAC Appliance release 4.1(8) no longer contain any default third-party Trusted Certificate Authorities. However, with upgrades to release 4.1(8), 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(8) 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(8). You must correct your certificate chain to successfully upgrade to release 4.1(8). For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.1(8), refer to the [How to Fix Certificate Errors on the CAM/CAS After Upgrade](#) Troubleshooting Tech Note.

Certificate chains can only be 10 certificates long (including intermediate and root certificates) in Cisco NAC Appliance Release 4.1(8).

- 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(8) 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 56 for more details.
- Only releases 4.1(8), 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(8) via web upgrade, just like any other Clean Access Server. If upgrading to release 4.1(8), 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(8) 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)+, 4.1(3)+, 4.1(6) to release 4.1(8). See [Console/SSH Upgrade—Standalone Machines](#), page 89.

- 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 CAM HA pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in [Console/SSH Instructions for Upgrading CAM and CAS HA Pairs, page 95](#).

- 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(8) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(8) 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(8) via the instructions in [Upgrading to Release 4.1\(8\)—Standalone Machines, page 83](#) or [Upgrading to 4.1\(8\)—HA Pairs, page 93](#). 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\(8\) Upgrade, page 79](#) for additional information.

- If you upgrade the CAS to release 4.1(8) and are using CAS Fallback with the old default settings, the upgrade script modifies those **Detect Interval** and **Detect Timeout** settings to the new default values, notifies the administrator of the change, and inserts an entry in the upgrade logs. If the administrator specified new (non-default) values for the CAS Fallback feature settings, then the upgrade script recommends that the admin user modify the CAS Fallback settings manually to maintain expected behavior.
- **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(8). 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 75 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 75.
- **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(8), 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(8), 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(8) software and some running 4.1.(6) or 4.1(3) 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(8) to 4.1.8.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(8) 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 84](#) 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(6) or earlier database snapshot to a 4.1(8) CAM.

- **Software Downgrade**

Once you have upgraded your software to 4.1(8), if you wish to revert to your previous release of Cisco NAC Appliance, you will need to reinstall the previous release from the CD and recover your configuration based on the backup you performed prior to upgrading to 4.1(8).

- **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(8)—Standalone Machines

**Note**

“In-place” upgrade from version 3.5(x) to 4.1(8) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(8) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(8). 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 to the latest 4.1(8) release. You can upgrade 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+/4.1(3)+/4.1(6) standalone machines to the latest 4.1(8) release using one of the following two methods:

- [Web Console Upgrade—Standalone Machines, page 85](#)
- [Console/SSH Upgrade—Standalone Machines, page 89](#)

**Note**

- If upgrading high-availability (HA) pairs of CAM or CAS appliances, refer instead to [Upgrading to 4.1\(8\)—HA Pairs, page 93](#).

**Note**

Review the following sections before proceeding with the upgrade instructions:

- [Upgrading to 4.1\(8\), page 79](#)
- [Settings That May Change With Upgrade, page 81](#)
- [General Preparation for Upgrade, page 82](#)

Summary Steps for Web Upgrade to 4.1(8)

The sequence of steps for upgrading a standalone appliance to release 4.1(8) is as follows:

1. [Create CAM DB Backup Snapshot, page 84](#)
2. [Download the Upgrade File, page 85](#)
3. Perform [Web Console Upgrade—Standalone Machines](#) or [Console/SSH Upgrade—Standalone Machines, page 89](#), depending on your installation

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\(8\)](#)).

**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 to release 4.1(8), 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** Log in to the [Cisco NAC Appliance Software Download Site](#). You will likely be required to provide your CCO credentials.
- Step 2** Navigate to the Cisco NAC Appliance 4.1.8 subdirectory, download the latest 4.1(8) upgrade file (e.g. **cca_upgrade-*<version>*.tar.gz**), and save it to the local computer from which you are accessing the CAM web console.



Note

Upgrade files use the following format.

- cca_upgrade-4.1.8.x.tar.gz (CAM/CAS release upgrade file)
- cam_upgrade-4.1.8.x.tar.gz (CAM-only patch upgrade file)
- cas_upgrade-4.1.8.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-4.1.8.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-4.1.8.1.tar.gz**.

Web Console Upgrade—Standalone Machines



Note

Cisco recommends using console/SSH to upgrade your machines to release 4.1(8). See [Console/SSH Upgrade—Standalone Machines, page 89](#).

If you are upgrading the CAS to release 4.1(8) 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 CAM HA pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in [Console/SSH Instructions for Upgrading CAM and CAS HA Pairs, page 95](#).

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.
- A prior release of Cisco NAC Appliance must be installed and running on your CAM/CAS(es) before you can upgrade to release 4.1(8) via web console.
- Alternatively, you can always upgrade using the instructions in [Console/SSH Upgrade—Standalone Machines, page 89](#).
- If upgrading failover pairs, refer to [Upgrading to 4.1\(8\)—HA Pairs, page 93](#).

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 to release 4.1(8) 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 87](#).

-
- Step 1** [Create CAM DB Backup Snapshot, page 84](#).
- Step 2** [Download the Upgrade File, page 85](#).
- Step 3** From the CAM web console, access the CAS management pages as follows:
- Go to **Device Management > CCA Servers > List of Servers**.
 - Click the **Manage** button for the CAS to upgrade. The CAS management pages appear.
 - 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 87](#).

-
- Step 1** [Create CAM DB Backup Snapshot, page 84](#).
- Step 2** [Download the Upgrade File, page 85](#).

- Step 3** To access the Clean Access Server's direct access web admin console:
- 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**).
 - 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 CAM HA pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in [Console/SSH Instructions for Upgrading CAM and CAS HA Pairs, page 95](#).

- Step 1** [Create CAM DB Backup Snapshot, page 84](#).
- Step 2** [Download the Upgrade File, page 85](#).
- 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 to the latest 4.1(8) 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 appliances, refer instead to [Upgrading to 4.1\(8\)—HA Pairs, page 93.](#)
 - “In-place” upgrade from version 3.5(x) to 4.1(8) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(8) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(8). 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 4.1(8) console/SSH upgrade instructions:

- [Upgrading to 4.1\(8\), page 79](#)
- [Settings That May Change With Upgrade, page 81](#)
- [General Preparation for Upgrade, page 82](#)

Summary Steps for Console/SSH Upgrade to 4.1(8)

The sequence of steps for upgrading a standalone appliance to release 4.1(8) is 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 84.](#)
- Step 2** [Download the Upgrade File, page 85.](#)
- 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-4.1.8.tar.gz** to the `/store` directory on the Clean Access Manager.
- b. Copy **cca_upgrade-4.1.8.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-4.1.8.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-4.1.8.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-4.1.8.tar.gz
```

4. Execute the upgrade process:

```
cd cca_upgrade-4.1.8
./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(8) upgrade script automatically upgrades the Clean Access Agent files inside the CAM to Windows version 4.1.10.0 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-4.1.8.tar.gz
```

5. Execute the upgrade process:

```
cd cca_upgrade-4.1.8
./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(8)—HA Pairs



Note

“In-place” upgrade from version 3.5(x) to 4.1(8) is not supported. Customers wishing to upgrade a system from 3.5(11) to 4.1(8) must use the supported in-place upgrade procedure to upgrade from 3.5(11) to 4.0(6), and then upgrade to 4.1(8). 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 to the latest 4.1(8) release.

If you have standalone CAM/CAS servers, refer instead to [Upgrading to Release 4.1\(8\)—Standalone Machines](#), page 83.



Note

Your system must be running a previous Cisco NAC Appliance release 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 CAM HA pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in [Console/SSH Instructions for Upgrading CAM and CAS HA Pairs](#), page 95.



Note

Review the following before proceeding with the 4.1(8) HA upgrade instructions:

- [Upgrading to 4.1\(8\)](#), page 79
- [Settings That May Change With Upgrade](#), page 81
- [General Preparation for Upgrade](#), page 82

Steps for HA + Upgrade to 4.1(8)

The steps to upgrade HA systems are described in the following sections:

- [Access Web Consoles for High Availability](#)
- [Console/SSH Instructions for Upgrading CAM and CAS HA 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(8) 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 CAS HA 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 CAM and CAS HA 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 appliance 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 appliance. (Refer to [Download the Upgrade File and Copy to CAM/CAS, page 90](#) for instructions.)

Step 4

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

- Untar the upgrade package in the **/store** directory of each appliance:

```
tar xzvf cca_upgrade-4.1.8.tar.gz
```

- b. CD into the “cca_upgrade-4.1.8” directory on each appliance:

```
cd cca_upgrade-4.1.8
```

- c. Run the following command on each appliance:

```
./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 appliances, and the results should be that one appliance 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 94](#), 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** Stop services on the standby appliance by entering the following command via the console/SSH terminal:

```
service perfigo stop
```

Wait until the standby appliance has suspended services.

- Step 6** CD into the created “cca_upgrade-4.1.8” directory on the active appliance:

```
cd cca_upgrade-4.1.8
```

- Step 7** Run the following command on the active appliance:

```
./fostate.sh
```

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

- Step 8** Perform the upgrade on the active appliance, as follows:

- Make sure the upgrade package is untarred in the `/store` directory on the active appliance.
- From the untarred upgrade directory created on the active appliance (for example “cca_upgrade-4.1.8”), run the upgrade script on the active appliance:

```
./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(8) upgrade script automatically upgrades the Clean Access Agent files inside the CAM to Windows version 4.1.10.0 and Mac OS X version 4.1.3.1.

- Step 9** After the upgrade is completed, stop services on the active appliance by entering the following command via the console/SSH terminal:

```
service perfigo stop
```

Wait until the active appliance has suspended services.

- Step 10** Restart services on the standby appliance by entering the following command via the console/SSH terminal:

```
service perfigo start
```

- Step 11** Perform the upgrade to the standby appliance:

- a. Make sure the upgrade package is untarred in the **/store** directory on the standby appliance.
- b. CD into the untarred upgrade directory created on the standby appliance:

```
cd cca_upgrade-4.1.8
```

- c. Run the upgrade script on the standby appliance:

```
./UPGRADE.sh
```

- Step 12** After the upgrade is completed, stop services on the standby appliance by entering the following command via the console/SSH terminal:

```
service perfigo stop
```

- Step 13** Reboot the active appliance by entering the following command via the console/SSH terminal:

```
reboot
```

Wait until it is running normally and you are able to connect to the web console.

- Step 14** Reboot the standby appliance by entering the following command via the console/SSH terminal:

```
reboot
```

**Note**

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

Troubleshooting

This section provides troubleshooting information for the following topics:

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



Note

For additional troubleshooting information, see also [Known Issues for Cisco NAC Appliance, page 73](#).

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:
- Import the certificate to the client system's trusted root store.
 - 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 10](#)).
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 101](#).
9. If necessary, provide CAM support logs as described in [Creating CAM/CAS Support Logs, page 103](#).

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 14](#)) 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 12](#)), 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 **LogLevel1**.
- 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:
- Open **Start > Run**.
 - 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 13](#)), the Agent **event.log** file and **preference.plist** user preferences file are available under <username> > **Library > Application Support > Cisco Systems > CCAgent.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 | CCAgent.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 84](#) 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(8)*

Date	Description
5/26/09	Clean Access Agent Version 4.1.10.0: <ul style="list-style-type: none"> Updated Release 4.1(8) Compatibility Matrix, page 6 Updated Release 4.1(8) Agent Upgrade Compatibility Matrix, page 7 Added Windows Clean Access Agent Version 4.1.10.0, page 13 Added Resolved Caveats - Agent Version 4.1.10.0, page 59 Updated Clean Access Supported AV/AS Product List, page 15
2/25/08	<ul style="list-style-type: none"> Added caveat CSCsm61077 to Open Caveats - Release 4.1(8), page 47 Added Known Issue for Windows Vista and IP Refresh/Renew, page 75
2/19/09	Updated footnote in Table 4 on page 8 to explicitly instruct users to uninstall Mac OS X Agent before attempting to upgrade via web login
2/2/09	<ul style="list-style-type: none"> Added caveat CSCsx35438 to Open Caveats - Release 4.1(8), page 47 Added Known Issue with Mass DHCP Address Deletion, page 73 (to address caveat CSCsx35438)
1/29/09	Release 4.1(8)

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\(8\)](#)
- [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(8\)](#)
- [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 an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

